Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Upgrade Procedure

Policy Management
12.1.x to 12.2
Cloud Upgrade Procedure
Non-CMP Georedundancy Disabled

E84449-02

February 2017

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.
Before upgrading any system, please access Oracle's Customer Support site and review any Technical Service Bulletins (TSBs) that relate to this upgrade.
Refer to 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

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose and Scope

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

The non-georedundant MPE/MRA cluster scheme only has two servers 'Active' and 'Standby' co-located on one site.

Two sites may be used in Policy Management deployments, namely, a Site1 or Primary Site and a Site2 or Secondary Site. The primary MRA/MPE cluster of 'Active' & 'Standby' resides on Site1 while the secondary MRA/MPE cluster of 'Active' & 'Standby' resides on Site2 for disaster recovery.

1.2 Acronyms

BoD	Bandwidth on Demand - a type of component in a cable Policy Management solution
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
MA	Management Agent - a type of component in a cable Policy Management solution
MPE-LI	Multimedia Policy Engine - Lawful intercept
MPE	Multimedia Policy Engine
MPE-R	Routing MPE - a type of component in a cable Policy Management solution
MPE-S	Servicing MPE - a type of component in a cable Policy Management solution
MRA	Multiprotocol Routing Agent (also referred to as Policy Front End or PFE)
OCS	Online Charging System
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
Segment	A segment is a collection of HSGWs, P-GWs, DSRs, MPEs and MRAs that provide the PCRF service. A single MPE/MRA cluster may be part of only one PCRF Segment. A CMP manages all the MPE/MRAs at multiple sites. A CMP manages one or more PCRF Segments.
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment
UE	User Equipment
UM	Upgrade Manager – The CMP GUI pages that the operator uses to perform an upgrade
VO	Verification Office

1.3 Terminology

Primary Site (Site1) – A site where the MPE/MRA

primary cluster exists with co-located Active and Standby servers

Secondary Site (Site2) – A site where the MPE/MRA/MA/BoD secondary cluster exists with co-located Active and Standby servers for disaster recovery

1.4 Software Release Numbering

- Policy Management Release 12.2

2. UPGRADE OVERVIEW

This section lists the required materials and information needed to execute Policy Management Release 12.2 software upgrades.

2.1 Upgrade Status Values

Status	Condition
OK	All servers are up-to-date and no alarms are present.
Info	No alarms are present, but a condition (such as out-of-date) is present that the operator should be made aware of.
Minor	At least one minor alarm is present.
Major	At least one major alarm is present.
Offline	The server cannot be reached.
Degraded	At least one server in the cluster cannot be reached.
Critical	At least one critical alarm is present.
Active	The server is active.
Standby	The server is in standby mode as part of normal operations.
Forced Standby	The server is in standby mode because it has been placed into that state via direct operator intervention or as part of the upgrade.
Offline	The server cannot be reached.
Zombie	The server is in a state where it cannot recover automatically and requires direct operator intervention.

2.2 Upgrade Path

This upgrade document supports the following upgrade path:

- Policy Management 12.1.x to 12.2

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, or MPE depending on the mode. For a CMP cluster, the cluster status may also be Primary site and/or Secondary site.

A customer deployment may consist of multiple clusters.

Required Cluster Upgrade Sequence:

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

The following is the upgrade sequence, specific process will be documented by an Oracle provided MOP.

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

1. Upgrade Primary (Site1) CMP
2. Upgrade Secondary (Site2) CMP (if applicable)
3. Upgrade MPE/MRA (see note below)

NOTE: MPE/MRA clusters can be upgraded in parallel, a maximum of 8 at a time.

2.3.2 Policy Release Mixed-Version Operation & 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-12.2 release and 12.2 release in mixed configuration would support the performance and capacity of the pre-12.2 release. The mixed version Policy Management configuration would also support pre-12.2 features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the Release 12.2 CMP will be managing MRA/MPE/MA/BoD servers in a pre-12.2 release. In this mixed version configuration, a Release 12.2 CMP will 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 12.2 CMP has the following limitations while running in a mixed version environment:

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

Mixed-version configurations supported

Policy Management system components on	CMP R12.2	MRA R12.2	MPE R12.2
CMP 12.1.x	Yes	No	No
MRA 12.1.x	Yes	Yes	Yes
MPE 12.1.x	Yes	Yes	Yes

Note: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP to Release 12.2. The replication is automatically enabled once both active CMP and DR-CMP are upgraded to Release 12.2.

2.4 Customer Impacts

The cluster upgrade proceeds by upgrading the Standby server, switching over from the Active to the Standby, and upgrading the second server (i.e., the new Standby). The switchover of each cluster will have 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 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*.

2.7 Required Materials and Remote Access

1. Policy 12.2 software ISO's
2. Policy 12.2 software upgrade Release Notes.

3. The capability to remote login to the target server as *admusr*.

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

4. 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.
5. User logins, passwords, IP addresses and other administration information.
6. VPN access to the customer's 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.

2.7.1 Login Users and Passwords

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 among the customer sites. If not, record 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-1: Logins, Passwords and Server IP Addresses

Item	Value
CMP servers	GUI Administrator Login User/Password:
	admusr password:
MRA/MPE servers	**admusr** password:
Software Upgrade Target Release[1]	Target Release Number:
	Policy 12.2 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 'pulldown 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 no longer 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 presented to the operator as an option. However, the operator can see what has been done via the upgrade log.

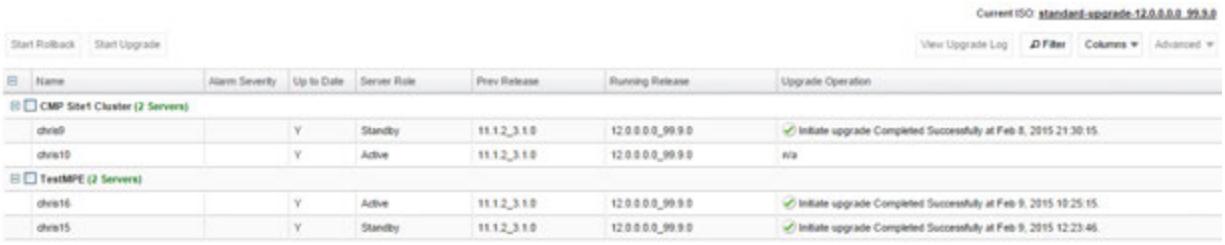


Figure 1: Sample display of the upgrade manager page.

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.

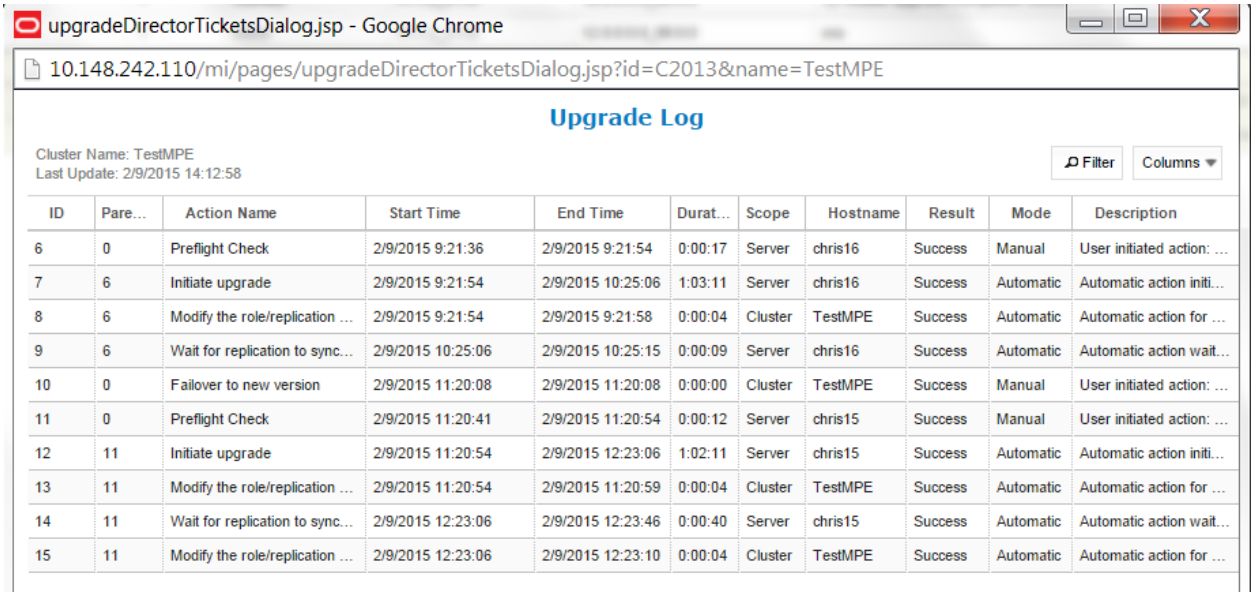
- Start Rollback/Start Upgrade buttons (upper left) – If these buttons are greyed out, it means that there isn't an appropriate action to take at this time. However, if a button isn't greyed out, then it means that there is a 'preferred' action that can be taken to upgrade (or backout) the cluster. Normally, upgrading a cluster is a well-defined fixed procedure. However, in some cases there are a number of valid sequences. Selecting the 'preferred' step will simply cause the upgrade director to choose the default sequence. It is strongly recommended to exclusively use these buttons to upgrade/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 will raise alarms simply to indicate that it is initiating upgrade activity.
    - Servers will report alarms to indicate that their mate servers are offline.

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

- Up to Date – This column is used to indicate the state of the code on the server.
  - 'N' -> The server is running old code needs to 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 will display attributes of the various actions (manual and automatic) that have been performed on the selected cluster. It is important to note that this is NOT the audit log. The audit log is meant to track what the operator has done. This log is meant to capture the sequence of upgrade activity – whether it was initiated by an operator or automatically triggered.



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

Figure 2: Upgrade Log

3.1.2 Optional actions

It is possible to perform every step in the upgrade process just using the 'Upgrade' and 'Backout' buttons. When the operator clicks these buttons, the upgrade director will perform the next 'preferred' action. However, there are times that the operator may want to take a slightly different – but still legal – procedure. For example, the upgrade director has a preferred order in which it will upgrade a 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 pulldown menu. It is important to note that this menu will ONLY be populated with legal/reasonable actions. Actions that are wrong/inconsistent will not be displayed.

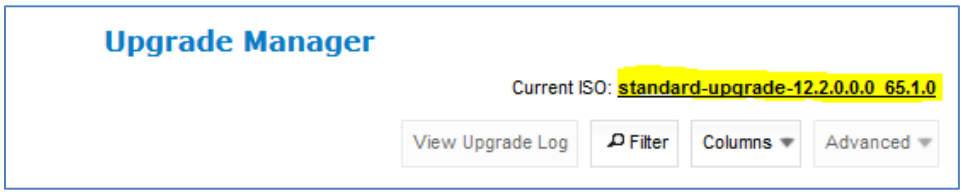
If the operator selects an optional action, they can go back to using the default/preferred at any time

3.1.3 The ISO select

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

"A standard (full) upgrade to version XXX"

"An incremental upgrade to version XXX"



When the operator wants to start a new upgrade, they click on this item. The upgrade director will search for valid upgrade procedures. In order to minimize confusion, these upgrade procedures are usually embedded within a CMP ISO. This way, the CMP ISO is always tightly tied to the corresponding upgrade procedure.

When you select a new ISO, you are telling the upgrade director to abandon its current upgrade procedure in favor of a brand 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. From a user perspective, the UD is largely hidden. However, there are conventions/operating principles that have user visible effects.

3.1.4.1 Alarm philosophy

In general, the upgrade director will raise alarms when

1) A server is taken out of service
2) A server goes into forced standby
3) A failover occurs

This is normal and expected during an upgrade. Most alarms clear by themselves as the upgrade procedure continues.

The table below lists some of the alarms that can be raised during a 12.2 upgrade.

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

Alarm Number	Severity	Name
70507	Minor	Upgrade in Progress

3.1.4.2 General upgrade procedure

In general, the upgrade of a server goes through 3 steps.

1) Preflight checks – look for certain conditions which guarantee a failed upgrade. If such conditions are detected, fail. There are two principles behind the preflight checks
    a. It is better to fail early in a recoverable way than to fail late in an unrecoverable way.
    b. Preflight checks are VERY narrow. 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 newly promoted Upgrade Director does not have the full history/context. It will wait until it can contact the unreachable server before it will take action on the server.

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

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

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 can't automatically recover from.

Any failure should generate an UPGRADE_OPERATION_FAILED alarm. In such cases, the operation can be attempted again. Ideally, the operator/support would investigate the original failure before repeating. However, if the server is in an indeterminate state, the server is declared a ZOMBIE and no further action can be taken on the server. It will require direct action by support/engineering to repair.

