Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Installation

Policy Management 15.0 to 15.0.x Upgrade Procedure

F92411-02

May 2024

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

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

Refer to Appendix C for instructions on accessing this site.

Contact the Oracle Customer Care Center (mailto:support@oracle.com) and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

Oracle Communications Policy Management 15.0 to 15.0.x Upgrade Procedure

TABLE OF CONTENTS

List of Procedures

List of Tables

List of Figures

1 GEOREDUNDANCY ENABLED

1.1 Introduction

1.1.1 Purpose and Scope

This document describes methods utilized and procedures run to perform a software upgrade of Oracle Communications Policy Management Release 15.0 to Release 15.0.x when georedundancy is enabled.

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

1.1.2 Acronyms

Acronym	Definition
CMP	Configuration Management Platform
DR-CMP	Configuration Management Platform for Disaster Recovery **NOTE:** It refers to the CMP on the secondary site
DSR	Diameter Signaling Router
GUI	Graphical User Interface
IPM	Initial Product Manufacture
LVM	Logical Volume Manager
MPE	Multimedia Policy Engine
MPE-LI	MPE for Lawful Intercept - a type of Multimedia Policy Engine
MRA	Multiprotocol Routing Agent (also known as the Policy Front End or PFE)
OCS	Online Charging System
OOS	Out of Service
PCEF	Policy Control Enforcement Function
PCRF	Policy and Charging Rules Function—Oracle MPE
TPD	Tekelec Platform Distribution

1.1.3 Terminology

Term	Description
Primary Site (Site1)	Site where the MPE/MRA Server-A and Server-B are deployed.
Secondary Site (Site2)	Site where the MPE/MRA Server-C is deployed.
Spare Server or Server-C	Server that is ready to take over from the Active server if both the Active and Standby servers fail. It is generally in a different location than the Active and Standby servers.

1.1.4 Software Release Numbering

- COMCOL: 6.6
- TPD: 8.x
- Policy Management release 15.0

1.2 Upgrade Overview

This section lists the required materials and information needed to run Policy Management release 15.0.x software upgrades.

1.2.1 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.

1.2.2 Upgrade Paths

This upgrade document supports the following upgrade path:

- Policy Management 15.0 (fresh install) to 15.0.x (full DIU ISO) (Major Path)

NOTE:

- If the official upgrade paths mentioned in the release documents of each supported version are not followed, please contact Oracle Support before upgrading to 15.0.x.
  (Refer to individual patch release document to see the supported upgrade paths.)
- 15.0 to 15.0.x upgrade is only applicable for VM based environments.

1.2.3 Upgrade Information

This procedure applies to Active, Standby, and Spare servers. A group of servers is referred to as a cluster. The cluster types are CMP, MRA, and MPE.

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

A Policy Management deployment can consist of multiple clusters.

NOTE: In a cluster with single node, upgrade is not supported.

1.2.3.1 Required Cluster Upgrade Sequence

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

The following is the upgrade sequence, specific process is documented by an Oracle provided Maintenance Operation Procedure (MOP).

1. Upgrade Primary CMP
2. Upgrade Secondary CMP (if applicable)
3. Site 1 Segment 1—Upgrade non-CMP clusters (see note below)
4. Site 2 Segment 1—Upgrade non-CMP clusters (see note below)
5. Site 1 Segment 2—Upgrade non-CMP clusters (see note below)
6. Site 2 Segment 2—Upgrade non-CMP clusters (see note below)

NOTE: Up to 16 non-CMP clusters can be upgraded in parallel.

1.2.3.2 Policy Management Release Mixed-Version Operation and Limitation

The general expectation is that a system that is running in a mixed version configuration should support features, and perform at a level of the previous version. Thus, the system that is running pre-15.0.x release and release 15.0.x mixed configuration would support the performance and capacity of pre-15.0.x release. The mixed version Policy Management configuration would support pre-15.0.x release features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the release 15.0.x CMP is managing servers in both the previous release and release 15.0.x. In this mixed version configuration, release 15.0.x CMP does not prevent an operator from configuring anything that you could configure in a previous release and all configuration items from the previous release are still available. However, the configuration changes during the upgrade of Policy Management system are discouraged and have limited support.

In the mixed version Policy Management configuration release 15.0.x 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 you and Oracle before deployment to verify that these policies indeed do not use new conditions or actions.
- The support for configuration of MPE/MRA servers is limited to parameters that are available in the previous version. Specifically, Network Elements can be added.

Table 1 Mixed-version configurations supported

Policy Management system components on	CMP R15.0.x	MRA R15.0.x	MPE R15.0.x
CMP 15.0	Yes	No	No
MRA 15.0	Yes	Yes	Yes
MPE 15.0	Yes	Yes	Yes

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of the CMP and DR-CMP from the previous release to release 15.0.x. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to release 15.0.x.

1.2.4 Customer Impacts

The cluster upgrade proceeds by upgrading the standby server, then switching over from the active to the standby, then the spare server, and upgrading the new standby. The switchover of each non-CMP cluster has a small impact on traffic being processed at that cluster.

1.2.5 Rollback/Backout

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

1.2.6 TPD Version

The Tekelec Platform Distribution (TPD) version needed for this release is included in the Policy Application Software Upgrade DIU ISO, and the TPD is upgraded to version 8.x as part of this procedure.

1.2.7 Loading Application Software

For upgrade of server application software, the recommended method is to copy the application DIU ISO images to the servers using the `scp` or `ftp` command.

1.2.8 Required Materials and Remote Access

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

- Policy Management 15.0.x software DIU ISO files
- Policy Management 15.0.x software Release Notes
- The capability to remotely login to the target server as admusr.

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

- 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.
- User login IDs, passwords, IP addresses, and other administration information.
- VPN access to your network is required if that is the only method for remotely logging into the target servers. It must be also possible to access the Policy Management GUI.

1.2.8.1 Upgrade Media

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

1.2.8.2 Login User IDs and Passwords

You must confirm login information for key interfaces, and document the information using Table 2.

NOTES:

- It is assumed that the login information may be common across sites. If not, record the information for each site.
- Consider the sensitivity of the information recorded in this table. While all of the information in the table is required to complete the upgrade, there may be security policies in place that prevent the actual recording of this information in a permanent form.

Table 2 Login IDs, Passwords and release Information

Item	Value
CMP servers **NOTE:** Some older releases do not use admusr, instead use the default root Login using SSH.	GUI Administrator Login User/Password
	admusr password:
MPE/MRA servers	admusr password:
Target OA	OA Administrator Login User/Password
Software Upgrade Target Release[1]	Target Release Number
	Policy Management 15.0.x software DIU ISO image filenames

1.3 Theory of Operation

1.3.1 Upgrade Manager Page

The Upgrade Manager was not up to the operator, with assistance from an MOP, to know the correct sequence of server selects and menu selections. The Upgrade Manager takes a different approach. It determines the next course of action to either

- Begin/continue upgrading a cluster
- Begin/continue backing out a cluster.

IMPORTANT: There is a point implicit in the list above: upgrade is now presented from a cluster perspective, instead of a server perspective.

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

Certain operations are performed automatically on behalf of the operator. These operations are not presented to the operator as an option. However, the operator can see what has been done using the upgrade log.

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

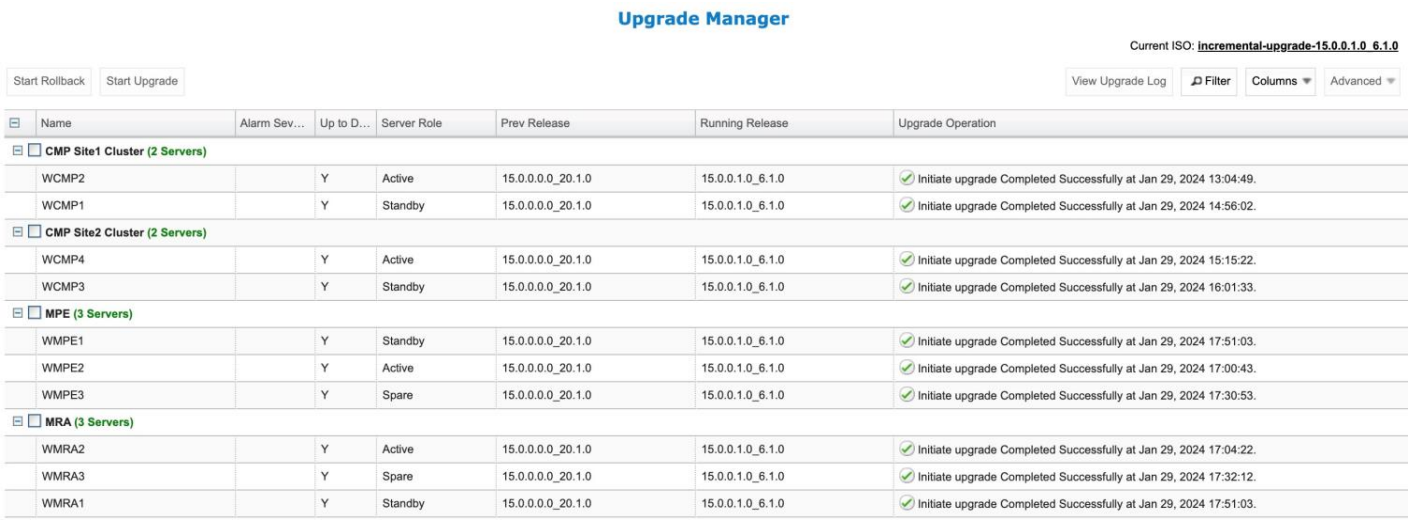


Figure 1 Sample display of the Upgrade Manager page

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

- **Start Rollback** and **Start Upgrade** buttons (upper left):

  If a cluster is selected and these buttons are disabled (grey), it means that there is not an appropriate action to take at this time. However, if a button is not disabled (white), then it means that there is a preferred action that can be taken to upgrade (or backout) the cluster. Normally, upgrading a cluster is a well-defined fixed procedure. However, in some cases there are a number of valid sequences. Selecting the preferred step causes the Upgrade Director to choose the default sequence. Only use the Upgrade Manager to perform upgrades unless the instructions direct otherwise.

- **Alarm Severity**:

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

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

  Servers reports alarms to indicate that their mate servers are offline.

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

- **Up to Date**: This column is used to indicate the state of the code on the server.

  N—Server is running old code and must be upgraded

  Y—Server is running new code.

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

1.3.1.1 The Upgrade Log

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

Upgrade Log

Cluster Name: MPE
Last Update: 01/30/2024 11:08:10

Filter | Columns

ID	Parent ID	Action Name	Start Time	End Time	Duration	Scope	Hostname	Result	Mode	Description
21	0	Preflight Check	01/16/2024 16:56:23	01/16/2024 16:57:05	0:00:42	Server	WMPE2	Success	Manual	User initiated action: …
23	21	Upgrading server	01/16/2024 16:57:05	01/16/2024 17:02:50	0:05:44	Server	WMPE2	Success	Automatic	Automatic action initi…
24	21	Modify the role/replication attribut…	01/16/2024 16:57:05	01/16/2024 16:57:07	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
27	21	Wait for replication to synchronize	01/16/2024 17:02:50	01/16/2024 17:12:25	0:09:35	Server	WMPE2	Success	Automatic	Automatic action wai…
29	0	Failover to new version	01/17/2024 10:33:28	01/17/2024 10:33:28	0:00:00	Cluster	MPE	Success	Manual	User initiated action: …
30	0	Preflight Check	01/17/2024 10:36:37	01/17/2024 10:37:27	0:00:49	Server	WMPE3	Success	Manual	User initiated action: …
32	30	Upgrading server	01/17/2024 10:37:27	01/17/2024 10:44:05	0:06:38	Server	WMPE3	Success	Automatic	Automatic action initi…
33	30	Modify the role/replication attribut…	01/17/2024 10:37:27	01/17/2024 10:37:28	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
37	30	Wait for replication to synchronize	01/17/2024 10:44:05	01/17/2024 10:53:17	0:09:11	Server	WMPE3	Success	Automatic	Automatic action wai…
38	30	Modify the role/replication attribut…	01/17/2024 10:44:05	01/17/2024 10:44:07	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
41	0	Preflight Check	01/17/2024 10:56:25	01/17/2024 10:57:17	0:00:51	Server	WMPE1	Success	Manual	User initiated action: …
42	41	Upgrading server	01/17/2024 10:57:17	01/17/2024 11:03:46	0:06:28	Server	WMPE1	Success	Automatic	Automatic action initi…
43	41	Modify the role/replication attribut…	01/17/2024 10:57:17	01/17/2024 10:57:19	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
47	41	Wait for replication to synchronize	01/17/2024 11:03:46	01/17/2024 11:13:07	0:09:21	Server	WMPE1	Success	Automatic	Automatic action wai…
48	41	Modify the role/replication attribut…	01/17/2024 11:03:46	01/17/2024 11:03:47	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
53	0	Backing out server upgrade	01/23/2024 12:58:01	01/23/2024 13:00:21	0:02:20	Server	WMPE1	Success	Manual	User initiated action: …
54	53	Modify the role/replication attribut…	01/23/2024 12:58:01	01/23/2024 12:58:02	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
56	53	Waiting for replication to synchron…	01/23/2024 13:00:21	01/23/2024 13:04:15	0:03:53	Server	WMPE1	Success	Automatic	Automatic action wai…
59	0	Backing out server upgrade	01/23/2024 13:18:56	01/23/2024 13:21:28	0:02:32	Server	WMPE3	Success	Manual	User initiated action: …
60	59	Modify the role/replication attribut…	01/23/2024 13:18:56	01/23/2024 13:18:58	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
62	59	Waiting for replication to synchron…	01/23/2024 13:21:28	01/23/2024 13:25:05	0:03:36	Server	WMPE3	Success	Automatic	Automatic action wai…
63	0	Failover to old version	01/23/2024 13:43:11	01/23/2024 13:43:11	0:00:00	Cluster	MPE	Success	Manual	User initiated action: …
67	0	Backing out server upgrade	01/23/2024 13:54:38	01/23/2024 13:56:54	0:02:15	Server	WMPE2	Success	Manual	User initiated action: …
68	67	Modify the role/replication attribut…	01/23/2024 13:54:38	01/23/2024 13:54:40	0:00:01	Cluster	MPE	Success	Automatic	Automatic action for …
69	67	Waiting for replication to synchron…	01/23/2024 13:56:54	01/23/2024 14:00:35	0:03:40	Server	WMPE2	Success	Automatic	Automatic action wai…

Figure 2 Upgrade Log

1.3.1.2 Optional Actions

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

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

1.3.1.3 The ISO Select

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

An upgrade to version *XXX*

To start a new upgrade, click on this item. The Upgrade Director searches for valid upgrade procedures. In order to minimize confusion, these upgrade procedures are usually embedded within a CMP ISO file. This way, the CMP ISO file is always tied to the corresponding upgrade procedure.

