Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Upgrade Procedure

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

E85335-01

July 2017

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

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

Refer to Appendix C for instructions on accessing this site.

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

EMAIL: support@oracle.com

Oracle Communications Policy Management 12.1.x/12.2.x to 12.3 Upgrade Procedure, Georedundancy Disabled
Copyright © 2013, 2017 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures to perform a software upgrade of Oracle Communications Policy Management Release 12.1.x/12.2.x to Release 12.3 when georedundancy on non-CMP components (MPE/MRA/Mediation) is disabled.

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

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

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

1.2 Acronyms

Table 1: Acronyms

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

Acronym	Meaning
IPM	Initial product manufacture

1.3 Terminology

Table 2: Terminology

Term	Description
Primary Site (Site1)	A site where the MPE/MRA/ Mediation primary cluster exists with co-located Active and Standby servers.
Secondary Site (Site2)	A site where the MPE/MRA/Mediation secondary cluster exists with co-located Active and Standby servers for disaster recovery.
Mediation	Message Distribute Function (for Wireless-C Policy Management deployment)

1.4 Software Release Numbering

- PMAC: 6.0.3
- TVOE: 3.0.3
- TPD: 7.0.3
- COMCOL: 6.4
- Policy Management Release 12.3
- Oracle Firmware: 3.1.5
- HP Firmware: Firmware Upgrade Pack Minimum: 2.2.10

2. UPGRADE OVERVIEW

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

2.1 Upgrade Status Values

Table 3: 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 Path

This upgrade document supports the following upgrade paths:

1. Policy Management 12.1.x to 12.3
2. Policy Management 12.2.x to 12.3

2.3 Upgrade Information

2.3.1 Upgrade Sequence

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

A deployment may consist of multiple clusters.

2.3.1.1 Required Cluster Upgrade Sequence

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

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

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

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

NOTE: MPE/MRA/Mediation clusters can be upgraded in parallel. (upgrades from 12.1.x where 8 clusters can be upgraded in parallel, and from 12.3.x where 16 clusters can be upgraded in parallel).

2.3.2 Policy Management Release Mixed-Version Operation and Limitation

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

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

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

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

Table 4: Mixed-version configurations supported

Policy Management system components on	CMP R12.3	MRA R12.3	MPE R12.3	Mediation 12.3
CMP 12.1.x, 12.2.x	Yes	No	No	No
MRA 12.1.x, 12.2.x	Yes	Yes	Yes	Yes
MPE 12.1.x, 12.2.x	Yes	Yes	Yes	Yes
Mediation 12.2.x	Yes	Yes	Yes	Yes

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

2.4 Customer Impacts

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

2.5 Rollback/Backout

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

2.6 TPD Version

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

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

2.7 Server Hardware Platforms

The Policy Management Release 12.3 software upgrade can be applied on any server that previously had Policy Management Release 12.1.x or 12.2.x

2.8 Loading Application software

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

NOTE: PM&C is not used during the Upgrade and Backout procedures.

2.9 Required Materials and Remote Access

1. Policy Management 12.3 software ISO files and TPD software ISO
2. Policy Management 12.3 software upgrade Release Notes.
3. TVOE, PM&C upgrade/installation documentation, software ISO files. (If applicable)
4. Firmware Upgrade Pack 2.2.10 (or higher) documentation and ISO files. (If applicable)

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

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

7. 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.
8. User logins, passwords, IP addresses and other administration information.
9. VPN access to the network is required if that is the only method for remote logging into the target servers. It must be also possible to access the Policy Manager GUI, and the PM&C GUI.

2.9.1 Upgrade Media

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

2.9.2 Logins, Passwords and Server IP Addresses

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

Further, need to confirm login information for key interfaces, and document in table below.

It is assumed that the logins may be common across sites. If not, record the information for each site.

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

Table-5: Logins, Passwords and Server IP Addresses

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

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

3. THEORY OF OPERATION

3.1 Upgrade Manager Page

The Upgrade Manager represents a significant shift from some of the previous upgrade pages. In the past it was up to the operator, with assistance from a MOP, to know the correct sequence of server selects and menu selects. 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.

There is an important point implicit in the list above:

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

The shift in perspective has a number of ramifications, most noticeably it is not possible to select individual servers or bulk select a group of servers. In fact, in order to perform any operation, it is necessary to select a cluster first.

Another major shift is that certain operations are performed automatically on behalf of the operator. These operations are not even visible to the operator as an option. However, the operator can see what has been done via the upgrade log.

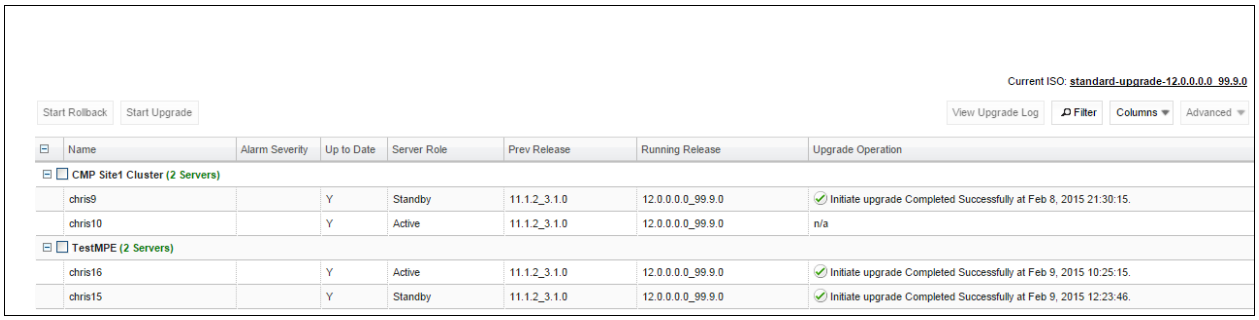


Figure 1: Sample display of the upgrade manager page.

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

- **Start Rollback** or **Start Upgrade** buttons (upper left)

  If these buttons are greyed out, it means that there is not an appropriate action to take at this time. However, if a button is not greyed out, then it means that there is a preferred action that can be taken to upgrade (or backout) the cluster. Normally, upgrading a cluster is a well-defined fixed procedure. However, in some cases there are a number of valid sequences. Selecting the preferred step causes the upgrade director to choose the default sequence. It is strongly recommended to exclusively use these buttons to upgrade or backout a cluster.

- Alarm Severity

  This column is used to indicate if there are alarms associated with a server. If so, it displays the severity of the most severe alarm here. It is important to explain the intent of this column. The intent is to give a visual indication that the particular server is experiencing alarms. This is not a reason to panic: During the upgrade we expect servers to raise alarms:

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

- Servers report alarms to indicate that their mate servers are offline.

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

- Up to Date

  This column is used to indicate the state of the code on the server.

  - N

    The server is running old code and must be upgraded

  - Y

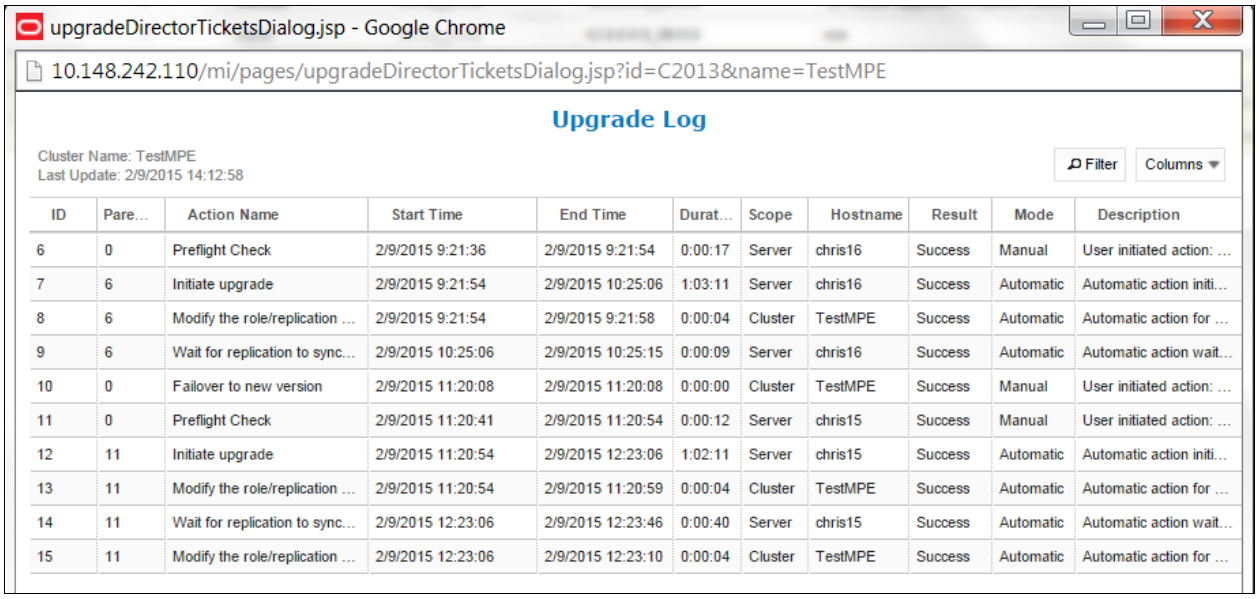
    The server is running new code.

  - N/A

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

3.1.1 The Upgrade Log

Within the Upgrade Manager page, the operator can access the upgrade log. This displays attributes of the various actions (manual and automatic) that have been performed on the selected cluster. It is important to note that this is NOT the audit log. The audit log is meant to track what the operator has done. This log is meant to capture the sequence of upgrade activity—whether it was initiated by an operator or automatically triggered.



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

Figure 2: Upgrade Log

3.1.2 Optional Actions

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

If the operator selects an optional action, they can go back to using the default/preferred at any time.

3.1.3 The ISO Select

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

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

To start a new upgrade, click this item. The upgrade director searchs for the valid upgrade procedures. To minimize confusion, the upgrade procedures are embedded in the CMP ISO file. This way, the CMP ISO file is tied to the corresponding upgrade procedure.

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

3.1.4 Introducing Upgrade Director Behavior

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

3.1.4.1 Alarm Philosophy

In general, the Upgrade Directo raises alarms if:

- A server is somehow impaired.
- There is activity expected of an operator.

The table summarizes the alarms that can be raised during a 12.3 upgrade.

Alarm ID	Name	Description
70500	SYSTEM_MIXED_VERSION	The servers in the topology are running different versions of software. Upgrade of the system is not complete.
70501	CLUSTER_MIXED_VERSION	The servers in the specified cluster are running different versions of software. The upgrade of the cluster is not complete.
70502	REPLICATION_INHIBITED	Replication is inhibited to the specified server. It is not receiving session information.
70503	SERVER_FORCED_STANDBY	The specified server has been placed in forced standby and cannot provide service.
70506	UPGRADE_OPERATION_FAILED	An upgrade operation failed on the specified server.

Alarm ID	Name	Description
70507	UPGRADE_IN_PROGRESS	An upgrade/backout is currently in progress on the server. It may leave the cluster, become unreachable or even reboot.
70508	ZOMBIE_SERVER	The server is in an indeterminate state and must be repaired by support.

3.1.4.2 General Upgrade Procedure

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

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

This procedure is in place so that it should not be necessary for an operator to login to the target server to verify conditions. They should be able to comfortably stay on the upgrade manager page.

3.1.4.3 Unreachable Servers

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

3.1.4.4 Reversing Directions

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

3.1.4.5 Mixed Version and Forced Standby

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

3.1.4.6 Failure Handling and Recovery

Failures fall into two categories:

- Failures that the upgrade director is able to recover from.
- Failures that the upgrade director cannot automatically recover from.

Any failure should generate an UPGRADE_OPERATION_FAILED alarm. In such cases, the operation can be attempted again. Ideally, the operator/support would investigate the original failure before repeating.

However, if the server is in an indeterminate state, the server is declared a ZOMBIE and no further action can be taken on the server. It requires direct action by support or engineering to repair.

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

4. UPGRADE PREPARATION

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

Overview:

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 (Site1) CMP
5. Upgrade Secondary (Site2) CMP (if applicable)
6. Segment 1 Site 1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
    c. Upgrade Mediation/MS clusters (for WIRELESS-C. If needed, recommend to upgrade UDR clusters first to compatible version)
7. Segment 1 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
    c. Upgrade Mediation/MS clusters (for WIRELESS-C)
8. Segment 2 Site 1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
    c. Upgrade Mediation clusters (for WIRELESS-C)
9. Segment 2 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
    c. Upgrade Mediation clusters (for WIRELESS-C)

4.1 Prerequisites

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

Procedure 1 TVOE, PM&C and Firmware might need to be upgraded prior to Upgrade to Policy Management Release 12.3.

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

4.2 TVOE and PM&C Server Upgrade

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

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

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

4.3 Firmware Upgrade

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

4.4 Plan and Track Upgrades

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

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

The following table 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:

1. Policy changes or configuration changes should NOT be made while the system is in mixed-version operation.

2. Time estimates are for upgrade procedures without backout procedure. Backout procedure time is typically same as, or less than the upgrade procedure.

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

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

4.5 Convert to Using Interval Statistics

Prior to Release 12.2, Oracle Communications Policy Management offers two methods for gathering statistics: Manual and Interval statistics. They operate as follows:

- Manual.

  When configured to use this method, CMP records the cumulative values from the time the blade became active or the operator manually reset the statistics. Statistics which represent maximum values contain the peak value since the blade became active or was reset. This is the system default.

- Interval.

  When configured to use this method, all counters reset automatically at the beginning of every interval and write the cumulative values at the end of the interval. Statistics which represent maximum values contain the peak value which occurred during the interval. The user-definable interval length can be 5, 10, 15, 20, 30 or 60 minutes. The default interval is 15 minutes.

Since OCPM release 12.2 Manual statistics are not available. If upgrading from 12.1.x, you must migrate to Interval statistics before upgrading to Release 12.3. After upgrading to R12.3, Oracle Communications Policy Management only uses Interval statistics and any Manual statistics not migrated is lost.

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

It is recommended that the following actions are taken before you perform the upgrade procedure:

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

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

For addition information, see the following publications:

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

4.6 Perform System Health Check

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

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

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

---End of Procedure---		

4.7 Deploy Policy Management Upgrade Software

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

4.7.1 Deploying Policy Management Upgrade Software to Servers

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

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

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

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

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

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

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

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

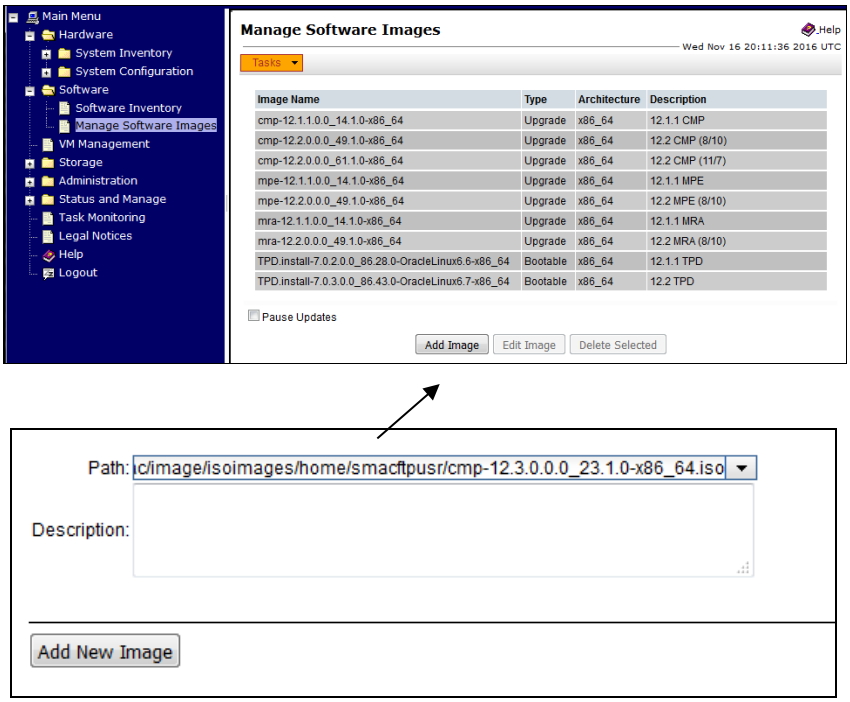
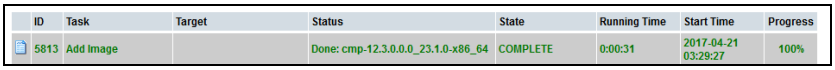
NOTE: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows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

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

Step	Procedure	Result
1. ☐	**PM&C GUI:** Verify that ther are not any Release 12.3 ISO files.	1. Log on to the PM&C Server GUI 2. Navigate to **Software → Manage Software Images.** 3. If release 12.3 ISO files are in the list, remove them.

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

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

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

4.7.3 Distribute Application ISO Image Files to Servers

This procedure applies to all server types. It assumes that the ISO image files are copied to the sites to be upgraded.

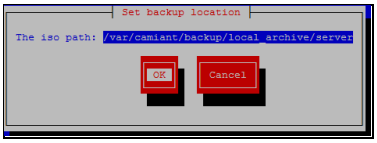
NOTE: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows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

Software Upgrade Procedure

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

4.7.4 Backups and Backup Locations

Step	Procedure	Result

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

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

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

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

4.7.5 Changing Non-Default root and admusr Passwords

4.7.5.1 Improve Password Security

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

4.7.5.2 Impact

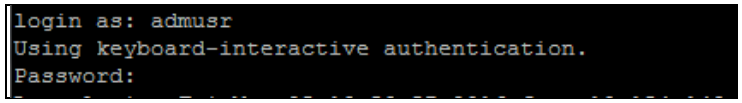
After this procedure is run, the root and admusr password is hashed with the strongest possible method, SHA512.

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

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

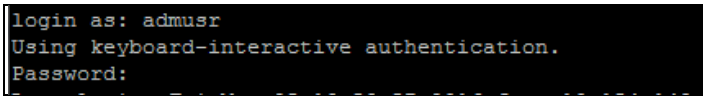
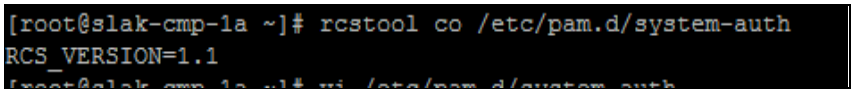
Order to perform this procedure on an In-Service Policy Management system.

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

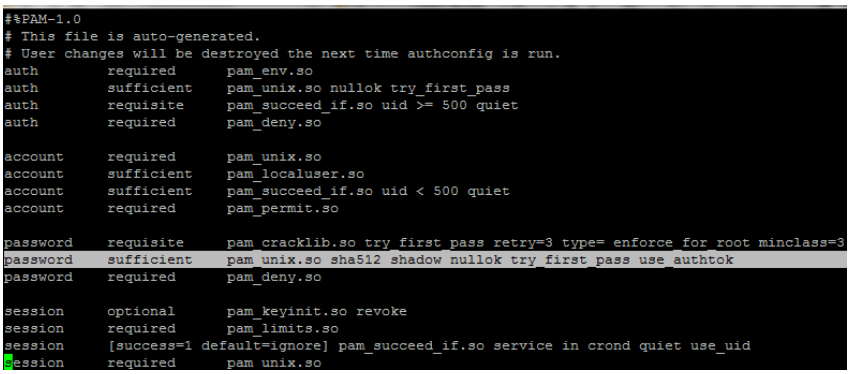
Step	Procedure	Result
1. ☐	Login to the server	**For an upgrade from 12.1/12.2.x**, login as admusr and change to root using the following command: `$sudo su` 

Step	Procedure	Result

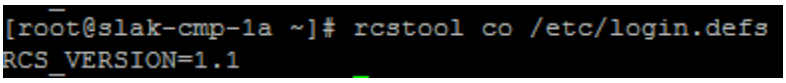
2. ☐	Check the password field of root and admusr	Issue the following
		`#egrep '^(root|admusr)' /etc/shadow`
		Example output:
		`root:$6$mErKrEsA$83n5G8dR3CgBJjMEABi6b4847EXusUnzTaWNJgEi347B.WhLbIc.Cga.nmYCdQYSNwkst1CtUBi.tBSwWujUd.:16825:0:99999:7:::`
		`admusr:$6$mUstAfa$gn2B8TsW1Zd7mqD333999Xd6NZnAEgyioQJ7qi4xufHSQpls6A5Jxhu8kjDT8dIgcYQR5QlZAtSN8OG.7mkyq/:16825::::::`
		If the first two characters after the colon (:) is $6, 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.

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

Step	Procedure	Result

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

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

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

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

Step	Procedure	Result

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

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

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

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

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

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

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

5.1 Upgrade CMP Clusters Overview

The following is an overview of CMP Cluster upgrade.

1. Upgrade Primary CMP cluster

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

   a. Start Upgrade

   b. Failover

   c. Log back into the CMP GUI

   d. Continue Upgrade

2. Upgrade The Secondary CMP cluster

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

   a. Start Upgrade

   b. Failover

   c. Continue Upgrade

It is assumed that the CMPs may be deployed as 2 Geo-Redundant clusters, identified as Site-1 and Site-2 as displayed on the CMP GUI. When deployed as such, one site is designated as the Primary Site (which is the site that is managing the Policy Management system), and the other is as Secondary site (this site is ready to become Primary site, if needed).

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

Note the Information on this CMP cluster:

Cluster Name_____

Server-A Hostname _____

Server-A IP Address _____

Server-A Status _____

Server-B Hostname _____

Server-B IP Address _____

Server-B Status _____

IMPORTANT:

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

5.1.1 Upgrade Primary CMP Cluster

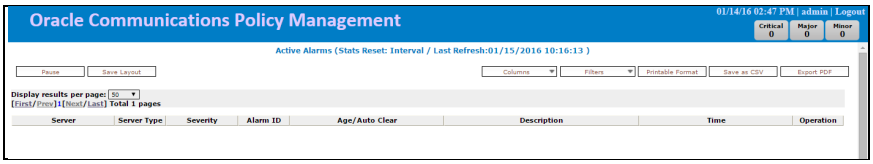
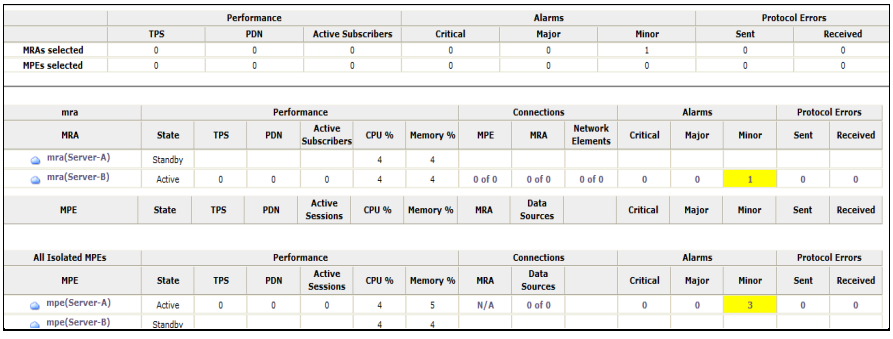
Use this procedure to upgrade a Primary CMP Cluster.