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

4. UPGRADE PREPARATION

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

Overview:

1. Upgrade Primary (Site1) CMP
2. Upgrade Secondary (Site2) CMP (if applicable)
3. Segment 1 Site 1:

   Upgrade MPE/MRA clusters
4. Segment 1 Site 2:

   Upgrade MPE/MRA clusters
5. Segment 2 Site 1:

   Upgrade MPE/MRA clusters
6. Segment 2 Site 2:

   Upgrade MPE/MRA clusters

4.1 Pre-requisites

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

Procedure 1

Step	Procedure	
1. ☐	Verify all required materials are present	As listed in Section: "Required Materials & Remote Access"
2. ☐	Review Release Notes	Review Policy Release 12.2 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 12.2, only Mozilla Firefox and Google Chrome are fully supported.**

4.2 Plan and Track Upgrades

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

1. Upgrade CMP cluster(s)

2. 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:

- *Policy changes or configuration changes should NOT be made while the system is in mixed-version operation.*
- *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 Site1 and Site2 CMP clusters	Site Names _____ & _____		3 hrs

Step	Procedure	Result	Engineer	Time
3. ☐	Upgrade Site1 non-CMP clusters for Segment-1 ***NOTE:*** *Maximum of 8 clusters performed in parallel*	Site Names _____ Cluster List:		2 hrs
4. ☐	Upgrade Site2 clusters for Segment-1 ***NOTE:*** *Maximum of 8 clusters performed in parallel*	Site Names _____ Cluster List:		2 hrs
5. ☐	Upgrade Site1 clusters for Segment-2 ***NOTE:*** *Maximum of 8 clusters performed in parallel*	Site Names _____ Cluster List:		2 hrs
6. ☐	Upgrade Site2 clusters for Segment-2 ***NOTE:*** *Maximum of 8 clusters performed in parallel*	Site Names _____ Cluster List:		2 hrs

4.3 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 when Interval statistics is enabled.

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

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

It is recommended that the following actions are taken well in advance of the upgrade procedure:

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

For completeness and assuredness, it is recommended to collect *at least* 24 hours of interval statistics before upgrading to 12.2

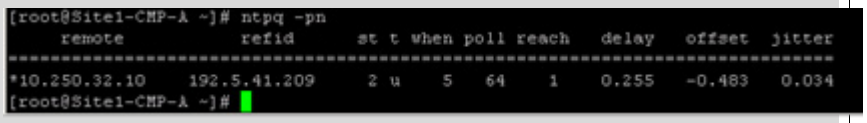
For addition information, see the following publications:

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

4.4 Perform System Health Check

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

Step	Procedure	Result
1. ☐	CMP GUI access	Open a browser 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, please ensure that all Active Alarms are well understood and resolved.*
3. ☐	View KPI reports	Verify that the system is running within expected parameters. Export current KPIs to save into a file.

Step	Procedure	Result
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.*	- Validate the IP connectivity between the server and NTP servers with the command *ping* if available. - Confirm that time is synchronized on each server with CLI shell command of: ntpq –np  The "*" sign besides the NTP server IP indicates the NTP server is in sync. - Confirm the date is correct on each server. - Check that BIOS clock is synced with the clock (by showing the expected time) using the shell command: hwclock

4.5 Deploy Policy Upgrade Software

Software should be deployed to each policy server */var/TKLC/upgrade* directory, before the actual upgrade activities. This will typically be done with utilities such as SCP/WGET/SFTP and also using the Upgrade Manager. Because of the large size of the software ISOs, sufficient time should be planned to accomplish this step. For Policy Release 12.2, each ISO image size is about 1.0 Gigabytes.

4.5.1 Deploying Policy Upgrade Software to Servers

There are several possible software images in this upgrade (CMP, MPE, MPE-LI, MRA). A single image must be deployed to the upgrade *(/var/TKLC/upgrade*) directory of each server to be upgraded, where the image is the correct type for that server. i.e., the new CMP software image must be deployed to the CMP servers, the new 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, etc.) does not match the existing installed software type, the upgrade will fail. Example: an attempt to upgrade a CMP with a MPE software image will fail during the upgrade action.*

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

If multiple images are copied into the */var/TKLC/upgrade* directory, the upgrade will fail.

4.5.2 Distribute Application ISO image files to servers

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

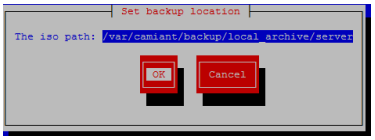
NOTE: *ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance windows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

Step	Procedure	Result

1. ☐	**Transfer ISOs to Policy Servers.**	- Transfer release 12.2 ISO files (CMP and non-CMP) into the directory **/var/TKLC/upgrade** on the respective server via either of the following SCP or WGET command
		
		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-12.2x>:/var/TKLC/upgrade/`
		
		Copy MPE software ISO to ONE of the other MPE servers:
		`$sudo scp 872-* <mpe-12.2x>:/var/TKLC/upgrade/`
		
		Copy MPE-Li software ISO to ONE of the other MPE-Li servers:
		`$sudo scp 872-* <mpe-li-12.2x>:/var/TKLC/upgrade/`
		
		Copy MRA software ISO to ONE of the other MRA servers:
		`$sudo scp 872-* <mra-12.2x>:/var/TKLC/upgrade/`
		
		NOTE: After copying the ISO to one of the respective servers, the ISO Maintenance option will be used to distribute the ISO to the rest of the servers.

THIS PROCEDURE HAS BEEN COMPLETED		

4.5.3 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.*** • Login into the ACTIVE Primary CMP server. Navigate to the following through platcfg utility. `$sudo su – platcfg` **Policy Configuration→Backup and Restore→Server Backup** • Provide an ISO backup filename (or use the suggested one) in the default backup location path: */var/camiant/backup/local_archive/serverbackup/<serverbackup.iso>*  Press OK. Go back to the previous menu (**Policy Configuration→Backup and Restore**) and select: **→System Backup** • Provide 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 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: _____ _____ _____
THIS PROCEDURE HAS BEEN COMPLETED		

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

4.5.4.1 Improve Password Security

The default password hash prior to Policy 12.0 is MD5. MD5 is now considered a weak hash that can be brute-force cracked in a reasonable amount of time. The best hash to use is SHA512. This is currently the strongest hash supported on the platform. Due to this change, during upgrade all non-default passwords are automatically expired. This may cause issues during upgrade from pre-12.1 to 12.2 and above. To prevent those issues, the following procedure has been created.

4.5.4.2 Impact

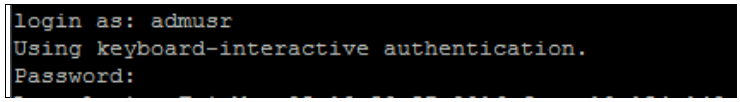
After this procedure is run, the *root* and *admusr* password will be hashed with the strongest possible method, SHA512.

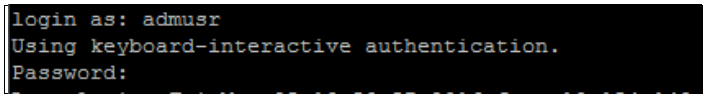
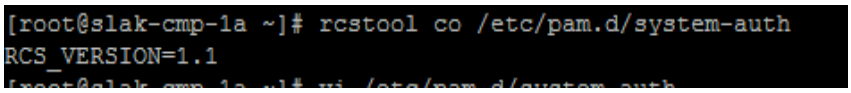
This procedure only addresses root and admusr passwords. Other users should also update their password to benefit from the new hashing. If they are not changed prior to the upgrade to 12.2, they will be expired post upgrade.

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

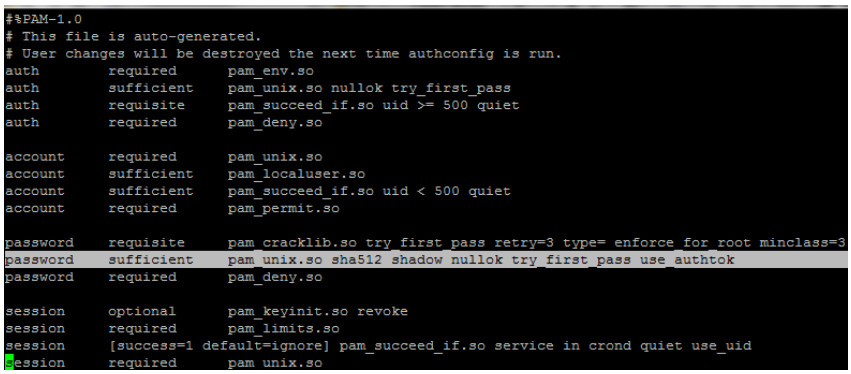
Order to perform this procedure on an 'In-Service' Policy Management

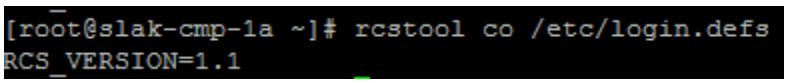
1. Standby CMPs
2. Active CMPs
3. Standby MPEs/MRAs/MAs/BoDs
4. Active MPEs/MRAs/MAs/BoDs

Step	Procedure	Result
1. ☐	Login to the every server	• **For an upgrade from 12.1.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, then this procedure is not needed on this server. Skip to the next section.** **If the first two characters after the colon are not $6, then it is probably $1 (MD5) and this procedure should be followed for this server. Continue on with step 4**
3. ☐	**Order to perform the change**	**Perform steps 4-17 in the following order:** 1. **Standby CMPs** 2. **Active CMPs** 3. **Standby non-CMP servers** 4. **Active non-CMP servers**
4. ☐	Login to the server as admusr	• **For an upgrade from 12.1.x**, login as *admusr* and change to *root* using the following command: **$sudo su** 
5. ☐	Checkout revisions	Issue the following command **#rcstool co /etc/pam.d/system-auth** 

Step	Procedure	Result

6. ☐	Modify the 'system-auth' file	Open the *system-auth* file:
		#vi /etc/pam.d/system-auth
		Modify the file. Change the following line from md5 to sha512
		Modify the below line with sha512 instead of md5 (Current line indicates currently configured in server. Modified Line indicates modification which needs to 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 already 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) Open the *login.defs* file: `#vi /etc/login.defs` *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 Comment out the following line if necessary: ***MD5_CRYPT_ENAB yes***

Step	Procedure	Result

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

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

12. ☐	Edit libuser.conf	**Open the *libuser.conf* file:** `#vi /etc/libuser.conf` ***Modify the below line with sha512 instead of md5*** *Current Line:* crypt_style = md5 *Modified Line:* crypt_style = sha512 NOTE: The line to edit 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 already was configured
		`#rcstool unco /etc/libuser.conf`

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

15. ☐	Verify	**Logout of the current session and re-login using the new password credentials.**
THIS PROCEDURE HAS BEEN COMPLETED		

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

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 system), and the other is designated as the Secondary Site (this site is ready to take over in case the primary site fails).

This procedure will 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.

5.1 Upgrade CMP Clusters Overview

Upgrade the Primary CMP cluster

1) Upgrade CMP Site1
    a. Start upgrade on the standby server
    b. Failover
    c. Continue upgrade with the remaining Site1 CMP server

Upgrade the Secondary CMP cluster

2) Upgrade CMP Site2
    d. Start upgrade on the standby server
    e. Failover
    f. 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.

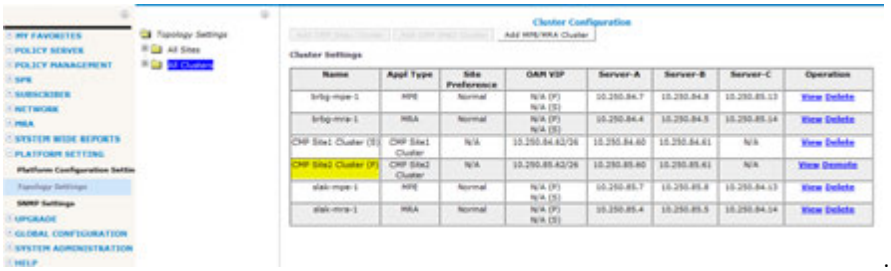
Identify the CMP sites to be upgraded here, and verify which site is Primary and which one is Secondary:

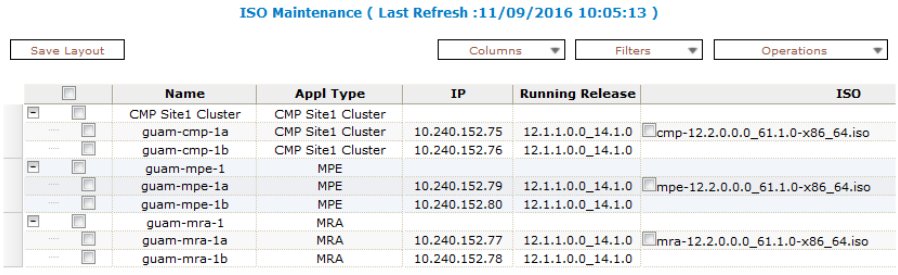
CMP Sites	Operator Site Name	Topology Site Designation (Site1 or Site2)	CMP Server-A	CMP Server-B
Primary Site			Server-A Hostname _____ Server-A IP Address _____ Server-A HA Status _____	Server-B Hostname _____ Server-B IP Address _____ Server-B HA Status _____
Secondary Site			Server-A Hostname _____ 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*
- *Both Primary and Secondary CMP clusters must be upgraded before non-CMP servers*

5.1.1 Upgrade primary CMP cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Alarm Status.	**System Wide Reports → Alarms → Active Alarms** • Confirm that any existing alarm is well understood and is of no impact to the upgrade procedure. • Capture a screenshot and save it into a file for reference.
2. ☐	**CMP GUI:** Identify and Record the CMP Cluster(s)	**Navigate to Platform Setting → Topology Settings** • Note which cluster is the primary and which one is the secondary.  The Primary CMP will be noted with "(P)". The Secondary CMP, with "(S)".