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

1.3.1.4 Upgrade Director Behavior

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

1.3.1.5 Alarm Philosophy

During an upgrade, the Upgrade Manager asserts (that is, generates) and displays alarms. An upgrade typically triggers multiple minor, major, and critical alarms as servers are taken out of service, go into forced standby, or fail over. This is normal and to be expected. Figure 3 shows an example of an upgrade in progress asserting multiple transient alarms.

NOTE: Click on the active alarms summary, in the upper right corner of every CMP page, to display a list of current active alarms.

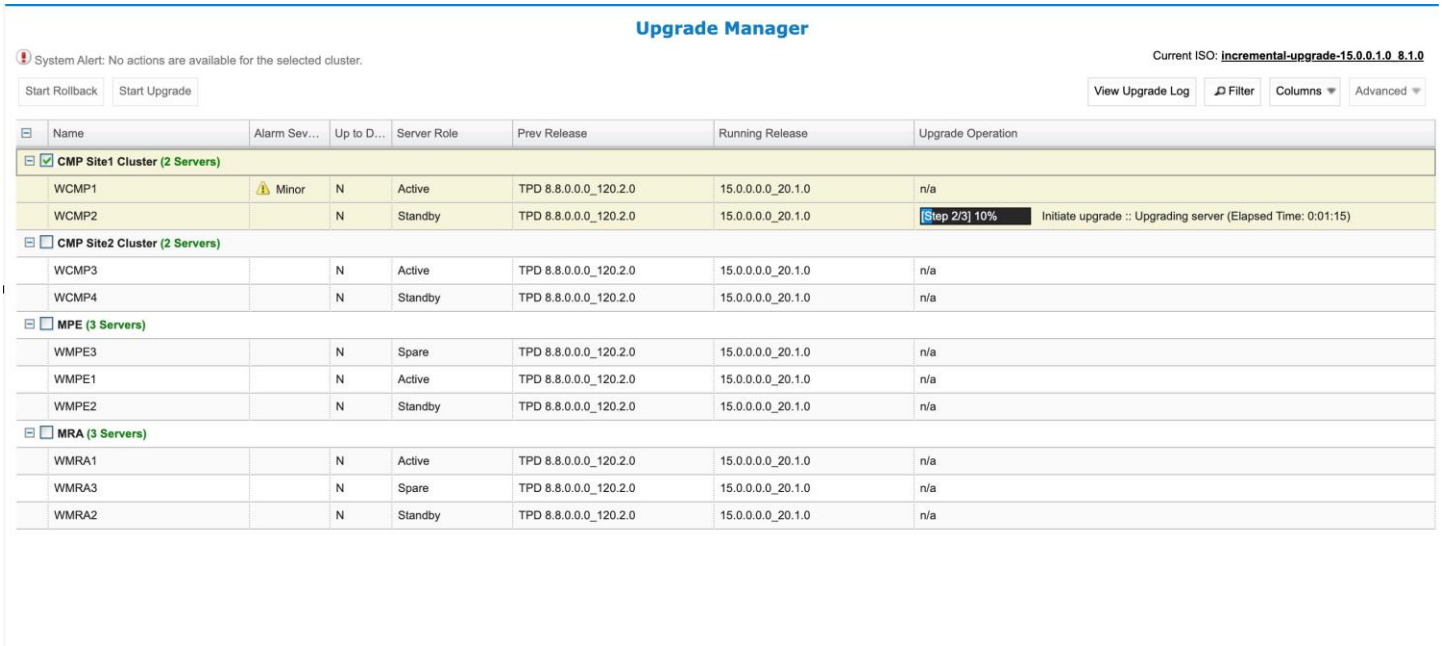


Figure 3 Upgrade in Progress Showing Transient Alarms

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

Table 3 Transient Alarms Asserted During a Typical Upgrade

Alarm Number	Severity	Name
31227	Critical	HA availability status failed
31102	Minor	DB Replication from a master node DB has failed
31283	Critical	Lost Communication with server
70001	Critical	QP_procmgr failed
70007	Critical	Not all QP resources are ready
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
31102	Minor	DB replication from a master node DB has failed
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
70506	Minor	Upgrade Operation Failed
70507	Minor	Upgrade in Progress
70508	CRITICAL	Zombie Server

The Upgrade Manager also asserts an alarm if an unexpected error prevents it from continuing the upgrade. You should review all active alarms after each upgrade step to ensure that the alarms are expected. Alarms are described in the *Troubleshooting Guide*, Release 15.0, available at the Oracle Help Center.

1.3.1.6 General Upgrade Procedure

In general, the upgrade of a server goes through the following steps:

1. Preflight checks—look for certain conditions which guarantee a failed upgrade. If such conditions are detected, fail. There are two principles behind the preflight checks.
2. It is better to fail early in a recoverable way than to fail late in an unrecoverable way.
3. Preflight checks are VERY narrow. This prevents false positives for an otherwise valid upgrade.
4. The upgrade itself

5. Wait for replication to synchronize.

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

Upgrade Order

With a two-server cluster, there is only a single valid order:

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

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

1. Upgrade the standby server
2. Failover
3. Reapply the configuration

   NOTE: This requires you to navigate away from the Upgrade Manager page

4. Upgrade the spare server
5. Upgrade the remaining server in the primary site

Unreachable Servers

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

Reversing Directions

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

Mixed version and Forced Standby

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

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

Failure Handling and Recovery

Failures fall into two categories:

- Failures that the Upgrade Director is able to recover from.
- Failures that the Upgrade Director cannot automatically recover from.

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

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

For the current release, recovery or even deep failure diagnosis is not exposed via the GUI.

1.4 Upgrade Preparation

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

NOTE: If Veritas NetBackup is being used on the system, see the Maintenance Operation Procedure for pre and post upgrade steps.

Overview of steps:

1. Upgrade Primary (Site1) CMP
2. Upgrade Secondary (Site2) CMP (if applicable)
3. Segment 1 Site1:
   a. Upgrade MPE clusters
   b. Upgrade MRA clusters
4. Segment 1 Site2:
   a. Upgrade MPE clusters
   b. Upgrade MRA clusters
5. Segment 2 Site1:
   a. Upgrade MPE clusters
   b. Upgrade MRA clusters
6. Segment 2 Site2:
   a. Upgrade MPE clusters
   b. Upgrade MRA clusters

1.4.1 Prerequisites

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

Procedure 1 Prerequisites

Step	Procedure	Details
1. ☐	Verify all required materials are present	As listed in section 1.2.8 Required Materials and Remote Access.
2. ☐	Review Release Notes	Review Policy Management 15.0.x Release Notes for the following information: • Individual software components and versions included in target release. • New features included in target release. • Issues (bugs) resolved in target release.

Step	Procedure	Details
		• 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 15.0.x, only Mozilla Firefox and Google Chrome are fully supported.
—End of Procedure—		

1.4.2 Plan and Track Upgrades

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

1. Upgrade CMP clusters
2. Upgrade MPE/MRA clusters

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

NOTES:

- Policy changes or configuration changes should NOT be made while the system is in mixed-version operation.
- Time estimates are for upgrade procedure without backout procedure. Backout procedure time is typically the same as, or less than the upgrade procedure.

Table 4 Upgrade information

Step	Procedure	Result	Engineer	Time
1. ☐	Use the following checklist to plan the cluster upgrades for the entire system.	Maintenance windows are planned		
2. ☐	Upgrade Site1 and Site2 CMP clusters. Each cluster takes approximately 40-50 minutes to complete	Site Names _____ and _____		3 hrs
3. ☐	Upgrade Site1 MPE/MRA clusters for Segment-1	Site Names _____ Cluster List:		2 hrs

Step	Procedure	Result	Engineer	Time
4. ☐	Upgrade Site2 clusters for Segment-1	Site Names _____ Cluster List:		2 hrs
5. ☐	Upgrade Site1 clusters for Segment-2	Site Names _____ Cluster List:		2 hrs
6. ☐	Upgrade Site2 clusters for Segment-2	Site Names _____ Cluster List:		2 hrs
—End of Procedure—				

1.4.3 Perform System Health Check

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

Procedure 2 Perform system health check

Step	Procedure	Result
1. ☐	CMP GUI Access	Open a supported browser (Mozilla Firefox or Google Chrome) to access the Primary CMP GUI on its VIP address and login to verify access.

Step	Procedure	Result
2. ☐	View Active Alarms	Identify the cause of any existing active alarms, and determine if these may have impact on the upgrade. Export current alarms to save into a file. ***IMPORTANT: Before starting any upgrade activity, ensure that all active alarms are understood and resolved.***
3. ☐	View KPI reports	Verify that the system is running within expected parameters. Export current KPIs into a file.

4. ☐	Confirm NTP servers are reachable from all the servers (CMP, MPEs and MRAs) to be upgraded
	NOTE: If the time across the servers is out of synch, fix it and re-validate this step, before starting the upgrade procedures.
		1. Validate the IP connectivity between the server and NTP servers by PING.
		2. Confirm that time is synchronized on each server using the following CLI shell command:
		`$sudo chronyc tracking`
		3. Confirm that date is correct on each server.
		4. Check that BIOS clock is synced with the clock using the following CLI shell command:
		`$sudo hwclock`

—End of Procedure—		

1.4.4 Deploy Policy Management Upgrade Software

Software should be deployed to each Policy Management server `/var/TKLC/upgrade` directory, before the actual upgrade activities. This is typically done with utilities such as SCP, WGET or SFTP. Because of the large size of the software DIU ISO file, sufficient time should be planned to accomplish this step. For Policy Management release 15.0.x, each DIU ISO image size is about 8GB for CMP and about 7GB for non-CMP servers.

1.4.6.1 Deploying Policy Management Upgrade Software to Servers

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

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

Also, if multiple images are copied into the `/var/TKLC/upgrade` directory, the upgrade fails.

1.4.6.2 Distribute Application DIU ISO Image Files to Servers

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

NOTE: DIU 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 DIU ISO transfers to the target systems should be performed prior to and outside of the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Manual Distribution

Procedure 3 Manual Distribution

Step	Procedure	Result
1.	Transfer DIU ISO files to Policy Management server.	1. Transfer release 15.0.x DIU ISO files (CMP and non-CMP) into the `/var/TKLC/upgrade` directory on the respective server using one of the following methods: - SCP/WGET command - USB drive 2. If the images are on a server in the same network, **scp** the files using the CLI, for example, for CMP: 3. Copy CMP software DIU ISO file to ONE of the other CMP servers: `$sudo cp /var/TKLC/upgrade/cmp-15.0.0.1.0_x.x.0-x86_64-DIU.iso user@remote_host.com:/var/TKLC/upgrade` 4. Repeat for one server of all clusters. **NOTE:** After copying the DIU ISO to one of the respective servers, the DIU ISO Maintenance is used to upload to the rest of the servers.
—End of Procedure—		

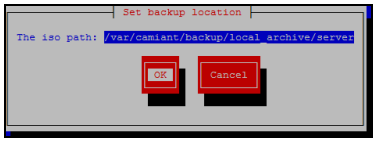
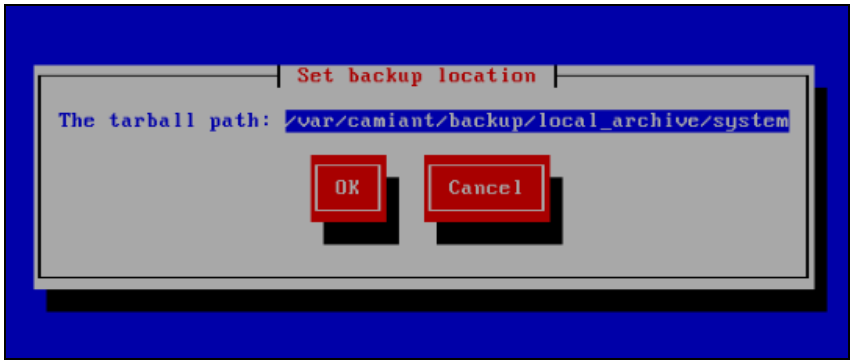
1.4.6.3 Backups and Backup Locations

Perform the backups prior to the maintenance window period.