NOTES:

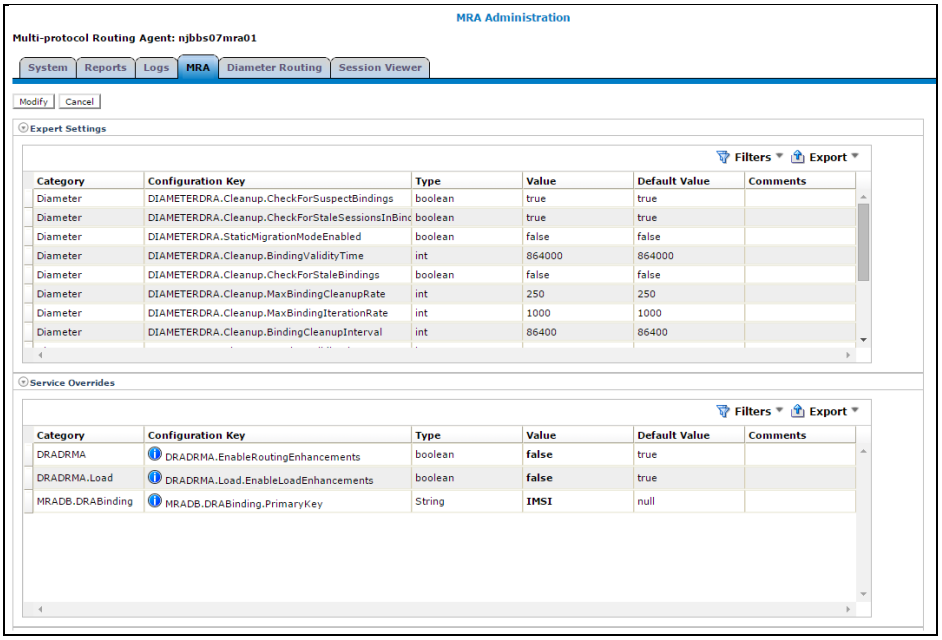
- This procedure must be performed in a maintenance window.
- This procedure takes approximately 60-120 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

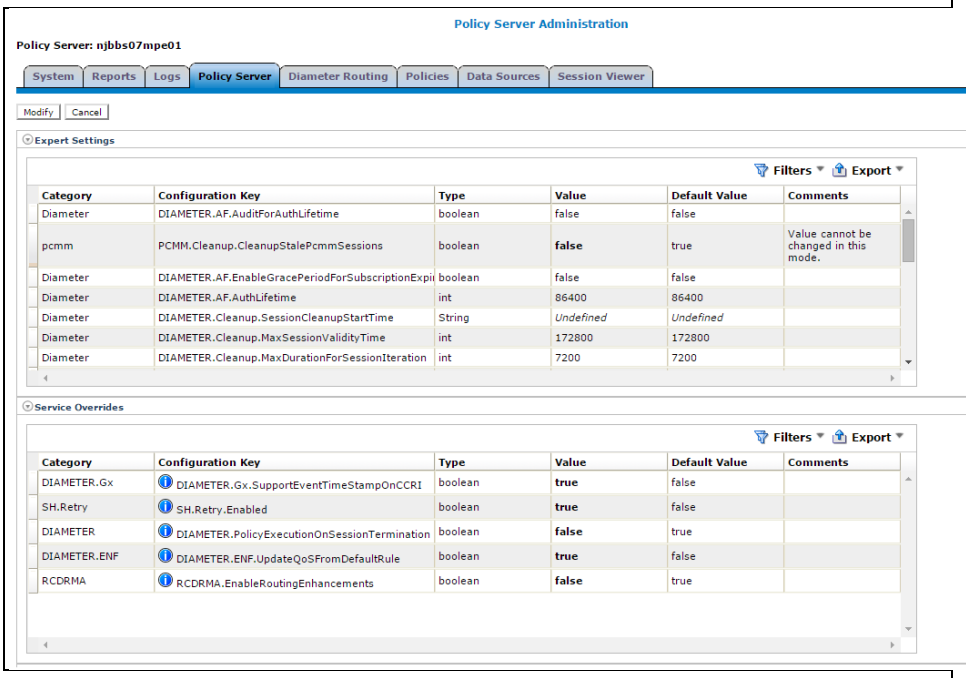
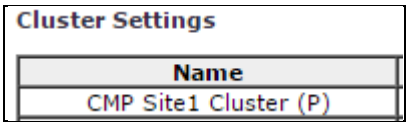
Procedure 2: Upgrade CMP Cluster

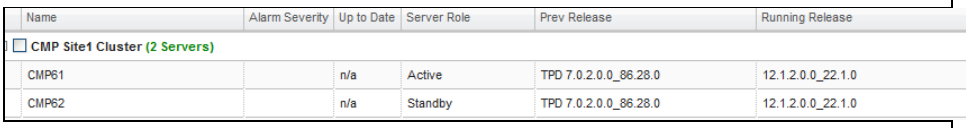
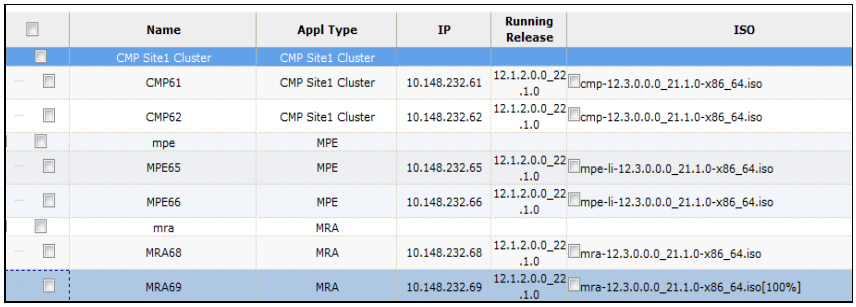
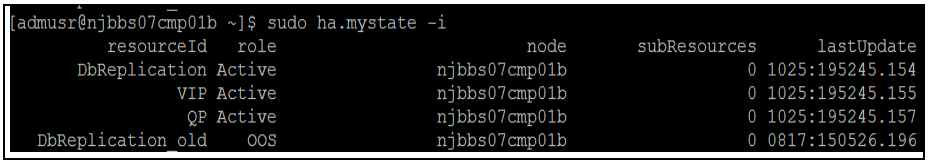
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Alarm Status.	1. Navigate to **System Wide Reports → Alarms → Active Alarms** 2. Confirm that any existing alarm is understood and there is not any impact to the Upgrade procedure. 3. Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP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

Step	Procedure	Result
3. ☐	**CMP GUI:** Capture MRA Advanced Settings	1. Capture screenshots of the advanced settings on the MRA prior to upgrading the CMP and save them into files for future reference check. 2. Navigate to **MRA → Configuration →** <*MRA*> **→ MRA** 3. Click **Advanced Settings**.



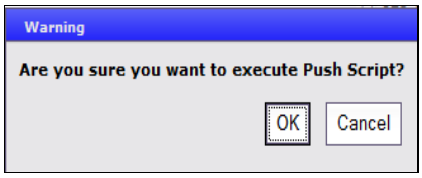
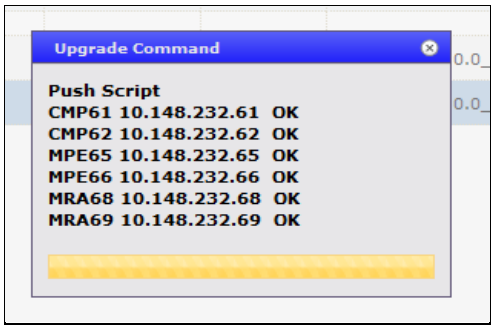
Alternatively, settings can be exported using the **Export** button on the right within each setting.

Step	Procedure	Result
4. ☐	**CMP GUI:** Capture MPE Advanced Settings	1. Capture screenshots of the advanced settings on the MPE prior to upgrading the CMP and save them for future reference. 2. Navigate to **Policy Server → Configuration →** <*MPE*> **→ Policy Server** 3. Click **Advanced Settings**.  Policy Server Administration Policy Server: njbbs07mpe01 System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sources | Session Viewer Modify | Cancel Expert Settings Filters ▾ Export ▾ Category | Configuration Key | Type | Value | Default Value | Comments Diameter | DIAMETER.AF.AuditForAuthLifetime | boolean | false | false | pcmm | PCMM.Cleanup.CleanupStalePcmmSessions | boolean | **false** | true | Value cannot be changed in this mode. Diameter | DIAMETER.AF.EnableGracePeriodForSubscriptionExpi | boolean | false | false | Diameter | DIAMETER.AF.AuthLifetime | int | 86400 | 86400 | Diameter | DIAMETER.Cleanup.SessionCleanupStartTime | String | *Undefined* | *Undefined* | Diameter | DIAMETER.Cleanup.MaxSessionValidityTime | int | 172800 | 172800 | Diameter | DIAMETER.Cleanup.MaxDurationForSessionIteration | int | 7200 | 7200 | Service Overrides Filters ▾ Export ▾ Category | Configuration Key | Type | Value | Default Value | Comments DIAMETER.Gx | DIAMETER.Gx.SupportEventTimeStampOnCCRI | boolean | **true** | false | SH.Retry | SH.Retry.Enabled | boolean | **true** | false | DIAMETER | DIAMETER.PolicyExecutionOnSessionTermination | boolean | **false** | true | DIAMETER.ENF | DIAMETER.ENF.UpdateQoSFromDefaultRule | boolean | **true** | false | RCDRMA | RCDRMA.EnableRoutingEnhancements | boolean | **false** | true | Alternatively, settings can be exported using the **Export** button on the right within each setting.
5. ☐	**CMP GUI:** Identify and Record the CMP Cluster(s)	1. Navigate to Platform Setting → Topology Settings → All Clusters. 2. Note which cluster is the primary and which is the secondary. 3. Save a screenshot for future reference. The primary CMP is noted with a P  Cluster Settings Name CMP Site1 Cluster (P)

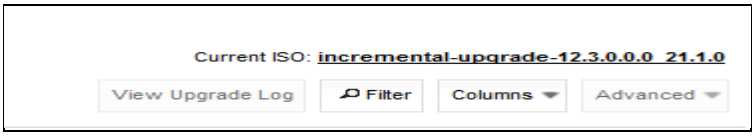
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>6. ☐</td><td>CMP GUI: Verify Status of CMP clusters and ISO files are copied to each server</td><td>1. Navigate to Upgrade → Upgrade Manager.
2. Verify that the CMP clusters have the following:
- Server Role: Active/Standby status.
- Running Release:12.1 or 12.2 version.
 
<table>
<tr><th>Name</th><th>Alarm Severity</th><th>Up to Date</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th></tr>
<tr><td colspan="6">CMP Site1 Cluster (2 Servers)</td></tr>
<tr><td>CMP61</td><td></td><td>n/a</td><td>Active</td><td>TPD 7.0.2.0.0_86.28.0</td><td>12.1.2.0.0_22.1.0</td></tr>
<tr><td>CMP62</td><td></td><td>n/a</td><td>Standby</td><td>TPD 7.0.2.0.0_86.28.0</td><td>12.1.2.0.0_22.1.0</td></tr>
</table>
3. Navigate to Upgrade → ISO Maintenance.
4. Corresponding Release 12.3.x ISO files copied to each of the servers (CMP/MRA/MPE/Mediation)
 
<table>
<tr><th></th><th>Name</th><th>Appl Type</th><th>IP</th><th>Running Release</th><th>ISO</th></tr>
<tr><td></td><td>CMP Site1 Cluster</td><td>CMP Site1 Cluster</td><td></td><td></td><td></td></tr>
<tr><td></td><td>CMP61</td><td>CMP Site1 Cluster</td><td>10.148.232.61</td><td>12.1.2.0.0_22.1.0</td><td>cmp-12.3.0.0.0_21.1.0-x86_64.iso</td></tr>
<tr><td></td><td>CMP62</td><td>CMP Site1 Cluster</td><td>10.148.232.62</td><td>12.1.2.0.0_22.1.0</td><td>cmp-12.3.0.0.0_21.1.0-x86_64.iso</td></tr>
<tr><td></td><td>mpe</td><td>MPE</td><td></td><td></td><td></td></tr>
<tr><td></td><td>MPE65</td><td>MPE</td><td>10.148.232.65</td><td>12.1.2.0.0_22.1.0</td><td>mpe-li-12.3.0.0.0_21.1.0-x86_64.iso</td></tr>
<tr><td></td><td>MPE66</td><td>MPE</td><td>10.148.232.66</td><td>12.1.2.0.0_22.1.0</td><td>mpe-li-12.3.0.0.0_21.1.0-x86_64.iso</td></tr>
<tr><td></td><td>mra</td><td>MRA</td><td></td><td></td><td></td></tr>
<tr><td></td><td>MRA68</td><td>MRA</td><td>10.148.232.68</td><td>12.1.2.0.0_22.1.0</td><td>mra-12.3.0.0.0_21.1.0-x86_64.iso</td></tr>
<tr><td></td><td>MRA69</td><td>MRA</td><td>10.148.232.69</td><td>12.1.2.0.0_22.1.0</td><td>mra-12.3.0.0.0_21.1.0-x86_64.iso[100%]</td></tr>
</table></td></tr>
<tr><td>7. ☐</td><td>SSH Primary Active CMP: SSH CLI Primary Active CMP and verify the Primary Active CMP Role</td><td>1. SSH into the Primary Active CMP with its VIP address.
Login: admusr
Password: <provided password>
2. Run the sudo ha.mystate -i command to confirm the role is Active.
$ sudo ha.mystate -i
 
<pre>[admusr@njbbs07cmp01b ~]$ sudo ha.mystate -i
         resourceId   role   node   subResources   lastUpdate
     DbReplication Active   njbbs07cmp01b   0 1025:195245.154
               VIP Active   njbbs07cmp01b   0 1025:195245.155
                QP Active   njbbs07cmp01b   0 1025:195245.157
  DbReplication_old   OOS   njbbs07cmp01b   0 0817:150526.196</pre>
NOTE: DbReplication_old_OOS is a non-issue status event.</td></tr>
</table>

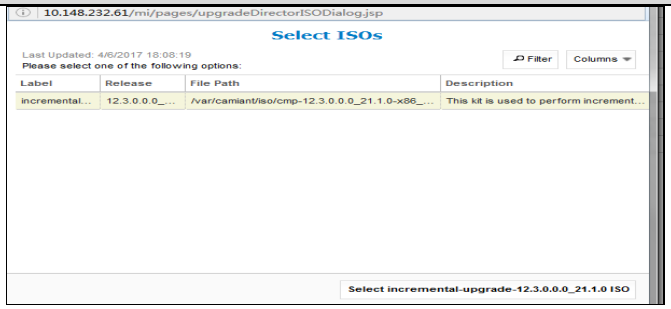
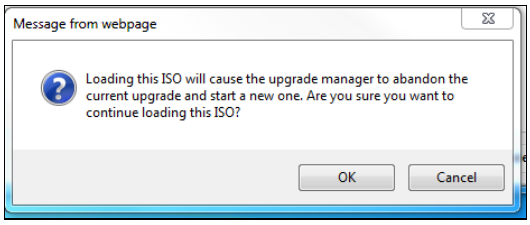
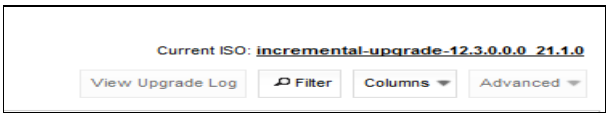
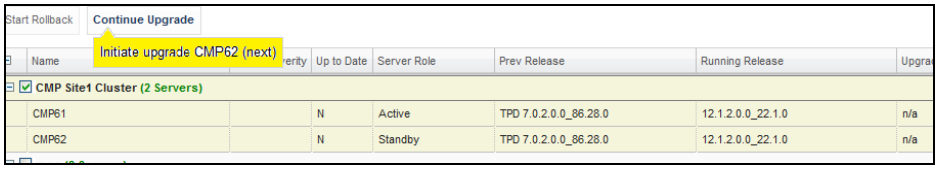
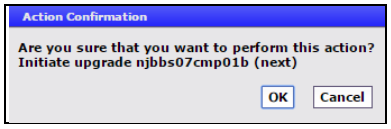
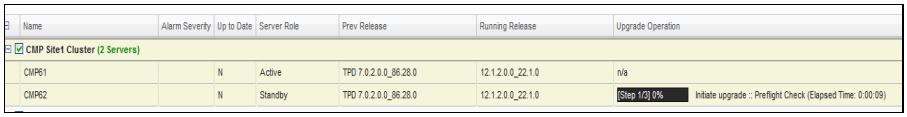
Step	Procedure	Result

8. ☐	**SSH Primary Active CMP:** exchange keys	1. Exchange keys to all servers from the SITE 1 Active Primary CMP.
		2. Login as admusr user.
		NOTE: This step could be skipped if your system was fresh installed in R12.1 or R12.2.
		`$ sudo mount -o loop /var/TKLC/upgrade/cmp-12.3.0.0_x.x.0-x86_64.iso /mnt/upgrade/`
		`$ sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		NOTE: If prompted, answer Yes to all.
		`$ sudo umount /mnt/upgrade`
		`$ sudo qpSSHKeyProv.pl --prov`
		• Required to enter the PASSWORD for admusr user.
		• Ensure that the Keys are exchanged successfully with all the server clusters
		For example:
		`$ sudo qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:<admusr password>`
		`Connecting to admusr@njbbs07cmp01b ...`
		`Connecting to admusr@njbbs07cmp01a ...`
		`Connecting to admusr@txsls07mra01b ...`
		`Connecting to admusr@njbbs07mpe02a ...`
		`Connecting to admusr@txsls07mpe01b ...`
		`Connecting to admusr@njbbs07mra01a`
		`[16/17] Provisioning SSH keys on txsls07mpe02b ...`
		`[17/17] Provisioning SSH keys on njbbs07mra01b ...`
		`SSH keys are OK.`

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

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

11. ☐	**CMP GUI:** Select the 12.3.x Upgrade release	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Current ISO.  This opens a dialog box with a description of the ISO that was copied into the `/var/camiant/iso` directory. 3. Highlight the available 12.3.x ISO. 4. Click **Select incremental-upgrade-12.3.0.0.0_x.x.0 ISO** on the bottom right hand corner of the window.

Step	Procedure	Result
		 5. Click **OK**.  Within a few seconds, the Up to date column changes from Y (meaning up-to-date) to N (meaning needs upgrade).
12. ☐	**CMP GUI**: Upgrade Primary CMP cluster **NOTE:** This takes approximately 30 minutes at most to complete. **NOTE:** Up to 8 clusters can be upgraded at the same time, selecting one at a time.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Click **Filter** and enter `CMP` in the **Name** field.  3. Select the Primary CMP Server Cluster. 4. Click **Continue Upgrade**.  5. Click **OK** to confirm and continue with the operation.  The specific action taken is determined by the Upgrade Manager and based on the specific version change being performed. This continues to upgrade the standby server only in the CMP Cluster In the Upgrade Operation column, the In Progress status along with the upgrade activities cdisplays. 

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td>Upgrade Status changes to completed when done.

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

<u>Expected Critical Alarms</u>

70001 The qp_procmgr process has failed
31227 The high availability status is failed due to raised alarms
70025 The MySQL slave has a different schema version than the master
31283 High availability server is offline

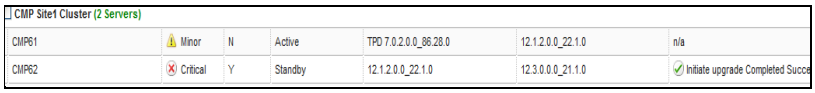
<u>Expected Major Alarms</u>

70004 The QP processes have been brought down for maintenance
31233 High availability path loss of connectivity
70021 The MySQL slave is not connected to the master

<u>Expected Minor Alarms</u>

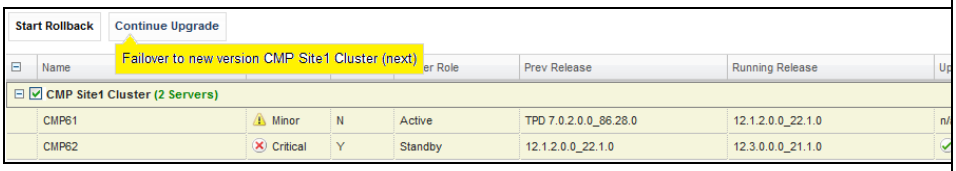
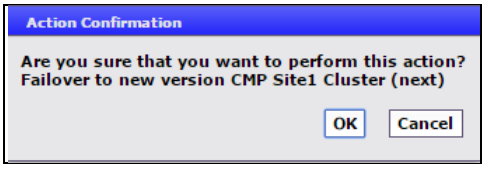
70503 The server is in forced standby
70507 An upgrade/backout action on a server is in progress
70501 The Cluster is running different versions of software
70500 The system is running difference versions of software
31101 DB replication to a slave DB has failed
31106 DB merging to the parent Merge Node has failed
31107 DB merging from a child Source Node has failed
31102 DB replication from a master DB has failed
31114 DB Replication of configuration data via SOAP has failed
31105 The DB merge process (inetmerge) is impaired by a s/w fault

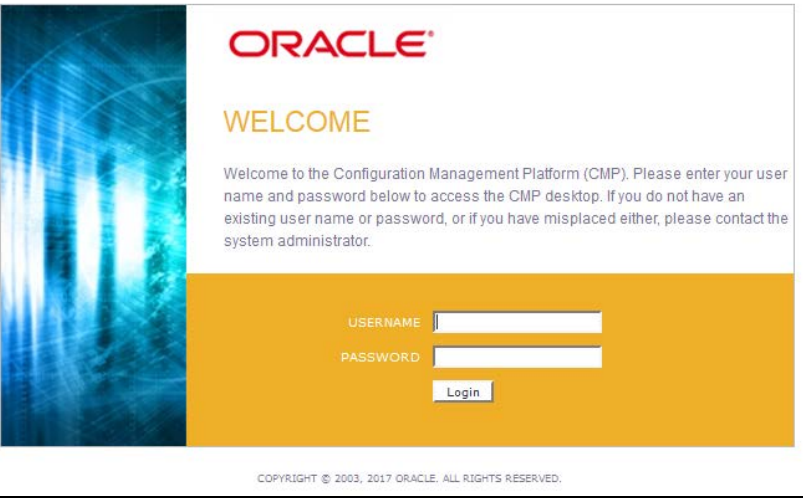
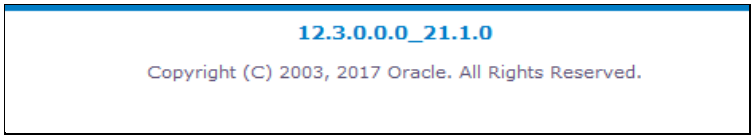
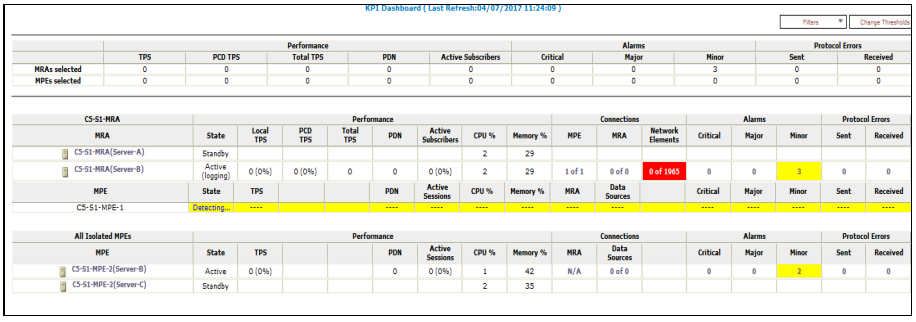
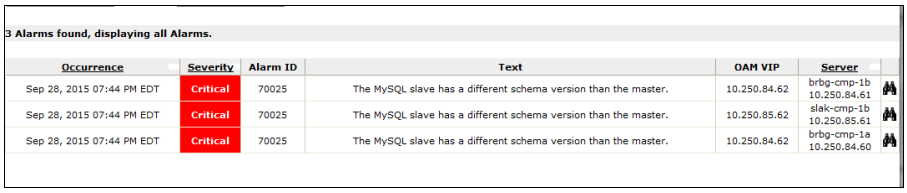
Upgrade is complete on the first CMP server in the cluster when the following message (completed successfully) displays in the Upgrade Operation column.
 
</td></tr>
<tr><td>13. ☐</td><td>CMP GUI: Verify the upgrade is successful</td><td>1. Navigate to Upgrade → Upgrade Manager.

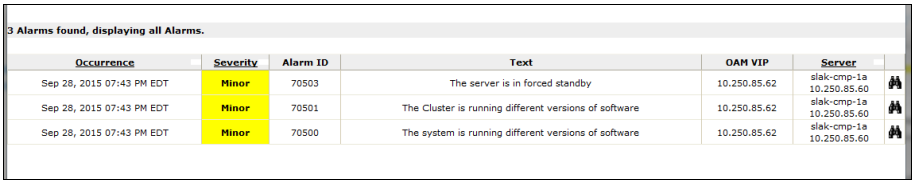
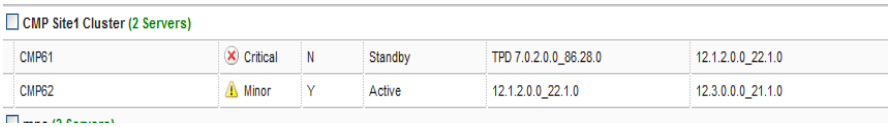
2. View the cluster. At this point, one server is on 12.3.x and the other server in the cluster is on 12.1. The Up To Date column shows Y for the 12.3.x server and N for the 12.1 server.
 
</td></tr>
</table>

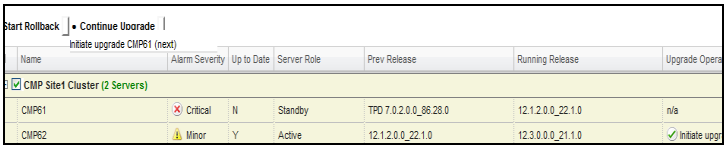
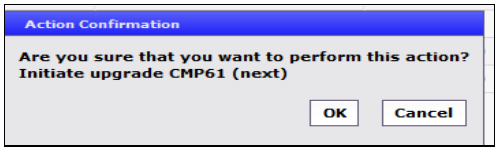
Step	Procedure	Result

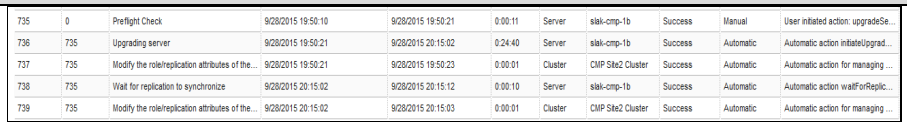
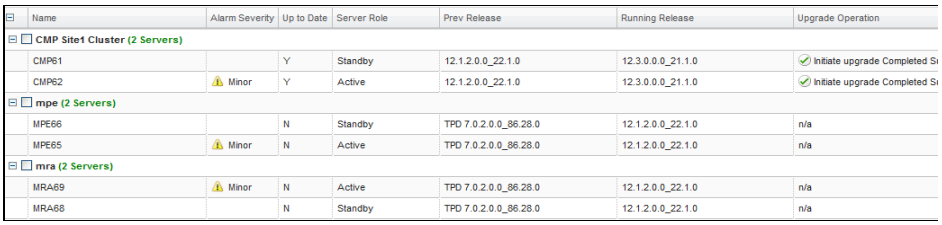
14. ☐	**CMP CLI:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the upgrade is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		
		To resolve this situation permanently, perform the following: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

15. ☐	**CMP GUI:** Verify System Wide Reports—KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Verify that report shows all normal traffic processing for the MPEs/MRAs. Observe it for a few refresh updates.
16. ☐	**CMP GUI:** Continue Upgrade CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server cluster. 3. Click **Continue Upgrade**. Notice the failover to new version message. **NOTE:** This causes a failover of the Primary CMP cluster  4. Click **OK** to confirm and continue with the operation.  The action takes less than a minute to complete.

Step	Procedure	Result
17. ☐	**CMP GUI:** Re-login to the CMP server VIP	Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Management Release 12.3.x CMP GUI Login displays as shown. Login and password credentials are the same as the pre-upgrade. 
18. ☐	**CMP GUI:** Verify Policy Management Release	1. Navigate to **Help→About**. 2. Verify the release displayed is 12.3.x 
19. ☐	**CMP GUI:** Verify traffic	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Verify that report shows all normal traffic processing for the MPEs/MRAs. Observe it for few updates refresh. 
20. ☐	**CMP GUI:** Critical Alarms	Multiple critical alarms (70025) are seen until the SQL Database matches the master (12.3.x). Thise alarms are expected and remain until all CMPs have been upgraded to the same version. 