3. ☐	**CMP GUI**: Verify Status of CMP Clusters	**Upgrade → Upgrade Manager**
		• Confirm the CMP clusters are:
		  ○ In Active/Standby status
		  ○ Running release 12.1.x software
		Upgrade → ISO Maintenance
		• Ensure Release 12.2 ISO files have been copied to at least one of each corresponding server types (CMP, MPE, MRA, etc.)
		 

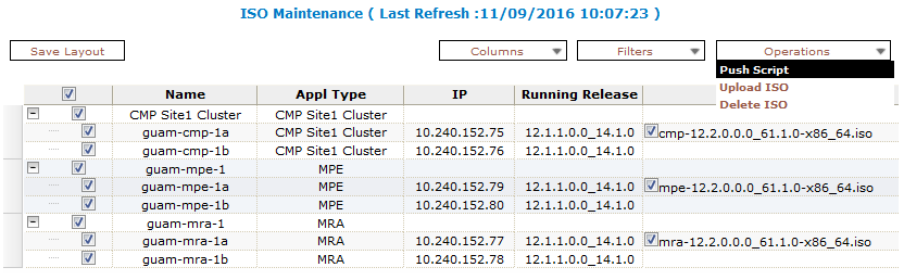
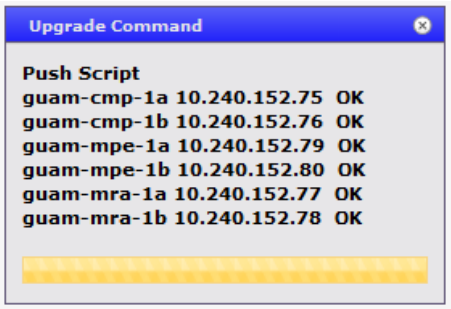
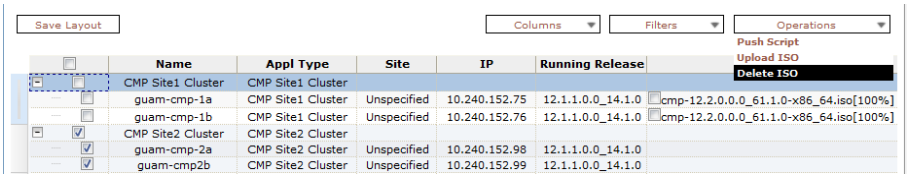
ISO Maintenance (Last Refresh :11/09/2016 10:05:13)

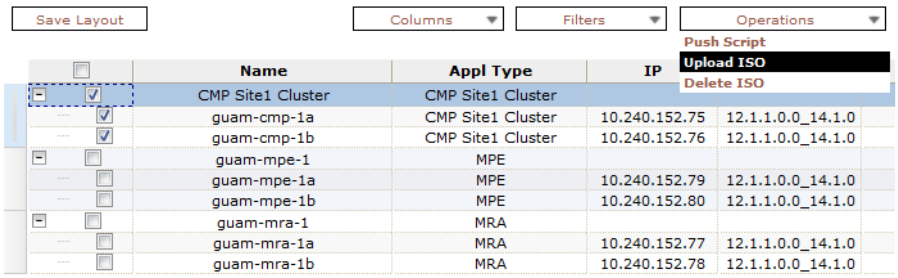
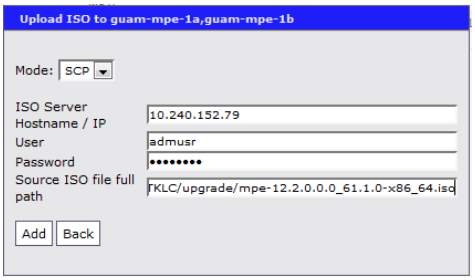
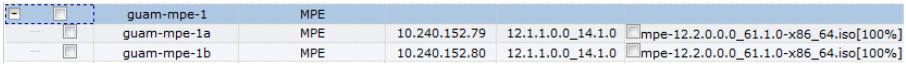
Save Layout | Columns | Filters | Operations

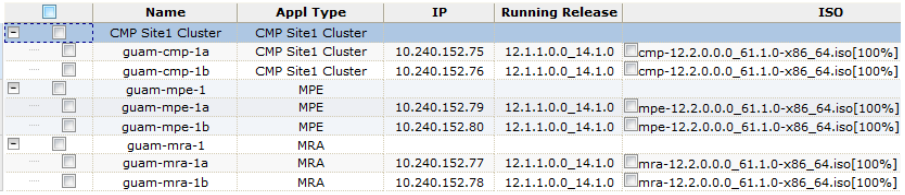
Name	Appl Type	IP	Running Release	ISO
CMP Site1 Cluster	CMP Site1 Cluster			
guam-cmp-1a	CMP Site1 Cluster	10.240.152.75	12.1.1.0.0_14.1.0	cmp-12.2.0.0.0_61.1.0-x86_64.iso
guam-cmp-1b	CMP Site1 Cluster	10.240.152.76	12.1.1.0.0_14.1.0	
guam-mpe-1	MPE			
guam-mpe-1a	MPE	10.240.152.79	12.1.1.0.0_14.1.0	mpe-12.2.0.0.0_61.1.0-x86_64.iso
guam-mpe-1b	MPE	10.240.152.80	12.1.1.0.0_14.1.0	
guam-mra-1	MRA			
guam-mra-1a	MRA	10.240.152.77	12.1.1.0.0_14.1.0	mra-12.2.0.0.0_61.1.0-x86_64.iso
guam-mra-1b	MRA	10.240.152.78	12.1.1.0.0_14.1.0	

Step	Procedure	Result

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

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

Step	Procedure	Result
7. ☐	**CMP GUI:** Distribute ISOs to CMP/MPE/MRA/etc. servers **NOTE:** This step depends on the ISO type. Distribute ISOs accordingly.	**Upgrade → ISO Maintenance** - Filter by server type (optional but preferred step) - One application at a time, check one server type (MPE/MRA/CMP/etc.) to be upgraded and perform the '**Upload ISO**' operation • Click <cluster type> -> Operations -> Upload ISO  • Fill in the dialogue with the appropriate information*:* Mode = SCP ISO Server Hostname / IP = *<IP address where the ISOs are located>* User = admusr Password = *<admusr password of the server>* Source ISO Full Path = /var/TKLC/upgrade/*<server type iso filename>*  • Click 'Add' • When completed, the ISO column will be populated with the ISO and a notification of "[100%]"  • Repeat for all cluster types

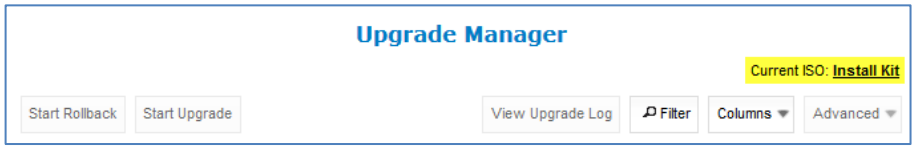
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>8. ☐</td><td>CMP GUI: Verify ISO distribution to all the Servers</td><td>Upgrade → ISO Maintenance
• Verify that the Release 12.2 ISO file of the correct type is shown for each server.
• When completed, the ISO column is populated with the ISO and a notification of “[100%]”
 
<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>guam-cmp-1a</td><td>CMP Site1 Cluster</td><td>10.240.152.75</td><td>12.1.1.0.0_14.1.0</td><td>cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td></td><td>guam-cmp-1b</td><td>CMP Site1 Cluster</td><td>10.240.152.76</td><td>12.1.1.0.0_14.1.0</td><td>cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td></td><td>guam-mpe-1</td><td>MPE</td><td></td><td></td><td></td></tr>
<tr><td></td><td>guam-mpe-1a</td><td>MPE</td><td>10.240.152.79</td><td>12.1.1.0.0_14.1.0</td><td>mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td></td><td>guam-mpe-1b</td><td>MPE</td><td>10.240.152.80</td><td>12.1.1.0.0_14.1.0</td><td>mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td></td><td>guam-mra-1</td><td>MRA</td><td></td><td></td><td></td></tr>
<tr><td></td><td>guam-mra-1a</td><td>MRA</td><td>10.240.152.77</td><td>12.1.1.0.0_14.1.0</td><td>mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
<tr><td></td><td>guam-mra-1b</td><td>MRA</td><td>10.240.152.78</td><td>12.1.1.0.0_14.1.0</td><td>mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]</td></tr>
</table>

<u>NOTE</u>: For those servers for which the ISO was copied to from the local machine, there will not be a ‘100%’ indicator. This indicator is only available when transferring ISOs using the ISO management feature.</td></tr>
<tr><td>9. ☐</td><td>Primary Active CMP: ssh to primary active CMP and copy ISO to /var/camiant/iso</td><td>Logon to the primary active CMP as admusr and copy the 12.2 ISO to the directory /var/camiant/iso

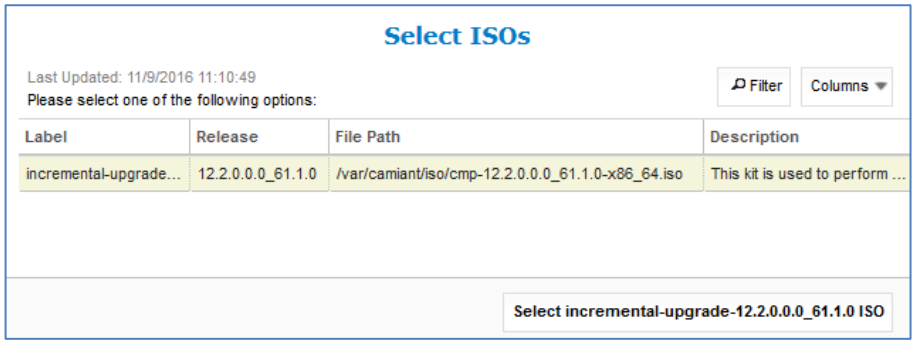
<code>$ sudo cp –p /var/TKLC/upgrade/cmp-12.2.<…>.iso /var/camiant/iso/</code>

Verify the file was successfully copied:

<code>$ ls /var/camiant/iso/</code></td></tr>
<tr><td>10. ☐</td><td>CMP GUI: Locate the 12.2 Upgrade ISO</td><td>Upgrade → Upgrade Manager

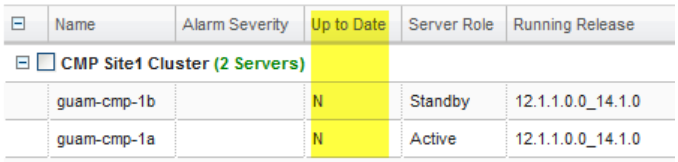
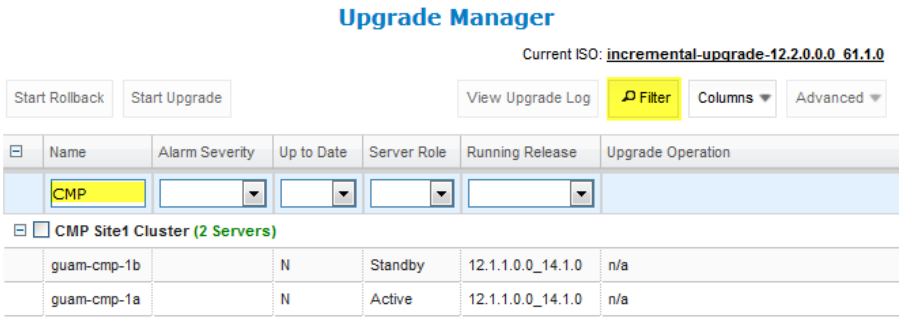
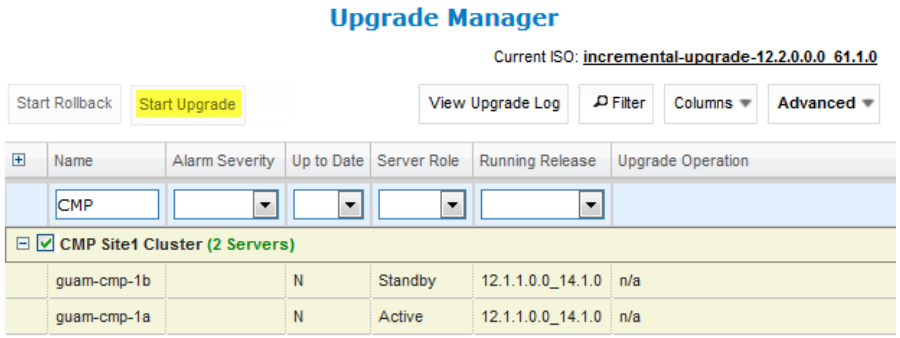
Select the current ISO, in this case it is labeled Install kit.
 