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

Procedure 4 Backups and Backup Locations

Step	Procedure	Result

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

Step	Procedure	Result

2. ☐	**SSH CLI/iLO:** Verify the backup DIU ISO file	If default location is accepted in the previous step, change to the following directory and verify the file. For example for an MPE server backup:
		`$ cd /var/camiant/backup/local_archive/serverbackup`
		`$ ls <hostname>-cmp_15.0.0.0.0_20.1.0-serverbackup-<yyyy><mm><dd><hhmm>.iso`
		And for the system backup:
		`$ cd /var/camiant/backup/local_archive/systembackup`
		`$ ls <hostname>-cmp_15.0.0.0.0_20.1.0-systembackup-<yyyy><mm><dd><hhmm>.tar.gz`

3. ☐	Copy backup files.	1. Copy the files to remote server or local workstation/laptop.
		2. Example of a remote server copy.
		`$ sudo scp /var/camiant/backup/local_archive/systembackup/xx_tar.gz <remoteserver_ipaddress>:<destinationpath>`
		3. Remove the backup ISO file from the TPD Sever.
		`$sudo rm <backup_filename>.iso`

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

1.5 Upgrade CMP clusters (15.0 to 15.0.x)

Use this procedure to upgrade the Site1 CMP cluster, and if needed, upgrade the Site2 CMP cluster in a single maintenance window.

1.5.1 Upgrade CMP clusters Overview

1. Upgrade Primary CMP cluster
2. Start upgrade
3. Failover
4. Log back into the CMP GUI
5. Continue upgrade
6. Upgrade Secondary CMP cluster
7. Start upgrade
8. Failover
9. Continue upgrade

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

It is assumed that the CMPs may be deployed as 2 georedundant clusters, identified as Site1 and Site2 as displayed on the CMP GUI. When deployed as such, one site is designated as the Primary Site (which is the site that is managing the Policy Management system), and the other is as Secondary site (this site is ready to become Primary site, if needed).

If the System is deployed with only ONE CMP, then the upgrade of the Secondary CMP can be skipped.

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

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

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

IMPORTANT:

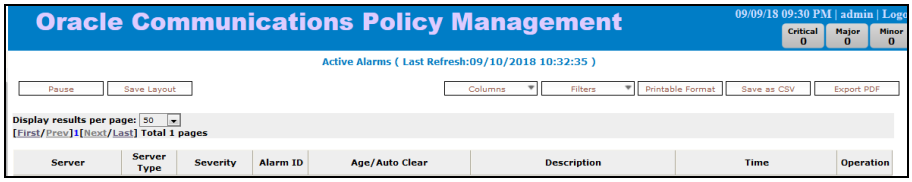
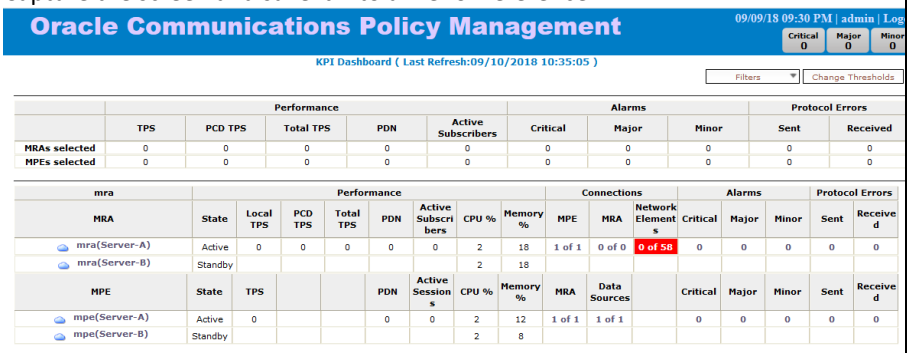
- Site1 CMP MUST be upgraded to the new release before the Site2 CMP
- CMP servers MUST be upgraded before the non-CMP clusters

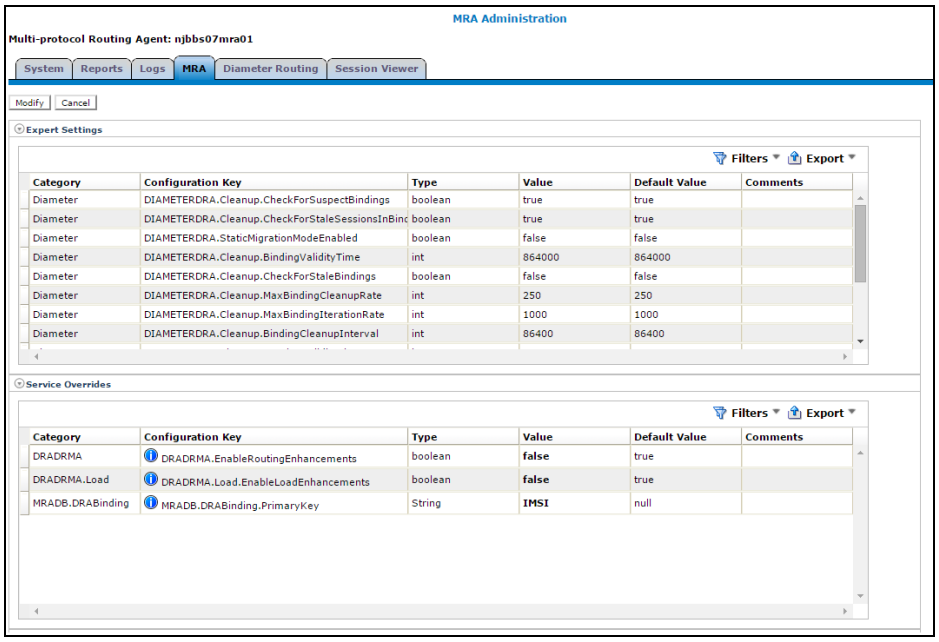
NOTE: The following steps use build 15.0 as example.

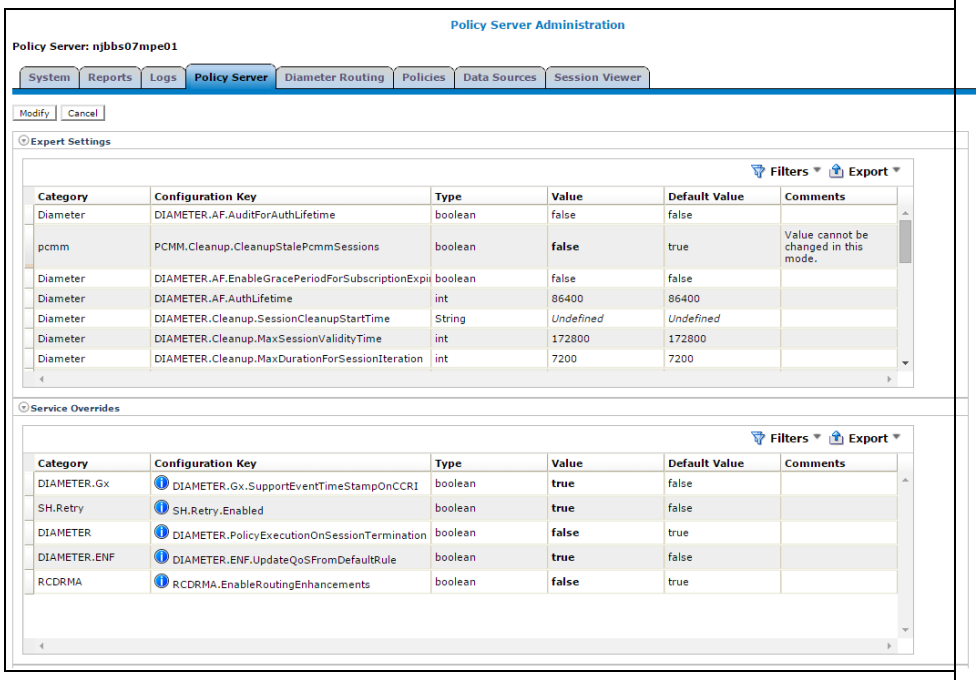
1.5.2 Upgrade Primary CMP cluster

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

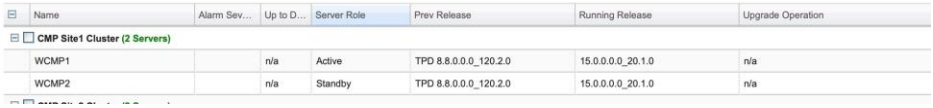
Procedure 5 Upgrade Primary CMP cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify alarm status.	1. Navigate to **System Wide Reports → Alarms→Active Alarms**. 2. Confirm that any existing alarm is understood and is not an impact to the upgrade procedure. If has critical alarm like 70020 (The current MYSQL master has an outdated database), should solve this alarm then continue to upgrade. 3. Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP GUI:** Verify Traffic Status - KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Confirm that all Connections and Traffic status are as expected. Observe it for a few refresh updates. 3. Capture the screen and save it into a file for reference. 

Step	Procedure	Result
3. ☐	**CMP GUI:** Capture MRA Advanced Settings	1. Capture screenshots of the advanced settings on the MRA prior to upgrading the CMP and save them into files for future reference check. 2. Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ MRA**. 3. Click **Advanced Settings**.  4. Alternatively, settings can be exported clicking **Export** on the right within each setting.

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>4. ☐</td><td>CMP GUI: Capture MPE Advanced Settings</td><td>
1. Capture screenshots of the advanced settings on the MPE prior to upgrading the CMP and save them into files for future reference check.
2. Navigate to Policy Server → Configuration → <mpe_cluster name> → Policy Server
3. Click Advanced Settings.


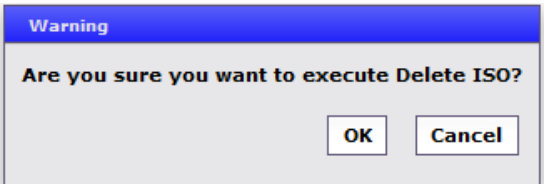
4. Alternatively, settings can be exported clicking Export on the right within each setting.
</td></tr>
<tr><td>5. ☐</td><td>CMP GUI: Identify and record the CMP cluster(s)</td><td>
1. Navigate to Platform Setting→Topology Settings → All Clusters.
Cluster Settings
<table>
<tr><th>Name</th><th>Appl Type</th><th>Site Preference</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Server-C</th><th>Operation</th></tr>
<tr><td>CMP Site1 Cluster (P)</td><td>CMP Site1 Cluster</td><td>N/A</td><td>10.75.175.65/25</td><td>10.75.175.45</td><td>10.75.175.55</td><td>N/A</td><td>View Demote</td></tr>
<tr><td>CMP Site2 Cluster (S)</td><td>CMP Site2 Cluster</td><td>N/A</td><td>10.75.175.66/25</td><td>10.75.175.46 (FS)</td><td>10.75.175.56</td><td>N/A</td><td>View Delete</td></tr>
<tr><td>mpe300</td><td>MPE</td><td>Normal</td><td>10.75.175.67/25 (P)
N/A (S)</td><td>10.75.175.37</td><td>10.75.175.47</td><td>10.75.175.57</td><td>View Delete</td></tr>
<tr><td>mra300</td><td>MRA</td><td>Normal</td><td>10.75.175.68/25 (P)
N/A (S)</td><td>10.75.175.38</td><td>10.75.175.48</td><td>10.75.175.58</td><td>View Delete</td></tr>
</table>
2. Note which cluster is the primary and which cluster is the secondary.
3. The Primary CMP is noted with a P in parenthesis and a Secondary CMP is noted with an S in parenthesis.
4. Save a screenshot for future reference.
</td></tr>
</table>

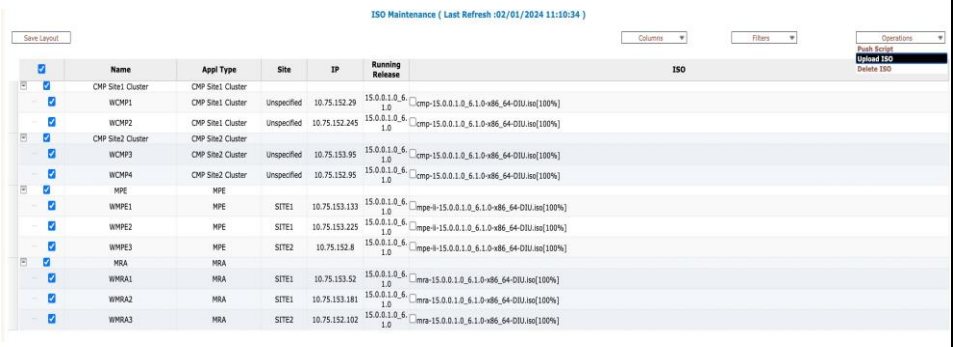
Step	Procedure	Result
6. ☐	**CMP GUI:** Verify the status of the CMP clusters	1. Navigate to **Upgrade → Upgrade Manager**.  2. Confirm the CMP clusters have the following: - Active/Standby status - Running release 15.0  3. Navigate to **Upgrade → ISO Maintenance**.  Release 15.0.x ISO files copied to at least one of each server types (CMP/MRA/MPE)—Meaning, a copy of the MPE ISO file is on one of the MPE servers, an MRA ISO file is on one of the MRA servers and a copy of the CMP ISO file is on one CMP server