Step	Procedure	Result
		Current Minor Alarms **70503** Server Forced Standby **70501** Cluster Mixed Version **70500** System Mixed Version  3 Alarms found, displaying all Alarms. Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Sep 28, 2015 07:43 PM EDT | Minor | 70503 | The server is in forced standby | 10.250.85.62 | slak-cmp-1a 10.250.85.60 Sep 28, 2015 07:43 PM EDT | Minor | 70501 | The Cluster is running different versions of software | 10.250.85.62 | slak-cmp-1a 10.250.85.60 Sep 28, 2015 07:43 PM EDT | Minor | 70500 | The system is running different versions of software | 10.250.85.62 | slak-cmp-1a 10.250.85.60 **NOTE:** The Upgrade Manager also displays alarms.
21. ☐	**CMP GUI:** Verify the Policy Management Release 12.3.x CMP is Active	1. Navigate to **Upgrade→ Upgrade Manager** 2. Verify the following - - Active server is on Running Release 12.3.x - Standby server is on the previous Release 22.  CMP Site1 Cluster (2 Servers) CMP61 | Critical | N | Standby | TPD 7.0.2.0.0_86.28.0 | 12.1.2.0.0_22.1.0 CMP62 | Minor | Y | Active | 12.1.2.0.0_22.1.0 | 12.3.0.0.0_21.1.0 As noted, the Active CMP server is now on the Running Release of 12.3.x

Step	Procedure	Result
23. ☐	**CMP GUI:** Complete the Upgrade of the Primary CMP Cluster **NOTE:** This takes approximately30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server Cluster. 3. Click **Continue Upgrade**. Notice the message Initiate upgrade.  4. Click **OK** in the dialog to continue the upgrade on the remaining server in the CMP cluster.  **NOTE:** The remaining CMP server takes approximately 30 minutes to complete. Server getting upgraded goes into OOS state. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **70022** The MySQL slave failed synchronizing with the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault
24. ☐	**CMP GUI:** Tracking the upgrade complete	1. Navigate to **Upgrade → Upgrade Manager**. The last step in the upgrade for the first CMP cluster is to wait for replication to complete. 2. Select the upgraded CMP cluster. 3. Click **View Upgrade** Log.

Step	Procedure	Result
		
25. ☐	**CMP GUI:** Verify the status of the upgraded CMP server.	Navigate to **Upgrade Manager → Upgrade Manager**.  • Successful upgrade status shows both servers running the Release 12.3.x in the Running Release column and Y for both servers in the Up To Date column • Active/standby state for both servers in the Primary CMP Cluster.
26. ☐	Proceed to next upgrade procedure	At this point, the Primary Site-1 is running Release 12.3.x • Secondary SITE is on R12.1.x or R12.2.x • Proceed to the next procedure to upgrade the secondary CMP cluster.
---End of Procedure---		

5.1.2 Upgrade Secondary CMP Cluster

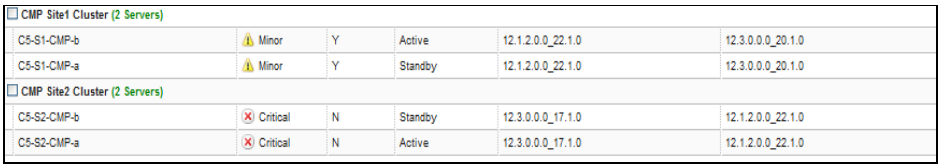
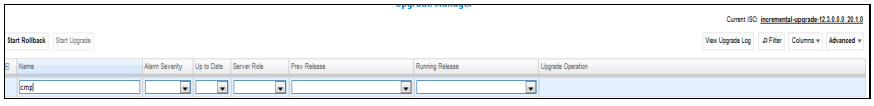
Use this procedure to upgrade Secondary CMP Cluster.

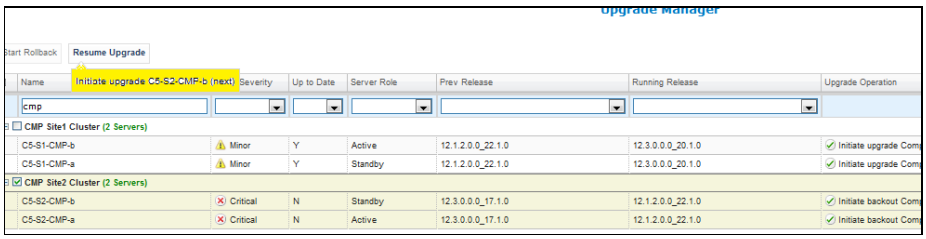
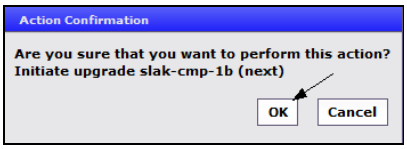
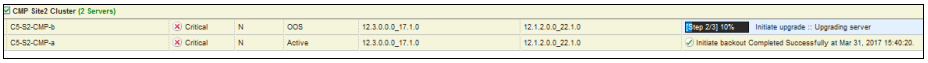
NOTES:

- This procedure must be performed in a maintenance window.
- This procedure takes approximately 60-120 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

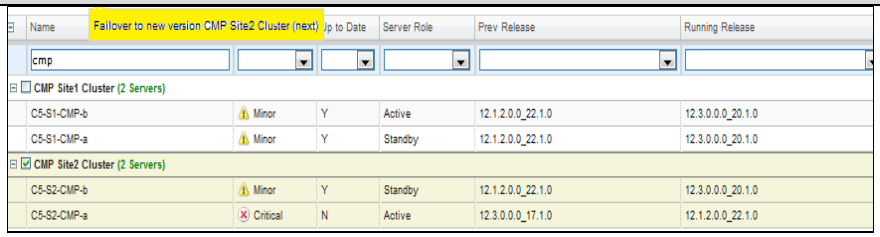
Procedure 3: Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Status of CMP Cluster	Navigate to **Upgrade → Upgrade Manager**. • Primary CMP is completely upgraded to 12.3.x • Secondary CMP Cluster is on 12.1.x 
2. ☐	**CMP GUI**: Upgrade the Secondary CMP cluster **NOTE:** This takes approximately30 minutes to	1. Navigate to **Upgrade → Upgrade Manager**. 2. Click **Filter** and enter `CMP` in the **Name** field. 

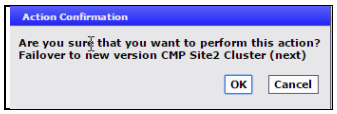
Step	Procedure	Result
	complete.	3. Select the Secondary CMP Server Cluster at Site-2 4. Click **Continue Upgrade** or **Resume Upgrade**.  5. Click **OK** to confirm and continue with the operation.  The specific action taken is determined by the Upgrade Manager and based on the specific version change being performed. This continues to upgrade the standby server only in the CMP Cluster The Upgrade Operation column displays the In Progress status along with the upgrade activities.  During the Upgrade activities, the following alarms may be generated and are considered normal reporting events: **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault LOG FILE from the GUI showing complete on the 1st server on the secondary site.

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>740</td><td>0</td><td>Preflight Check</td><td>9/28/2015 20:18:57</td><td>9/28/2015 20:19:11</td><td>0:00:14</td><td>Server</td><td>brbg-cmp-1b</td><td>Success</td><td>Manual</td><td>User initiated action: upgradeSer...</td></tr>
<tr><td>741</td><td>740</td><td>Upgrading server</td><td>9/28/2015 20:19:11</td><td>9/28/2015 20:44:02</td><td>0:24:50</td><td>Server</td><td>brbg-cmp-1b</td><td>Success</td><td>Automatic</td><td>Automatic action initiateUpgrade ...</td></tr>
<tr><td>742</td><td>740</td><td>Modify the role/replication attributes of the ...</td><td>9/28/2015 20:19:11</td><td>9/28/2015 20:19:13</td><td>0:00:01</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>9/28/2015 20:44:02</td><td>9/28/2015 20:44:12</td><td>0:00:10</td><td>Server</td><td>brbg-cmp-1b</td><td>Success</td><td>Automatic</td><td>Automatic action waitForReplicat...</td></tr>
</table>
</td></tr>
<tr><td>3. ☐</td><td>CMP GUI: Verify the upgrade is successful</td><td>1. Navigate to Upgrade → Upgrade Manager.
2. Select the partially upgraded cluster.
3. Click View Upgrade Log.
Upgrade Log
Cluster Name: CMP Site1 Cluster
Last Update: 1/20/2016 18:44:39
Filter Columns
<table>
<tr><th>ID</th><th>Pare...</th><th>Action Name</th><th>Start Time</th><th>End Time</th><th>Dura...</th><th>Scope</th><th>Hostname</th><th>Result</th><th>Mode</th><th>Description</th></tr>
<tr><td>9</td><td>7</td><td>Patching server</td><td>1/6/2016 12:13:36</td><td>1/6/2016 12:14:16</td><td>0:00:40</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Automatic</td><td>Automatic action pat...</td></tr>
<tr><td>10</td><td>7</td><td>Modify the role/replication ...</td><td>1/6/2016 12:13:36</td><td>1/6/2016 12:13:38</td><td>0:00:02</td><td>Cluster</td><td>CMP Site1...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
<tr><td>11</td><td>7</td><td>Wait for replication to sync...</td><td>1/6/2016 12:14:16</td><td>1/6/2016 12:14:26</td><td>0:00:10</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Automatic</td><td>Automatic action wai...</td></tr>
<tr><td>12</td><td>7</td><td>Modify the role/replication ...</td><td>1/6/2016 12:14:16</td><td>1/6/2016 12:14:18</td><td>0:00:02</td><td>Cluster</td><td>CMP Site1...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
<tr><td>135</td><td>0</td><td>Preflight Check</td><td>1/19/2016 21:24:58</td><td>1/19/2016 21:2...</td><td>0:00:14</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Manual</td><td>User initiated action:...</td></tr>
<tr><td>136</td><td>135</td><td>Upgrading server</td><td>1/19/2016 21:25:12</td><td>1/19/2016 21:5...</td><td>0:24:50</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Automatic</td><td>Automatic action initi...</td></tr>
<tr><td>137</td><td>135</td><td>Modify the role/replication ...</td><td>1/19/2016 21:25:12</td><td>1/19/2016 21:2...</td><td>0:00:03</td><td>Cluster</td><td>CMP Site1...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
<tr><td>138</td><td>135</td><td>Wait for replication to sync...</td><td>1/19/2016 21:50:02</td><td>1/19/2016 21:5...</td><td>0:00:09</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Automatic</td><td>Automatic action wai...</td></tr>
<tr><td>139</td><td>0</td><td>Failover to new version</td><td>1/19/2016 22:43:30</td><td>1/19/2016 22:4...</td><td>0:00:00</td><td>Cluster</td><td>CMP Site1...</td><td>Success</td><td>Manual</td><td>User initiated action:...</td></tr>
<tr><td>140</td><td>0</td><td>Preflight Check</td><td>1/19/2016 22:47:14</td><td>1/19/2016 22:4...</td><td>0:00:17</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Manual</td><td>User initiated action:...</td></tr>
<tr><td>141</td><td>140</td><td>Upgrading server</td><td>1/19/2016 22:47:31</td><td>1/19/2016 23:1...</td><td>0:24:40</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Automatic</td><td>Automatic action initi...</td></tr>
<tr><td>142</td><td>140</td><td>Modify the role/replication ...</td><td>1/19/2016 22:47:31</td><td>1/19/2016 22:4...</td><td>0:00:04</td><td>Cluster</td><td>CMP Site1...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
<tr><td>143</td><td>140</td><td>Wait for replication to sync...</td><td>1/19/2016 23:12:11</td><td>1/19/2016 23:1...</td><td>0:00:09</td><td>Server</td><td>njbbs07cm...</td><td>Success</td><td>Automatic</td><td>Automatic action wai...</td></tr>
<tr><td>144</td><td>140</td><td>Modify the role/replication ...</td><td>1/19/2016 23:12:11</td><td>1/19/2016 23:1...</td><td>0:00:04</td><td>Cluster</td><td>CMP Site1...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
</table>
</td></tr>
<tr><td>4. ☐</td><td>CMP CLI: Verify eth01 is primary device interface</td><td>This step only applies if the server has a condition in which after the upgrade is successful, ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
To resolve this situation permanently, perform the following:
1. As admusr, run the following:
$ sudo cat /proc/net/bonding/bond0
2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable when primary is set to eth11.
3. If this blade is the active blade, change it to standby before performing the following operations.
$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0
4. Find the the keyword rimary=eth11.
5. Change primary=eth11 to primary=eth01
6. Save and exit (for example, vi uses ESC :wq!)
$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0
$ sudo reboot</td></tr>
<tr><td>5. ☐</td><td>CMP GUI: Continue Upgrade of Secondary CMP cluster
NOTE: This takes approximately30 minutes to</td><td>1. Navigate to Upgrade → Upgrade Manager.
2. Select the Secondary CMP Server Cluster at Site-2.
3. Click Continue Upgrade. Notice the failover to new version message.</td></tr>
</table>

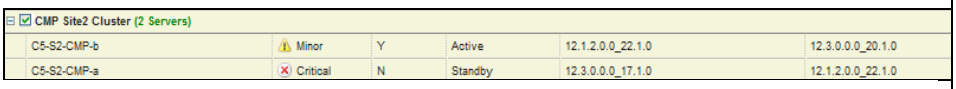
Step	Procedure	Result
	complete.	



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

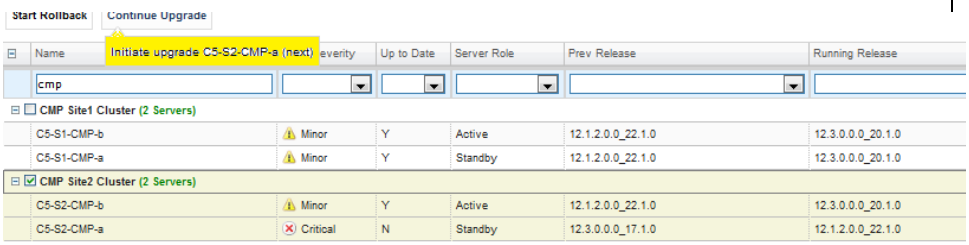


5. The specific action takes approximately a minute to complete. Wait until the upgraded server is active, as shown below.

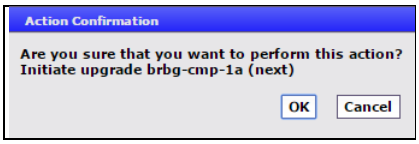


6. Select the Secondary CMP Server Cluster at Site-2

7. Click **Continue Upgrade**. When hovering over the **Continue Upgrade** button, the message displays the next action, which is upgrading the remaining CMP hostname.



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



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

Expected Critical Alarms

70001 The qp_procmgr process has failed
31227 The high availability status is failed due to raised alarms
70025 The MySQL slave has a different schema version than the master
31283 High availability server is offline

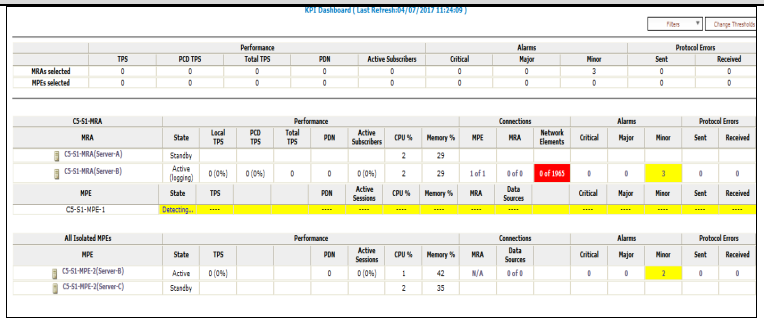
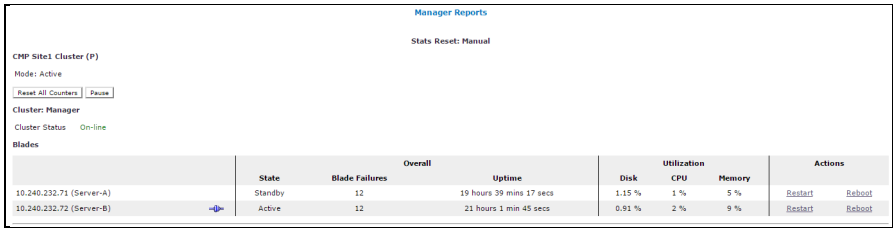
Expected Major Alarms

70004 The QP processes have been brought down for maintenance
31233 High availability path loss of connectivity
70021 The MySQL slave is not connected to the master
70022 The MySQL slave failed synchronizing with the master

Step	Procedure	Result
		Expected Minor Alarms **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault
6. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	Navigate to **Upgrade → Upgrade Manager**. • Successful upgrade status shows the Release 12.3.x in the Running Release column. • Also, in the Upgrade Operation column, it displays the Initiate Upgrade Completed Successfully message with the correct date and time.

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

8. ☐	**CMP GUI:** Verify Alarms	Navigate to **System Wide Reports → Alarms → Active Alarms**. **Expected Minor Alarms** **70500** The system is running different versions of software
9. ☐	**CMP GUI:** Verify System Wide Reports—KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**.

Step	Procedure	Result
		 2. Verify that report shows all normal traffic processing for the MPEs/MRAs.
10. ☐	**CMP GUI:** Verify System Administration Reports	Navigate to **System Administration → Reports**. 
11. ☐	**CMP GUI:** Verify Advanced settings on the MPE and MRA.	• Compare the current advanced settings on the MRA and MPE with the captured screenshots saved prior to upgrading the CMP cluster.
12. ☐		• All CMP Clusters Upgrade are complete and running Release 12.3.x. • ALL MRAs and MPEs are on Release 12.1.x or 12.2.x At this point, the OCPM system is running in mixed-version mode.
---End of Procedure---		

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

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

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

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

6.1 Upgrade CMP Clusters Overview

1. Upgrade the Primary CMP cluster

   Upgrade CMP Site1

   a. Start upgrade on the standby server

   b. Failover

   c. Continue upgrade with the remaining Site1 CMP server

2. Upgrade the Secondary CMP cluster

   Upgrade CMP Site2

   a. Start upgrade on the standby server

   b. Failover

   c. Continue upgrade with the remaining Site2 CMP server

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

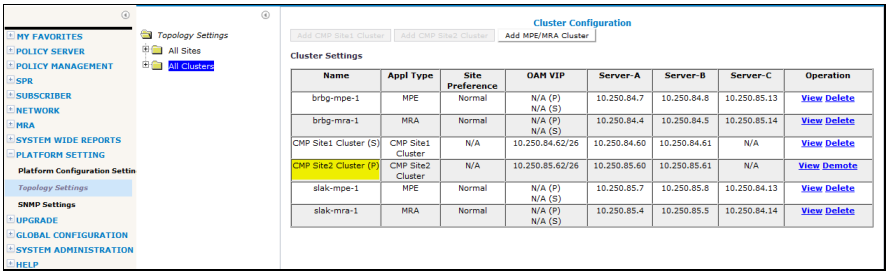
Identify the CMP sites to be upgraded here, and verify which site is Primary and which one is Secondary:

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

IMPORTANT:

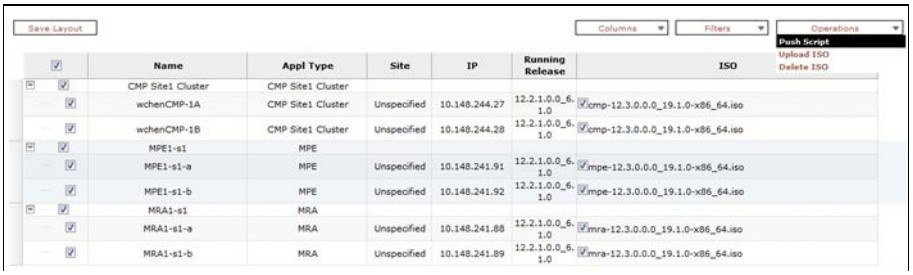
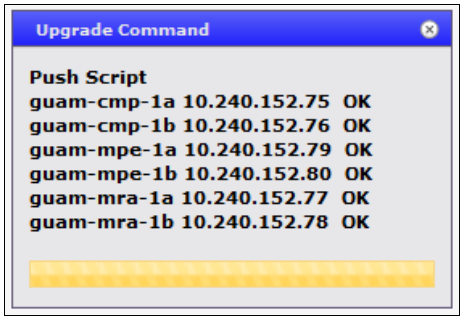
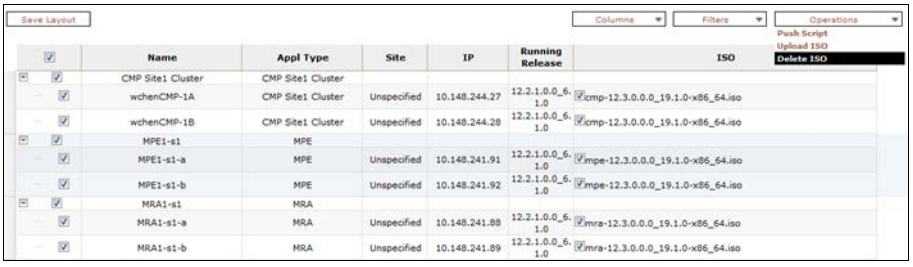
- The Primary CMP site must be upgraded to the new release before the Secondary CMP Site
- CMP servers must be upgraded before non-CMP servers

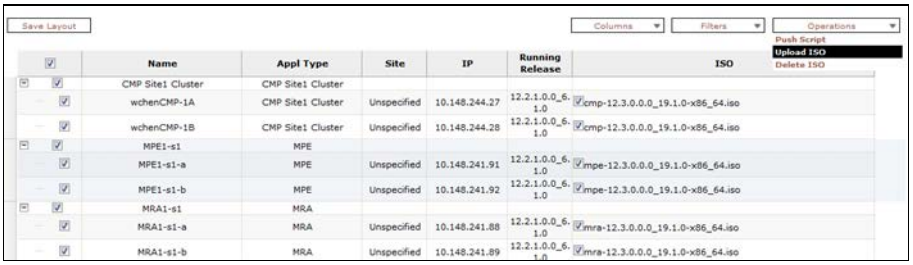
6.1.1 Upgrade Primary CMP cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Alarm Status.	**System Wide Reports → Alarms → Active Alarms** 1. Confirm that any existing alarm is understood and that there is of not any impact to the upgrade procedure. 2. Capture a screenshot and save it into a file for reference.
2. ☐	**CMP GUI:** Identify and Record the CMP Cluster(s)	1. Navigate to **Platform Setting → Topology Settings** 2. Note which cluster is the primary and which one is the secondary.  **NOTE:** The Primary CMP is noted with (P). The Secondary CMP with (S).
3. ☐	**CMP GUI**: Verify Status of CMP Clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm the CMP clusters are: - In Active/Standby status - Running release 12.2.x software 3. Navigate to Upgrade → ISO Maintenance. Verify that Release 12.3 ISO files have been copied to at least one of each corresponding server types (CMP, MPE, MRA, Mediation). 

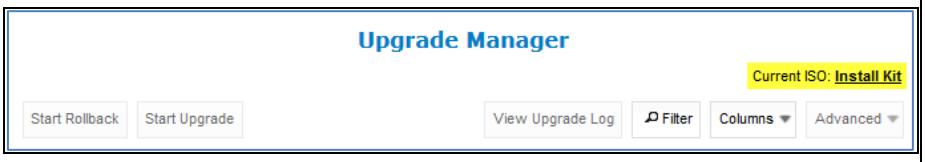
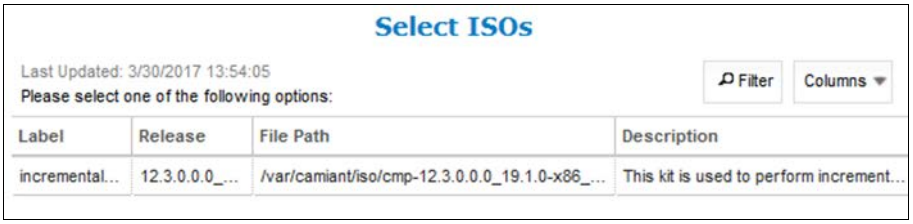
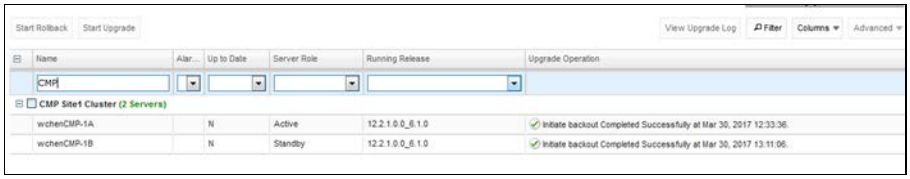
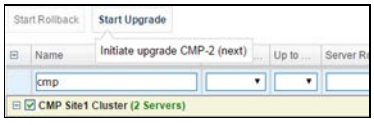
Step	Procedure	Result

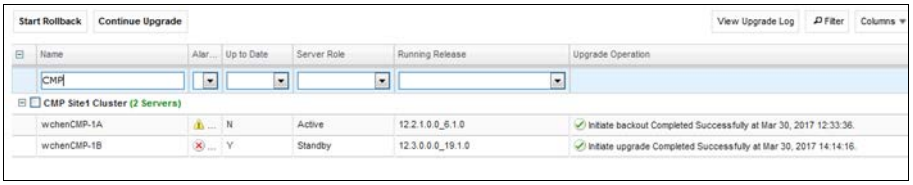
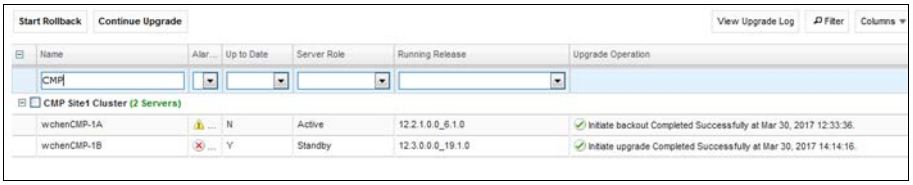
4. ☐	**SSH CLI Primary Active CMP:** Exchange Keys	1. Exchange keys to all servers from the Site1 (Primary) Active CMP. Login as admusr user and run the following command:
		`$sudo qpSSHKeyProv.pl --prov`
		`[admusr@guam-cmp-1a ~]$ sudo qpSSHKeyProv.pl -prov`
		`The password of admusr in topology:`
		2. Enter the password for admusr user.
		3. Ensure that the keys are exchanged successfully with all the server clusters:
		`Connecting to admusr@guam-cmp-1a ...`
		`Connecting to admusr@guam-mpe-1b ...`
		`Connecting to admusr@guam-mra-1b ...`
		`Connecting to admusr@guam-mpe-1a ...`
		`Connecting to admusr@guam-cmp-1b ...`
		`Connecting to admusr@guam-mra-1a ...`
		`[1/6] Provisioning SSH keys on guam-cmp-1a ...`
		`[2/6] Provisioning SSH keys on guam-mra-1b ...`
		`[3/6] Provisioning SSH keys on guam-mpe-1b ...`
		`[4/6] Provisioning SSH keys on guam-mpe-1a ...`
		`[5/6] Provisioning SSH keys on guam-cmp-1b ...`
		`[6/6] Provisioning SSH keys on guam-mra-1a ...`
		`SSH keys are OK.`

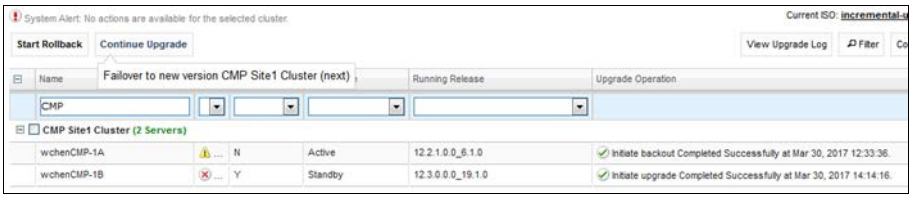
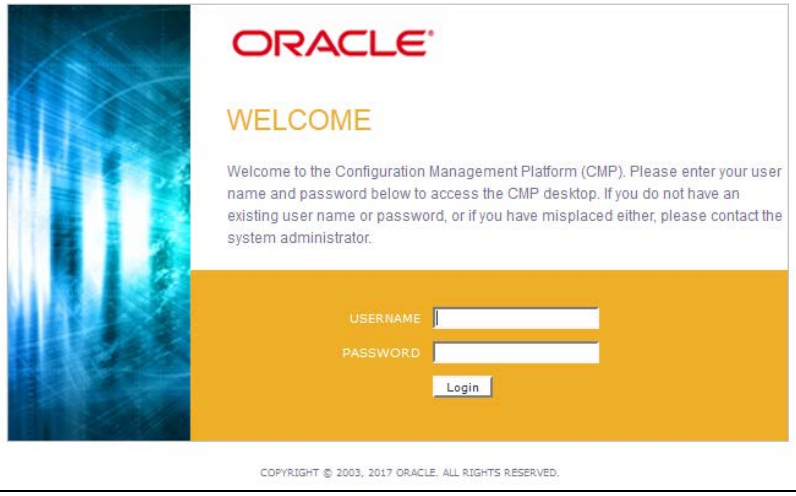
Step	Procedure	Result
5. ☐	**CMP GUI**: Push the Release 12.2 upgrade scripts to all servers	**Upgrade → ISO Maintenance** Notes: Upgrade scripts to be pushed has been placed in var/TKLC/upgrade. 1. Select all the servers in the topology as shown. 2. Select **Operations → Push Script** operation.  3. Click **OK** to continue the operation. 4. After approximately a minute, a successful dialog opens similar to the following: 
6. ☐	**CMP GUI Access** into Primary CMP Server—Remove old ISO files from servers, if any.	**Upgrade → ISO Maintenance** 1. Select the server(s) that show any old ISO files. 2. From the Operations menu, select **Delete ISO** operation to remove any older ISO files present.  3. Click **OK** to continue and wait until the successful deletion message displays. 4. Wait until the ISO Maintenance page is refreshed and the ISO column does not show any old ISO files.