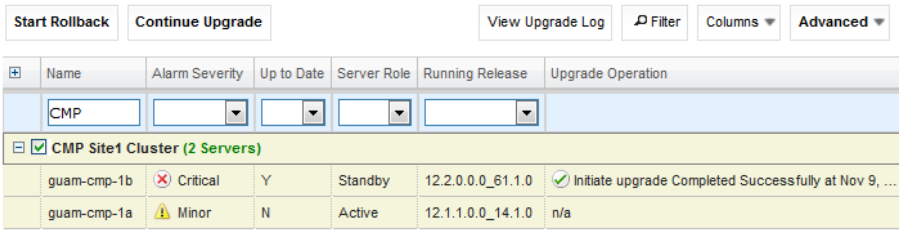
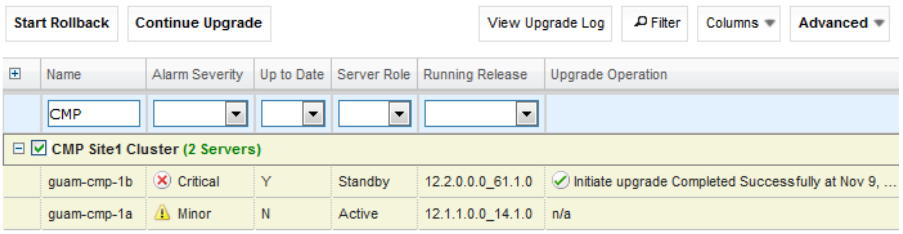
This will pop up a dialog box with a description of the ISO that was copied into <code>/var/camiant/iso</code>

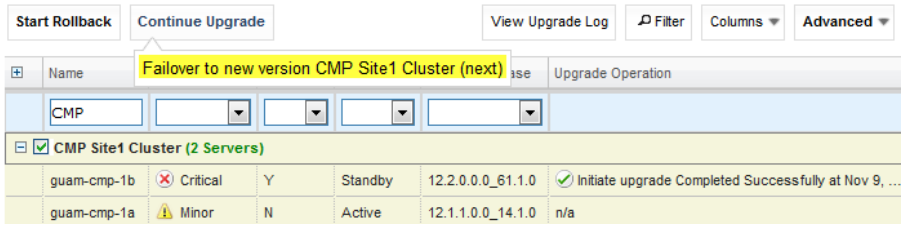
Highlight the available ISO and click the “Select incremental-upgrade-12.2…” button on the bottom of the pop-up window:
 

At the confirmation popup click OK.

Within a few seconds, the ‘Up to Date’ column transitions from ‘Y’ (meaning up-to-date) or</td></tr>
</table>

Step	Procedure	Result
		'N' (meaning needs upgrade).  Name / Alarm Severity / Up to Date / Server Role / Running Release CMP Site1 Cluster (2 Servers) guam-cmp-1b — N — Standby — 12.1.1.0.0_14.1.0 guam-cmp-1a — N — Active — 12.1.1.0.0_14.1.0
11. ☐	**CMP GUI**: Upgrade Primary CMP cluster	**Upgrade → Upgrade Manager** NOTE: The **Filter** button can be used to show only the CMP servers. Type *CMP* under **Name**.  Upgrade Manager Current ISO: incremental-upgrade-12.2.0.0.0_61.1.0 Start Rollback / Start Upgrade / View Upgrade Log / Filter / Columns / Advanced Name / Alarm Severity / Up to Date / Server Role / Running Release / Upgrade Operation CMP CMP Site1 Cluster (2 Servers) guam-cmp-1b — N — Standby — 12.1.1.0.0_14.1.0 — n/a guam-cmp-1a — N — Active — 12.1.1.0.0_14.1.0 — n/a • Click the checkbox for the Primary CMP Cluster • Click the 'Start Upgrade' button.  Upgrade Manager Current ISO: incremental-upgrade-12.2.0.0.0_61.1.0 Start Rollback / Start Upgrade / View Upgrade Log / Filter / Columns / Advanced Name / Alarm Severity / Up to Date / Server Role / Running Release / Upgrade Operation CMP CMP Site1 Cluster (2 Servers) guam-cmp-1b — N — Standby — 12.1.1.0.0_14.1.0 — n/a guam-cmp-1a — N — Active — 12.1.1.0.0_14.1.0 — n/a • Click "OK" to confirm and continue with the operation. • The specific action taken will be determined by the Upgrade Manager based on the specific version change being performed. • The first action will be to upgrade the standby server in the CMP Cluster. ***NOTE:*** *This will take approximately 30 minutes to complete.* • The "Upgrade Operation" column will show a progress bar along with the upgrade activities. • During the upgrade activities, the server being updated will 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

Step	Procedure	Result
		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…" shows under 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 12.2 and the other server in the cluster is on 12.1.x. The Up To Date column will show 'Y' for the 12.2 server and 'N' for the 12.1.x server.  The critical alarm 70025 ("The MySQL slave has a different schema version than the master" will be active as well as the minor alarms 70500 and 70501 "The system is running different versions of software" / "The cluster is running different versions of software."

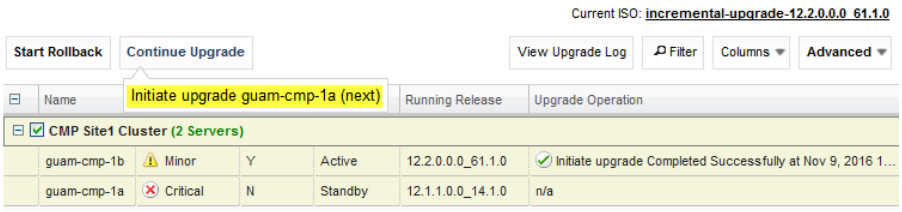
Step	Procedure	Result
13. ☐	**CMP GUI**: Continue upgrade on CMP cluster	**Upgrade → Upgrade Manager** • Make sure the checkbox for the Primary CMP Cluster is still checked • Click the 'Continue Upgrade' button. Notice the message "Failover to new version"  • Click "OK" to confirm and continue with the operation. • The specific action will take about a minute to complete.
14. ☐	**CMP GUI:** Re-login to the CMP VIP	• Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. • The Policy Release 12.2 CMP GUI login form should appear as shown – Login and password credentials are the same as the pre-upgrade. 
15. ☐	**CMP GUI:** Verify new Policy release	**Navigate to HELP→About.** Verify the release displayed is 12.2 

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>16. ☐</td><td>CMP GUI: Critical Alarms</td><td>Critical alarm 70025 and the minor alarms 70503, 70501, 70500 will still be seen.
These alarms are expected and will 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>17. ☐</td><td>CMP GUI: Verify the Policy Release 12.2 CMP is Active</td><td>Upgrade → Upgrade Manager
• Verify the following:
○ The Active server is running release 12.2
○ The Standby server is running the previous release

<table>
<tr><th></th><th>Name</th><th>Alarm Severity</th><th>Up to Date</th><th>Server Role</th><th>Running Release</th><th>Upgrade Operation</th></tr>
<tr><td></td><td colspan="6">CMP Site1 Cluster (2 Servers)</td></tr>
<tr><td></td><td>guam-cmp-1b</td><td>Minor</td><td>Y</td><td>Active</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at Nov 9, 2...</td></tr>
<tr><td></td><td>guam-cmp-1a</td><td>Critical</td><td>N</td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>n/a</td></tr>
</table>
</td></tr>
</table>

Step	Procedure	Result
18. ☐	**CMP GUI:** Complete the Upgrade of the Primary CMP Cluster	**Upgrade → Upgrade Manager** • Click the checkbox for the Primary CMP Cluster • Click the 'Continue Upgrade' button. Notice the message "Initiate upgrade *<standbyserver>* (next)"  Click OK on the pop-up to continue the upgrade on the remaining server in the CMP cluster NOTE: Remaining CMP server will take approximately 30 minutes to complete. NOTE: Server getting upgraded will go OOS **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

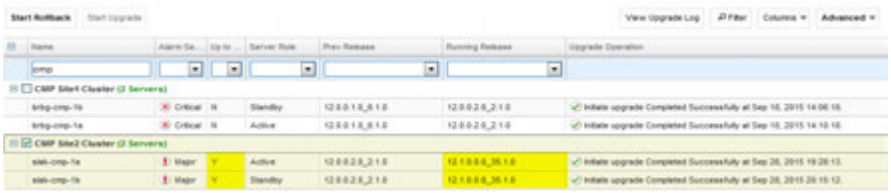
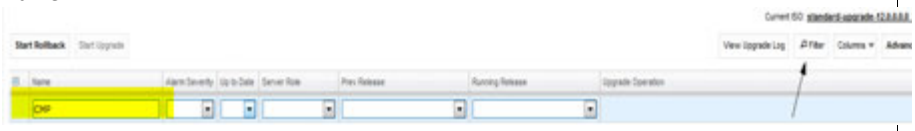
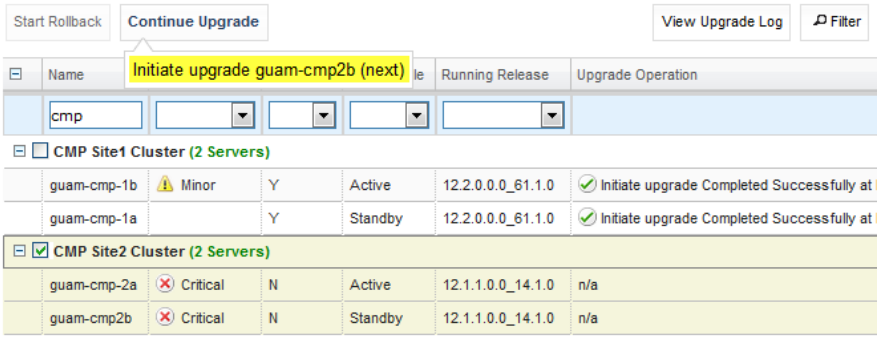
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>19. ☐</td><td>CMP GUI: Tracking the upgrade complete</td><td>Upgrade → Upgrade Manager

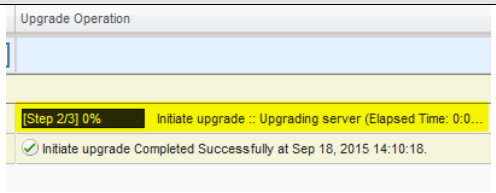
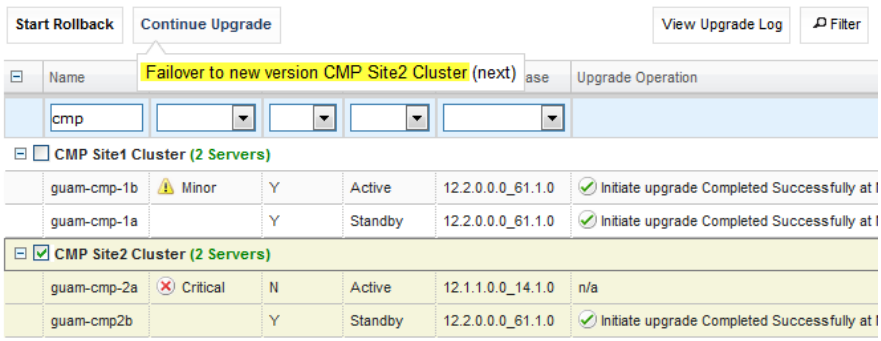
<u>The last step in the upgrade for the first CMP cluster will be to wait for replication to complete.</u>

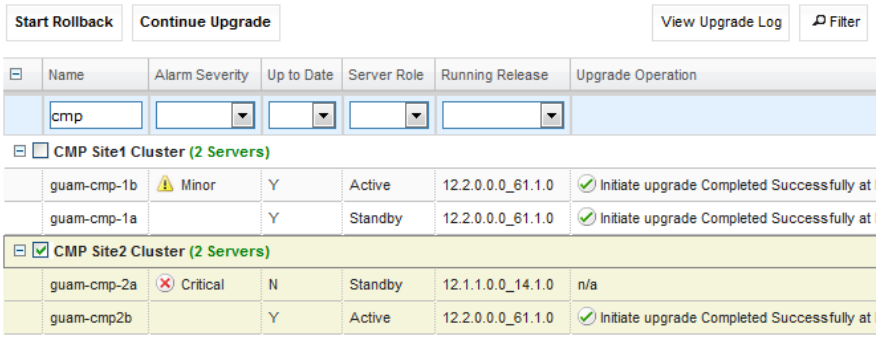
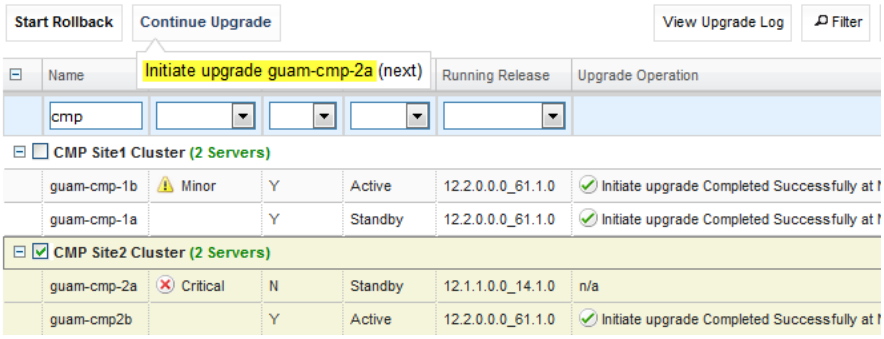
With the CMP cluster checkbox still checked, click on the “View Upgrade Log” button, a popup window will appear where you can verify that synchronization has taken place:

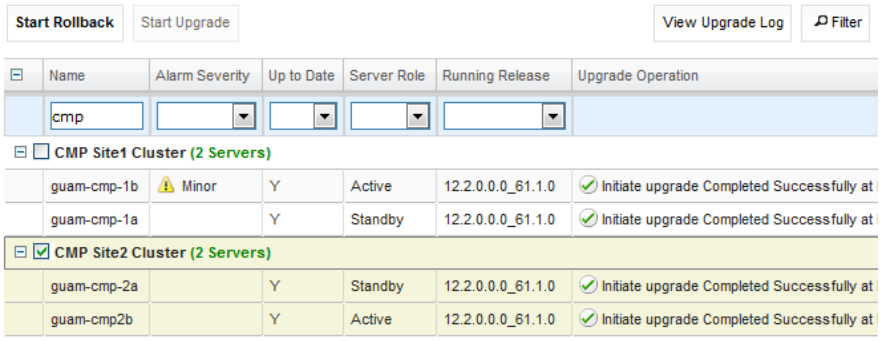
Upgrade Log
Cluster Name: CMP Site1 Cluster
Last Update: 11/10/2016 9:01:00
<table><tr><th>ID</th><th>Parent ID</th><th>Action Name</th><th>Duration</th><th>Scope</th><th>Hostname</th><th>Result</th><th>Mode</th></tr><tr><td>1</td><td>0</td><td>Preflight Check</td><td>0:00:15</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Manual</td></tr><tr><td>2</td><td>1</td><td>Upgrading server</td><td>0:22:00</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Automatic</td></tr><tr><td>3</td><td>1</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr><tr><td>4</td><td>1</td><td>Wait for replication to synchronize</td><td>0:00:09</td><td>Server</td><td>guam-cmp-1b</td><td>Success</td><td>Automatic</td></tr><tr><td>5</td><td>0</td><td>Failover to new version</td><td>0:00:00</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Manual</td></tr><tr><td>6</td><td>0</td><td>Preflight Check</td><td>0:00:15</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Manual</td></tr><tr><td>7</td><td>6</td><td>Upgrading server</td><td>0:21:50</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Automatic</td></tr><tr><td>8</td><td>6</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr><tr><td>9</td><td>6</td><td>Wait for replication to synchronize</td><td>0:00:29</td><td>Server</td><td>guam-cmp-1a</td><td>Success</td><td>Automatic</td></tr><tr><td>10</td><td>6</td><td>Modify the role/replication attributes of the server</td><td>0:00:01</td><td>Cluster</td><td>CMP Site1 Cluster</td><td>Success</td><td>Automatic</td></tr></table></td></tr>
<tr><td>20. ☐</td><td>CMP GUI: Verify the status of the upgraded CMP server.</td><td>Upgrade → Upgrade Manager
<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><th>Upgrade Operation</th></tr><tr><td colspan="7">CMP Site1 Cluster (2 Servers)</td></tr><tr><td>guam-cmp-1b</td><td>Minor</td><td>Y</td><td>Active</td><td>12.1.1.0.0_14.1.0</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at...</td></tr><tr><td>guam-cmp-1a</td><td></td><td>Y</td><td>Standby</td><td>12.1.1.0.0_14.1.0</td><td>12.2.0.0.0_61.1.0</td><td>Initiate upgrade Completed Successfully at...</td></tr></table>
Successful upgrade status will now show both servers running the Release 12.2 under the “Running Release” column and ‘Y’ for both servers under the ‘Up To Date’ column
Active/standby state for both servers in the Primary CMP Cluster.</td></tr>
<tr><td>21. ☐</td><td>Proceed to next upgrade procedure</td><td>At this point, the primary site is running Release 12.2
The Secondary site, if it exists, is still on release 12.1.x
Proceed to the next procedure to upgrade the secondary CMP cluster.</td></tr>
<tr><td colspan="3">THIS PROCEDURE HAS BEEN COMPLETED</td></tr>
</table>

5.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Status of CMP Cluster	**Upgrade → Upgrade Manager** - Primary CMP is completely upgraded to 12.2 - Secondary CMP Cluster is on 12.1.x 
2. ☐	**CMP GUI**: Upgrade Secondary CMP cluster	**Upgrade → Upgrade Manager** NOTE: The Filter button can be used to show only the CMP servers. Type in CMP under Name.  • Click the checkbox for the Secondary CMP Cluster at Site2 • Click the 'Continue Upgrade' Button.  • Click "OK" to confirm and continue with the operation. • The specific action taken will be determined by the Upgrade Manager based on the specific version change being performed. • This will continue to upgrade the standby server only in the CMP Cluster • ***NOTE:*** *This will take ~30 minutes to complete.* • Under "Upgrade Operation" column, it will show the In Progress status along with the upgrade activities.

Step	Procedure	Result
		 • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events - **Expected Critical alarm:** **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
3. ☐	**CMP GUI**: Continue Upgrade Secondary CMP cluster	**Upgrade → Upgrade Manager** • Click the checkbox for the Secondary CMP Server Cluster at Site2 • Click the 'Continue Upgrade' Button. Notice the message "Failover to new version CMP Site2 Cluster"  • Click "Ok" to confirm and continue with the operation, • The specific action will take a minute to complete. Wait until the newly upgraded server is active, running 12.2 as shown below.

Step	Procedure	Result
		 • Click the checkbox for the Secondary CMP Server Cluster at Site2 • Click the 'Continue Upgrade' button. When hovering over the continue upgrade button, the message will display the next action, which is upgrading the remaining CMP in standby, still running 12.1.x  • Click "OK" to confirm and continue with the operation, • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events - **Expected Critical alarm:** **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
4. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	**Upgrade → Upgrade Manager** • Successful upgrade status will show the Release 12.2 under the "Running Release" column. • The "Upgrade Operation" column will show "Inititiate Upgrade Completed

Step	Procedure	Result
		Successfully at…" 
5. ☐	**CMP GUI:** Verify Alarms	**System Wide Reports → Alarms → Active Alarms:** **Expected Minor Alarms:** **70500** Upgrade Director System Mixed Version
6. ☐	Procedure is complete.	• All CMP Clusters Upgrade are complete and running Release 12.2. • ALL MRAs and MPEs are on Release 12.1.x At this point, the Policy Management system is running in mixed-version mode.

6. UPGRADE NON-CMP CLUSTERS (MPE, MRA)

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

NOTES:

1. An upgrade of up to 8 clusters can be running at the same time.
2. 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.

6.1 Site/Segment Upgrade Preparation

6.1.1 Configuration Preparation

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into CMP server	• Use the supported browser to login as *admin* or user with admin privileges.
2. ☐	**CMP GUI:** Verify Current Upgrade Manager status and Software Release 12.2 ISO files	**Upgrade → Upgrade Manager** • Verify that all CMP Clusters have both Active, Standby status. • Verify that all MPE & MRA Clusters have both Active, Standby. • Verify that the CMP cluster is upgraded successfully and running Policy Release 12.2 **Upgrade -> ISO Maintenance** • Verify that Policy release 12.2 ISO files are available for all clusters. One ISO per server
THIS PROCEDURE HAS BEEN COMPLETED		

6.2 Upgrade non-CMP Clusters

This procedure will upgrade one or more non-CMP clusters at a site/segment.

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

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

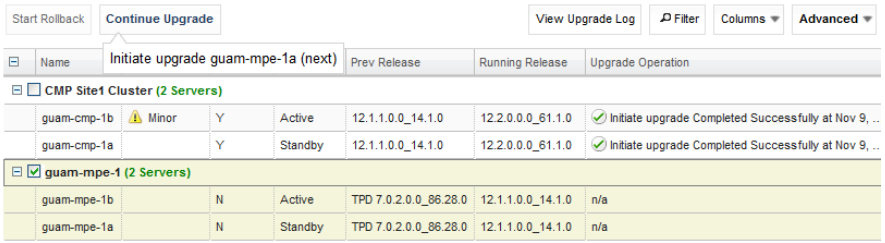
Up to eight clusters can be upgraded in parallel.

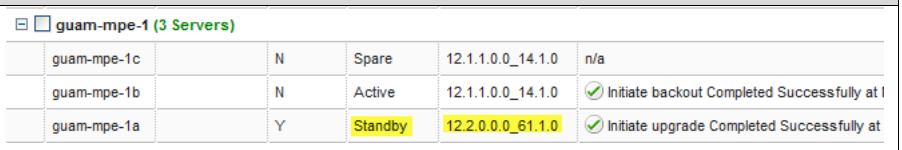
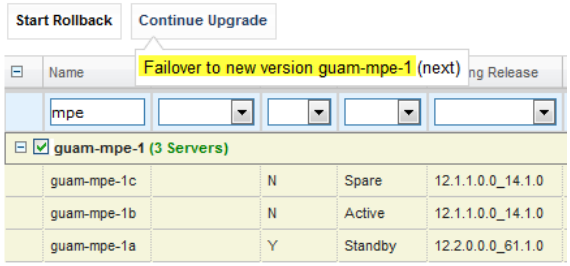
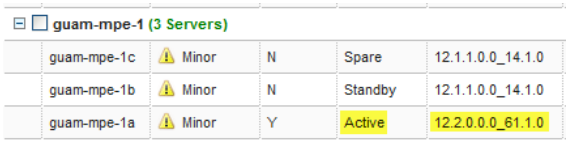
1) Select and start upgrade on Standby server
2) Failover
3) Re-apply configuration
4) Continue upgrade on remaining server

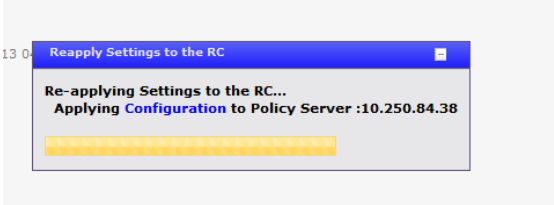
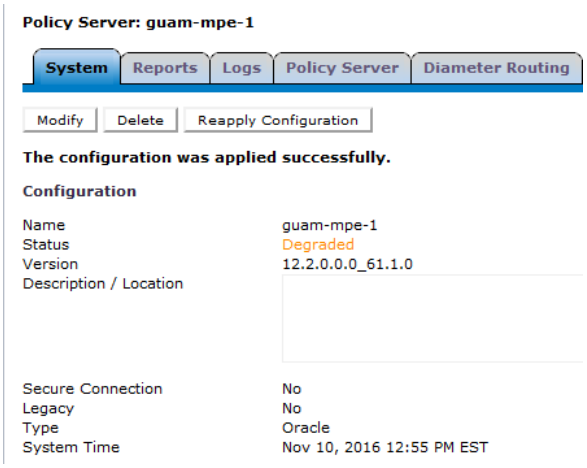
NOTES:

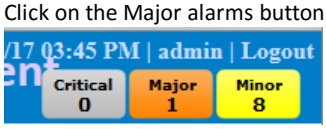
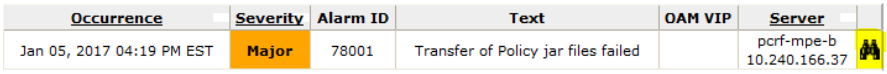
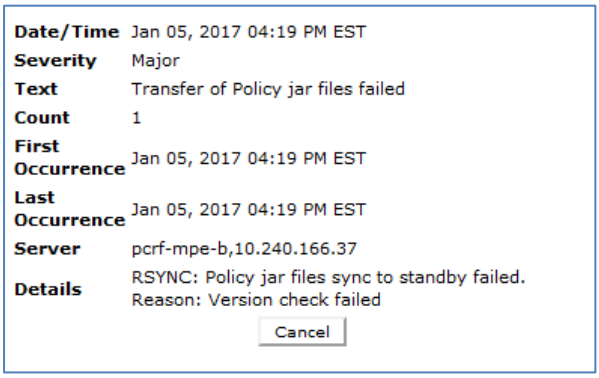
- **All CMP clusters have been upgraded to Policy release 12.2 before executing the following procedures.**
- **The maximum clusters to be running the upgrade at one time is 8.**
- **Only ONE Cluster can be selected for upgrade activity, 'bulk selection' of servers is not supported in release 12.2**

Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the servers to be upgraded	• Perform the following: - Check for current active alarms - Reset server counters to make a baseline For the MPE: **Policy Server→Configuration→Reports → Reset Counters** For the MRA: **MRA→Configuration→Reports → Reset Counters** - Check KPI Dashboard *(capture and save screenshot to a file)*
2. ☐	**CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment	**Upgrade →Upgrade Manager** • Verify information for the MRAs/MPEs: - **Current Release 12.1.x installed** - **Running with Active/Standby status** **Upgrade → ISO Maintenance** - Verify the ISO version to be deployed is 12.2 ☐ Name | Appl Type | IP | Running Release | ISO CMP Site1 Cluster | CMP Site1 Cluster guam-cmp-1a | CMP Site1 Cluster | 10.240.152.75 | 12.2.0.0.0_61.1.0 | cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%] guam-cmp-1b | CMP Site1 Cluster | 10.240.152.76 | 12.2.0.0.0_61.1.0 | cmp-12.2.0.0.0_61.1.0-x86_64.iso[100%] guam-mpe-1 | MPE guam-mpe-1a | MPE | 10.240.152.79 | 12.1.1.0.0_14.1.0 | mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%] guam-mpe-1b | MPE | 10.240.152.80 | 12.1.1.0.0_14.1.0 | mpe-12.2.0.0.0_61.1.0-x86_64.iso[100%] guam-mra-1 | MRA guam-mra-1a | MRA | 10.240.152.77 | 12.1.1.0.0_14.1.0 | mra-12.2.0.0.0_61.1.0-x86_64.iso[100%] guam-mra-1b | MRA | 10.240.152.78 | 12.1.1.0.0_14.1.0 | mra-12.2.0.0.0_61.1.0-x86_64.iso[100%]