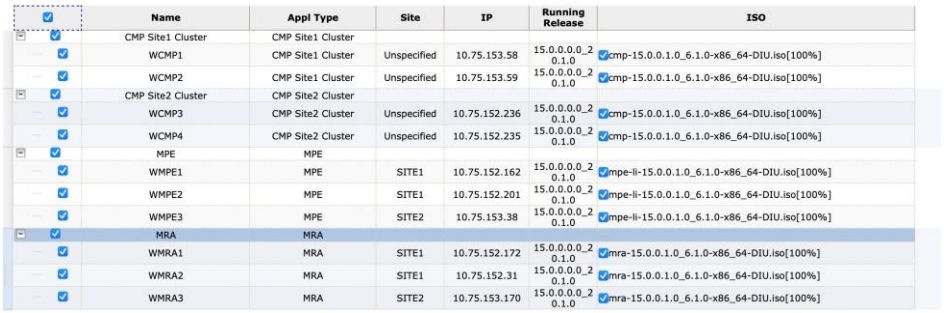
Name	Alarm Sev...	Up to D...	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
WCMP1		n/a	Active	TPD 8.8.0.0.0_120.2.0	15.0.0.0.0_20.1.0	n/a
WCMP2		n/a	Standby	TPD 8.8.0.0.0_120.2.0	15.0.0.0.0_20.1.0	n/a

Step	Procedure	Result

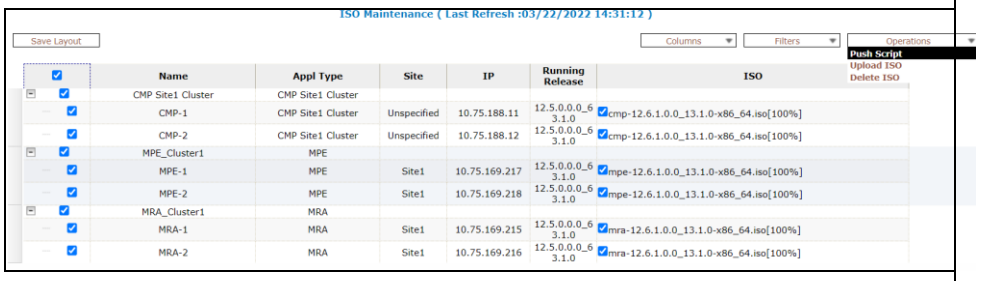
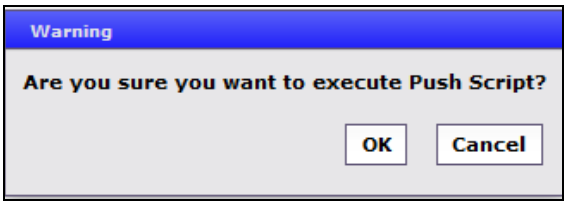
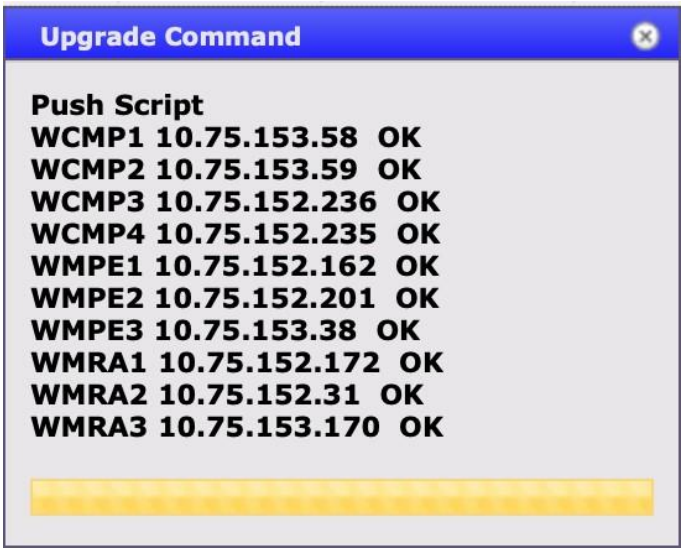
7. ☐	**SSH CLI Primary Active CMP:** Exchange Keys	1. Exchange keys to all servers from the Site1 (Primary) Active CMP. Login as admusr and run the following command:
		`$sudo qpSSHKeyProv.pl --prov`
		`[admusr@guam-cmp-1a ~]$ sudo qpSSHKeyProv.pl -prov`
		`The password of admusr in topology:`
		2. Enter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

8. ☐	**CMP GUI:** Access into Primary CMP Server— Remove old ISO files from servers.	1. Navigate to **Upgrade → ISO Maintenance**. 2. Select the servers that show old ISO files. 3. Select the server cluster. 4. Select **Operations → Delete ISO** to remove any older ISO files. 5.  6. Click **OK** to continue and wait until seeing the successful deletion message  7. Wait until the ISO Maintenance page is refreshed and the ISO column does not show any old ISOs.

Step	Procedure	Result
9. ☐	**CMP GUI:** Distribute ISO files to CMP/MPE/ MRA servers **NOTE:** This step depends on the ISO file type. Distribute ISO files accordingly.	1. Navigate to **Upgrade → ISO Maintenance**. 2. Filter by server type (optional, but preferred step) 3. One application at a time, select one server type (CMP, MPE, etc.) to be upgraded. **NOTE:** The ISO files for each application type must be copied over to at least one server. See Distribute Application DIU ISO Image Files to Servers. 4. Select **Operations → Upload ISO**.  5. Fill in the dialog with the following information: Mode: Select **SCP** ISO Server Hostname/IP: <*IP_address_where_ISO_files_are_located*> 6. User: admusr Password: <*admusr_password_for_the_server*> Source ISO file full path: `/var/TKLC/upgrade/` <*server_type_iso_filename*> 7. Click **Add**. 8. When completed, the ISO column is populated with the ISO filename and a notification of [100%] 9. Repeat for all cluster types.

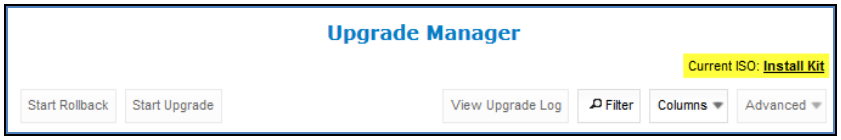
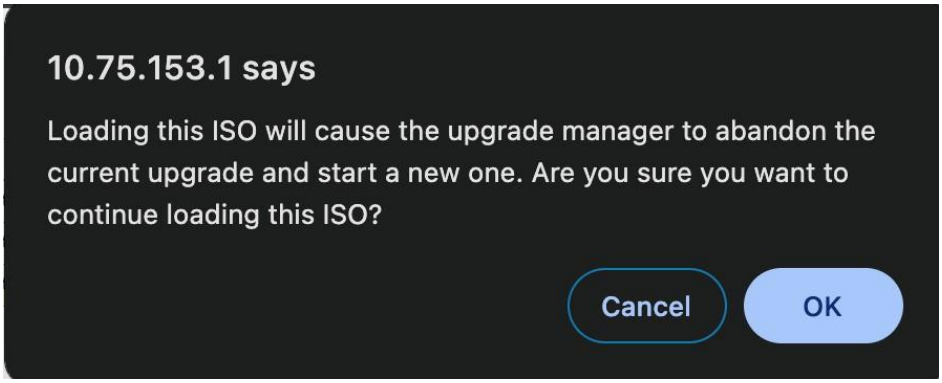
Step	Procedure	Result
10. ☐	**CMP GUI:** Verify ISO distribution to all the server	1. Navigate to **Upgrade → ISO Maintenance**. 2. Verify that the release 15.0.x DIU ISO file of the correct type is shown for each server. 3. When completed, the ISO column is populated with the ISO filename and a notification of [100%]. **NOTE:** For those servers where the ISO file was copied from the local machine, there is not be a 100% indicator. This indicator is only available when transferring ISO files using the ISO management feature. 

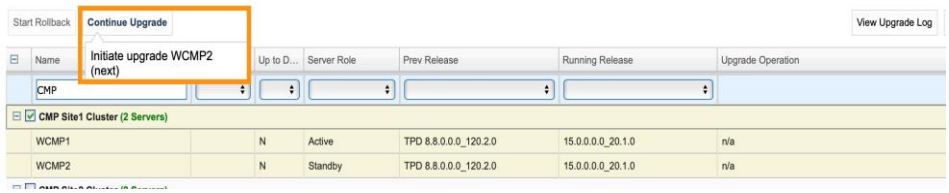
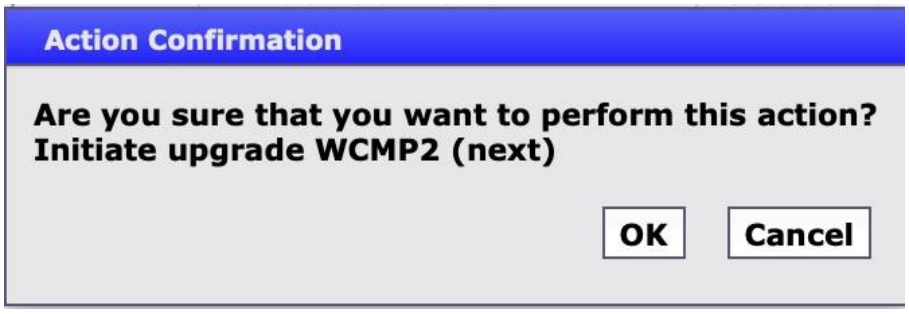
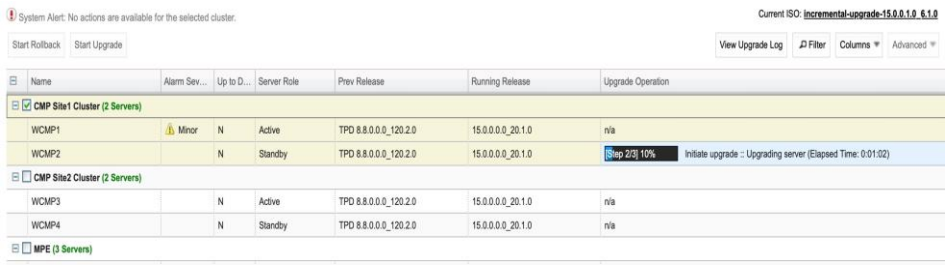
Name	Appl Type	Site	IP	Running Release	ISO
CMP Site1 Cluster	CMP Site1 Cluster				
WCMP1	CMP Site1 Cluster	Unspecified	10.75.153.58	15.0.0.0.0_2 0.1.0	cmp-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
WCMP2	CMP Site1 Cluster	Unspecified	10.75.153.59	15.0.0.0.0_2 0.1.0	cmp-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
CMP Site2 Cluster	CMP Site2 Cluster				
WCMP3	CMP Site2 Cluster	Unspecified	10.75.152.236	15.0.0.0.0_2 0.1.0	cmp-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
WCMP4	CMP Site2 Cluster	Unspecified	10.75.152.235	15.0.0.0.0_2 0.1.0	cmp-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
MPE	MPE				
WMPE1	MPE	SITE1	10.75.152.162	15.0.0.0.0_2 0.1.0	mpe-li-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
WMPE2	MPE	SITE1	10.75.152.201	15.0.0.0.0_2 0.1.0	mpe-li-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
WMPE3	MPE	SITE2	10.75.153.38	15.0.0.0.0_2 0.1.0	mpe-li-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
MRA	MRA				
WMRA1	MRA	SITE1	10.75.152.172	15.0.0.0.0_2 0.1.0	mra-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
WMRA2	MRA	SITE1	10.75.152.31	15.0.0.0.0_2 0.1.0	mra-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]
WMRA3	MRA	SITE2	10.75.153.170	15.0.0.0.0_2 0.1.0	mra-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]

Step	Procedure	Result
11. ☐	**CMP GUI:** Push the Release 15.0.x upgrade scripts to all servers	1. Navigate to **Upgrade → ISO Maintenance**.  2. Select all the servers in the topology as shown. 3. Select **Operations → Push Script** operation.  4. On the warning dialog, click **OK** to continue the operation.  After a minute or so, a successful popup window similar to this should appear: 

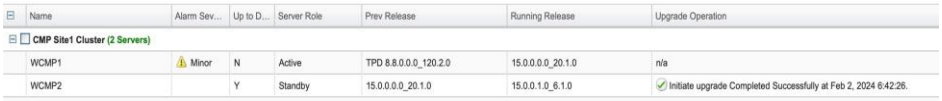
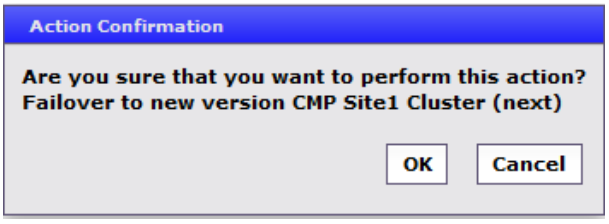
Step	Procedure	Result