Step	Procedure	Result
7. ☐	**CMP GUI:** Distribute ISO files to CMP/MPE/MRA/ Mediation servers **NOTE:** This step depends on the ISO type. Distribute ISO files accordingly.	1. Navigate to **Upgrade → ISO Maintenance**. 2. (Optional) Filter by server type. Click **Filter** and enter `CMP` in the **Name** field. 3. Select one cluster type (MPE/MRA/CMP/Mediation) to be upgraded. **<*cluster type*> → Operations → Upload ISO**.  4. Enter the configuration information: Mode = SCP ISO Server Hostname/IP = <*IP address where the ISO files are located*> User = admusr Password = <*admusr password of the server*> Source ISO Full Path = /var/TKLC/upgrade/<*server type iso filename*> 5. Click **Add**. When completed, the ISO column displays the ISO and a notification of [100%]. 6. Repeat for all cluster types.
8. ☐	**CMP GUI:** Verify ISO distribution to all the Servers	**Upgrade → ISO Maintenance** 1. Verify that the Release 12.3 ISO file of the correct type is shown for each server. 2. When completed, the ISO column displays the ISO and a notification of [100%]  **NOTE**: For those servers where the ISO file was copied to the local machine, there is not a [100%] indicator. This indicator is only available when transferring ISO files using the ISO management feature.

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

Step	Procedure	Result
10. ☐	**CMP GUI:** Locate the 12.2 Upgrade ISO	**Upgrade → Upgrade Manager** 1. Select the current ISO, in this case it is labeled Install kit.  This opens a dialog box with a description of the ISO that was copied into `/var/camiant/iso` 2. Highlight the available ISO and click **Select incremental-upgrade-12.3…** at the bottom of the window:  3. Click **OK** to confirm. Within a few seconds, the Up to Date column transitions from Y (meaning up-to-date) to N (meaning needs upgrade). 
11. ☐	**CMP GUI**: Upgrade Primary CMP cluster	1. Navigate to U**pgrade → Upgrade Manager**. 2. Click **Filter** and enter `CMP` in the **Name** field.  3. Select the Primary CMP Cluster 4. Click **Start Upgrade**.  5. Click **OK** to confirm and continue with the operation. 6. The first action is to upgrade the standby server in the CMP Cluster. **NOTE:** This takes approximately 30 minutes to complete. 7. The Upgrade Operation column displays a progress bar along with the upgrade activities.

Step	Procedure	Result
		During the upgrade activities, the server being updated is change to OOS (Out of Service) and the following alarms may be generated. They are considered normal reporting events: **Expected Critical Alarm** **31283** HA Server Offline **31227** HA Availability Status Failed **70025** QP Slave Database is a Different Version than the Master **70001** QP_procmgr failed **Expected Major Alarm** **70004** QP Processes Down for Maintenance. **Expected Minor Database Replication Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31114** DB replication over SOAP has failed **31282** HA Management Fault Upgrade is complete on the first server in the cluster when the message `Initiate upgrade completed successfully at…` displays in the Upgrade Operation column. 
12. ☐	**CMP GUI:** Verify the upgrade is successful	**Upgrade → Upgrade Manager** View the cluster. At this point, the standby server is on 12.3 and the other server in the cluster is on 12.2.x. The Up To Date column shows Y for the 12.3 server and N for the 12.2.x server.  The critical alarm 70025 (The MySQL slave has a different schema version than the master is active as well as the minor alarms 70500 (The system is running different versions of software) and 70501 (The cluster is running different versions of software).

Step	Procedure	Result
13. ☐	**CMP GUI:** Continue upgrade on CMP cluster	**Upgrade → Upgrade Manager** 1. Make sure the Primary CMP Cluster is still selected. 2. Click **Continue Upgrade**. Notice the message Failover to new version.  3. Click **OK** to confirm and continue with the operation. 4. The specific action takes approximately a minute to complete.
14. ☐	**CMP GUI:** Re-login to the CMP VIP	1. Close the current CMP GUI browser tab. 2. Open another browser tab with the same CMP VIP address. The Policy Management Release 12.3 CMP GUI login opens. 3. Login and password credentials are the same as the pre-upgrade. 
1. ☐	**CMP GUI:** Verify Policy Management release	4. Navigate to **HELP→About**. 5. Verify the release displayed is 12.3. 

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>2. ☐</td><td>CMP GUI: Critical Alarms</td><td>Critical alarm 70025 and the minor alarms 70503, 70501, 70500 are displayed.

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

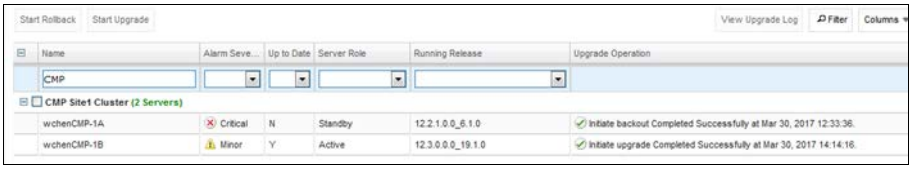
<table>
<tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th><th>OAM VIP</th><th>Server</th></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Critical</td><td>70025</td><td>The MySQL slave has a different schema version than the master.</td><td>10.240.152.88</td><td>guam-cmp-1a
10.240.152.75</td></tr>
</table>

Current Minor Alarms

<table>
<tr><th>Occurrence</th><th>Severity</th><th>Alarm ID</th><th>Text</th><th>OAM VIP</th><th>Server</th></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Minor</td><td>70503</td><td>The server is in forced standby</td><td>10.240.152.88</td><td>guam-cmp-1b
10.240.152.76</td></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Minor</td><td>70501</td><td>The Cluster is running different versions of software</td><td>10.240.152.88</td><td>guam-cmp-1b
10.240.152.76</td></tr>
<tr><td>Nov 09, 2016 04:08 PM EST</td><td>Minor</td><td>70500</td><td>The system is running different versions of software</td><td>10.240.152.88</td><td>guam-cmp-1b
10.240.152.76</td></tr>
</table>
</td></tr>
<tr><td>15. ☐</td><td>CMP GUI: Verify the Policy Management Release 12.3 CMP is active</td><td>Upgrade → Upgrade Manager

Verify the following:

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



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

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

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>17. ☐</td><td>CMP GUI: Tracking the upgrade complete</td><td>Upgrade → Upgrade Manager

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

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

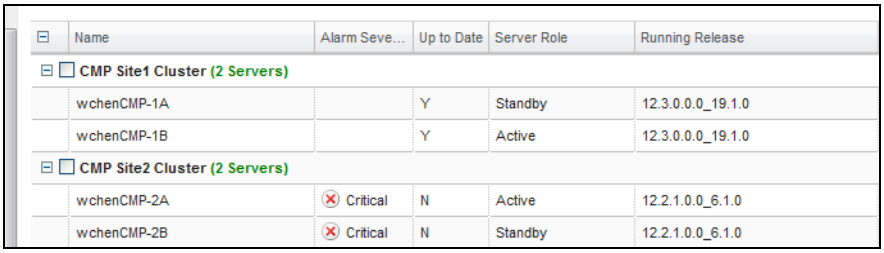
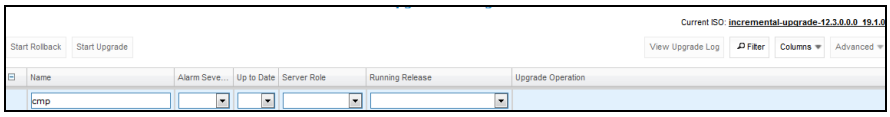
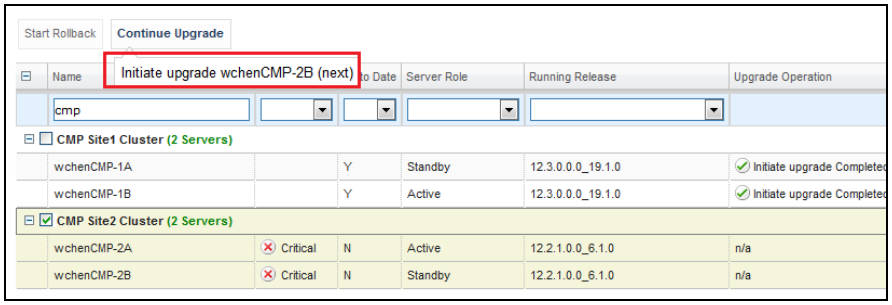
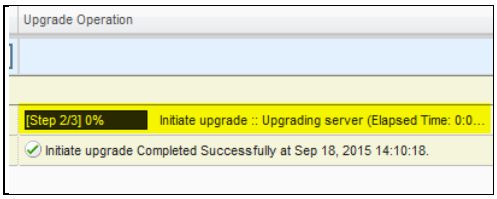
Upgrade Log
Cluster Name: CMP Site1 Cluster
Last Update: 11/10/2016 9:01:00
<table><tr><th>ID</th><th>Parent ID</th><th>Action Name</th><th>Duration</th><th>Scope</th><th>Hostname</th><th>Result</th><th>Mode</th></tr><tr><td>1</td><td>0</td><td>Preflight Check</td><td>0:00:15</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Manual</td></tr><tr><td>2</td><td>1</td><td>Upgrading server</td><td>0:22:00</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Automatic</td></tr><tr><td>3</td><td>1</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr><tr><td>4</td><td>1</td><td>Wait for replication to synchronize</td><td>0:00:09</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Automatic</td></tr><tr><td>5</td><td>0</td><td>Failover to new version</td><td>0:00:00</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Manual</td></tr><tr><td>6</td><td>0</td><td>Preflight Check</td><td>0:00:15</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Manual</td></tr><tr><td>7</td><td>6</td><td>Upgrading server</td><td>0:21:50</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Automatic</td></tr><tr><td>8</td><td>6</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr><tr><td>9</td><td>6</td><td>Wait for replication to synchronize</td><td>0:00:29</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Automatic</td></tr><tr><td>10</td><td>6</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr></table></td></tr>
<tr><td>18. ☐</td><td>CMP GUI: Verify the status of the upgraded CMP server.</td><td>Upgrade → Upgrade Manager

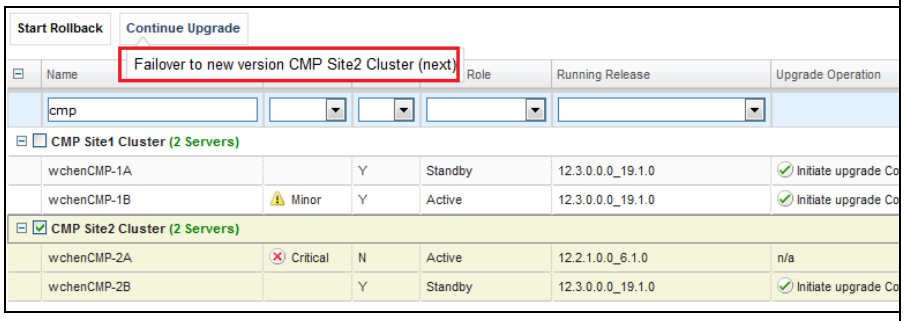
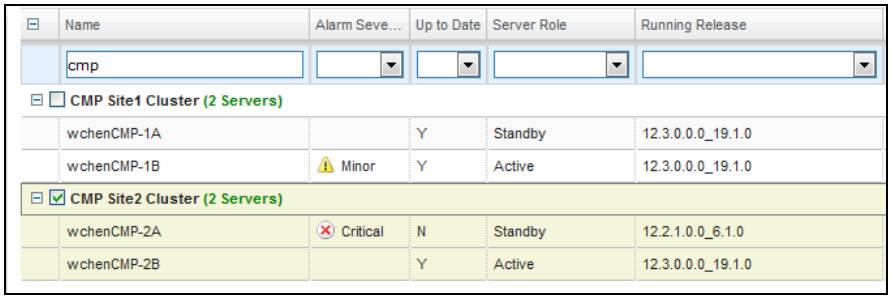
 

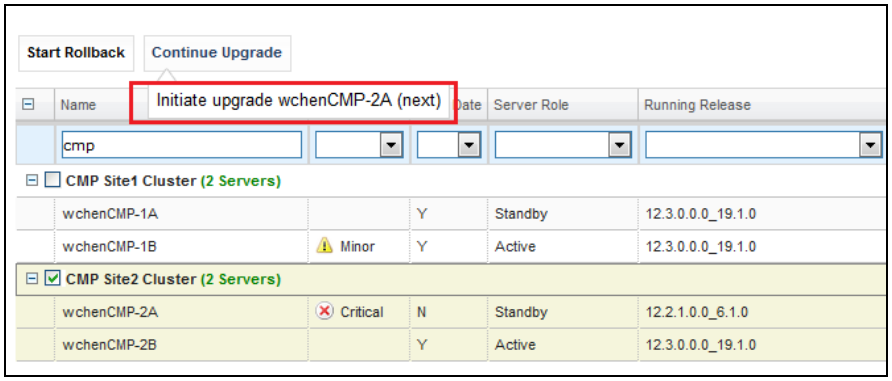
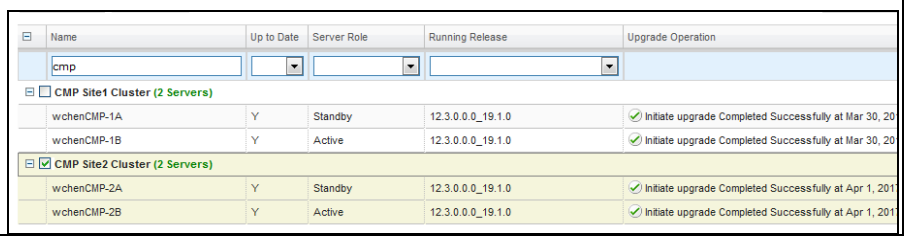
• Successful upgrade status shows both servers running the Release 12.3 in the Running Release column and Y for both servers in the Up To Date column
• Active/standby state for both servers in the Primary CMP Cluster.</td></tr>
<tr><td>19. ☐</td><td>Proceed to next upgrade procedure</td><td>At this point:

• The primary site is running Release 12.3
• The Secondary site, if it exists, is still on release 12.2.x
• Proceed to the next procedure to upgrade the secondary CMP cluster.</td></tr>
<tr><td colspan="3">---End of Procedure---</td></tr>
</table>

6.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Status of CMP Cluster	**Upgrade → Upgrade Manager** • Primary CMP is completely upgraded to 12.3 • Secondary CMP Cluster is on 12.2.x 
2. ☐	**CMP GUI**: Upgrade Secondary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Click **Filter** and enter `CMP` in the **Name** field.  3. Select the Secondary CMP Cluster at Site2 4. Click **Continue Upgrade**.  5. Click **OK** to confirm and continue with the operation. 6. This continues to upgrade the standby server only in the CMP Cluster 7. **NOTE:** This takes approximately 30 minutes to complete. 8. The Upgrade Operation column displays the In Progress status along with the upgrade activities.  During the Upgrade activities, the following alarms may be generated and are considered normal reporting events. 9.

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

Step	Procedure	Result
		the message displays the next action, which is upgrading the remaining CMP in standby, still running 12.2.x.  6. Click **OK** to confirm and continue with the operation, During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical alarm** **31283** Lost Communication with server **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault
1. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	**Upgrade → Upgrade Manager** • Successful upgrade status shows the Release 12.3 in the Running Release column. • The Upgrade Operation column shows Inititiate Upgrade Completed Successfully at… 

Step	Procedure	Result
4. ☐	**CMP GUI:** Verify Alarms	Navigate to **System Wide Reports → Alarms → Active Alarms**. **Expected Minor Alarms** **70500** System Mixed Version
5. ☐	Procedure is complete.	• All CMP Clusters Upgrade are complete and running Release 12.3. • ALL MRAs and MPEs are on Release 12.2.x At this point, the Policy Management system is running in mixed-version mode.
---End of Procedure---		

7. UPGRADE NON-CMP CLUSTERS 12.1.X/12.2.X TO 12.3

Use the following procedures to upgrade a site/segment containing one or more non-CMP clusters such as MPEs, MRAs.

NOTES: Different types of non-CMP clusters can be upgraded at the same time. 2 MPEs and 2 MRAs, for example, can be upgraded in parallel.

7.1 Site/Segment Upgrade Preparation

7.1.1 Configuration Preparation

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

7.2 Upgrade Non-CMP Clusters

Use this procedure to upgrade one or more non-CMP clusters at a site/segment.

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

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

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

1. Upgrade MPEs
2. Upgrade MRAs
3. Upgrade Mediation Servers

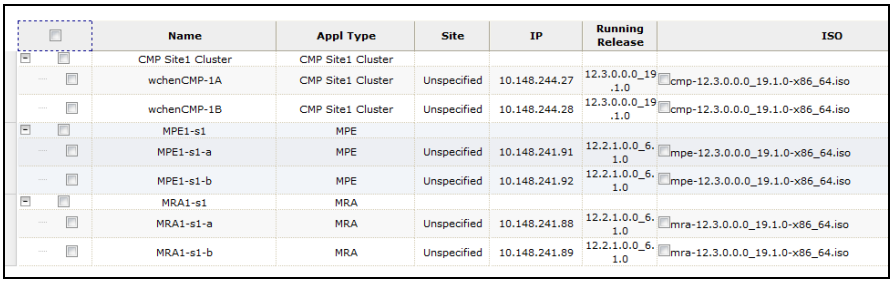
The upgrade procedure is essentially the same for any non-CMP cluster.

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

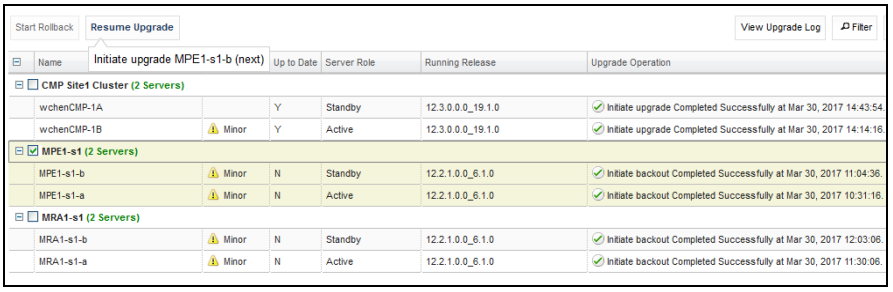
NOTES:

- All CMP clusters must have been upgraded to Policy Management release 12.3 before performing the following procedures.
- The maximum clusters to be running the upgrade at one time is 8, except for release 12.3.x where 16 clusters can be upgraded in parallel.

Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the servers to be upgraded	1. Check for current active alarms - For the MPE: **Policy Server→Configuration→Reports → Reset Counters** - For the MRA: **MRA→Configuration→Reports → Reset Counters** 2. Check KPI Dashboard (capture and save screenshot to a file)

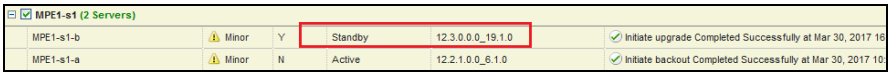
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>2. ☐</td><td>CMP GUI: Verify upgrade status of selected MPE/MRA site/segment</td><td>1. Navigate to Upgrade → Upgrade Manager.
2. Verify information for the MRAs/MPEs/Mediations:
- Current Release 12.1.x or 12.2.x installed
- Running with Active/Standby status
3. Navigate to Upgrade → ISO Maintenance.
4. Verify the ISO version to be deployed is 12.3
 
<table>
<tr><th></th><th>Name</th><th>Appl Type</th><th>Site</th><th>IP</th><th>Running Release</th><th>ISO</th></tr>
<tr><td></td><td>CMP Site1 Cluster</td><td>CMP Site1 Cluster</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>wchenCMP-1A</td><td>CMP Site1 Cluster</td><td>Unspecified</td><td>10.148.244.27</td><td>12.3.0.0.0_19.1.0</td><td>cmp-12.3.0.0.0_19.1.0-x86_64.iso</td></tr>
<tr><td></td><td>wchenCMP-1B</td><td>CMP Site1 Cluster</td><td>Unspecified</td><td>10.148.244.28</td><td>12.3.0.0.0_19.1.0</td><td>cmp-12.3.0.0.0_19.1.0-x86_64.iso</td></tr>
<tr><td></td><td>MPE1-s1</td><td>MPE</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>MPE1-s1-a</td><td>MPE</td><td>Unspecified</td><td>10.148.241.91</td><td>12.2.1.0.0_6.1.0</td><td>mpe-12.3.0.0.0_19.1.0-x86_64.iso</td></tr>
<tr><td></td><td>MPE1-s1-b</td><td>MPE</td><td>Unspecified</td><td>10.148.241.92</td><td>12.2.1.0.0_6.1.0</td><td>mpe-12.3.0.0.0_19.1.0-x86_64.iso</td></tr>
<tr><td></td><td>MRA1-s1</td><td>MRA</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>MRA1-s1-a</td><td>MRA</td><td>Unspecified</td><td>10.148.241.88</td><td>12.2.1.0.0_6.1.0</td><td>mra-12.3.0.0.0_19.1.0-x86_64.iso</td></tr>
<tr><td></td><td>MRA1-s1-b</td><td>MRA</td><td>Unspecified</td><td>10.148.241.89</td><td>12.2.1.0.0_6.1.0</td><td>mra-12.3.0.0.0_19.1.0-x86_64.iso</td></tr>
</table></td></tr>
<tr><td>3. ☐</td><td>CMP GUI: Upgrade clusters

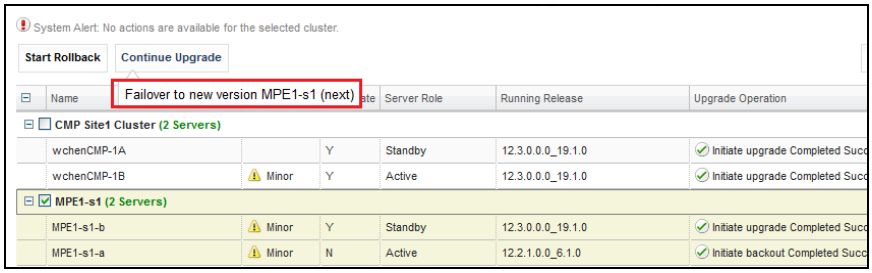
NOTE: The upgrade of one server takes approximately 35 minutes to complete.</td><td>Start the upgrade on ONE cluster. Wait until the cluster shows OOS state, then continue with the next cluster and so on. Up to 4 clusters (8 for 12.1.x) may be running upgrade at any one time.