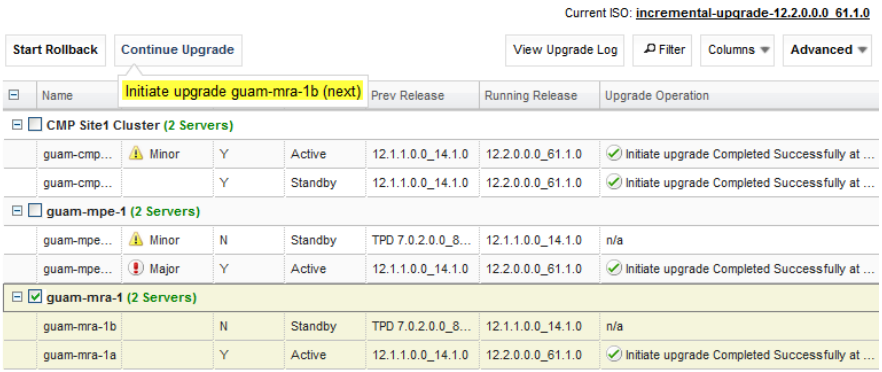
Step	Procedure	Result
3. ☐	**CMP GUI**: Upgrade clusters ***NOTE:*** *Each upgrade of one blade server will take ~35 minutes to complete.*	**Start the upgrade on ONE cluster. Wait until the cluster shows "OOS", then continue with the next cluster and so on. Up to 8 clusters maximum may be running upgrade at any one time.** **Upgrade → Upgrade Manager** • Click the checkbox for the desired cluster (one cluster at a time.) It can be an MRA or an MPE. • Click the 'Continue Upgrade' Button  • Click "OK" to confirm and continue with the operation. It will begin to upgrade the standby server of that cluster. • Wait until the standby server reports "OOS" before selecting the next cluster • Follow the progress status under the "Upgrade Operation" column. • During the upgrade activities, the following alarms may be generated and considered normal reporting events – these will be cleared after the clusters are completely upgraded. **Expected Critical Alarms:** **31283** High availability server is offline **70001** QP_procmgr failed **31227** High availability status failed **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 message "Initiate upgrade completed successfully at…" shows under the 'Upgrade Operation' column. The server will go back to 'standby' state when the upgrade completes.

Step	Procedure	Result
		 • 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
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** • Click the checkbox for the cluster (one cluster at a time). It can be an MRA or MPE. • Click the 'Continue Upgrade' button. When hovering over the continue upgrade button, it will say 'Failover to new version'  • Click "OK" to confirm and continue with the operation. It will begin to failover the cluster. • Wait until failover completes, i.e., the server running 12.2 is now Active, before failing over the next cluster. 
5. ☐	**CMP GUI:** Reapply configuration on the MPE/MRA cluster that failed over successfully.	**For MPE: Policy Server → Configuration → *<MPE cluster>* → System Tab** **For MRA: MRA→Configuration →*<MRA cluster>*→System tab** • The selected cluster will have the status shown as "Degraded" still showing the old release version. 'Config mismatch' may be displayed as well. • Select "Reapply Configuration" operation. • NOTE, a progress banner appears for the MPE reapply configuration and NOT the MRA reapply configuration

Step	Procedure	Result
		 • Verify that the "Version" is successfully changed to the upgraded Release 12.2 • The cluster will still show the "Degraded" status: 
6. ☐	**CMP GUI**: Current alarms	**Some of the alarms below may appear:** **Expected Critical alarm** None **Expected Major Alarm** 78001 Rsync Failed **Expected Minor Alarms:** **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 **78001** RSYNC Failed **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: • Select the checkbox for the partially upgraded cluster, and select **Operations → Rollback.** • The pre-12.2 MPE server should become active and resume handling traffic.

Step	Procedure	Result
8 ☐	**CMP GUI:** Reapply configuration	• **Policy Server → Configuration → <mpe_cluster name> → System tab** or **MRA → Configuration → <mra_cluster name> → System tab** • Click **Reapply Configuration** • Verify that the version is changed back to 12.1.x, and the action report success. • If NOT, stop and contact Oracle support to back out of the partially upgraded cluster.
9. ☐	**CMP GUI: 78001 Major Alarm**	During the upgrade activities, *Major* alarm 78001 in particular may be generated. And even though it's a normal event, the alarm will not clear by itself. Before continuing we should make sure that the alarm is cleared. Click on the Major alarms button in the upper right part to display the alarms:  Now click on the binoculars icon on the right to display details about the 78001 Major alarm  You should see in the last line of the details that the reason for the major alarm is "Version check failed".  If you see a different reason, stop and contact My Oracle Support. If you see the "Version check failed" reason, continue here. Navigate to System Wide Reports > Alarms > Active Alarms and select the 78001 Major alarm  Click on the trash can icon on the right to clear this alarm.
10. ☐	**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 8 clusters may be running upgrade at one time.** **Upgrade → Upgrade Manager** • Click the checkbox for a cluster (one cluster at a time), it can be an MRA or an MPE. • Click the 'Continue Upgrade' button. When hovering over the continue upgrade button, it will say 'Initiate upgrade…' on the standby server

Step	Procedure	Result



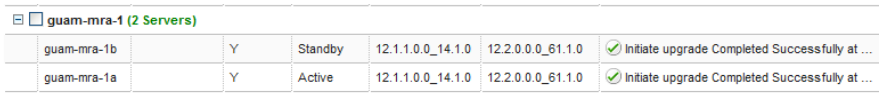
- Click “OK” to confirm and continue with the operation. It will begin the final server upgrade of the cluster
- If you plan to perform the upgrade for several clusters in parallel (up to 4), wait until the server being upgraded changes to “OOS” before moving on to the next cluster
- Follow the progress status under the ”Upgrade Operation” column.
- During the upgrade activities, the following alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely upgraded.

Expected Critical Alarms:
31283 High availability server is offline
31227 High availability Status Failed
70001 QP_procmgr failed

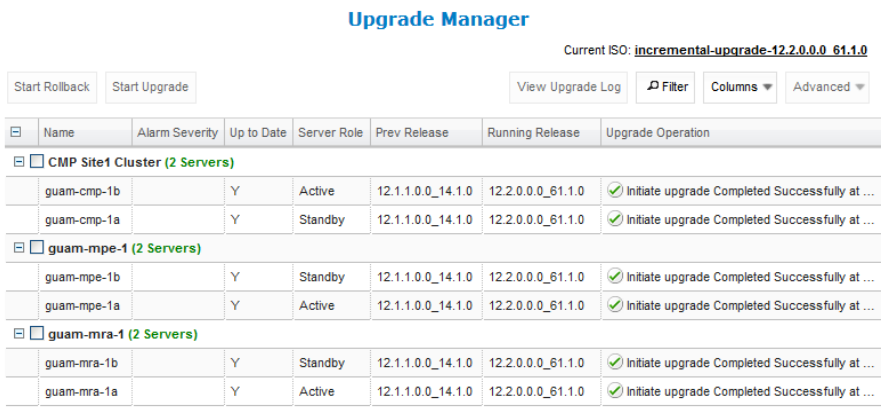
Expected Major Alarm:
70004 QP Processes down for maintenance

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
78001 RSYNC Failed
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 message “Initiate upgrade completed successfully at…” appears under the ‘Upgrade Operation’ Column. The server will go back to ‘Standby’ state and the Up to Date column will show a Y (YES)

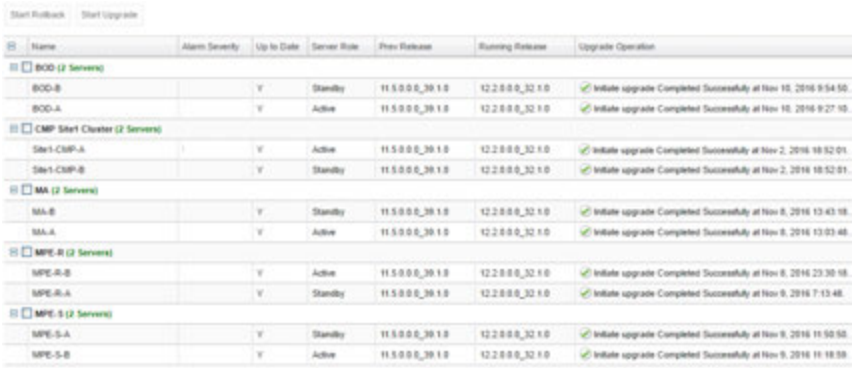


Possible alarms:
Minor:
70500

Step	Procedure	Result
11. ☐	REPEAT the above Steps (1) – (10) for next MPE/MRA cluster(s)	• Proceed with the next cluster(s) until all clusters have been upgraded 
THIS PROCEDURE HAS BEEN COMPLETED		

7. POST UPGRADE HEALTH CHECK

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

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

Verify all clusters and servers are in OK state.

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

Cable:
 
</td></tr>
<tr><td>5 ☐</td><td>Verify System Health</td><td>Use the command sudo syscheck on every server. Verify that each class test returns “OK”.

<code>$ sudo syscheck</code>

LOG LOCATION: /var/TKLC/log/syscheck/fail_log</td></tr>
<tr><td colspan="3">THIS PROCEDURE HAS BEEN COMPLETED</td></tr>
</table>

8. BACKOUT (ROLLBACK)

This procedure is executed if an issue is found during the upgrade, or during the post-upgrade if somethings impacts network performance.

The Policy system will be backed out to the previous release.

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

8.1 Backout Sequence

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

1. Backout MRA/MPE
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 needs to be maintained even if there are unexpected failures.

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

8.2 Pre-requisites

1) No new policies or features have been configured or executed on the upgraded release.
2) The CMP cluster cannot be backed out if other Policy servers (MPEs & MRAs) are still on the upgraded release.

8.3 Backout of Fully Upgraded Cluster

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

This procedure is used to backout a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster will be on pre-12.2 release with Active/Standby status.

Expected pre-conditions:

1. The primary active CMP is on release 12.2
2. The cluster servers to be backed out are all on release 12.2
3. One server of target cluster is on Release 12.2 in "Active" role
4. One server of target cluster is on Release 12.2 in either "Standby" or "Force Standby"

8.3.1 Backout Sequence

This procedure applies to a cluster. The non-CMP cluster types (MRA, MPE) will be in non-georedundant mode with active and 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, you must click one cluster at a time, staggering by about 1 minute each.

Overview on Backout/Rollback MRA/MPE cluster:

1) Back out of the standby server
2) Fail over
3) Back out of the new standby server

Backout Secondary CMP (if applicable):

NOTE:

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

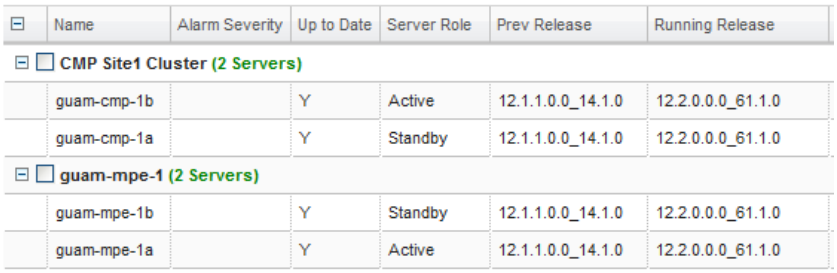
1) Use the CMP Upgrade Manager to backout the Secondary CMP Cluster

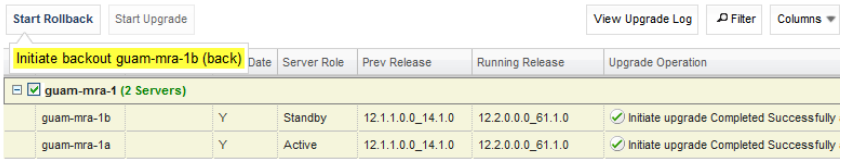
Backout the Primary CMP:

1) Use the CMP Upgrade Manager to backout the CMP Cluster

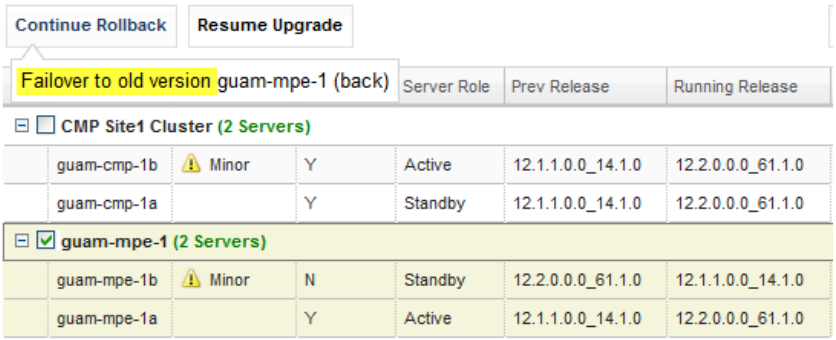
8.3.2 Backout Fully Upgraded MPE/MRA Cluster