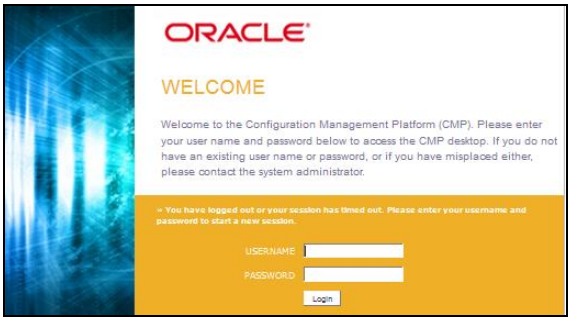
12. ☐	**Primary Active CMP:** SSH to primary active CMP and copy DIU ISO file to `/var/camiant/iso` directory	1. Logon to the primary active CMP as admusr and copy the 15.0.x DIU ISO file to the `/var/camiant/iso` directory:
		`$sudo cp /var/TKLC/upgrade/cmp-15.0.0.1.0_x.x.0-x86_64-DIU.iso /var/camiant/iso/`
		2. Verify the copy by using the following command:
		`$ ls /var/camiant/iso/`

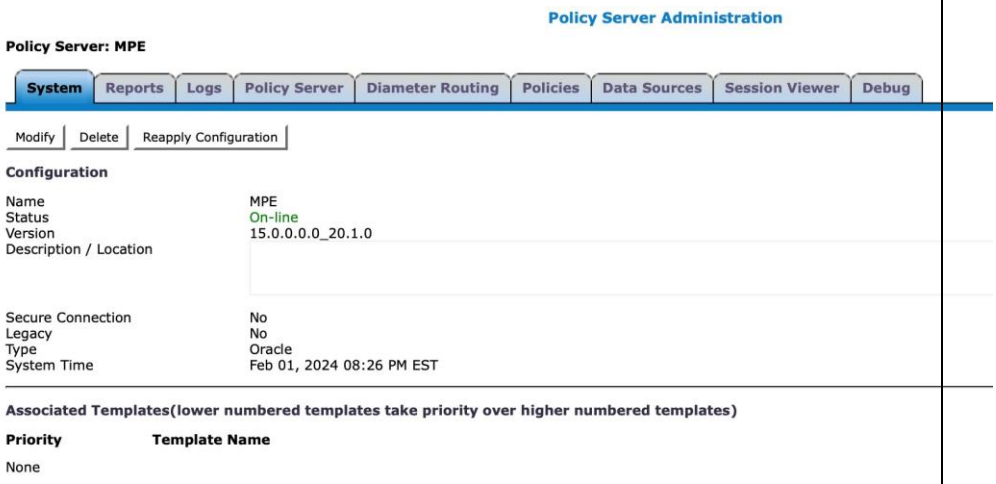
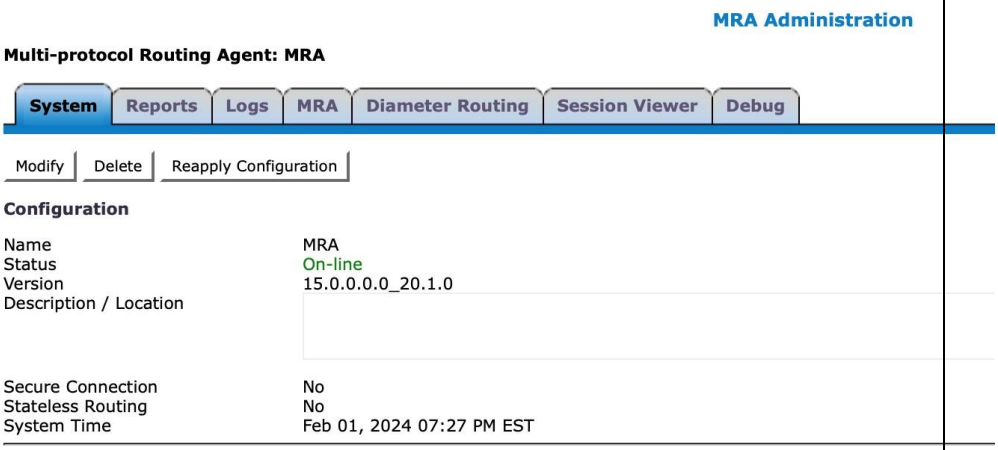
Step	Procedure	Result
13. ☐	**CMP GUI:** Locate the new 15.0.x upgrade manual	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the **Current ISO**. In this case it is labeled Install Kit.  A dialog box with a description of the ISO file that was copied into the `/var/camiant/iso` directory opens. 3. Highlight the ISO file and click **Select incremental-upgrade-15.0.x…** located in the bottom right-hand corner of the window.  4. When the confirmations message displays, click **OK**.  5. Within a few seconds, the Up to Date column changes from Y (meaning up-to-date) or N (meaning needs upgrade). Note: After a few seconds, refresh this page. 
14. ☐	**CMP GUI:** Upgrade Primary CMP cluster **NOTE:** This takes approximate	1. Navigate to **Upgrade → Upgrade Manager**. 2. **NOTE:** Click **Filter** and enter `CMP` in the Name field to show the CMP servers only.

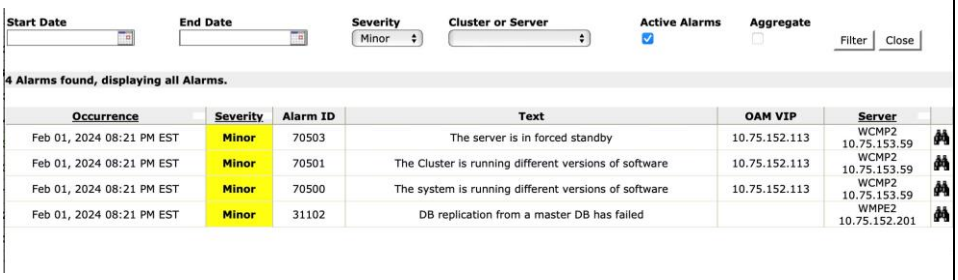
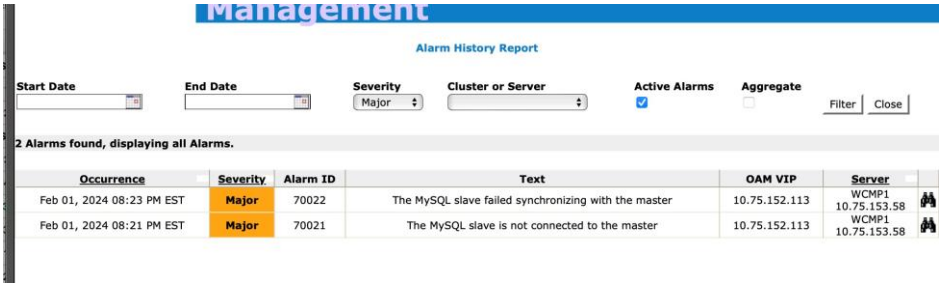
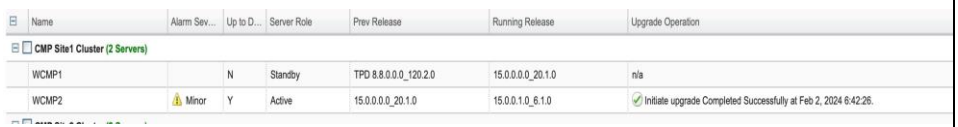
Step	Procedure	Result
	ly 20 minutes to complete.	 3. Select the Primary CMP Server cluster 4. Click **Continue Upgrade**.  5. Click **OK** to confirm and continue with the operation.  This continues to upgrade the standby server only in the CMP cluster The Upgrade Operation column shows a progress bar along with the upgrade activities.  Upgrade Operation column indicates to completed when done. During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical alarm** **31283** Lost Communication with server **31227** HA availability status failed

Step	Procedure	Result
		70025 QP Slave database is a different version than the master **70001** QP_procmgr failed **70007** Not all QP resources are ready **Expected Major Alarm** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Database replication Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **70502** Cluster Replication Inhibited **31102** DB Replication from a master node DB has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31114** DB replication over SOAP has failed **31282** HA Management Fault Upgrade is complete on the standby server of the CMP cluster when the Initiate upgrade Completed successfully at… message displays in the Upgrade Operation column. 

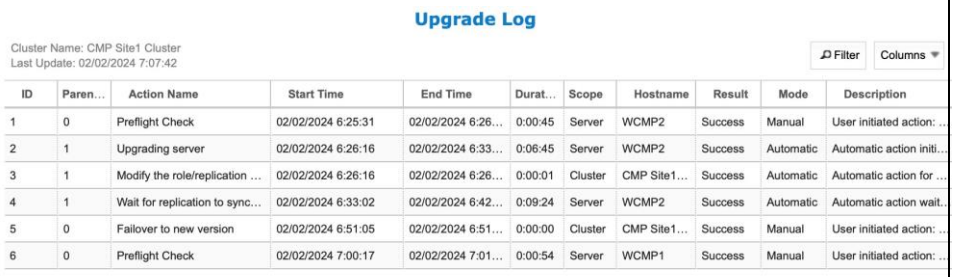
Step	Procedure	Result
15. ☐	**CMP GUI:** Verify that the upgrade is successful	1. Navigate to **Upgrade → Upgrade Manager**. 2. View the cluster. 3. Verify the following information: - The standby server is on 15.0.x - The other server in the cluster is on 15.0 - The Up to Date column shows Y for the 15.0.x server and N for the 15.0 server. - Has alarm: 70025 – QP Slave database is a different version than the master 70501 – Cluster Mixed Version 70503 – Server Forced Standby 
16. ☐	**CMP GUI:** Continue to upgrade CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server cluster. 3. Click **Continue Upgrad**e. Notice the Failover to new version CMP Site1 Cluster message.  4. Click **OK** to confirm and continue with the operation.  The specific action takes a minute to complete. After failover, the current CMP GUI browser could not access, please do next step.

Step	Procedure	Result
17. ☐	**CMP GUI:** Login to the CMP server VIP	Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Management release CMP GUI login page opens as shown—login and password credentials are the same as the pre-upgrade. 
18. ☐	**CMP GUI:** Verify new Policy Management release	Navigate to **Help→About**. Verify the release displayed is 15.0.x. **15.0.0.1.0_6.1.0** Copyright (C) 2003, 2024 Oracle. All Rights Reserved.

Step	Procedure	Result
19. ☐	**CMP GUI:** Reapply Configuration on MPE/MRA cluster	• MPE Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ System** • MRA: Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ System** Click **Reapply Configuration**. **MPE:**  **MRA** 

Step	Procedure	Result
20. ☐	**CMP GUI:** Critical alarms	Critical alarm 70025, "QP Slave database is a different version than the master", can be seen if the SQL Database does not match the master (15.0.x). This alarm is expected and remains until all CMP servers are upgraded to the same version. **Current Minor Alarms** **70503** Server Forced Standby **70500** System Mixed Version **70501** Cluster Mixed Version **31102** DB Replication from a master DB has failed  Start Date End Date Severity: Minor Cluster or Server Active Alarms Aggregate Filter Close 4 Alarms found, displaying all Alarms. Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Feb 01, 2024 08:21 PM EST | Minor | 70503 | The server is in forced standby | 10.75.152.113 | WCMP2 10.75.153.59 Feb 01, 2024 08:21 PM EST | Minor | 70501 | The Cluster is running different versions of software | 10.75.152.113 | WCMP2 10.75.153.59 Feb 01, 2024 08:21 PM EST | Minor | 70500 | The system is running different versions of software | 10.75.152.113 | WCMP2 10.75.153.59 Feb 01, 2024 08:21 PM EST | Minor | 31102 | DB replication from a master DB has failed | | WMPE2 10.75.152.201 **Current Major Alarms** **70022** The MySQL slave failed synchronizing with the master **70021** The MySQL slave is not connected to the master  Management Alarm History Report Start Date End Date Severity: Major Cluster or Server Active Alarms Aggregate Filter Close 2 Alarms found, displaying all Alarms. Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Feb 01, 2024 08:23 PM EST | Major | 70022 | The MySQL slave failed synchronizing with the master | 10.75.152.113 | WCMP1 10.75.153.58 Feb 01, 2024 08:21 PM EST | Major | 70021 | The MySQL slave is not connected to the master | 10.75.152.113 | WCMP1 10.75.153.58 **NOTE:** The Upgrade Manager shows alarms as well.
21. ☐	**CMP GUI:** Verify the Policy Management release 15.0.x CMP is Active	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify the following - Active server is running release15.0.x - Standby server is on the previous release  Name | Alarm Sev... | Up to D... | Server Role | Prev Release | Running Release | Upgrade Operation CMP Site1 Cluster (2 Servers) WCMP1 | N | Standby | TPD 8.8.0.0.0_120.2.0 | 15.0.0.0.0_20.1.0 | n/a WCMP2 | Minor | Y | Active | 15.0.0.0.0_20.1.0 | 15.0.0.1.0_6.1.0 | Initiate upgrade Completed Successfully at Feb 2, 2024 6:42:26.