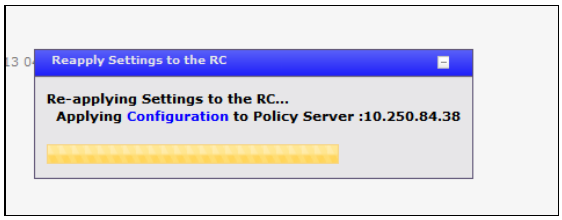
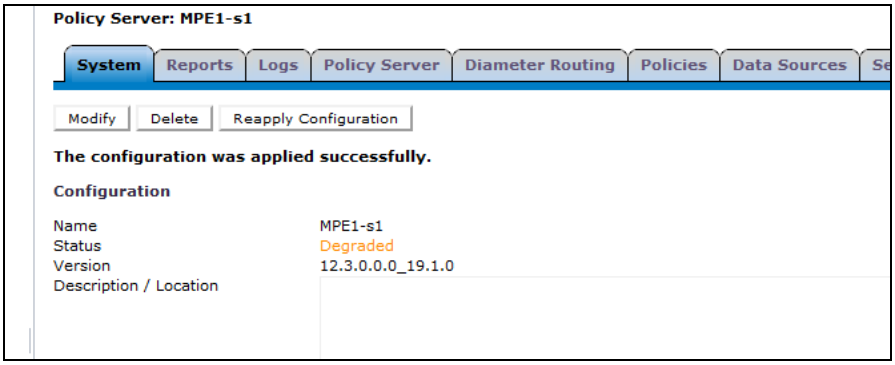
Upgrade → Upgrade Manager
1. Click the checkbox for the desired cluster (one cluster at a time.) It can be an MRA or an MPE.
2. Click Continue Upgrade or Resume Upgrade
 
<table>
<tr><td>Start Rollback</td><td>Resume Upgrade</td><td colspan="2">Initiate upgrade MPE1-s1-b (next)</td><td></td><td></td><td>View Upgrade Log</td><td>Filter</td></tr>
<tr><td>Name</td><td></td><td>Up to Date</td><td>Server Role</td><td>Running Release</td><td>Upgrade Operation</td></tr>
<tr><td colspan="6">CMP Site1 Cluster (2 Servers)</td></tr>
<tr><td>wchenCMP-1A</td><td></td><td>Y</td><td>Standby</td><td>12.3.0.0.0_19.1.0</td><td>Initiate upgrade Completed Successfully at Mar 30, 2017 14:43:54.</td></tr>
<tr><td>wchenCMP-1B</td><td>Minor</td><td>Y</td><td>Active</td><td>12.3.0.0.0_19.1.0</td><td>Initiate upgrade Completed Successfully at Mar 30, 2017 14:14:16.</td></tr>
<tr><td colspan="6">MPE1-s1 (2 Servers)</td></tr>
<tr><td>MPE1-s1-b</td><td>Minor</td><td>N</td><td>Standby</td><td>12.2.1.0.0_6.1.0</td><td>Initiate backout Completed Successfully at Mar 30, 2017 11:04:36.</td></tr>
<tr><td>MPE1-s1-a</td><td>Minor</td><td>N</td><td>Active</td><td>12.2.1.0.0_6.1.0</td><td>Initiate backout Completed Successfully at Mar 30, 2017 10:31:16.</td></tr>
<tr><td colspan="6">MRA1-s1 (2 Servers)</td></tr>
<tr><td>MRA1-s1-b</td><td>Minor</td><td>N</td><td>Standby</td><td>12.2.1.0.0_6.1.0</td><td>Initiate backout Completed Successfully at Mar 30, 2017 12:03:06.</td></tr>
<tr><td>MRA1-s1-a</td><td>Minor</td><td>N</td><td>Active</td><td>12.2.1.0.0_6.1.0</td><td>Initiate backout Completed Successfully at Mar 30, 2017 11:30:06.</td></tr>
</table>
3. Click OK to confirm and continue with the operation. It begins the upgrade of the standby server for that cluster.
4. Wait until the standby server reports OOS before selecting the next cluster
5. Follow the progress status in the Upgrade Operation column.
6. During the upgrade activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the clusters are completely upgraded.

<u>Expected Critical Alarms</u>

31283 High availability server is offline
70001 QP_procmgr failed
31227 High availability status failed</td></tr>
</table>

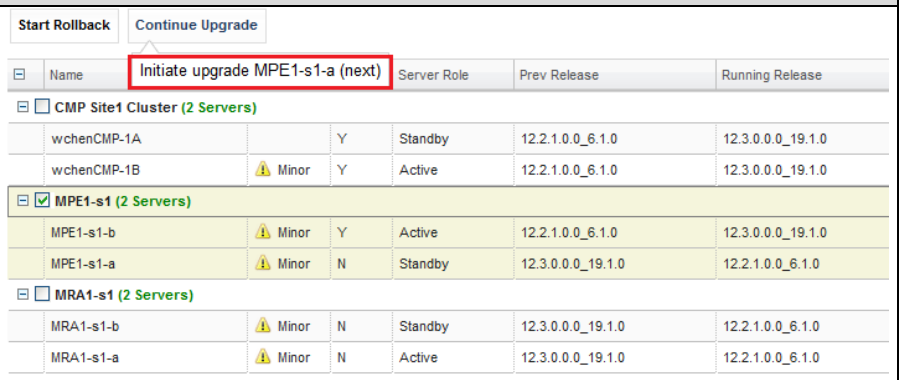
Step	Procedure	Result
		Expected Major Alarm: **70004** QP Processes down for maintenance **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31102** DB replication from a master DB has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault **78001** RSYNC Failed Upgrade is complete on the first server of the cluster when the Initiate upgrade completed successfully at… message displays in the Upgrade Operation column. The server goes back to standby state when the upgrade completes.  A number of different alarms may be raised at this point: **Expected Minor Alarms** **78001** RSYNC Failed **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **70503** The server is in forced standby

Step	Procedure	Result
4. ☐	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Next operation is a failover. **NOTE:** 8 clusters can be running the upgrade process at one time.	Failover ONE cluster at a time. Wait for a minute, before moving on to the next cluster. **Upgrade → Upgrade Manager** 1. Select the cluster (one cluster at a time). It can be an MRA or MPE. 2. Click **Continue Upgrade**. When hovering over the **Continue Upgrade** button, it displays the Failover to new version message.  3. Click **OK** to confirm and continue with the operation. It begins to failover the cluster. 4. Wait until failover completes, that is, the server running 12.3 becomes the active server before failing over the next cluster. 

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

Step	Procedure	Result
6. ☐	**CMP GUI:** Current alarms	Some of the alarms below may appear: **<u>Expected Critical alarm</u>** None **<u>Expected Major Alarm</u>** **78001** Rsync Failed **<u>Expected Minor Alarms</u>** **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **70503** The server is in forced standby **71402** Diameter Connectivity Lost **31101** DB Replication To Slave Failure **31113** DB Replication Manually Disabled
7. ☐	**CMP GUI:** Verify traffic becomes active within 90 seconds	**Upgrade Manager → System Maintenance** • If traffic is active, go to step 9. • If traffic does not become active within 90 seconds: 1. Select the checkbox for the partially upgraded cluster, and select **Operations → Rollback**. 2. The pre-12.3 MPE server should become active and resume handling traffic.
8. ☐	**CMP GUI:** Reapply configuration	1. **Policy Server → Configuration →** *<mpe_cluster name>* **→ System** or **MRA → Configuration →** *<mra_cluster name>* **→ System** 2. Click **Reapply Configuration** • Verify that the version is changed back to 12.1.x or 12.2.x, and the action report success. • If NOT, stop and contact Oracle support to back out of the partially upgraded cluster.
9. ☐	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Upgrade on the Standby server	Continue the upgrade on ONE cluster at a time and when the server goes into OOS, continue with the next cluster and so on. Up to 4 clusters (8 for 12.1.x) may be running upgrade at one time. 1. Naviaget to **Upgrade → Upgrade Manager**. 2. Select a cluster (one cluster at a time), it can be an MRA or an MPE. 3. Click **Continue Upgrade**. When hovering over the **Continue Upgrade** button, it displays the Initiate upgrade… on the standby server message.

Step	Procedure	Result



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

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

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

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

Expected Critical Alarms

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

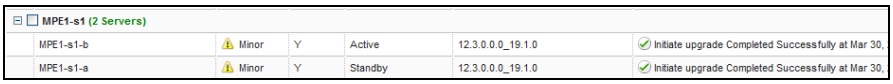
Expected Major Alarm

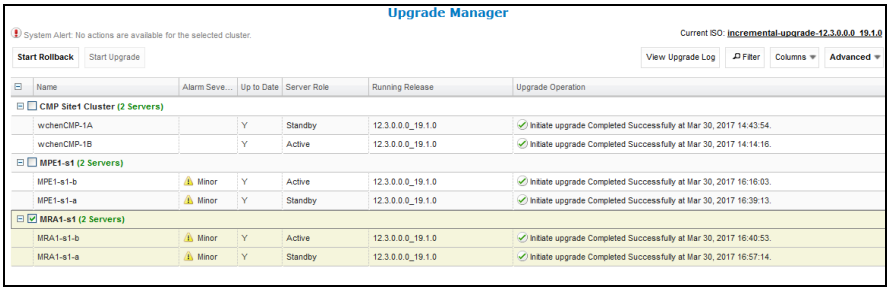
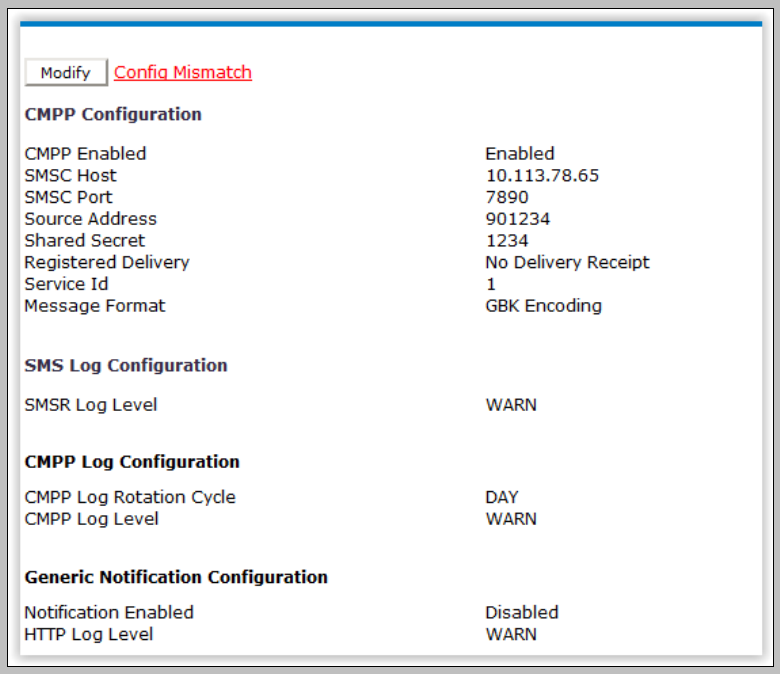
70004 QP Processes down for maintenance

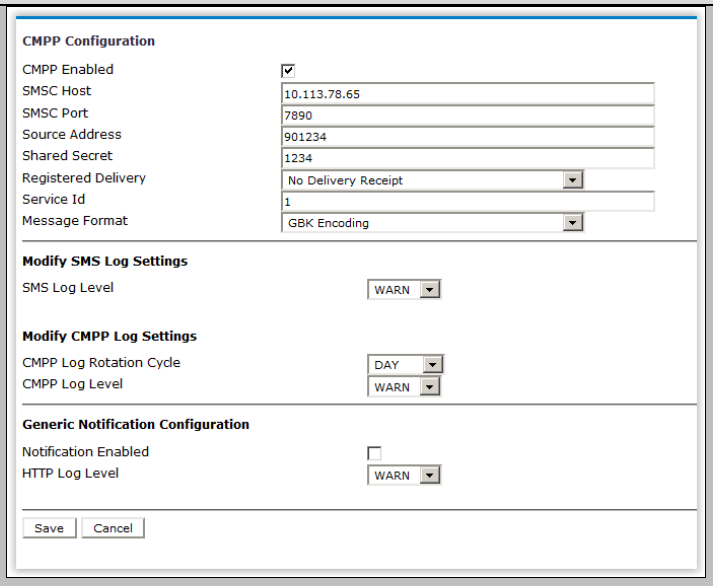
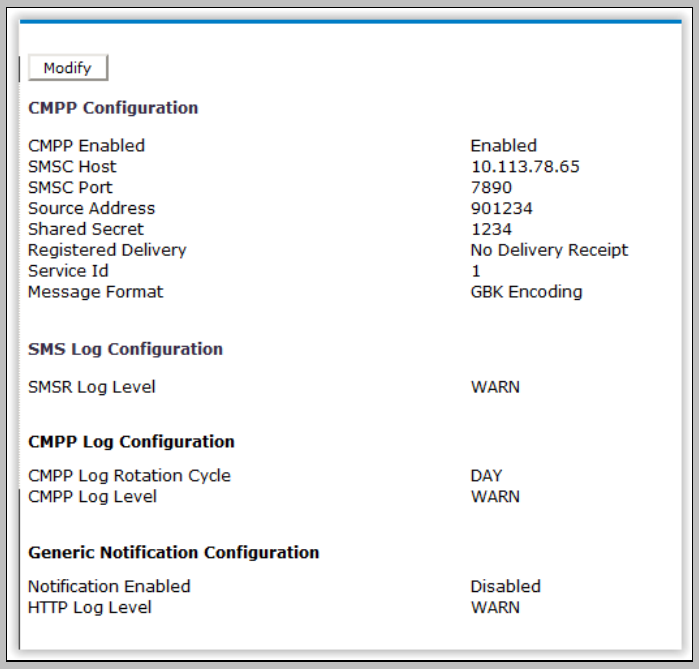
Expected Minor Alarms

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

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

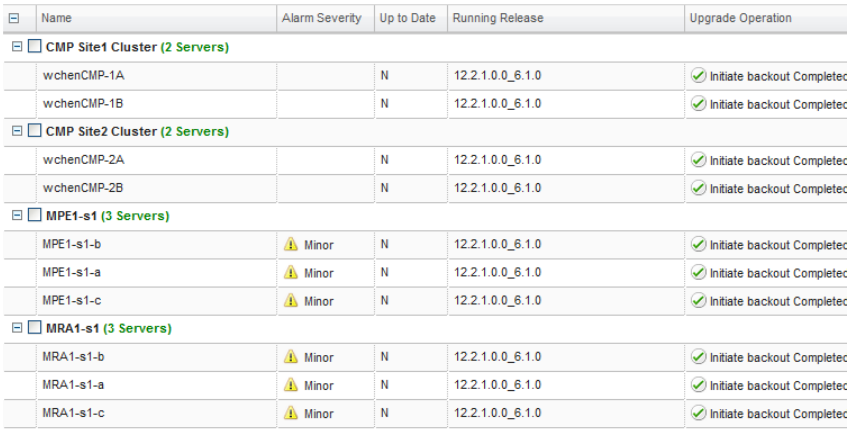
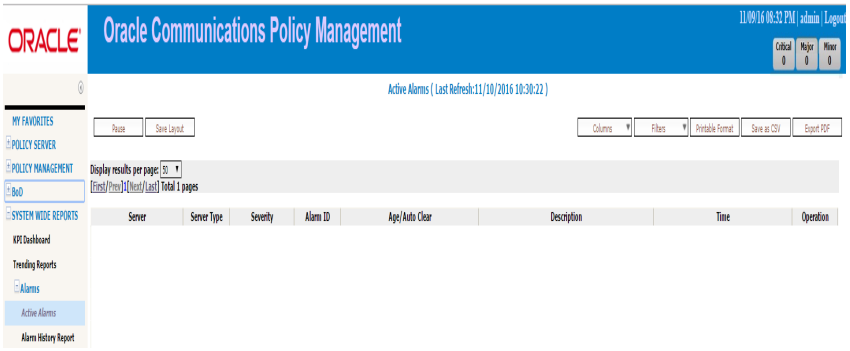
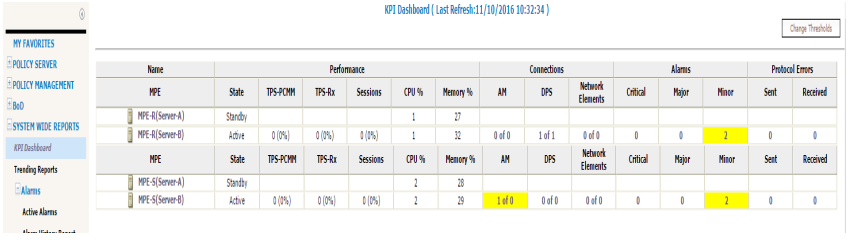


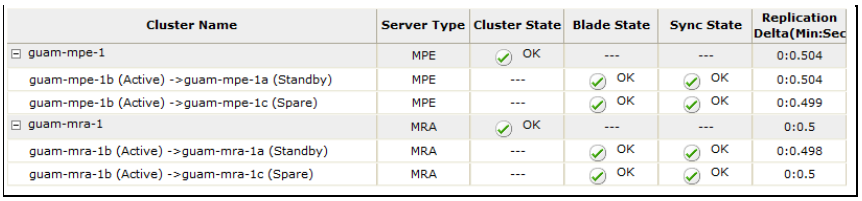
Step	Procedure	Result
10. ☐	REPEAT steps 1 through 10 for next MPE/MRA cluster(s)	Proceed with the next clusters until all clusters have been upgraded 
11. ☐	**CMP GUI:** Modify/save SMSR configuration	**System Administration → SMS Relay → Modify** **NOTE:** This step is only for Wireless-C system. If you cannot find sms relay under system administration, just skip this step. Initial access into this configuration upon upgrade to release 12.3, the configuration shows as such with Config Mismatch.  1. Click **Modify.** The following is an example of the SMSR configuration. DO NOT change any of the configuration if it has been working in the past.

Step	Procedure	Result
		 2. Click **Save** to save the configuration and continue as shown.  **NOTE:** The Config Mismatch message is not there with the saved configuration.
---End of Procedure---		

8. POST UPGRADE HEALTH CHECK FOR WIRELESS SYSTEMS

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

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

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>4. ☐</td><td>CMP GUI: Replication stats</td><td>1. Navigate to System Wide Reports→Others→MPE/MRA Rep Stats (for a wireless system)
2. Verify all clusters and servers are in OK state.
 
<table>
<tr><th>Cluster Name</th><th>Server Type</th><th>Cluster State</th><th>Blade State</th><th>Sync State</th><th>Replication Delta(Min:Sec</th></tr>
<tr><td>⊟ guam-mpe-1</td><td>MPE</td><td>OK</td><td>---</td><td>---</td><td>0:0.504</td></tr>
<tr><td>guam-mpe-1b (Active) ->guam-mpe-1a (Standby)</td><td>MPE</td><td>---</td><td>OK</td><td>OK</td><td>0:0.504</td></tr>
<tr><td>guam-mpe-1b (Active) ->guam-mpe-1c (Spare)</td><td>MPE</td><td>---</td><td>OK</td><td>OK</td><td>0:0.499</td></tr>
<tr><td>⊟ guam-mra-1</td><td>MRA</td><td>OK</td><td>---</td><td>---</td><td>0:0.5</td></tr>
<tr><td>guam-mra-1b (Active) ->guam-mra-1a (Standby)</td><td>MRA</td><td>---</td><td>OK</td><td>OK</td><td>0:0.498</td></tr>
<tr><td>guam-mra-1b (Active) ->guam-mra-1c (Spare)</td><td>MRA</td><td>---</td><td>OK</td><td>OK</td><td>0:0.5</td></tr>
</table></td></tr>
<tr><td>5. ☐</td><td>Verify System Health</td><td>1. Use the <code>sudo syscheck</code> command on every server.
2. Verify that each class test returns OK. For example:
<code>$ sudo syscheck</code>
<code>Running modules in class disk... OK</code>
<code>Running modules in class hardware... OK</code>
<code>Running modules in class net... OK</code>
<code>Running modules in class proc... OK</code>
<code>Running modules in class system...OK</code>
LOG LOCATION: /var/TKLC/log/syscheck/fail_log</td></tr>
<tr><td colspan="3">---End of Procedure---</td></tr>
</table>

9. BACKOUT (ROLLBACK) 12.1.X WIRELESS OR 12.2.X

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

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

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

9.1 Backout Sequence

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

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

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

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

9.1.1 Pre-requisites

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

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

9.1.2 Backout of Fully Upgraded Cluster

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

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

Expected pre-conditions:

- The primary active CMP is on release 12.3
- The cluster servers to be backed out are on release 12.1/12.2

9.1.3 Backout Sequence

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

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

9.1.3.1 Overview on Backout/Rollback MRA/MPE cluster

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

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

9.1.3.2 Backout Secondary CMP (if applicable)

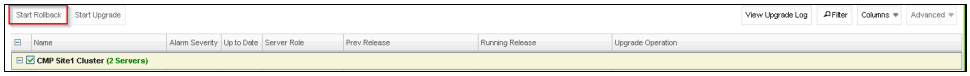
NOTE: At this time, all MPEs and MRAs must be backed out to the previous release.

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

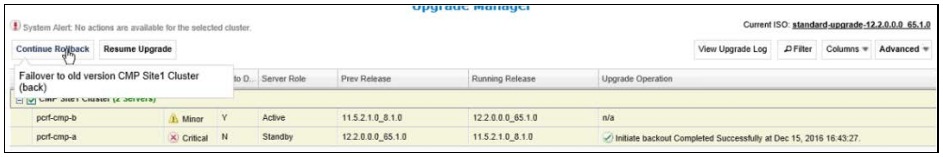
9.1.3.3 Backout Primary CMP (12.2.x)

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

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



3. Click **Continue Rollback**, which fails over to older version CMP cluster.



4. Log in to the Primary CMP VIP
5. Use the 12.1.x/12.2.x System Maintenance to complete backout of the Primary CMP cluster

	Name	Appl Type	Site	IP	Running Release	ISO
	CMP Site1 Cluster	CMP Site1 Cluster				
	wchenCMP-1A	CMP Site1 Cluster	Unspecified	10.148.244.27	12.2.1.0.0_6.1.0	cmp-12.3.0.0.0_23.1.0-x86_64.iso
	wchenCMP-1B	CMP Site1 Cluster	Unspecified	10.148.244.28	12.2.1.0.0_6.1.0	cmp-12.3.0.0.0_23.1.0-x86_64.iso

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

9.1.3.4 Backout Primary CMP (12.3.x)

Use the CMP GUI (Upgrade Manager) to backout the CMP cluster (the scenario is the same as previous section).

9.1.4 Back-out Partially Upgraded MPE/MRA Cluster

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

Expected Pre-conditions:

1. Primary Active CMP is on Release 12.3.x
2. Cluster is any of MPE or MRA
3. One server of target cluster is on Release 12.3.x
4. Other servers of target cluster are on Release 12.2.x or 12.1.x

NOTES:

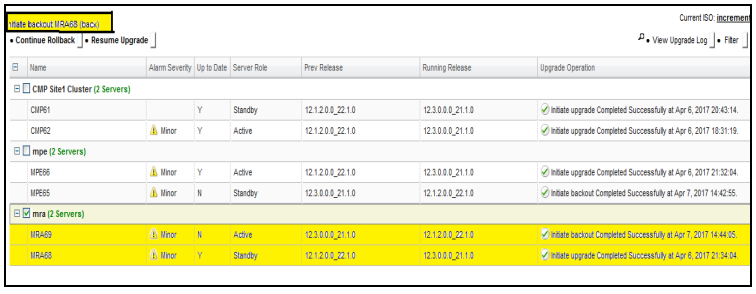
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 45 minutes at most per server.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

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

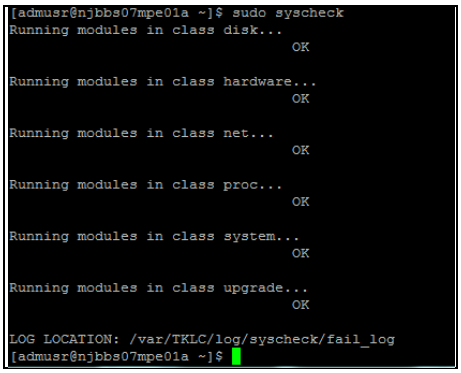
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected Clusters	1. Navigate to **Upgrade → Upgrade Manager** 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 12.3.x - Target Cluster has 1 server on Release 12.1.x, and 1 server on Release 12.3.x - Active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

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

3. ☐	**CMP GUI:** Verify the status of affected Clusters **NOTE:** This takes approximately30 minutes to complete.	1. Select **Start Rollback** or **Continue Rollback**. When hovering over the button, it indicates the server to get backed out.  2. Click **OK** to confirm and continue with the operation. It begins to back-out. 3. Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is

Step	Procedure	Result
		completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message **31284** High availability remote subscriber has not received a heartbeat **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the successful completion message (Initiate Back-out Completed Successfully) 

Step	Procedure	Result

4. ☐	**MPE/MRA SSH:** Verify syscheck and `/tmp` directory permission	1. Login to the back-out server and verify that there are no failures in syscheck:
		`$ sudo syscheck`
		 
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		3. If the permissions are not as listed above then perform the following; otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		4. Verify:
		`$ ls -l /`
		5. Perform syscheck again:
		`$ sudo syscheck`

Step	Procedure	Result

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

---End of Procedure---		

9.1.5 Back-out Fully Upgraded MPE/MRA Cluster

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

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

At the end of this procedure, all servers of the target cluster are on Release 12.1.x (MRA, MPE, CMP) with Active, Standby status.

Expected pre-conditions:

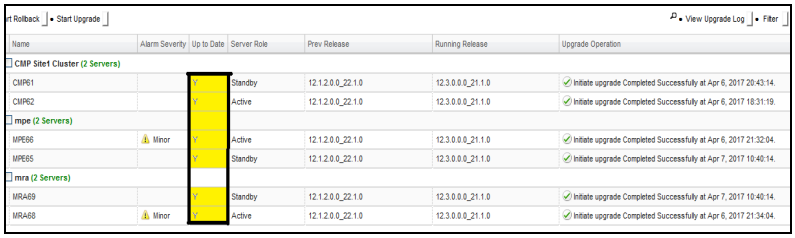
1. Primary Active CMP is on Release 12.3.x.
2. Cluster is of MPE or MRA.
3. Servers of target cluster are on Release 12.3.x in either in Active, Standby or Force Standby role.