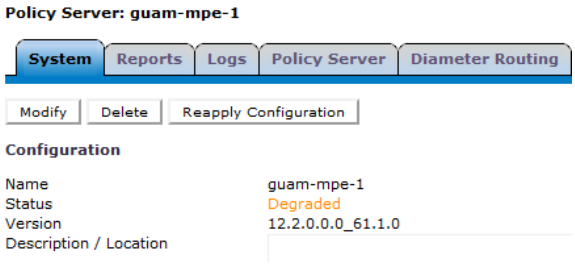
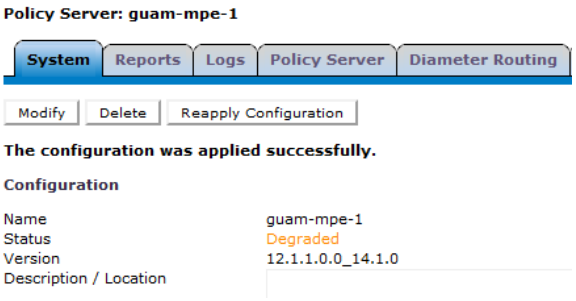
Step	Procedure	Result

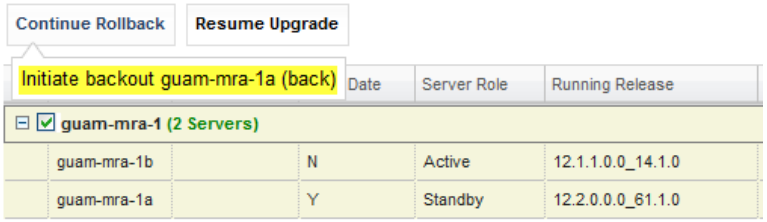
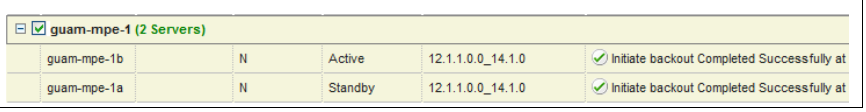
1. ☐	**CMP GUI:** Verify the status of affected clusters	**Upgrade → Upgrade Manager**
		• Confirm status of the cluster to be backed out
		  ○ Primary CMP is on Release 12.2
		  ○ All Standby servers are on Release 12.2
		  ○ Up to Date column shows 'Y' for all servers
		EXAMPLE:
		 

2. ☐	**CMP GUI**: Rollback standby MPE/MRA clusters ***NOTE:*** *Each backout of one blade server will approximately be completed within 40 minutes time.* ***NOTE:*** *Up to 8 upgraded clusters can be backed out at the same time, selecting one at a time.*	**Upgrade → Upgrade Manager** • Click the checkbox for the MPE or MRA cluster to be backed out • Click the 'Start Rollback' Button. When hovering over the button, it will inform you of the server to get backed out, in this case it will be the current standby server.  • Select "OK" to confirm and continue with the operation. It will begin to backout. • Follow the progress status under the "Upgrade Operation" column. • At this point, the server backing out will go into 'OOS' state • Wait until the server goes to an OOS state before selecting the next cluster to backout. • During the backout activities, the following alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **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 **31233** HA Path Down **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby

Step	Procedure	Result
		70507 Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **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 **31282** HA Management Fault • Backout of the server is complete when the message "Initiate backout completed successfully at…" shows under the 'Upgrade Operation' Column. The backed out server will show running the previous release and return to standby with an N in the Up to Date column.

Step	Procedure	Result
3. ☐	**CMP GUI**: Continue the backout of the MRA/MPE clusters. Next operation is « failover» to the server in the previous release. ***NOTE:*** *Up to 8 Clusters can be backed out at the same time, selecting one at a time.*	• Select the cluster to backout. Current state of the cluster needs to be as follows: Active server on 12.2 Release Standby server on pre-12.2 Release Some minor alarms (e.g., 70501 Cluster running different versions of software) are normal at this point. **Upgrade → Upgrade Manager** • Select the checkbox for the cluster • Select the 'Continue Rollback' button. When hovering over the button, it will inform that the next step is to fail over to the old version  • Select "OK" to confirm and continue with the operation. It will begin to failover. • Wait until the server fails over before selecting the next cluster. This will take a minute or two. **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 **31233** HA Path Down **31126** Audit Blocked **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 **78001** RSYNC Failed **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 **31282** HA Management Fault

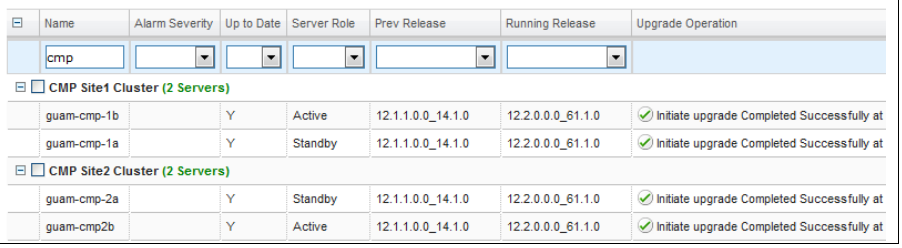
Step	Procedure	Result
4. ☐	**CMP GUI:** Reapply configuration on MPE/MRA cluster that completed the failover successfully.	**For MPE: Policy Server → Configuration → *<MPE cluster>* → System tab** **For MRA: MRA→Configuration→*<MRA cluster>*→System tab** • The selected cluster will have the status shown as "Degraded" running version 12.2  **Policy Server: guam-mpe-1** System Reports Logs Policy Server Diameter Routing Modify Delete Reapply Configuration **Configuration** Name guam-mpe-1 Status Degraded Version 12.2.0.0.0_61.1.0 Description / Location • Click "Reapply Configuration" - **The MPE will show a dialog box showing progress of the reapply, the MRA will not show anything.** • Note the "Version" is successfully changed to the previous release, for example 12.1.1  **Policy Server: guam-mpe-1** System Reports Logs Policy Server Diameter Routing Modify Delete Reapply Configuration **The configuration was applied successfully.** **Configuration** Name guam-mpe-1 Status Degraded Version 12.1.1.0.0_14.1.0 Description / Location **NOTE:** *The status still " shown as "Degraded" is a normal reporting event as the servers are in different status.*

Step	Procedure	Result
5. ☐	**CMP GUI**: Complete backout of cluster(s) ***NOTE:*** *Each backout of one blade server will approximately be completed within 35 minutes time.* .	**Select the partially backed out cluster** **Upgrade → Upgrade Manager** • Select the checkbox for the cluster • Select the 'Continue Rollback' button. When hovering over the button, it will inform you that the standy server running 12.2 will be backed out.  • Select "OK" to confirm and continue with the operation. • Follow the progress status under the "Upgrade Operation" column. • During the backout activities, the following alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit Blocked **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **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 **31282** HA Management Fault • Backout of the server is complete when the message "Initiate backout completed successfully at…" shows under the 'Upgrade Operation' Column. **Both servers in this cluster will be on a pre-12.2 release at this point and show active/standby.** 

Step	Procedure	Result
6. ☐		**Repeat this procedure for the remainder of the MPE/MRA servers, if necessary.**
THIS PROCEDURE HAS BEEN COMPLETED		

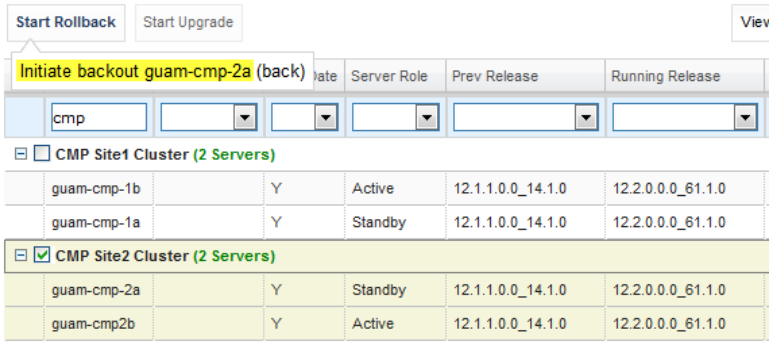
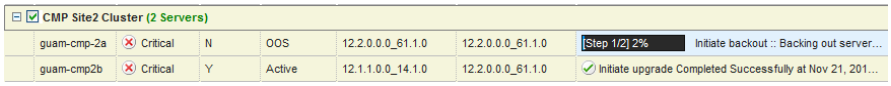
8.3.3 Backout Fully Upgraded Secondary CMP Cluster

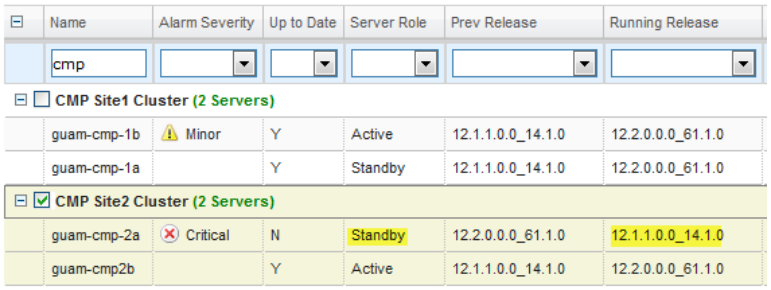
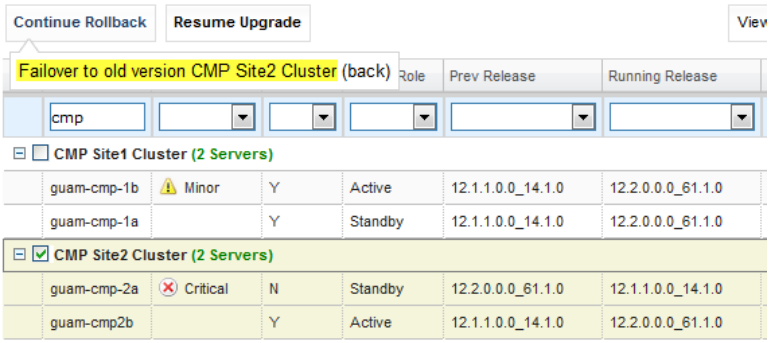
NOTE: The Secondary CMP Site2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site1 cluster.

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP Clusters	**Upgrade Manager → System Maintenance** • Confirm status of the cluster to be backed out: o Primary CMP is on Release 12.2 o All other non-CMP clusters are on a 12.1.x release o Up to Date Column shows 'Y' for all servers The Filter button can be used to show only CMP servers. Enter 'cmp' in the box as shown below *EXAMPLE:* 

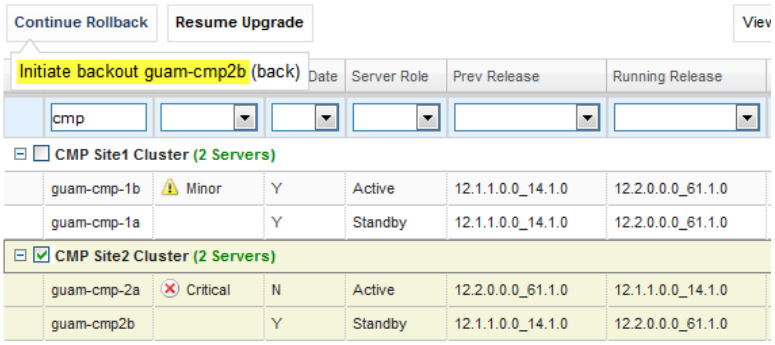
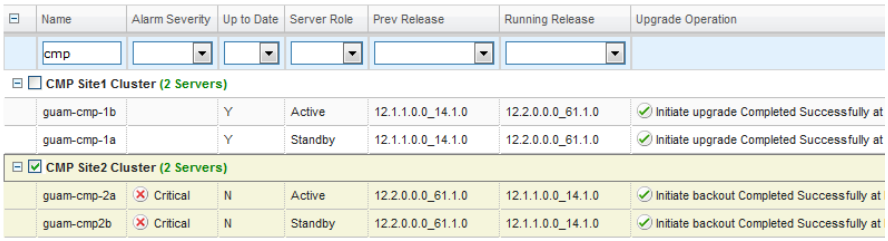
Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
cmp						
CMP Site1 Cluster (2 Servers)						
guam-cmp-1b		Y	Active	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-cmp-1a		Y	Standby	12.1.1.0.0_14.1.0	12.2.0.0.0_61.1.0	Initiate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

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

Step	Procedure	Result
2. ☐	**CMP GUI**: backout secondary cmp cluster ***NOTE:*** *Each backout of one server will take ~40 minutes to complete.*	**Upgrade → Upgrade Manager** • Select the checkbox for the secondary CMP Cluster • Select the 'Start Rollback' Button. When hovering over the button, it will inform you that the standby server will be backed out.  • Select "OK" to confirm and continue with the operation. It will begin to backout. Server will go in an 'OOS' server role • Follow the progress status under the "Upgrade Operation" column.  • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **70025** The MySQL slave has a different schema version than the master. **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit Blocked **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **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 **31282** HA Management Fault