Step	Procedure	Result
22. ☐	**CMP GUI:** Complete the upgrade of the Primary CMP cluster **NOTE:** Remaining CMP server takes approximately 20 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server cluster 3. Click **Continue Upgrade**. Notice the Initiate upgrade <*standbyserver*> (next) message when hovering over the button.  4. Click **OK** to continue the upgrade on the remaining server in the CMP cluster.  **NOTE:** The server that is being upgraded goes into an OOS state. **Expected Critical Alarms** **31227** HA availability status failed **31283** Lost Communication with server **70001** QP_procmgr failed **70007** Not all QP resources are ready **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **70502** Cluster Replication Inhibited **31102** DB Replication from a master node DB has failed **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault

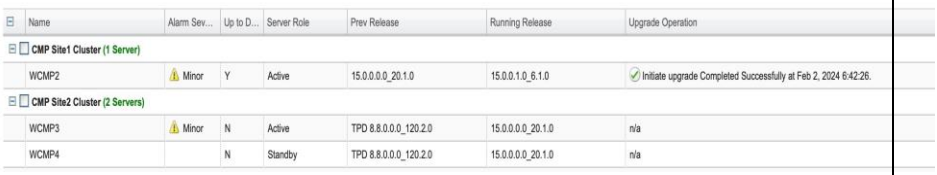
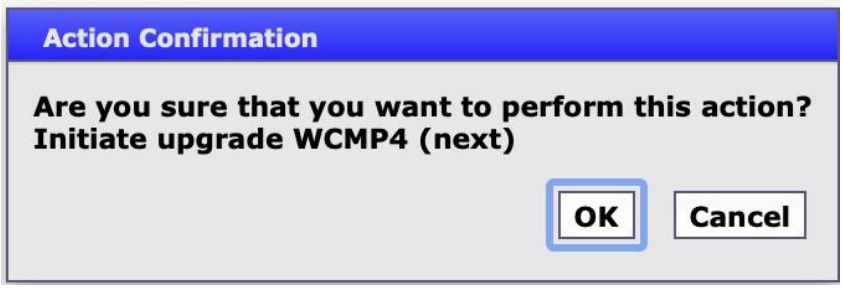
Step	Procedure	Result
23. ☐	**CMP GUI:** Tracking the upgrade complete	Navigate to **Upgrade → Upgrade Manager**. The last step of the upgrade for the first CMP cluster is to wait for replication to complete. With the CMP cluster selected, click **View Upgrade Log** to open a window where you can verify that synchronization has taken place:  **Upgrade Log** Cluster Name: CMP Site1 Cluster Last Update: 02/02/2024 7:07:42 Filter Columns ID | Paren… | Action Name | Start Time | End Time | Durat… | Scope | Hostname | Result | Mode | Description 1 | 0 | Preflight Check | 02/02/2024 6:25:31 | 02/02/2024 6:26… | 0:00:45 | Server | WCMP2 | Success | Manual | User initiated action: … 2 | 1 | Upgrading server | 02/02/2024 6:26:16 | 02/02/2024 6:33… | 0:06:45 | Server | WCMP2 | Success | Automatic | Automatic action initi… 3 | 1 | Modify the role/replication … | 02/02/2024 6:26:16 | 02/02/2024 6:26… | 0:00:01 | Cluster | CMP Site1… | Success | Automatic | Automatic action for … 4 | 1 | Wait for replication to sync… | 02/02/2024 6:33:02 | 02/02/2024 6:42… | 0:09:24 | Server | WCMP2 | Success | Automatic | Automatic action wait… 5 | 0 | Failover to new version | 02/02/2024 6:51:05 | 02/02/2024 6:51… | 0:00:00 | Cluster | CMP Site1… | Success | Manual | User initiated action: … 6 | 0 | Preflight Check | 02/02/2024 7:00:17 | 02/02/2024 7:01… | 0:00:54 | Server | WCMP1 | Success | Manual | User initiated action: …
24. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	Navigate to **Upgrade Manager → Upgrade Manager**.  WCMP2 Y Standby 15.0.0.0.0_20.1.0 15.0.0.1.0_6.1.0 Initiate upgrade Completed Successfully at Jan 29, 2024 13:04:49. WCMP1 Minor Y Active 15.0.0.0.0_20.1.0 15.0.0.1.0_6.1.0 Initiate upgrade Completed Successfully at Jan 29, 2024 14:56:02. Successful upgrade status shows the following for both servers in the Primary CMP cluster: • 15.0.x in the Running Release column for both servers • A Y in the Up to Date column • Active or Standby state for both servers in the Primary CMP cluster.
25. ☐	Proceed to next upgrade procedure	Verify the following information: • Primary Site1 is running release 15.0.x • Secondary Site is on release 15.0 • Proceed to the next procedure to upgrade the secondary CMP cluster.
—End of Procedure—		

NOTE: A message "This system has been upgraded but the upgrade has not yet been accepted or rejected. Please accept or reject the upgrade soon." will be displayed after upgrade of each node in the terminal. This message is just a reminder to accept or reject the upgrade and can be ignored.

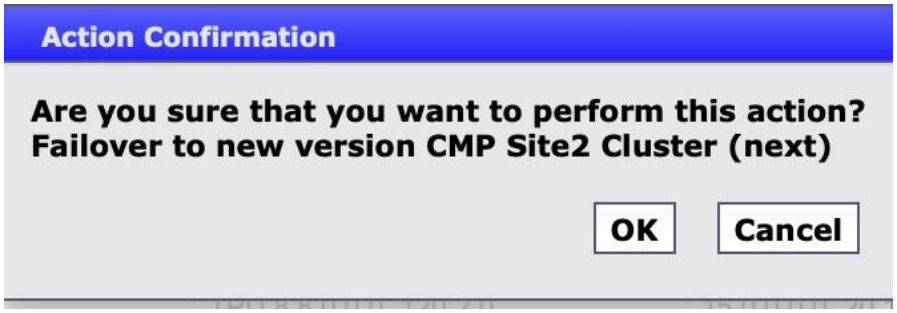
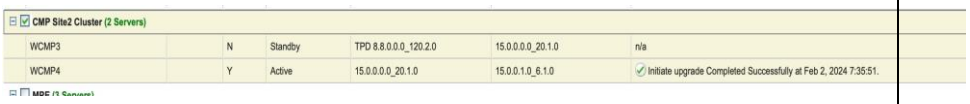
1.6 Upgrade Secondary CMP cluster

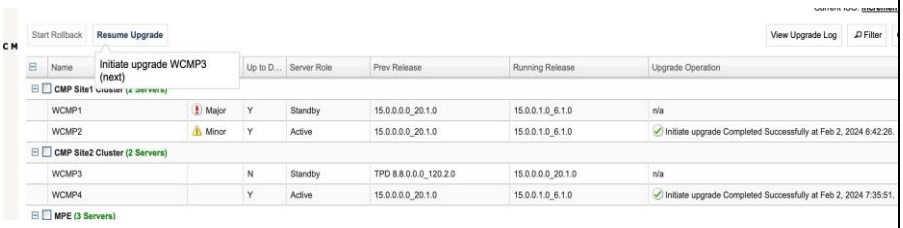
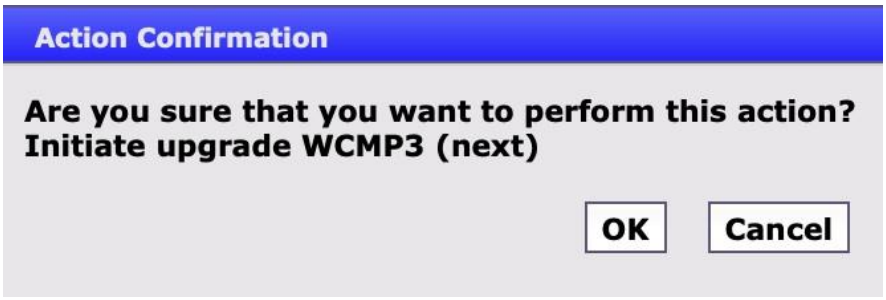
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 6 Upgrade Secondary CMP cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify status of CMP cluster	Navigate to **Upgrade → Upgrade Manager**. • Primary CMP is completely upgraded to 15.0.x • Secondary CMP cluster is on 15.0 
2. ☐	**CMP GUI:** Upgrade Secondary CMP cluster **NOTE:** This takes approximately 20 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. **NOTE:** Click **Filter** and enter CMP in the Name field to see only the CMP servers.  3. Select the Secondary CMP Server cluster at Site2 4. Click **Continue Upgrade**. When hovering over the button, it reads Initiate upgrade <*site2_standbyserver*> (next).  5. Click **OK** to confirm and continue with the operation.  This continues to upgrade the standby server only in the CMP cluster The Upgrade Operation column shows a progress bar along with the upgrade activities. Note: first version column is Prev Release, and second version column

Step	Procedure	Result
		is Running Release.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events: **Expected Critical alarm** **31283** Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **70007** Not all QP resources are ready **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **70502** Cluster Replication Inhibited **31102** DB Replication from a master node DB has failed **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault Upgrade is complete on the standby server of the Site2 CMP cluster when the Initiate upgrade Completed successfully at… message displays in the Upgrade Operation column. 

Step	Procedure	Result
3. ☐	**CMP GUI:** Failover of the Secondary CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP Server cluster at Site2. 3. Click **Continue Upgrade**. Notice the Failover to new version CMP Site2 Cluster message  4. Click **OK** to confirm and continue with the operation.  5. The failover takes about a minute to complete. Wait until the upgraded server is active, running 15.0.x as shown below. Note: first version column is Prev Release, and second version column is Running Release. 

Step	Procedure	Result
4. ☐	**CMP GUI:** Continue upgrade of the Secondary CMP cluster	1. Select the Secondary CMP Server cluster at Site2 2. Click **Continue Upgrade**. When hovering over the button, the message displays the next action, which is upgrading the remaining CMP in standby, still running 15.0.  3. Click **OK** to confirm and continue with the operation.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical alarm** **31283** Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **70007** Not all QP resources are ready **70025** QP Slave database is a different version than the master **Expected Major Alarm** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **70502** Cluster Replication Inhibited **31102** DB Replication from a master node DB has failed **31114** DB replication over SOAP has failed **31106** Database merge to parent failure

Step	Procedure	Result
		31107 Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault
5. ☐	**CMP GUI:** Verify that the upgrade completed successfully.	Navigate to **Upgrade → Upgrade Manager**. Successful upgrade status shows release 15.0.x in the Running Release column and the Upgrade Operation. The Upgrade Operation column shows: • Initiate Upgrade Completed Successfully at message • The correct date and time. 
6. ☐	**CMP GUI:** Verify alarms	Navigate to **System Wide Reports → Alarms → Active Alarms**. **Expected Minor Alarms** **70500** System Mixed Version
7. ☐	Procedure is complete.	Verify the following information: • All CMP clusters upgrades are complete and running release 15.0.x • All MRA and MPE clusters are running release 15.0 The Policy Management system is running in mixed-version mode.
—End of Procedure—		

NOTE: A message "This system has been upgraded but the upgrade has not yet been accepted or rejected. Please accept or reject the upgrade soon." will be displayed after upgrade of each node in the terminal. This message is just a reminder to accept or reject the upgrade and can be ignored.

1.7 Upgrade NON-CMP clusters (MPE, MRA)

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

NOTE: Different cluster types can be upgraded at the same time. For example, 2 MPEs and 2 MRAs can be upgraded in parallel.

The following steps use build 15.0 as example.

1.7.1 Upgrade Preparation

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

Procedure 7: Configuration Preparation

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into CMP server	Use the supported browser to login as the admin user or as a user with administrative privileges.
2. ☐	**CMP GUI:** Verify current Upgrade Manager status and software release 15.0.x DIU ISO files	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify that all CMP clusters have both Active, Standby status. 3. Verify that all MPE and MRA clusters have an Active, Standby, and Spare server. 4. Verify that Policy Management release 15.0.x DIU ISO files are available on `/var/TKLC/upgrade` for all MPE, and MRA clusters. One DIU ISO per server 5. Verify that the CMP cluster is upgraded successfully and running Policy Management release 15.0.x.
—End of Procedure—		

1.7.2 Upgrade MRA and MPE Servers

Use this procedure to upgrade one or more clusters (MPE and/or MRA).

This procedure is applicable for a 15.0 upgrade to 15.0.x

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

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

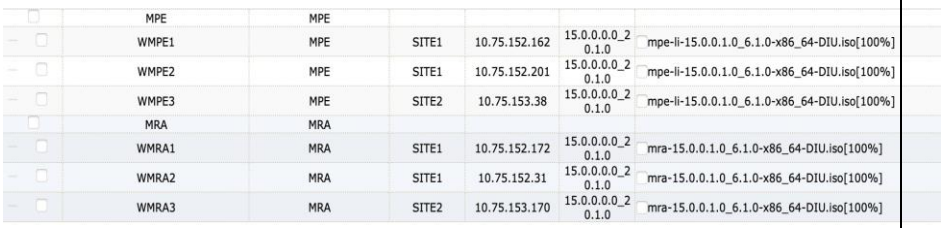
1. Select and start upgrade on the standby server
2. Failover
3. Re-apply configuration
4. Continue to upgrade the spare server
5. Continue upgrade on remaining server
6. (MPE only) Re-apply configuration one MPE cluster at a time

NOTES:

- All CMP clusters must be upgraded to Policy Management release 15.0.x prior to performing the following procedures.
- Four (4) clusters (8 for 15.0) can be running the upgrade at one time.
- Only ONE cluster can be selected for upgrade activity, bulk selection of servers is not supported in release 15.0.x.