NOTES:

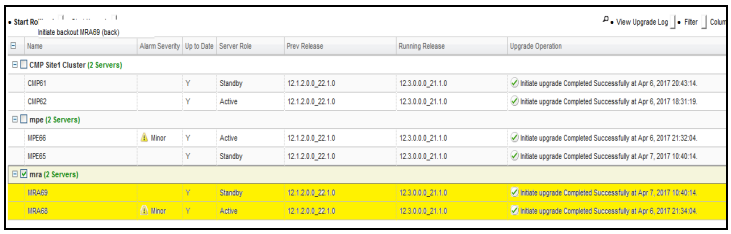
- This procedure must be performed within a maintenance window.
- This takes approximately 105 minutes per MPE or MRA cluster.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

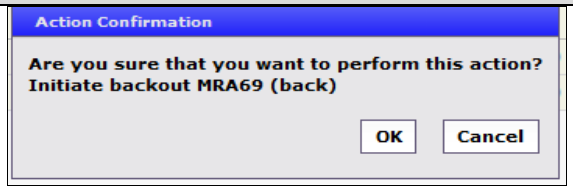
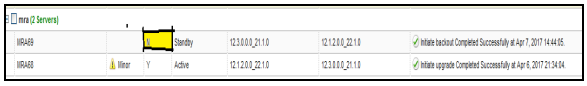
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

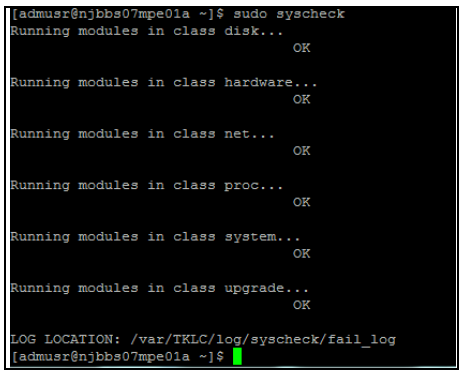
Procedure 5: Back-out Fully Upgraded MPE/MRA Cluster

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

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

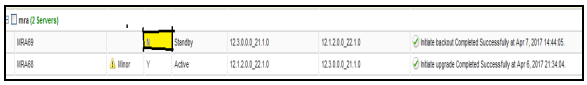
3. ☐	**CMP GUI:** Initiate Back-out **NOTES:** Each back-out of one blade server completes in approximately 30 minutes. Up to 8 clusters can be backed out at the same time, selecting one at a time.	1. Navigate to **Upgrade → Upgrade Manager** 2. Select the cluster (one cluster at a time) (can be an MRA or MPE) 3. Click **Start Rollback**. When hovering over the button, it indicates the server to be backed out. In this case it is the current standby server.  4. Click **OK** to confirm and continue with the operation. It begins to back-out.

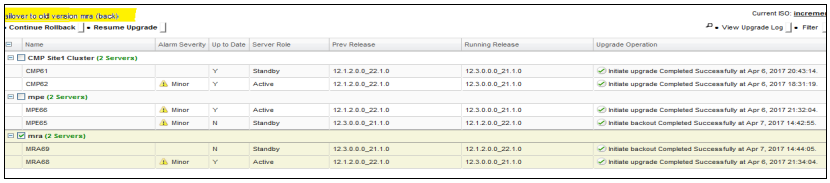
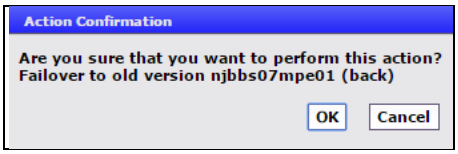
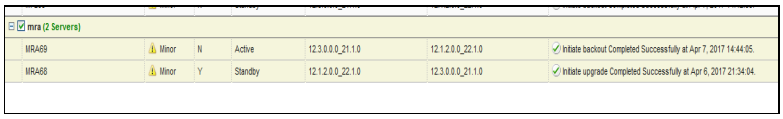
Step	Procedure	Result
		 5. Follow the progress status in the Upgrade Operation column. At this point, the server backing out goes into OOS state 6. Wait until the server goes to an OOS state before selecting the next cluster to back-out. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message …. **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the successful completion displays in the Upgrade Operation column. The server shows running release of 12.1.x and 12.2.x and return to standby with an N in the Up To Date Column. 

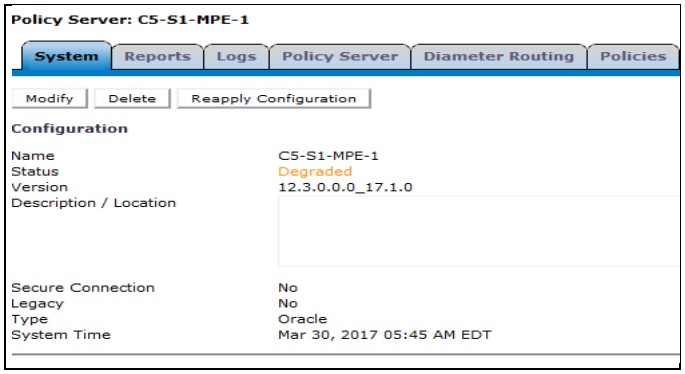
Step	Procedure	Result
4. ☐	**CMP GUI** Verify the back-out is successful	1. Select the partially Backed out cluster 2. Select the View Upgrade LOG  3. Check upgrade logs for the remainder of partially Backed out clusters.
5. ☐	**MPE/MRA SSH** Verify **`syscheck`** and `/tmp` directory permission	1. Log into the backed-out standby server and verify that there are no failures in syscheck: **`$ sudo syscheck`**  2. Verify the `/tmp` directory permissions: **`$ ls -l /`** **NOTE:** Permissions should be: **`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`** 3. If the permissions are not as listed above then perform the following otherwise skip to next step: **`$ sudo chmod 777 /tmp`** **`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`** **`$ sudo chmod +t /tmp`** 4. Verify: **`$ ls -l /`** 5. Perform syscheck again: **`$ sudo syscheck`**

Step	Procedure	Result

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

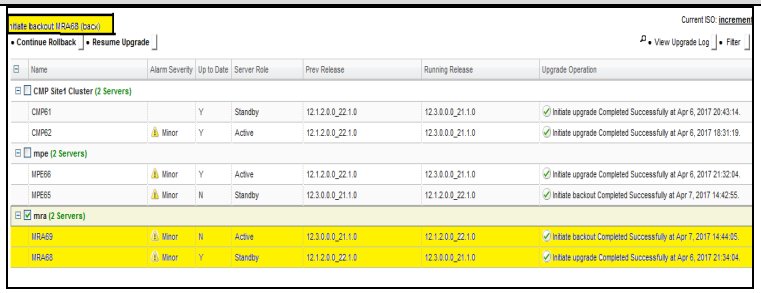
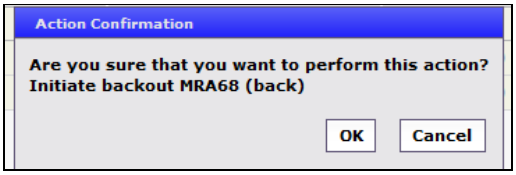
7. ☐	Confirm MPE/MRA server status	Ensure that the Active are on 12.3.x and the standby server shows running release of 12.1.x or 12.2.x 

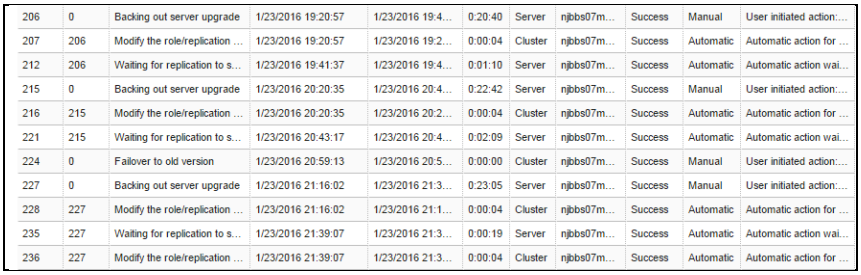
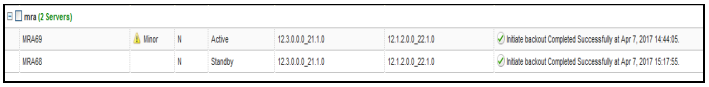
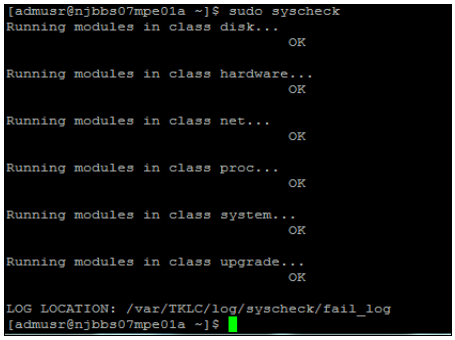
Step	Procedure	Result
8. ☐	**CMP GUI**: Continue the back-out of the MRA/MPE clusters. Next operation is failover to the 12.1.x server. **NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time.	Current state of the cluster must be as follows. • Active Server is on Release 12.3.x • Standby Server is on Previous release 1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click Continue Rollback. When hovering over the button, it informs you to failover to old version, which is 12.1.x  3. Click **OK** to confirm and continue with the operation. It begins to failover.  Wait until the server fails over before selecting the next cluster. This takes approximately 2 minutes **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **Expected Major Alarms** **74603** The number of failed MPE primary cluster reaches the threshold **Expected Minor Alarms** **70503** The server is in forced standby **31102** DB replication from a master DB has failed **71402** Diameter Connectivity Lost **31101** DB replication to a slave DB has failed **78001** Transfer of Policy jar files failed State of the cluster looks like the following when the failover completes. 

Step	Procedure	Result
9. ☐	**CMP GUI:** Reapply Configuration on MPE/MRA cluster that competed the failover successfully	• For MPE: Navigate to **Policy Server → Configuration →** <*MPE*> **→ System** • For MRA: Navigate to **MRA → Configuration →** <*MRA*> **→ System** The selected cluster status is Degraded as expected as shown:  Click **Reapply Configuration** operation. • The Version is successfully changed to the upgraded Release 12.1.x • The status is Degraded which is a normal reporting event as the servers are in different status. **MPE** 

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

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

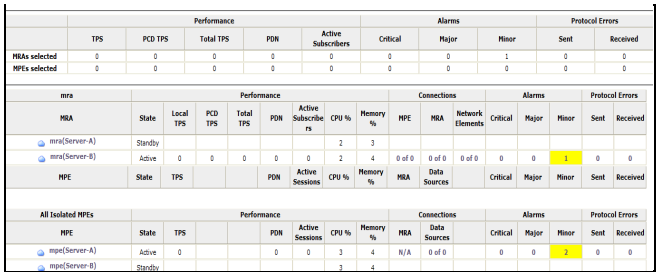
Step	Procedure	Result
	selecting one at a time. **NOTE:** Each back-out of one blade server completes in approximately 30 minutes	 3. Click **OK** to confirm and continue with the operation. It begins to back-out.  Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message **31284** High availability remote subscriber has not received a heartbeat **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault 4. Back-out of the server is complete when the successful completion message (initiate Back-out completed successfully) displays in the Upgrade Operation column.

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td>5. Verify in Upgrade Log that that back-out was successful:
 
<table>
<tr><td>206</td><td>0</td><td>Backing out server upgrade</td><td>1/23/2016 19:20:57</td><td>1/23/2016 19:4...</td><td>0:20:40</td><td>Server</td><td>njbbs07m...</td><td>Success</td><td>Manual</td><td>User initiated action:...</td></tr>
<tr><td>207</td><td>206</td><td>Modify the role/replication ...</td><td>1/23/2016 19:20:57</td><td>1/23/2016 19:2...</td><td>0:00:04</td><td>Cluster</td><td>njbbs07m...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
<tr><td>212</td><td>206</td><td>Waiting for replication to s...</td><td>1/23/2016 19:41:37</td><td>1/23/2016 19:4...</td><td>0:01:10</td><td>Server</td><td>njbbs07m...</td><td>Success</td><td>Automatic</td><td>Automatic action wai...</td></tr>
<tr><td>215</td><td>0</td><td>Backing out server upgrade</td><td>1/23/2016 20:20:35</td><td>1/23/2016 20:4...</td><td>0:22:42</td><td>Server</td><td>njbbs07m...</td><td>Success</td><td>Manual</td><td>User initiated action:...</td></tr>
<tr><td>216</td><td>215</td><td>Modify the role/replication ...</td><td>1/23/2016 20:20:35</td><td>1/23/2016 20:2...</td><td>0:00:04</td><td>Cluster</td><td>njbbs07m...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
<tr><td>221</td><td>215</td><td>Waiting for replication to s...</td><td>1/23/2016 20:43:17</td><td>1/23/2016 20:4...</td><td>0:02:09</td><td>Server</td><td>njbbs07m...</td><td>Success</td><td>Automatic</td><td>Automatic action wai...</td></tr>
<tr><td>224</td><td>0</td><td>Failover to old version</td><td>1/23/2016 20:59:13</td><td>1/23/2016 20:5...</td><td>0:00:00</td><td>Cluster</td><td>njbbs07m...</td><td>Success</td><td>Manual</td><td>User initiated action:...</td></tr>
<tr><td>227</td><td>0</td><td>Backing out server upgrade</td><td>1/23/2016 21:16:02</td><td>1/23/2016 21:3...</td><td>0:23:05</td><td>Server</td><td>njbbs07m...</td><td>Success</td><td>Manual</td><td>User initiated action:...</td></tr>
<tr><td>228</td><td>227</td><td>Modify the role/replication ...</td><td>1/23/2016 21:16:02</td><td>1/23/2016 21:1...</td><td>0:00:04</td><td>Cluster</td><td>njbbs07m...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
<tr><td>235</td><td>227</td><td>Waiting for replication to s...</td><td>1/23/2016 21:39:07</td><td>1/23/2016 21:3...</td><td>0:00:19</td><td>Server</td><td>njbbs07m...</td><td>Success</td><td>Automatic</td><td>Automatic action wai...</td></tr>
<tr><td>236</td><td>227</td><td>Modify the role/replication ...</td><td>1/23/2016 21:39:07</td><td>1/23/2016 21:3...</td><td>0:00:04</td><td>Cluster</td><td>njbbs07m...</td><td>Success</td><td>Automatic</td><td>Automatic action for ...</td></tr>
</table>
6. All of the servers are on Release 12.1.x at this point and show active/standby
 
<table>
<tr><td>mra (2 Servers)</td></tr>
<tr><td>MRA69</td><td>Minor</td><td>N</td><td>Active</td><td>12.3.0.0.0_21.1.0</td><td>12.1.2.0.0_22.1.0</td><td>Initiate backout Completed Successfully at Apr 7, 2017 14:44:05.</td></tr>
<tr><td>MRA68</td><td></td><td>N</td><td>Standby</td><td>12.3.0.0.0_21.1.0</td><td>12.1.2.0.0_22.1.0</td><td>Initiate backout Completed Successfully at Apr 7, 2017 15:17:55.</td></tr>
</table></td></tr>
<tr><td>12. ☐</td><td>MPE/MRA SSH:
Verify syscheck and /tmp directory permission</td><td>1. Login to the backed-out standby server as admusr.
2. Verify that there are no failures in syscheck:
$ sudo syscheck
 

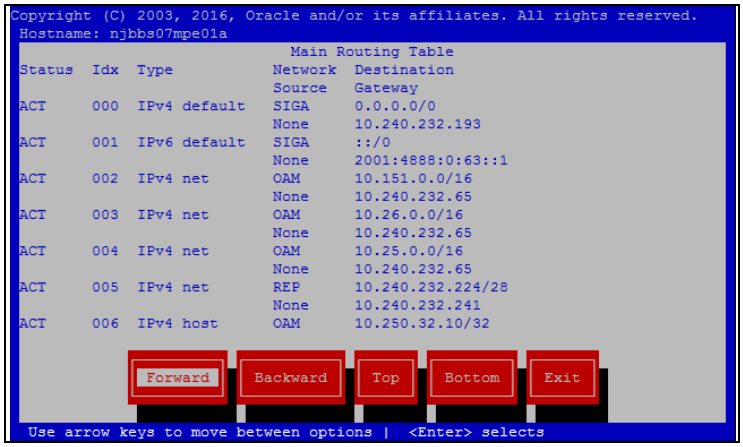
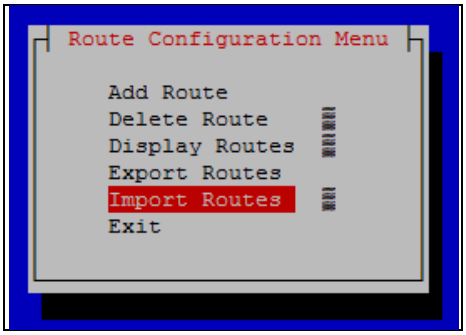
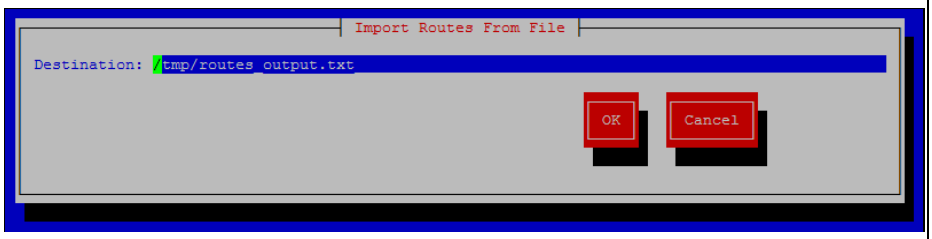
3. Verify /tmp directory permissions:
$ ls -l /
NOTE: Permissions should be the following,
drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp
4. If the permissions are not as listed above then perform the following otherwise skip to next step:
$ sudo chmod 777 /tmp
$ sudo chcon -h system_u:object_r:tmp_t:s0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

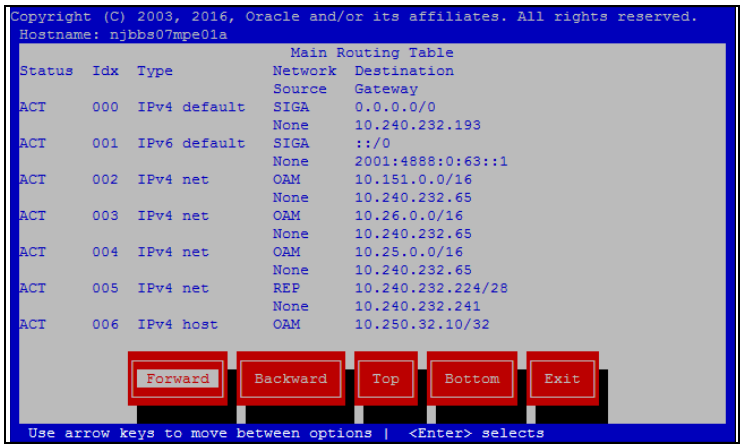
Step	Procedure	Result

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

14. ☐	**CMP GUI:** Verify that backed out cluster is processing traffic normally.	Verify Cluster is processing traffic normally. Navigate to **System Wide Reports → KPI Dashboard**. 
15. ☐	**CMP GUI:** Verify alarms	1. Navigate to System Wide Reports → Alarms → Active Alarms 2. Verify that there are no unexpected active alarms present. **NOTE:** Some alarms may take 30 minutes to 1 hour for auto clearing time.

16. ☐	**MPE/MRA SSH:** Verify routes	1. Login into MPE/MRA server as admusr.
		2. Copy routes_output.txt from the `/home/admusr` directoy to the `/tmp` directory.
		`$ sudo cp routes_output.txt /tmp`
		`$ cd /tmp`
		`$ ls`
		`routes_output.txt`
		WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance

Step	Procedure	Result
		Engineering. 3. Start the platcfg utility. `$ sudo su - platcfg` 4. Navigate to **Policy Configuration → Routing Config → Display Routes** 5. Click **Forward** to view all the routes. 6. Verify that all routes are present. **Example**  7. If any of the routes are missing then perform the following otherwise skip to step 20 8. Navigate back to Route Configuration Menu and select **Import Routes**.  9. Click **OK**.  Routes are imported from `/tmp/routes_output.txt` file and Route Configuration menu displays. 10. Select Display Routes 11. Verify that all routes are present.

Step	Procedure	Result
		12. Click **Forward** to view all the routes. **Example**  13. Exit platcfg utility **WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance Engineering.**
17. ☐	Repeat for other clusters as needed	Repeat this procedure for the remaining MPE/MRA servers.
18. ☐	Perform syscheck and verify that alarms are clear.	Another syscheck on all the back-out servers can be performed to ensure all modules are still operationally OK before progressing to the next Procedure. 1. Navigate to **System Wide Reports → Alarms → Active Alarms** 2. Verify that there are no unexpected active alarms present. **NOTE:** Some alarms may take 30 minutes to 1 hour for auto clearing time.
---End of Procedure---		

9.1.6 Back-out Fully Upgraded Secondary CMP Cluster

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

Expected Pre-conditions:

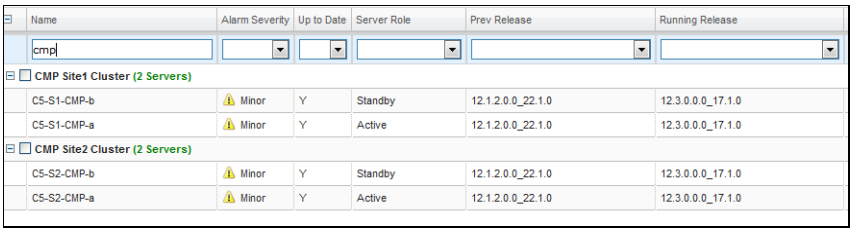
1. Primary Active CMP is on Release 12.3.x
2. Secondary CMP Cluster is on Release 12.3.x
3. All MPE/MRA/Mediation Clusters are on Release 12.1.x or 12.2.x

NOTES:

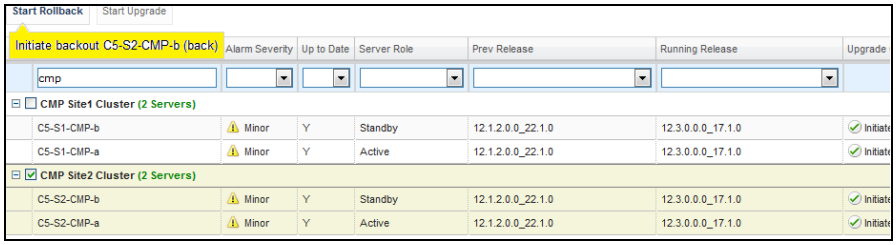
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

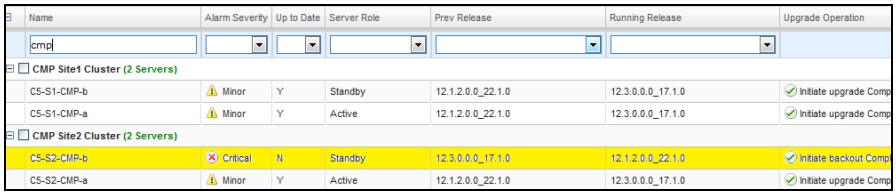
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 6: Back-out Fully Upgraded Secondary CMP Cluster

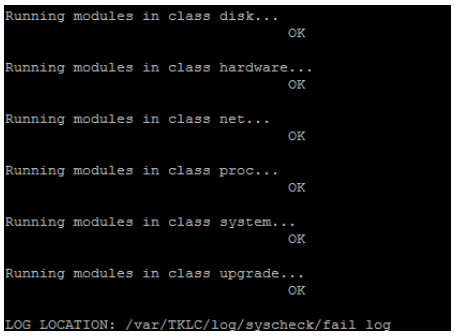
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of CMP Clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on release 12.3.x. - Secondary CMP Cluster is on release 12.3.x. - Up to Date Column shows Y for all servers.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

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

3. ☐	**CMP GUI:** Back-out clusters **NOTE:** Each back-out of one server takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager** 2. Select the Secondary CMP Cluster. 3. Click **Start Rollback**. When hovering over the button, it indicatess the back-out server.  4. Click **OK** to confirm and continue with the operation. It begins to back-out. The server goes into an OOS server role. 5. Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are

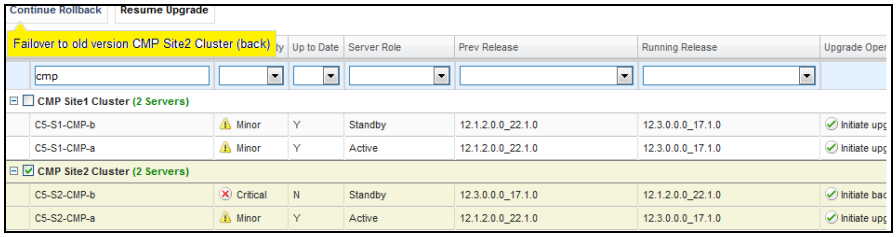
Step	Procedure	Result
		considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed Back-out of the server is complete when the successful completion message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server goes back to standby state and shows a running release of 12.1.x  Name / Alarm Severity / Up to Date / Server Role / Prev Release / Running Release / Upgrade Operation cmp CMP Site1 Cluster (2 Servers) C5-S1-CMP-b — Minor — Y — Standby — 12.1.2.0.0_22.1.0 — 12.3.0.0.0_17.1.0 — Initiate upgrade Comp C5-S1-CMP-a — Minor — Y — Active — 12.1.2.0.0_22.1.0 — 12.3.0.0.0_17.1.0 — Initiate upgrade Comp CMP Site2 Cluster (2 Servers) C5-S2-CMP-b — Critical — N — Standby — 12.3.0.0.0_17.1.0 — 12.1.2.0.0_22.1.0 — Initiate backout Comp C5-S2-CMP-a — Minor — Y — Active — 12.1.2.0.0_22.1.0 — 12.3.0.0.0_17.1.0 — Initiate upgrade Comp

Step	Procedure	Result

4. ☐	**CMP SSH:** Verify syscheck and `/tmp` directory permission	1. Login to the backed-out server and verify that there are no failures in syscheck:
		`$ sudo syscheck`
		 
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following:
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		3. If the permissions are not as listed above, perform the following, otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		4. Verify:
		`$ ls -l /`
		5. Perform syscheck again:
		`$ sudo syscheck`

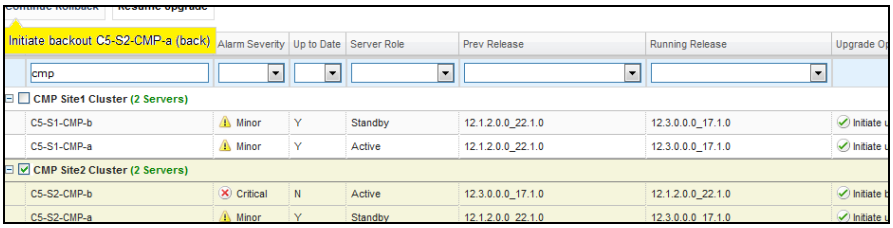
Step	Procedure	Result

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

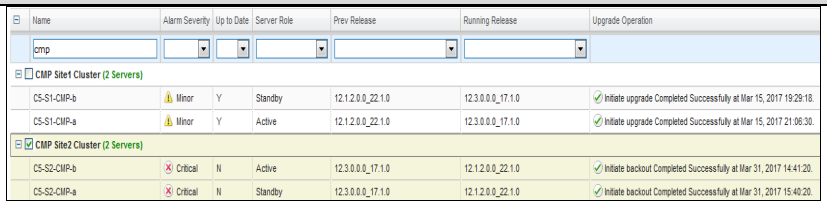
6. ☐	**CMP GUI**: Continue the back-out. Next operation is failover.	1. Select Secondary CMP Cluster. 2. Navigate to **Upgrade → Upgrade Manager** 3. Select the Secondary CMP cluster 4. Click **Continue Rollback**. When hovering over the button, it informs you of the failover.  5. Click **OK** to confirm and continue with the operation. It begins to failover. 6. Follow the progress status in the Server Role column. Wait for the server to show standby. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **74604** Policy cluster is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity

Step	Procedure	Result
		70021 The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software

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

8. ☐	**CMP GUI**: Continue the Backed-out. Next operation is «initiate Back-out» **NOTE:** Each back-out of one server takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager** 2. Select the Secondary CMP cluster. 3. Click **Continue Rollback**. When hovering over the button, it informs you of the rollback.  4. Click **OK** to confirm and continue with the operation. It begins to failover. 5. Follow the progress status in the Server Role column. Wait until the back-out server changes to Standby state before continuing. 6. Back-out of the server is complete when the successfully complete message displays in the Upgrade Operation column.