NOTE: The Secondary CMP Site2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site1 cluster.		
Step	**Procedure**	**Result**
		• Backout of the server is complete when the following message ("Initiate backout completed successfully at…") shows under the 'Upgrade Operation' Column. The server will go back to standby state and show the previous release 
3. ☐	**CMP GUI**: Continue the backout. Next Operation is "failover"	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP cluster • Select the 'Continue Rollback' Button. When hovering over the button, it will inform you it will failover to the previous version.  • Select "OK" to confirm and continue with the operation. It will begin to failover. • Wait until the previous release becomes active before continuing **Expected Critical alarm:** **70025** QP Slave database is a different version than the master **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70500** Upgrade Director System Mixed Version

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

Step	Procedure	Result
4. ☐	**CMP GUI**: Continue the backout. Next Operation is « initiate backout»	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP cluster • Select the 'Continue Rollback' Button. When hovering over the button, it will inform you it will back out the new standby server  • Select "OK" to confirm and continue with the operation. • Follow the progress status under the 'Upgrade Operation' Column. **Expected Critical alarm:** **70025** QP Slave database is a different version than the master **Expected Minor Alarms:** **70500** Upgrade Director System Mixed Version The procedure ends when both Secondary CMP servers are in the previous release.  S
THIS PROCEDURE HAS BEEN COMPLETED		

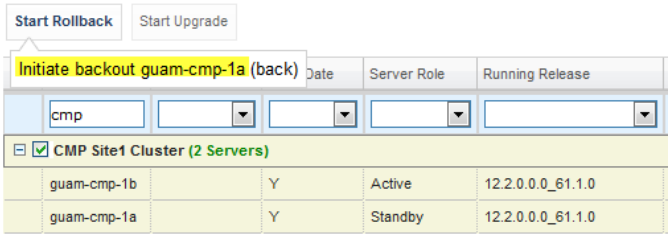
8.3.4 Backout Fully Upgraded Primary CMP Cluster

NOTE: For backout to a release prior to 12.1.x, the Primary CMP Site1 cluster uses both the Upgrade Manager and the pre-12.1.x System Maintenance option for backout. For backout to 12.1.x, you need only use the Upgrade Manager.

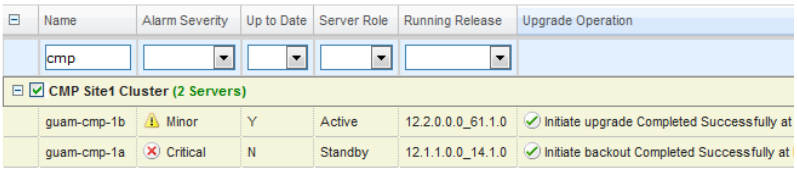
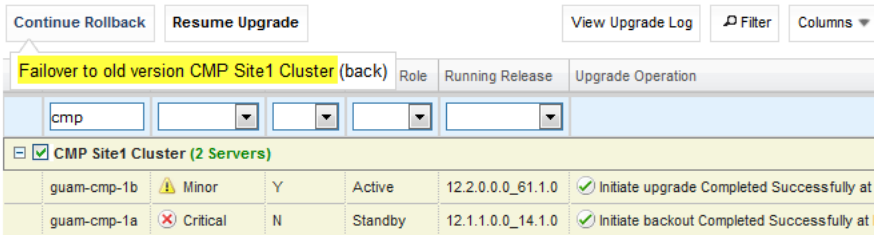
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of the CMP Clusters	**Upgrade Manager → System Maintenance** • Confirm status of the Primary CMP cluster: o Primary CMP cluster is on Release 12.2 o Secondary CMP Cluster (if present) is already on pre-12.2 Release o Up to Date Column shows 'Y' for all servers in Primary CMP Cluster *EXAMPLE:*

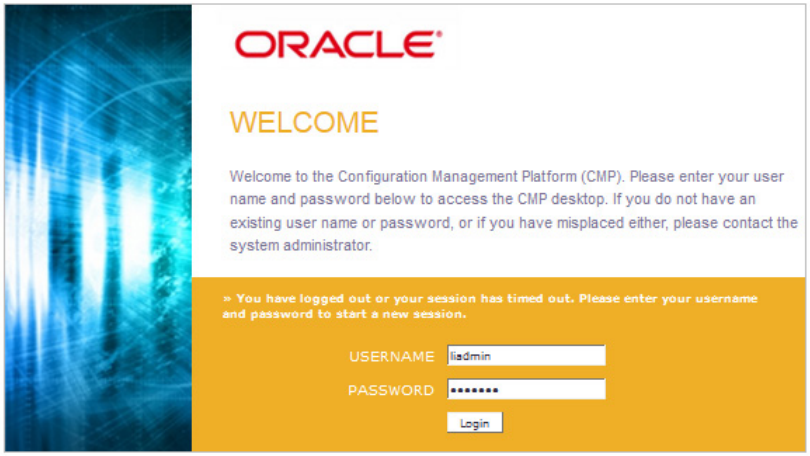
Name	Alarm Severity	Up to Date	Server Role	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)					
guam-cmp-1b		Y	Active	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
guam-cmp-1a		Y	Standby	12.2.0.0.0_61.1.0	Initiate upgrade Completed Successfully at
CMP Site2 Cluster (2 Servers)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

NOTE: For backout to a release prior to 12.1.x, the Primary CMP Site1 cluster uses both the Upgrade Manager and the pre-12.1.x System Maintenance option for backout. For backout to 12.1.x, you need only use the Upgrade Manager.

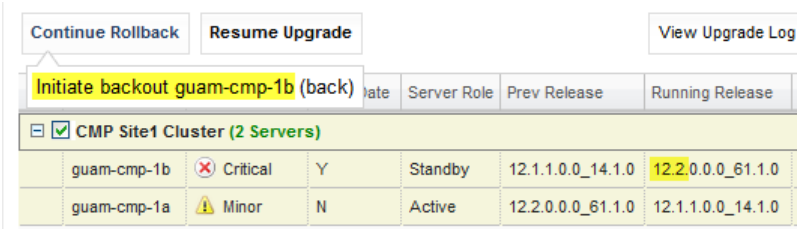
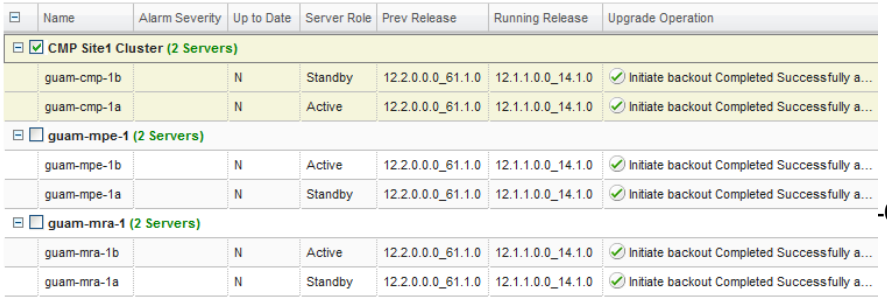
Step	Procedure	Result
2. ☐	**CMP GUI**: backout standby Primary CMP cluster ***NOTE:*** *backout of one server will take ~40 minutes to complete.*	**Upgrade → Upgrade Manager** • Use the Filter button and enter 'cmp' in the box to display CMP clusters only • Select the checkbox for the Primary CMP Cluster • Select the 'Start Rollback' Button. When hovering over the button, it will inform you that the standby server will be backed out.  • Select "OK" to confirm and continue with the operation. It will begin to backout. Server will go in an 'OOS' Server Role • Follow the progress status under the "Upgrade Operation" column. • During the backout activities, the following alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **31236** HA Link Down **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms:** **31114** DB Replication over SOAP has failed **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 **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited

NOTE: For backout to a release prior to 12.1.x, the Primary CMP Site1 cluster uses both the Upgrade Manager and the pre-12.1.x System Maintenance option for backout. For backout to 12.1.x, you need only use the Upgrade Manager.

Step	Procedure	Result
3. ☐		• Backout of the server is complete when the message "Initiate backout completed successfully at…" shows under the 'Upgrade Operation' Column. The server will go back to standby state and show the previous release. 
4. ☐	**CMP GUI**: Continue the backout. Next operation is « failover»	**Select Primary CMP Cluster.** **Upgrade → Upgrade Manager** • Click the checkbox for the Primary CMP cluster • Click the 'Continue Rollback' button. When hovering over the button, it will inform you that the next action is to fail over to the old CMP version.  • Select "OK" to confirm and continue with the operation. It will begin to failover. • **Failover takes a couple minutes.** • **Alarm 70025 "The MySQL slave has different schema version than the master" will appear.**

NOTE: For backout to a release prior to 12.1.x, the Primary CMP Site1 cluster uses both the Upgrade Manager and the pre-12.1.x System Maintenance option for backout. For backout to 12.1.x, you need only use the Upgrade Manager.		
Step	**Procedure**	**Result**
5. ☐	**CMP GUI**: Log back in to the Primary CMP VIP	**After failover, you will be required to log back in to the CMP GUI using the Primary CMP VIP.** 
6. ☐	**CMP GUI:** Verify release	**Navigate to help→About. Verify the proper pre-12.2 release number is displayed**

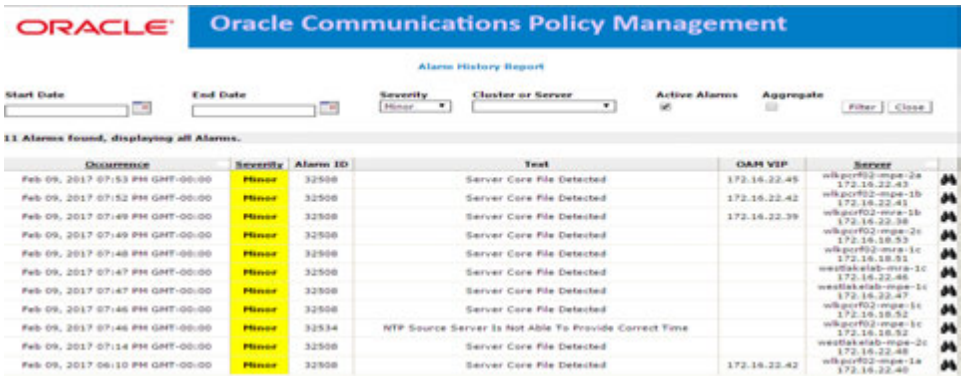
NOTE: For backout to a release prior to 12.1.x, the Primary CMP Site1 cluster uses both the Upgrade Manager and the pre-12.1.x System Maintenance option for backout. For backout to 12.1.x, you need only use the Upgrade Manager.

Step	Procedure	Result
7. ☐	**CMP GUI (Release 12.1.x)**: Continue the backout of the Primary CMP Cluster ***NOTE:*** *backout of one server will take ~40 minutes to complete.*	**Select Primary CMP cluster to complete the backout.** **Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP Cluster • Select the 'Continue Rollback' button. When hovering over the button, it will inform you that the standby server still running 12.2 will be backed out  • Select "OK" to confirm and continue with the operation. It will begin to backout. Server will go in an 'OOS' Server Role • Follow the progress status under the "Upgrade Operation" column. • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** 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 **78001** RSYNC Failed **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 • Backout of the server is complete when the message "Initiate backout completed successfully at…" shows under the 'Upgrade Operation' Column. The server will go back to standby state and show the previous release:  All backout-related alarms should also be cleared.

NOTE: For backout to a release prior to 12.1.x, the Primary CMP Site1 cluster uses both the Upgrade Manager and the pre-12.1.x System Maintenance option for backout. For backout to 12.1.x, you need only use the Upgrade Manager.		
Step	**Procedure**	**Result**
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX A. CORRECTING SERVER CORE FILE DETECTED ALARMS

Appendix A: Correcting Server Core File Detected Alarms

S T E P #	After the upgrades, if old core file detected alarms are generated, this procedure corrects these alarms. This procedure should be performed during a maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE. NOTE: THIS PROCEDURE SHOULD TAKE APPROXIMATELY 10 MINUTES PER BLADE OR RMS SERVER.	
1. ☐	**CMP GUI: Login into the CMP GUI using VIP address as 'admin' or user with admin privileges**	Login into the PCRF CMP GUI as **'admin'** using the VIP IP Address
2. ☐	**CMP GUI:** Verify active alarms	In the upper right hand corner of the GUI, click on Minor alarms and check if **'Server Core File Detected'** alarm(s) are present.  If **'Server Core File Detected'** alarms are present, then proceed to the next step, otherwise **Stop** and there is no need to perform this procedure.
3. ☐	**CMP GUI:** Note down the server IP(s) for which **'Server Core File Detected'** alarm was generated	Note down the server IP addresses for which **'Server Core File Detected'** alarm was generated.

4. ☐	**SSH CLI:** Login to each of the servers and verify that core files are present	Login as **'admusr'** to each of the noted servers using SSH
		Change the user to **'root'** and change directory to **/var/TKLC/core**
		`$ sudo su -`
		`# cd /var/TKLC/core`
		`# ls`
		Example:
		core.java.9499 core.java.9499.bt

Appendix A: Correcting Server Core File Detected Alarms

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

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

7.	**CMP GUI:** Verify alarms	On the CMP GUI, verify that the corresponding **'Server Core File Detected'** alarms have been cleared.

Appendix A: Correcting Server Core File Detected Alarms

☐		
This procedure has been completed.		

APPENDIX B. 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