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

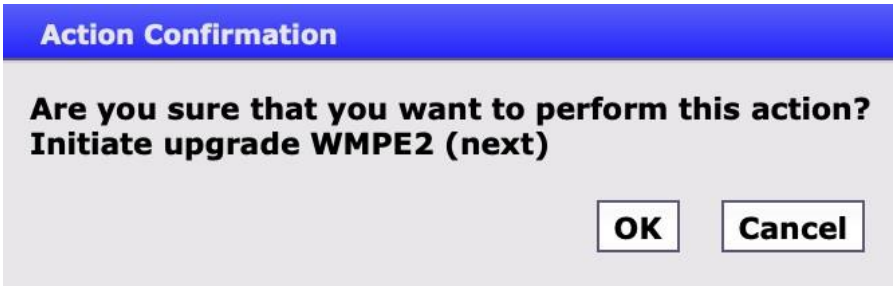
Procedure 8: Upgrade MRA and MPE Servers

Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the MPE/MRA servers to be upgraded	Perform the following: 1. Check for current active alarms 2. Reset MPE/MRA counters to make a baseline - For the MPE: **Policy Server → Configuration →** <*server_name*> **→ Reports → Reset Counters** - For the MRA: **MRA → Configuration →** <*server_name*> **→ Reports → Reset Counters** 3. Go to the KPI Dashboard and capture a screenshot. 4. **System Wide Reports → KPI Dashboard**
2. ☐	**CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify information for the MRA/MPE servers: - Current release 15.0 installed - Active/Standby/Spare status - DIU ISO version to be deployed is 15.0.x (verify the current DIU ISO files are 15.0.x by going to **Upgrade → ISO Maintenance**) Note: first version column is Prev Release, and second version column is Running Release. 
3. ☐	**CMP GUI:** Upgrade clusters **NOTE:** The upgrade of a single server takes approximately 20 minutes to complete.	**NOTE:** Start the upgrade on ONE cluster. Wait until the cluster shows OOS, and then continue with the next cluster and so on. Up to 16 clusters may be running upgrade at any time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the cluster to be upgraded, it can be an MRA or MPE 3. Click **Continue Upgrade**.

MPE	MPE					
WMPE1	MPE	SITE1	10.75.152.162	15.0.0.0.0_2 0.1.0	mpe-li-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]	
WMPE2	MPE	SITE1	10.75.152.201	15.0.0.0.0_2 0.1.0	mpe-li-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]	
WMPE3	MPE	SITE2	10.75.153.38	15.0.0.0.0_2 0.1.0	mpe-li-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]	
MRA	MRA					
WMRA1	MRA	SITE1	10.75.152.172	15.0.0.0.0_2 0.1.0	mra-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]	
WMRA2	MRA	SITE1	10.75.152.31	15.0.0.0.0_2 0.1.0	mra-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]	
WMRA3	MRA	SITE2	10.75.153.170	15.0.0.0.0_2 0.1.0	mra-15.0.0.1.0_6.1.0-x86_64-DIU.iso[100%]	

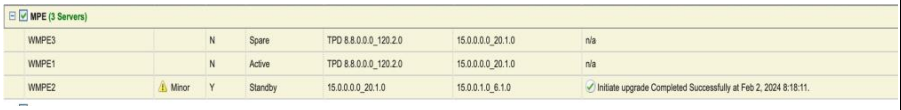
Step	Procedure	Result

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



Wait until the cluster reports OOS before selecting the next cluster.

Follow the progress in the Upgrade Operation column.



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

Expected Critical Alarms

31283 HA Server Offline / Lost Communication with server

70001 QP_procmgr failed

31227 HA availability status failed

70007 Not all QP resources are ready

Expected Major Alarm

31233 High availability path loss of connectivity

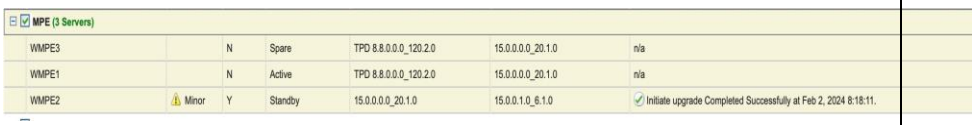
70004 QP Processes down for maintenance

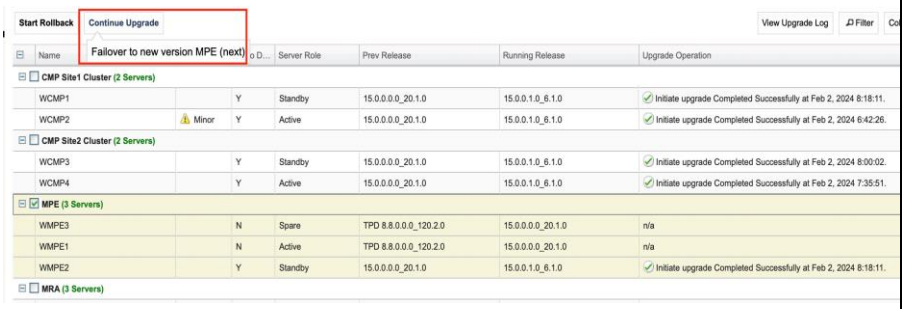
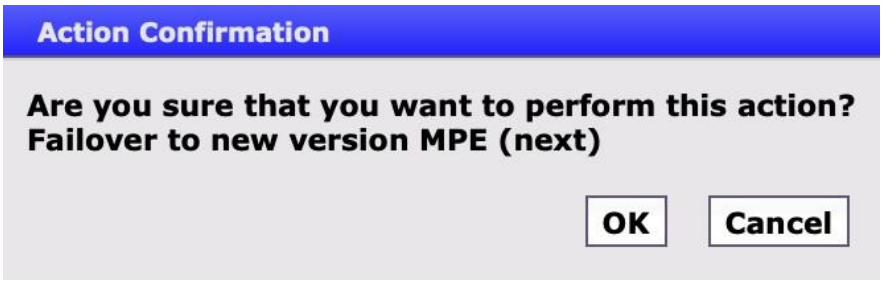
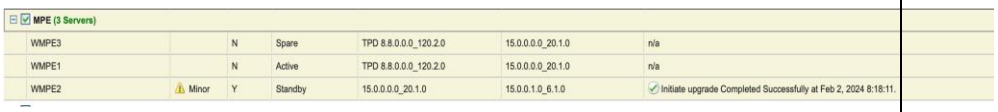
Expected Minor Alarms

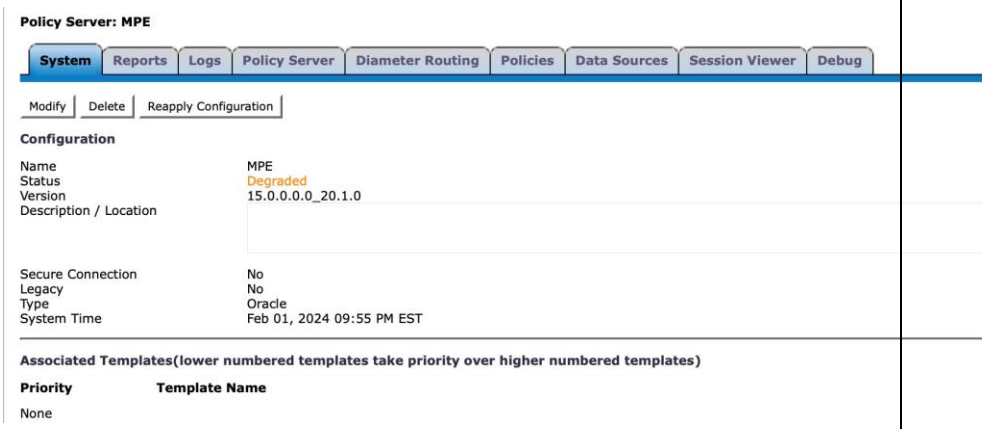
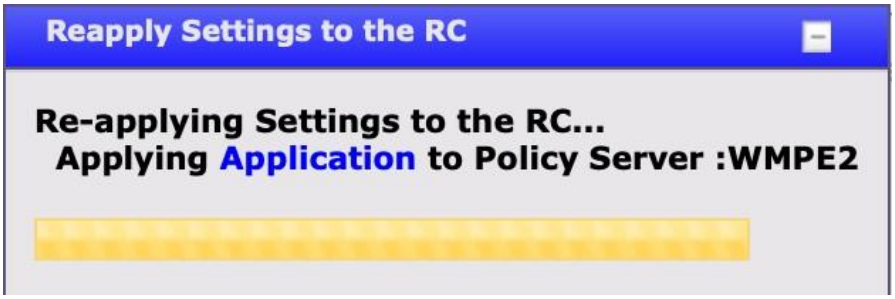
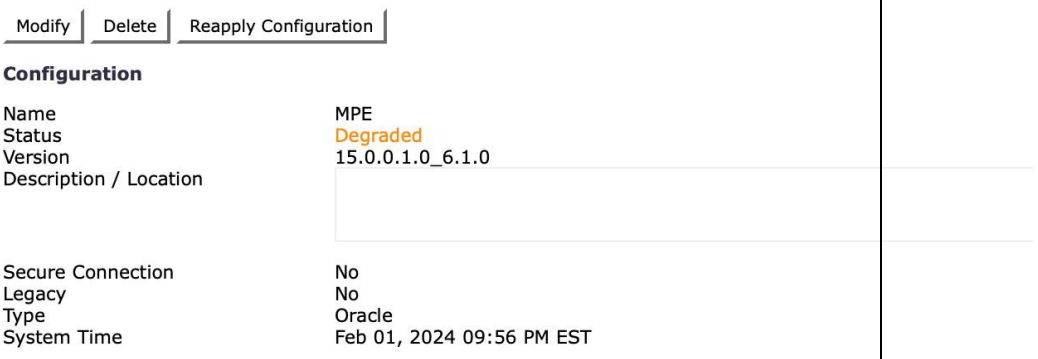
70503 Server Forced Standby

70507 Upgrade In Progress

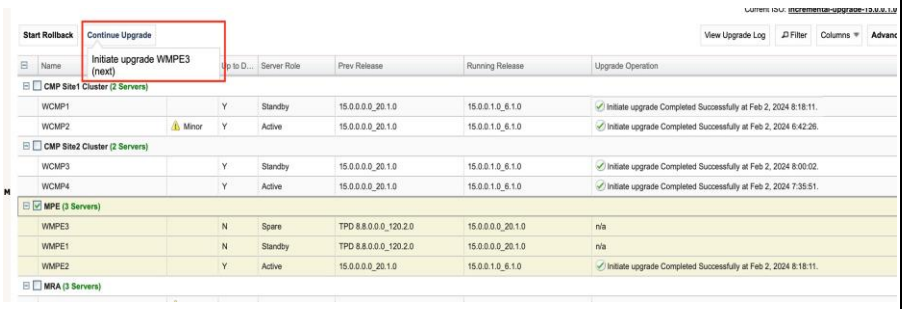
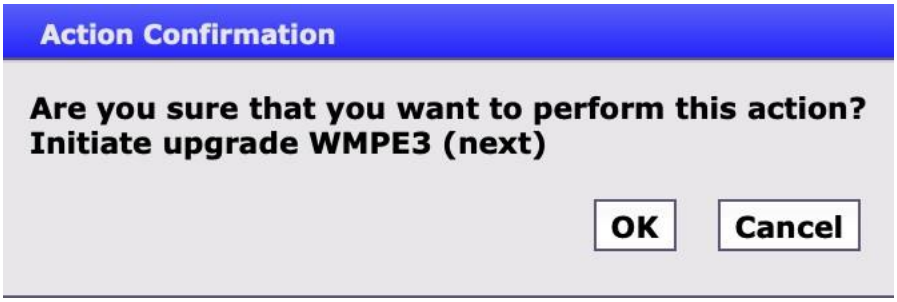
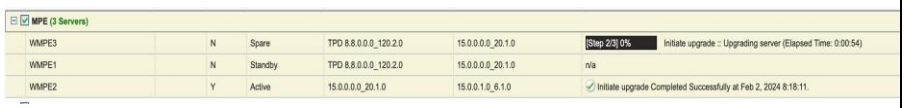
70500 System Mixed Version

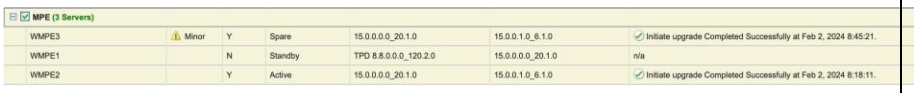
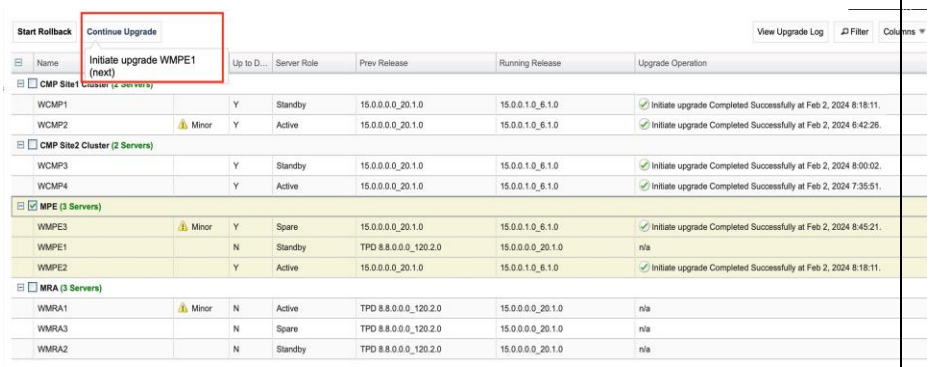
Step	Procedure	Result
		70501 Cluster Mixed Version **70502** Cluster Replication Inhibited **31102** DB Replication from a master node DB has failed **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31282** HA Management Fault **78001** Rsync Failed Upgrade is complete on the first server in the cluster when the Initiate upgrade completed successfully at… message displays in the Upgrade Operation column. The server goes back to Standby state when the upgrade completes. Note: first version column is Prev Release, and second version column is Running Release.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events. Alarm 31224—HA configuration error (major) is raised noting that there is a configuration error. This clears a few minutes after the upgrade completes on the first server. The following minor alarms may be present: **<u>Expected Minor Alarms</u>** **78001** Rsync Failed **70500** System Mixed Version **70501** Cluster Mixed Version **70503** Server Forced Standby