Step	Procedure	Result



Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
cmp						
CMP Site1 Cluster (2 Servers)						
CS-S1-CMP-b	Minor	Y	Standby	12.1.2.0.0_22.1.0	12.3.0.0.0_17.1.0	Initiate upgrade Completed Successfully at Mar 15, 2017 19:29:18.
CS-S1-CMP-a	Minor	Y	Active	12.1.2.0.0_22.1.0	12.3.0.0.0_17.1.0	Initiate upgrade Completed Successfully at Mar 15, 2017 21:06:30.
CMP Site2 Cluster (2 Servers)						
CS-S2-CMP-b	Critical	N	Active	12.3.0.0.0_17.1.0	12.1.2.0.0_22.1.0	Initiate backout Completed Successfully at Mar 31, 2017 14:41:20.
CS-S2-CMP-a	Critical	N	Standby	12.3.0.0.0_17.1.0	12.1.2.0.0_22.1.0	Initiate backout Completed Successfully at Mar 31, 2017 15:40:20.

Expected Critical Alarms

70001 The qp_procmgr process has failed.
31227 The high availability status is failed due to raised alarms
31283 High availability server is offline
70025 The MySQL slave has a different schema version than the master

Expected Major Alarms

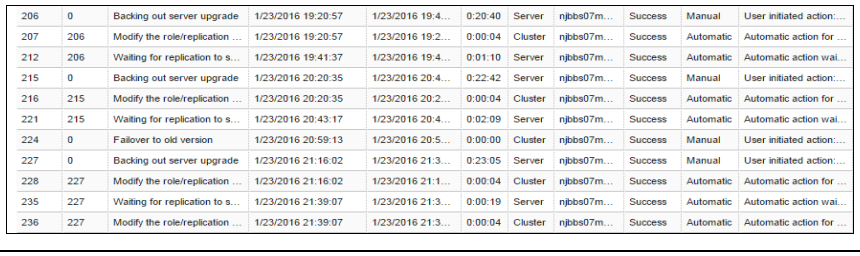
70004 The QP processes have been brought down for maintenance
31236 High availability TCP link is down
31233 High availability path loss of connectivity
70021 The MySQL slave is not connected to the master

Expected Minor Alarms

70503 The server is in forced standby
70507 An upgrade/backout action on a server is in progress
70501 The Cluster is running different versions of software
31232 High availability server has not received a message
31101 DB replication to a slave DB has failed
31102 DB replication from a master DB has failed
31107 DB merging from a child Source Node has failed
31114 DB Replication of configuration data via SOAP has failed
31106 DB merging to the parent Merge Node has failed
70500 The system is running different versions of software

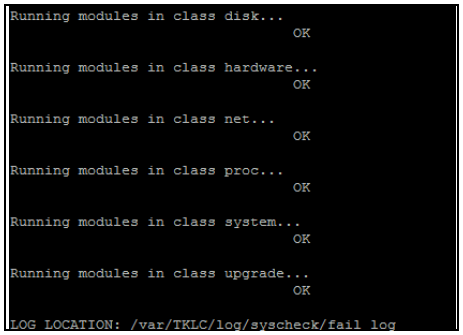
7. Verify in Upgrade Log that that back-out was successful:

All Secondary CMP servers are on Release 12.1.x at this point and show active/standby



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

Step	Procedure	Result

9. ☐	**CMP SSH:** Verify syscheck and `/tmp` directory permission	1. Login to the backed-out server as admusr
		2. Verify that there are no failures in syscheck.
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		4. **NOTE:** Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		5. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		6. Verify:
		`$ ls -l /`
		7. Perform syscheck again:
		`$ sudo syscheck`

Step	Procedure	Result

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

---End of Procedure---		

9.1.7 Back-out Fully Upgraded Primary CMP Cluster

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

Expected Pre-conditions:

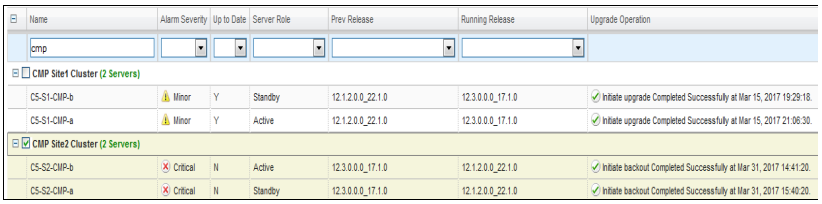
1. Primary Active CMP Cluster is on Release 12.3.x
2. Secondary CMP, MPE and MRA Clusters are on Release 12.1.x or 12.2.x

NOTES:

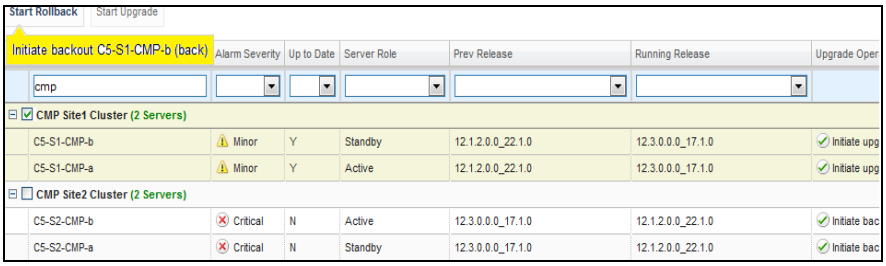
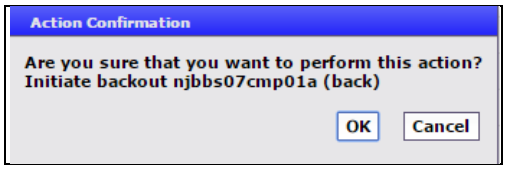
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

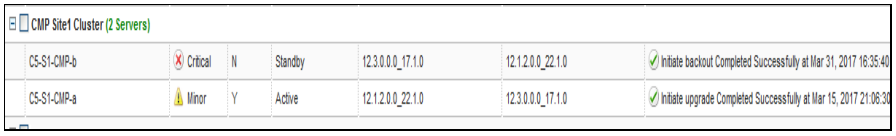
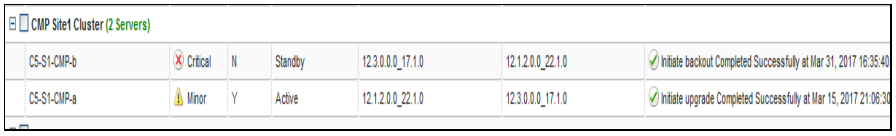
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 7: Back-out Fully Upgraded Primary CMP Cluster

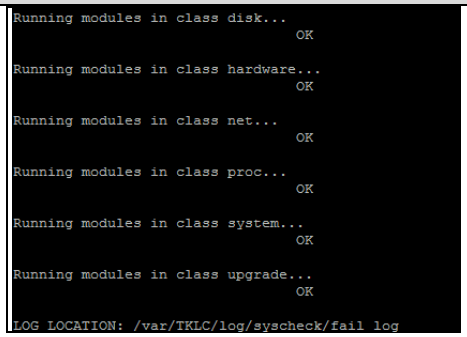
Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of CMP Clusters	1. Navigate to **Upgrade → Upgrade Manager** 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 12.3.x - Secondary CMP, MPE and MRA Clusters are on Release 12.1.x - Up to Date Column shows Y for all servers in Primary CMP Cluster 3. Click **Filter** and enter `CMP` in the **Name** field. **Example** 

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

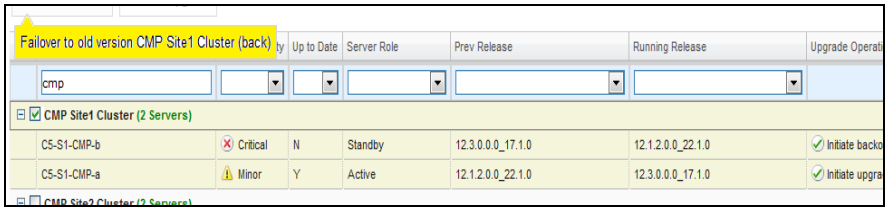
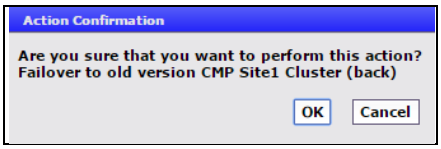
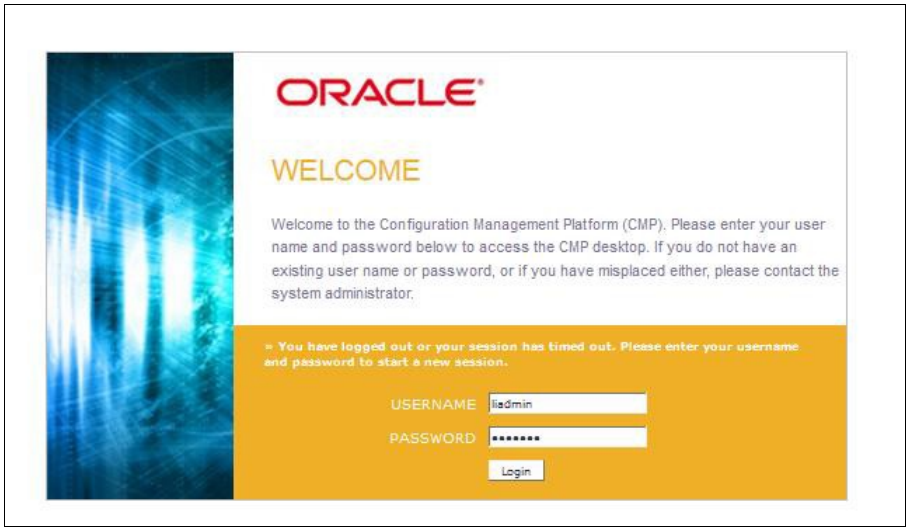
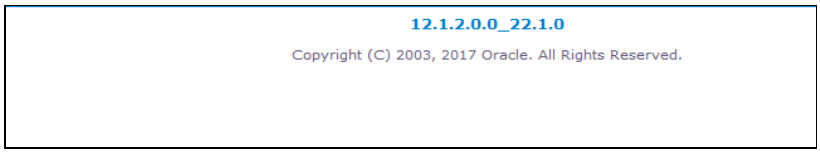
3. ☐	**CMP GUI:** Back-out standby server of Primary CMP cluster **NOTE:** Back-out of one server takes approximately 30 minutes to complete.	1. Select the Primary CMP Cluster 2. Click **Start Rollback**. When hovering over the button, it indicates the server to back out.  3. Click **OK** to confirm and continue with the operation. It begins to back-out.  4. Server goes into an OOS server role 5. Follow the progress status in the Upgrade Operation column.

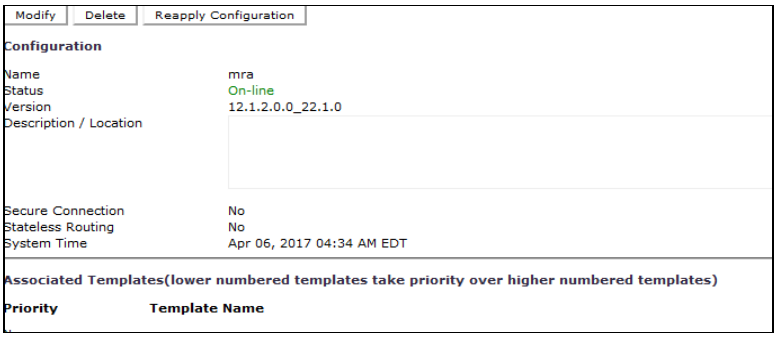
Step	Procedure	Details
		During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out.  CMP Site1 Cluster (2 Servers) C5-S1-CMP-b Critical N Standby 12.3.0.0.0_17.1.0 12.1.2.0.0_22.1.0 Initiate backout Completed Successfully at Mar 31, 2017 16:35:40 C5-S1-CMP-a Minor Y Active 12.1.2.0.0_22.1.0 12.3.0.0.0_17.1.0 Initiate upgrade Completed Successfully at Mar 15, 2017 21:06:30 **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software Back-out of the server is complete when the successful completion message displays in the Upgrade Operation column. The server goes back to standby state and shows a running release of 12.1.x  CMP Site1 Cluster (2 Servers) C5-S1-CMP-b Critical N Standby 12.3.0.0.0_17.1.0 12.1.2.0.0_22.1.0 Initiate backout Completed Successfully at Mar 31, 2017 16:35:40 C5-S1-CMP-a Minor Y Active 12.1.2.0.0_22.1.0 12.3.0.0.0_17.1.0 Initiate upgrade Completed Successfully at Mar 15, 2017 21:06:30
4. ☐	**CMP SSH:** Verify syscheck and `/tmp` directory permission	1. Login to the backed-out server as admusr 2. Verify that there are no failures in syscheck: `$ sudo syscheck`

Step	Procedure	Details

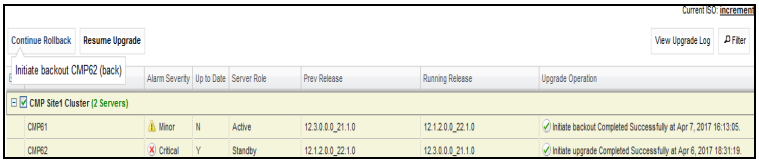
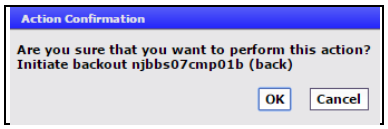
		
		3. Verify /tmp directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0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

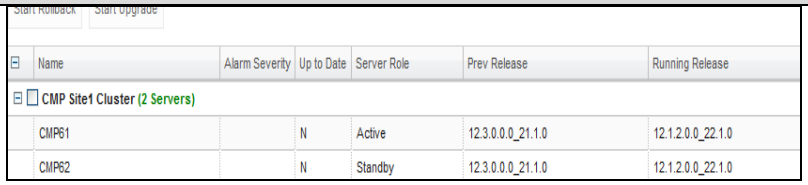
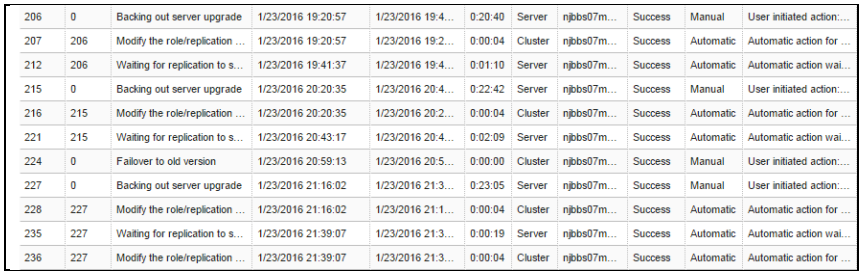
5. ☐	**CMP SSH:** Verify eth01 is primary device interface	This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.
		To resolve this situation permanently, perform the following: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

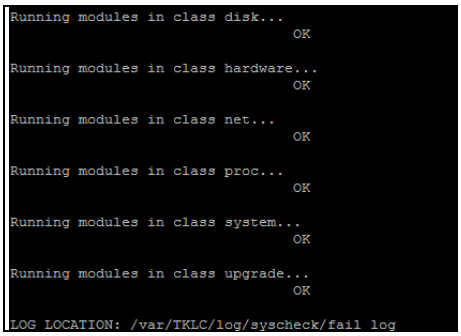
Step	Procedure	Details
6. ☐	**CMP GUI**: Continue the back-out. Next operation is failover	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP cluster 3. Click **Continue Rollback**. When hovering over the button, it informs you of the failover.  4. Click **OK** to confirm and continue with the operation. It begins to failover and takes couple of minutes to complete.  After a minute, you are required to log back in.
7. ☐	**CMP GUI:** Log back into the Primary CMP VIP	After failover, you are required to log back in to the CMP GUI using the Primary CMP VIP. 
8. ☐	**CMP GUI:** Verify previous Policy Management release	1. Navigate to **Help → About**. 2. Verify the release displayed is 12.1.x.x 

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

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

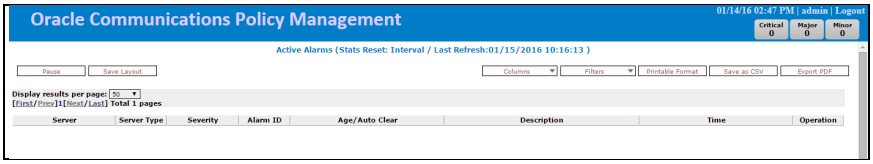
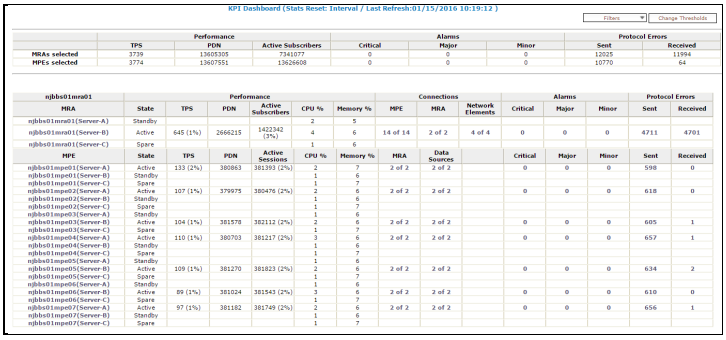
Step	Procedure	Details
11. ☐	**CMP GUI:** Continue the back-out of the Primary CMP Cluster **NOTE:** Back-out of one server takes approximately 30 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager** 2. Select the Primary CMP Cluster 3. Click **Continue Rollback**. When hovering over the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

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

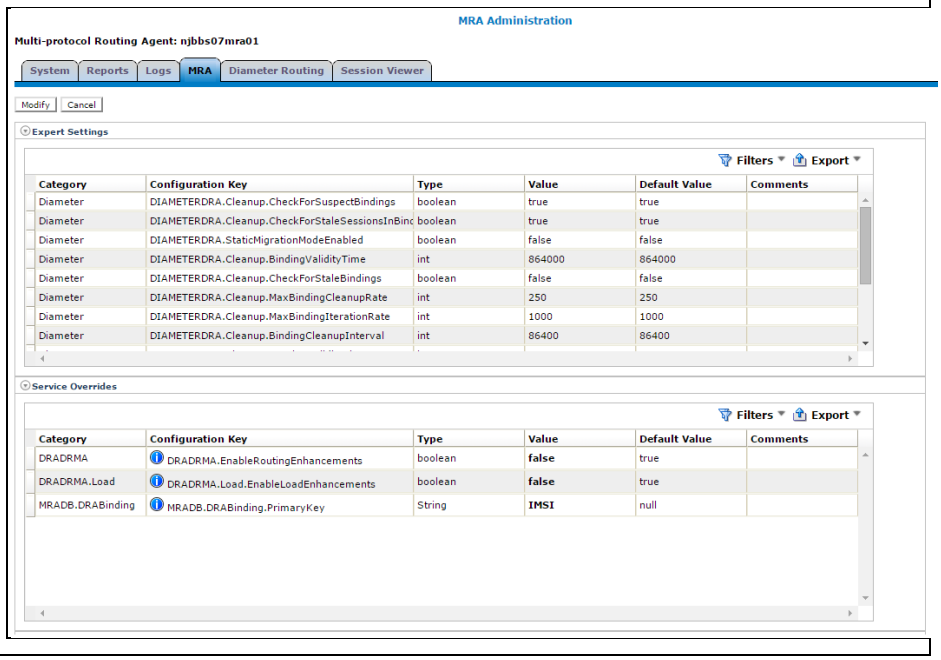
12. ☐	**CMP SSH:** Verify syscheck and `/tmp` directory permission	1. Login to the backed-out server as admusr.
		2. Verify that there are no failures in syscheck:
		`$ sudo syscheck`
		 
		Running modules in class disk... OK
		Running modules in class hardware... OK
		Running modules in class net... OK
		Running modules in class proc... OK
		Running modules in class system... OK
		Running modules in class upgrade... OK
		LOG LOCATION: /var/TKLC/log/syscheck/fail_log
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform syscheck again:
		`$ sudo syscheck`

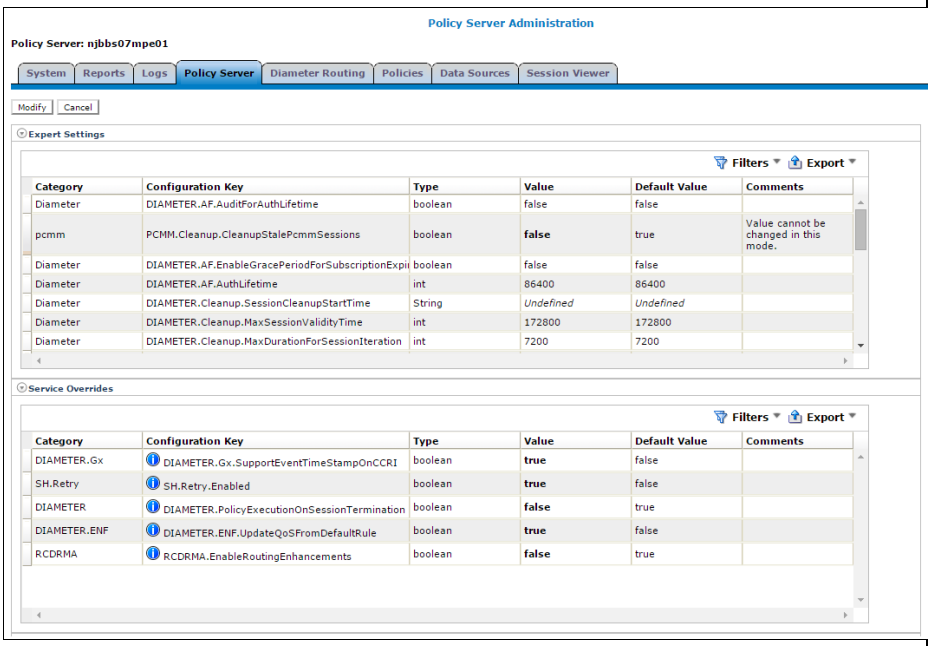
Step	Procedure	Details

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

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

Step	Procedure	Details
16. ☐	**CMP GUI:** Verify Advanced Settings on the MRA	1. Capture screenshots of the advanced settings on the MRA and compare it with prior to upgrade screen captures. 2. Verify that there are no differences. 3. Navigate to **MRA → Configuration →** <*MRA*> **→ MRA** 4. Click **Advanced**.



Step	Procedure	Details
17. ☐	**CMP GUI:** Verify Advanced Settings on the MPE	1. Capture screenshots of the advanced settings on the MPE and compare it with prior to upgrade screen captures. 2. Verify that there are no differences. 3. Navigate to **Policy Server → Configuration →** <*MPE Cluster*> **→ Policy Server** 4. Click **Advanced**.  Alternately, settings can be exported by clicking **Export** on the right within each setting.
---End of Procedure---		

APPENDIX A. TVOE AND PM&C SERVER UPGRADE

A.1 Adding TVOE software image to TVOE host

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

Check off (√) each step as it is completed. If this procedure fails, contact Oracle Support.

Step	Task	Description

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

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

---End of Procedure---		

A.2 TVOE Upgrade

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

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

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

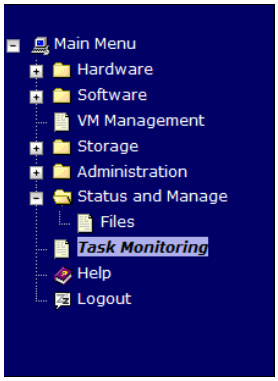
- TVOE Pre-Upgrade Validation
- Pre-Upgrade Backup
- Add TVOE Software Image to TVOE HOST
- Add PM&C Upgrade Software to PM&C Server
- Stand Alone TVOE Host Upgrade
- TVOE Post-Upgrade Validation
- PM&C upgrade
- Stand Alone TVOE Upgrade Accept
- PM&C Upgrade Accept

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

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

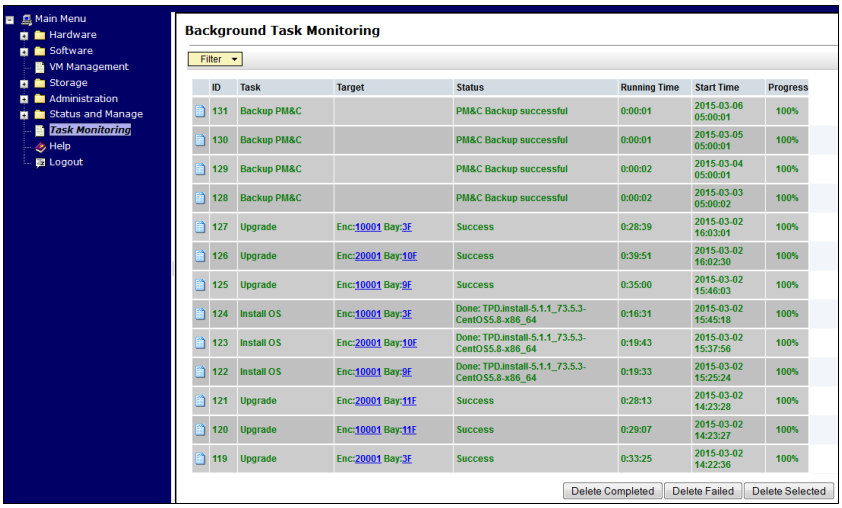
Step	Task	Description
1. ☐		**NOTE:** Upgrading the TVOE host shuts down all guest OS (including PM&C) during the upgrade. Prior to upgrading the TVOE host, ensure the PM&C server is gracefully shut down.

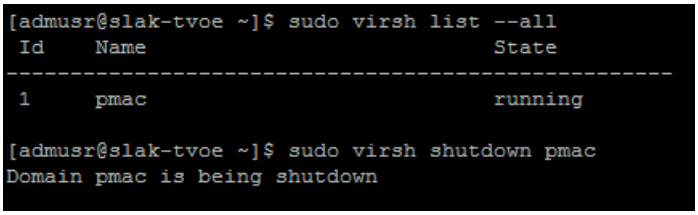
Step	Task	Description
2. ☐	Check any in-progress task(s) on PM&C	1. On a supported web browser, log in to PM&C GUI as pmacadmin 2. Navigate to PM&C GUI background tasks page: **Main Menu → Task Monitoring**

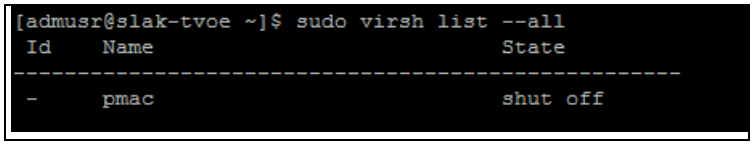


3. Verify all tasks are complete indicated by green 100% progress

NOTE: If any task shows in-progress (blue or red) then wait for the task to complete prior to continuing the next step.

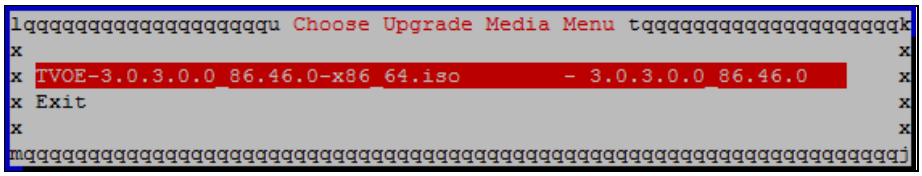


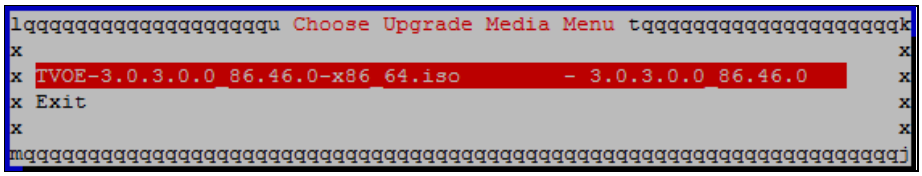
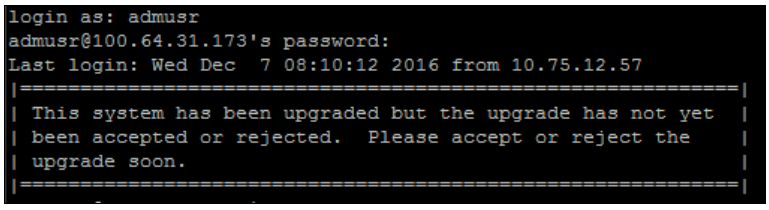
<table>
<tr><th>Step</th><th>Task</th><th>Description</th></tr>
<tr><td>3. ☐</td><td>Shutdown PM&C</td><td>
NOTE: Assuming all tasks are completed (previous step) it is safe to shut down PM&C
1. Log on to the TVOE host as admusr
2. Obtain the name of the PM&C guest by running the following command:
<pre>$ sudo virsh list --all
Id   Name   State
----
1   <pmac_name>   running</pre>
3. Stop the PM&C process by using the following command:
<pre>$ sudo virsh shutdown <pmac_name></pre>


NOTE: It is imperative to log in to the TVOE host instead of using SSH to the PM&C guest. The upgrade might fail otherwise.
</td></tr>
<tr><td>4. ☐</td><td>Verify PM&C guest is shut down</td><td>
1. Login to the TVOE host as admusr.
2. Verify that the PM&C is shut down with the following command:
<pre>[admusr@tvoe approximately]# sudo virsh list --all</pre>


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

Step	Task	Description

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

6. ☐	Start TVOE upgrade **NOTE:** The upgrade process takes 15 minutes	1. Press **Enter** to return to platcfg and then press Exit to go back to the Upgrade menu. Do not quit platcfg. 2. Select **Maintenance → Upgrade → Initiate Upgrade**. 3. Select the TVOE ISO filename.  4. Press **Enter** to initiate the upgrade. **NOTE:** The TVOE host is rebooted at the end of the upgrade process (about 15 minutes) and returns to the login prompt. At this point the TVOE upgrade is complete.
7. ☐	Verify the Upgrade status	1. Log in to TVOE as admusr  2. Verify the upgraded TVOE revision by running the following command: `$appRev` 3. You receive an output similar to this:

<table>
<tr><th>Step</th><th>Task</th><th>Description</th></tr>
<tr><td></td><td></td><td>
<pre>[admusr@slak-tvoe ~]$ appRev
        Install Time: Wed Dec 7 09:44:48 2016
        Product Name: TVOE
     Product Release: 3.0.3.0.0_86.46.0
 Base Distro Product: TPD
 Base Distro Release: 7.0.3.0.0_86.46.0
     Base Distro ISO: TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64.iso
            ISO name: TVOE-3.0.3.0.0_86.46.0-x86_64.iso
                  OS: OracleLinux 6.7</pre>
4. Run the following command:
$sudo verifyUpgrade
The command does not produce output. Any output that displays are potential issues.
5. Run the syscheck command:
$sudo syscheck
<pre>[admusr@slak-tvoe ~]$ sudo syscheck
Running modules in class disk...
                                OK

Running modules in class hardware...
                                OK

Running modules in class net...
                                OK

Running modules in class proc...
                                OK

Running modules in class system...
                                OK

Running modules in class upgrade...
                                OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
[admusr@slak-tvoe ~]$</pre>
NOTE: It is recommended not to accept TVOE upgrade until after PM&C upgrade has been accepted for the following reasons:
• Some older PM&C releases cannot be deployed on upgraded TVOE 3.0.3 system.
• If issues occurs during PM&C upgrade, disaster recovery may be required for which the TVOE upgrade has to be rejected to allow older PM&C to be re-deployed.
A reject cannot be performed after an upgrade has been accepted.
</td></tr>
<tr><td>8. ☐</td><td>Remove the TVOE ISO version file to free up disk space</td><td>Logged in from previous step, issue the following
$sudo rm /var/TKLC/upgrade/TVOE-3.0.3.0.0_86.46.0-x86_64.iso</td></tr>
<tr><td colspan="3">---End of Procedure---</td></tr>
</table>

A.3 PM&C Upgrade

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

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

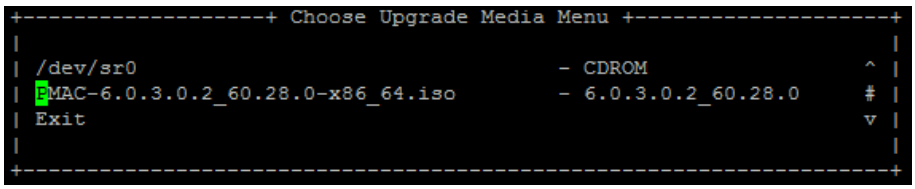
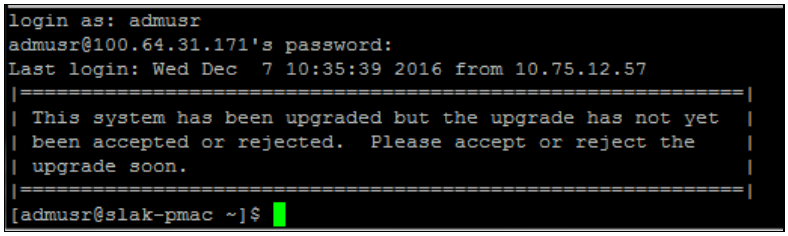
Step	Task	Description

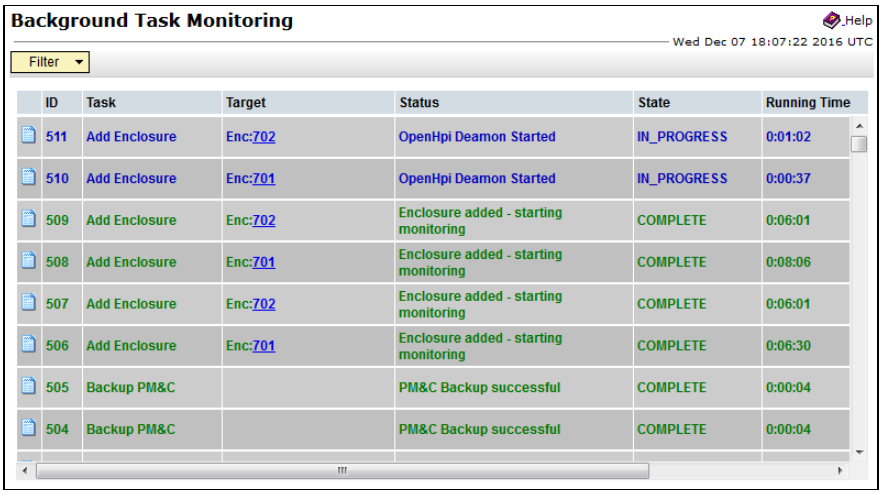
1. ☐	Start the PM&C guest	1. If not logged in to the TVOE host as admusr, do so.
		2. Start the PM&C guest if not started:
		3. Query the list of guests to check whether the PM&C guest is in the running state.
		`$ sudo virsh list --all`
		`Id Name State`
		`----------`
		`1 <pmac_name> running`
		-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

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

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

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

Step	Task	Description
5. ☐	In the platcfg utility, select **Initiate Upgrade** to start the upgrade process	1. In platcfg, select **Maintenance→Upgrade**. 2. Select **Initiate Upgrade** to start the upgrade process 3. Wait until the Choose Upgrade Media Menu window opens before proceeding to the next step  4. Select the PM&C 6.0.3 target ISO filename and press **Enter** to start the upgrade process. The upgrade begins and after 20 minutes the connection is lost as it reboots. - Do not take any action on the PM&C until the server reboots. The reboot takes approximately 5 minutes. - After you log back into PM&C, you see something similar to this: 

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

A.4 Verify PM&C Upgrade

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

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

Step	Task	Description

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

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

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

Step	Task	Description

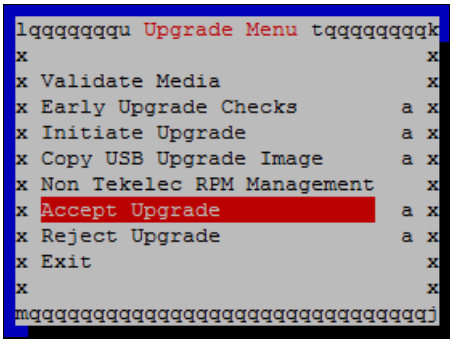
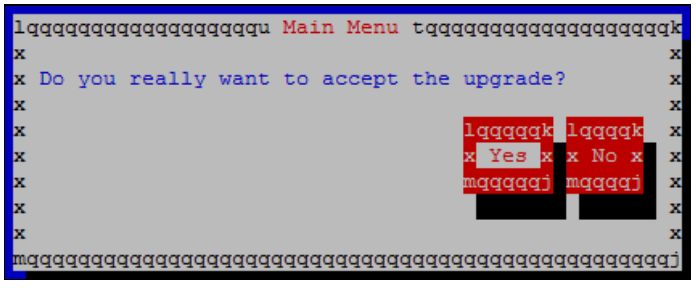
4. ☐	Verify successful completion through the upgrade log	Run the following commands on PM&C
		`$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log`
		`[admusr@brbgpmac ~]$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log`
		`1419272892::UPGRADE IS COMPLETE`
		`$sudo verifyUpgrade`
		NOTE: This command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

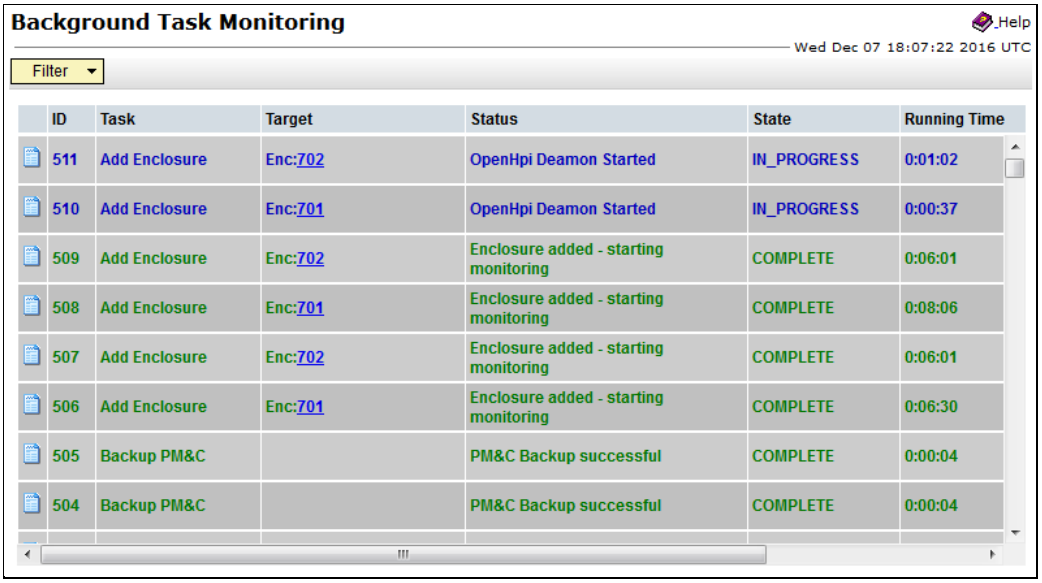
5. ☐	Run syscheck	Run syscheck and verify everything is correct. `$ sudo syscheck`

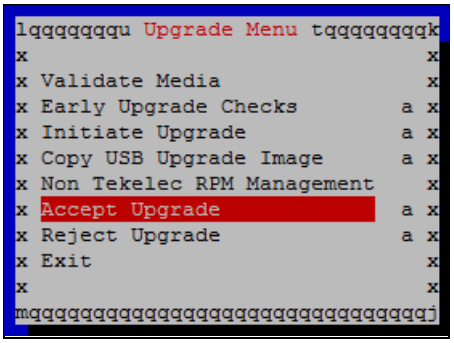
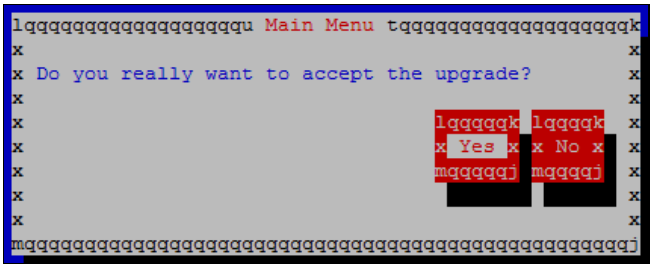
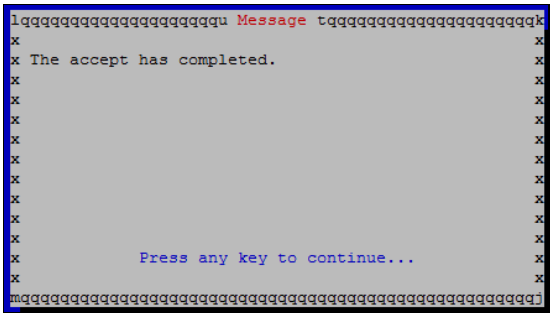
6. ☐	**PM&C SSH CLI:** Recreate the ssh_service with admusr credentials on PM&C guest console if it does not exist	1. Verify that the ssh service exists with admusr credentials by running the following command:
		`$ sudo netConfig --repo showService name=ssh_service`
		`[admusr@westlakelab-pmac ~]$ sudo netConfig --repo showService name=ssh_service`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 172.16. .`
		`Options:`
		`password: 390F1FAE4A420C1F2ABB05C372E30FA9`
		`usr: admusr`
		If the results are similar to the above, that is, options include usr: admusr and an encrypted password, skip to the next step.
		If the results do not include the usr: admusr option or if the service does not exist, continue with this step:
		2. Delete the ssh_service if it exists
		`$ sudo netConfig --repo deleteService name=ssh_service`
		3. Click **YES** to the message if prompted.
		4. Recreate ssh_service with admusr user.
		`$ sudo netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <pm&c_ip_address>`
		`Enter an option name (q to cancel): user`
		`Enter a value for user: admusr`
		`Enter an option name(q to cancel): password`
		`Enter a value for password: Duk******`
		`Verify Password : Duk******`
		`Enter an option name(q to cancel): q`
		Example output
		`Service type? (tftp, ssh, conserver, oa)ssh`
		`Service host? 10.250. .`
		`Enter an option name <q to cancel>: user`
		`Enter the value for user: admusr`
		`Enter an option name <q to cancel>: password`
		`Enter the value for password:`
		`Verify password:`
		`Enter an option name <q to cancel>: q`
		`Add service for ssh_service successful`

Step	Task	Description

		5. Verify that the information is correct by running the following command and comparing the output with the configuration in the last step.
		`$ sudo netConfig --repo showService name=ssh_service`
		Example output
		`[admusr@westlakelab-pmac ~]$ sudo netConfig --repo showService name=ssh_service`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 172.16. .`
		`Options:`
		`password: 390F1FAE4A420C1F2ABB05C372E30FA9`
		`usr: admusr`

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

Step	Task	Description
9. ☐	Health Checks	1. Perform a syscheck: `$sudo syscheck` 2. Open a browser and launch the PM&C GUI. 3. Verify the release at the top of the page.  4. Navigate to Task Manager and monitor as tasks complete. ***DO NOT continue to the next step until all tasks are complete. It may take more than 5 minutes to complete.*** 

Step	Task	Description
10. ☐	Accept the upgrade for TVOE	**NOTE:** It is recommended not to accept the TVOE upgrade until after the PM&C upgrade has been accepted for the following reasons: • Some older PM&C releases cannot be deployed on upgraded TVOE 3.0.3 system. • If issues occurs during PM&C upgrade it may require disaster recovery for which TVOE upgrade has to be rejected to allow older PM&C to be re-deployed. • A reject cannot be performed after an upgrade has been accepted. **NOTE:** After the upgrade is accepted, you cannot roll back to the previous release. 1. Login as admusr to TVOE host CLI and run the platcfg utility: `$ sudo su - platcfg` 2. Navigate to **Maintenance→Upgrade→Accept Upgrade**.  3. Select **Accept Upgrade** and press **Enter**.  4. Click **Yes** to start accept upgrade process. **NOTE:** A session is launched when accepting the upgrade, press **q** to close the window and return to platcfg.  5. Press any key and then press **Enter** on Exit or press **F12** until you exit platcfg. The upgrade process is now complete.
--END OF PROCEDURE--		

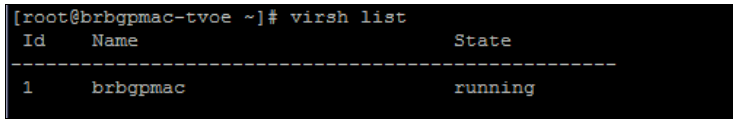
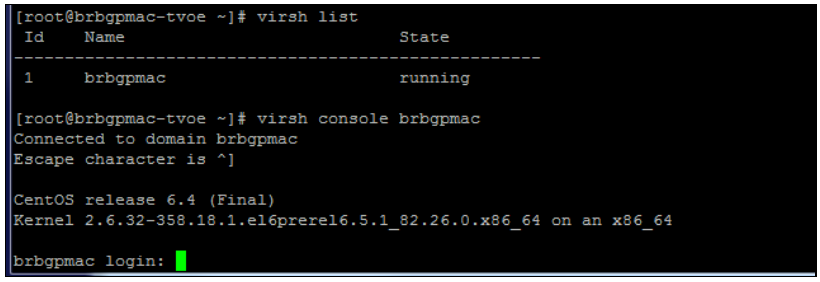
APPENDIX B. TVOE AND PM&C SERVER BACKOUT

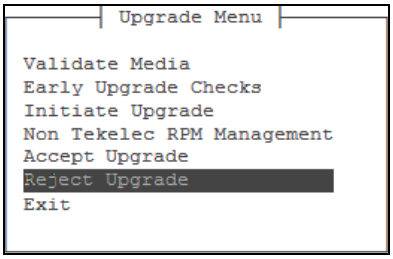
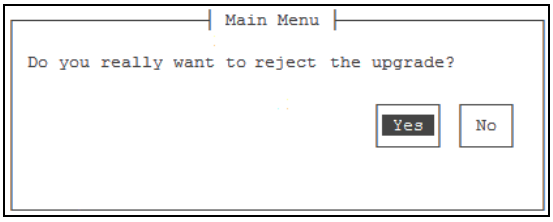
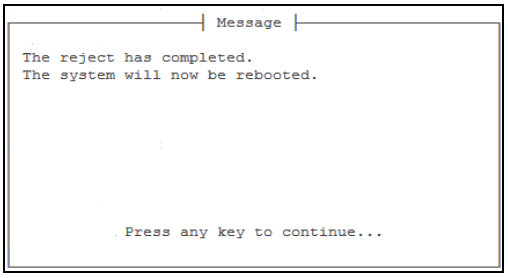
Use this procedure to backout/reject the PM&C server upgrade.

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

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

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

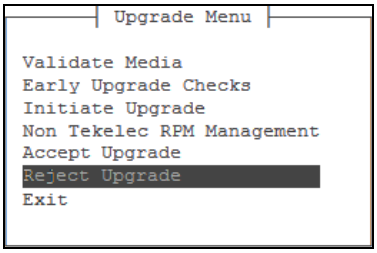
2. ☐	If necessary, access PM&C guest console	1. Log on to TVOE host as admusr
		2. Verify PM&C console is running by issuing the following command
		`$sudo virsh list`
		 
		3. Log on to PM&C guest console by issuing the following command
		`$sudo virsh console <pmacname>`
		 
		4. Log on to PM&C as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

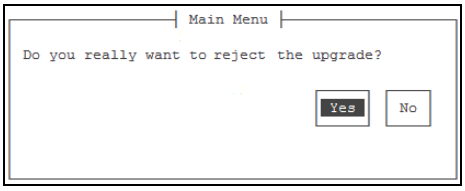
Step	Task	Description
3. ☐	Start the platcfg utility on the PM&C Server	1. At the prompt, run: `$sudo su - platcfg` 2. Navigate to Maintenance→Upgrade  3. Select **Reject Upgrade** and press **Enter** to start the reject process. The following window opens, click **Yes** to begin the backout.  **NOTE:**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

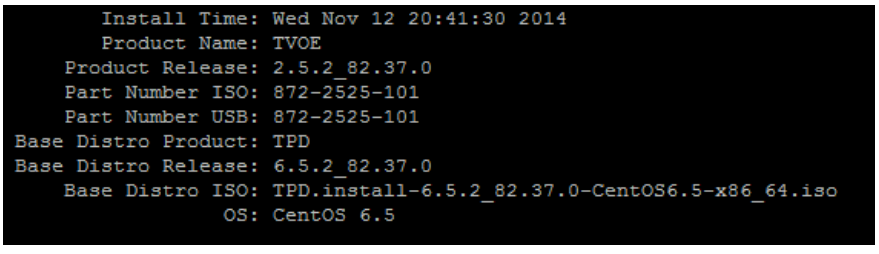
Step	Task	Description

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

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

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

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

The system undergoes a backout. As part of the process the system reboots several times.
After completing the final reboot the login prompt opens. Some of the final startup output along with an example of the login prompt is shown below:
5. Login as admusr
CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.16.0.x86_64 on an x86_64
hostname1342210584 login:</td></tr>
<tr><td>9. ☐</td><td>TVOE Server iLO:
check server health.</td><td>Log in and run the apprev command.
appRev
 
</td></tr>
<tr><td>10. ☐</td><td>TVOE Server iLO:
check server health</td><td>Run the following command to check the health of the server:
sudo alarmMgr --alarmStatus
If any output is produced, an alarm is present on the system. Contact Oracle for information about how to proceed.</td></tr>
<tr><td>11. ☐</td><td>Clear browser cache</td><td>Clear browser cache to ensure that browser has the latest client-side code loaded. Refer to browser documentation if necessary.</td></tr>
<tr><td>12. ☐</td><td>PM&C GUI</td><td>Login to the PM&C GUI to verify the old PM&C version</td></tr>
<tr><td colspan="3">--END OF PROCEDURE--</td></tr>
</table>

APPENDIX C. ACCESSING THE ORACLE CUSTOMER SUPPORT SITE AND HOTLINES

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

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