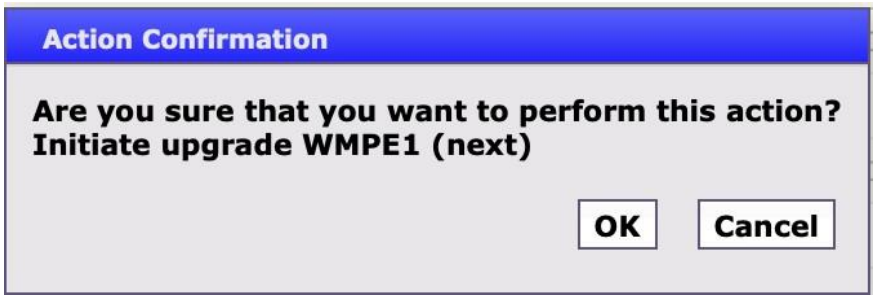
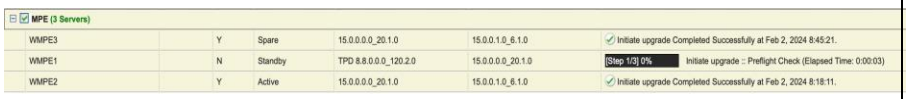
Step	Procedure	Result
4. ☐	**CMP GUI:** Continue to upgrade the MRA/MPE clusters. Next operation is a failover. **NOTE:** 4 clusters (8 for 15.0) can be running the upgrade process at one time.	Fail over ONE cluster at a time and wait until the upgraded server becomes active before moving on to the next cluster. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the cluster being upgraded (it can be an MRA or MPE) 3. Click **Continue Upgrade**. When hovering over the button, it says Failover to new version  4. Click **OK** to confirm and continue with the operation. It starts to failover the cluster.  Wait until failover completes before failing over the next cluster, This takes a minute or two to complete. Verify the 15.0.x server is now active. The process is complete when there is an active/standby at site 1 and spare at site 2. Note: first version column is Prev Release, and second version column is Running Release. 

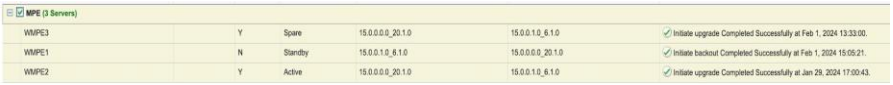
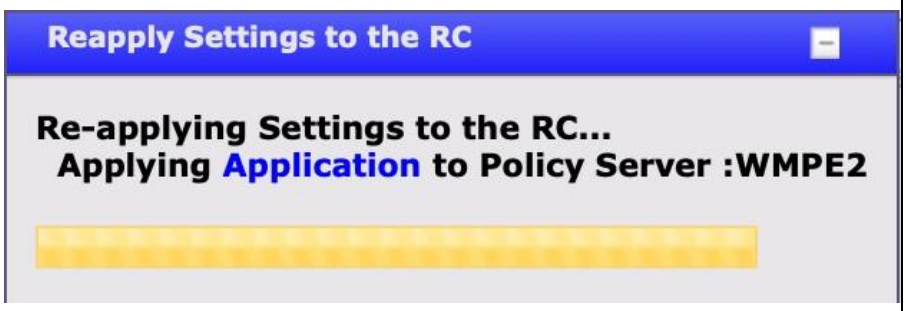
Step	Procedure	Result
5. ☐	**CMP GUI:** Reapply configuration on MPE/MRA cluster that completed the upgrade successfully.	• For MPE: **PolicyServer → Configuration →** <*mpe_cluster name*> **→ System** • For MRA: **MRA → Configuration →** <*mra_cluster name*> **→ System** The selected cluster shows status Degraded as it has different releases for the Active and Standby servers. It may display Config mismatch as well. This is expected. 1. Click **Reapply Configuration**.  **Policy Server: MPE** System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sources | Session Viewer | Debug Modify | Delete | Reapply Configuration **Configuration** Name: MPE Status: Degraded Version: 15.0.0.0.0_20.1.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Feb 01, 2024 09:55 PM EST **Associated Templates(lower numbered templates take priority over higher numbered templates)** **Priority** **Template Name** None **NOTE:** A progress bar displays for the MPE reapply configuration only. The MRA reapply configuration does not display the progress bar.  **Reapply Settings to the RC** **Re-applying Settings to the RC...** **Applying Application to Policy Server :WMPE2** 2. Note the version is successfully changed to the upgraded release 15.0.x. **NOTE:** The status shows Degraded because the servers are still in different releases.  Modify | Delete | Reapply Configuration **Configuration** Name: MPE Status: Degraded Version: 15.0.0.1.0_6.1.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Feb 01, 2024 09:56 PM EST

Step	Procedure	Result
6. ☐	**CMP GUI:** Current alarms	During the upgrade activities, the following alarms may be generated and are considered normal reporting events. **Expected Critical alarm** None **Expected Major Alarm** **78001** Rsync Failed **Expected Minor Alarms** **70503** Server Forced Standby **70502** Cluster Replication Inhibited **70500** System Mixed Version **70501** Cluster Mixed Version **71402** Connectivity Lost **31101** Database replication to slave failure
7. ☐	**CMP GUI:** Verify traffic becomes active within 90 seconds	1. Navigate to Upgrade Manager → System Maintenance. - If traffic is active, go to step 9. - If traffic does not become active within 90 seconds: 2. Select the Partially upgraded cluster, and select **Operations → Rollback**. The pre-15.0 MPE server should become active and resume handling traffic.
8. ☐	**CMP GUI:** Reapply configuration	• For MPE: **Policy Server → Configuration → <***mpe_cluster name***> → System** • For MRA: **MRA → Configuration → <***mra_cluster name***> → System** 1. Click Reapply Configuration 2. Verify that the version is changed back to 15.0, and the action report success. If NOT, stop and contact Oracle support to back out of the partially upgraded cluster.
9. ☐	**CMP GUI:** Continue upgrade of the MRA/MPE clusters. Next operation is initiate upgrade on the Spare server	Continue the upgrade on ONE cluster, when the server goes into OOS, continue with the next cluster and so on. **NOTE:** Up to 16 clusters can be running the upgrade process at one time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for a cluster. - Select one cluster at a time - Can be an either an MRA or MPE cluster 3. Click **Continue Upgrade**. When hovering over the button, it reads Initiate upgrade… on the spare server

Step	Procedure	Result
		 4. Click **OK** to confirm and continue with the operation.  Wait until the cluster reports OOS before selecting the next cluster Follow the progress in the Upgrade Operation column.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events—these is cleared after the MPE cluster is completely upgraded. **Expected Critical Alarms** **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **70007** Not all QP resources are ready **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **70502** Cluster Replication Inhibited

Step	Procedure	Result
		Upgrade is complete on the spare server in the georedundant cluster when: • The Initiate upgrade Completed successfully… message shows in the Upgrade Operation column. Note: first version column is Prev Release, and second version column is Running Release.  • The server goes back to the Spare state. • The Up to Date column shows a Y (YES). The Active and Spare servers are on release 15.0.x and the current Standby is on the previous release. Note: first version column is Prev Release, and second version column is Running Release.
10. ☐	**CMP GUI:** Continue to upgrade the MRA/MPE clusters. Next operation is Initiate upgrade on the standby server	Continue the upgrade on ONE cluster, when the server goes into OOS, continue with the next cluster and so on. Up to 16 clusters may be running the upgrade at one time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the checkbox for a cluster: - Select one cluster at a time - Can be an either an MRA or MPE cluster 3. Click **Continue Upgrade**. When hovering over the button, the message indicates the next action, which is to initiate the upgrade of the standby server.  4. Click **OK** to confirm and continue with the operation. It begins the final server upgrade of the cluster.

Step	Procedure	Result
		 Wait until the cluster reports OOS before selecting the next cluster Follow the progress in the Upgrade Operation column.  During the upgrade activities, the following alarms may be generated and are considered normal reporting events—these is cleared after the MPE cluster is completely upgraded. **Expected Critical Alarms** **31283** HA Server Offline / Lost Communication with server **31227** HA availability status failed **70001** QP_procmgr failed **70007** Not all QP resources are ready **Expected Major Alarm** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms** **70503** Server Forced Standby **70507** Upgrade In Progress **70500** System Mixed Version **70501** Cluster Mixed Version **70502** Cluster Replication Inhibited **31114** DB replication over SOAP has failed **31106** Database merge to parent failure **31107** Database merge from child failure **31101** Database replication to slave failure **31102** Database replication from master failure **31113** DB replication manually disabled Upgrade is complete on the third server in the georedundant cluster when: • The completed successfully message shows in the Upgrade Operation column.

Step	Procedure	Result
		• The server goes back to the Standby state. • The Up to Date column shows a Y (YES). Note: first version column is Prev Release, and second version column is Running Release.  All servers are now running release 15.0.x.
11. ☐	Exchange SSH Keys	1. Enter the following command: $ sudo qpSSHKeyProv.pl--prov You are prompted: The password of admusr in topology **Note**: The above command to exchange SSH keys needs to be run on the active CMP only. 2. Enter the admusr password (admusr_password). The procedure exchanges keys with the rest of the servers in the Policy Management topology. If the key exchange is successful, the procedure displays the message "SSH keys are OK."
12. ☐	**CMP GUI:** Reapply configuration on the fully upgraded MPE clusters.	1. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ System** 2. Click **Reapply Configuration**. **NOTE:** A progress bar displays for the MPE reapply configuration. 
13. ☐	Repeat steps 1 through 14 for the next MPE or MRA clusters	Proceed with next cluster(s)

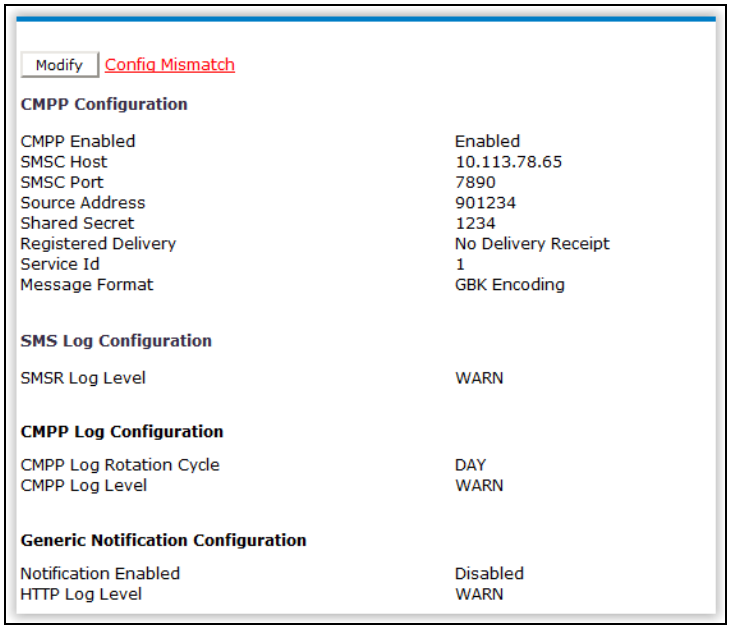
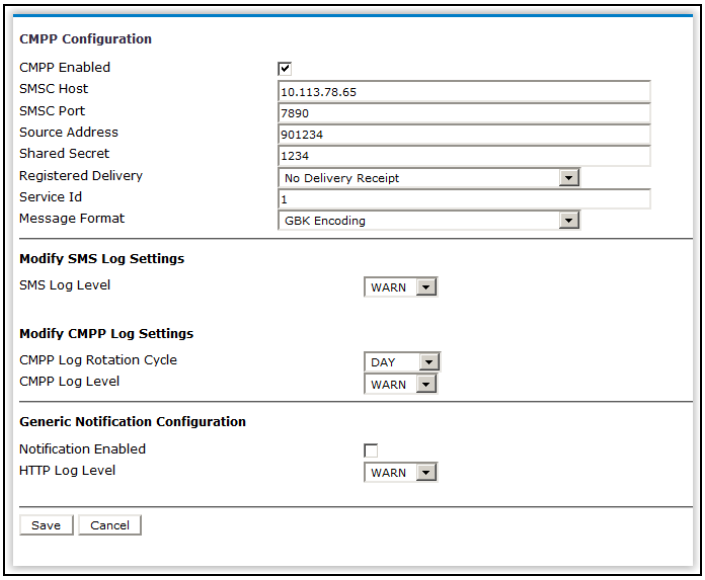
Step	Procedure	Result
14. ☐	Upgrade Completed	At this point all servers have been upgraded.

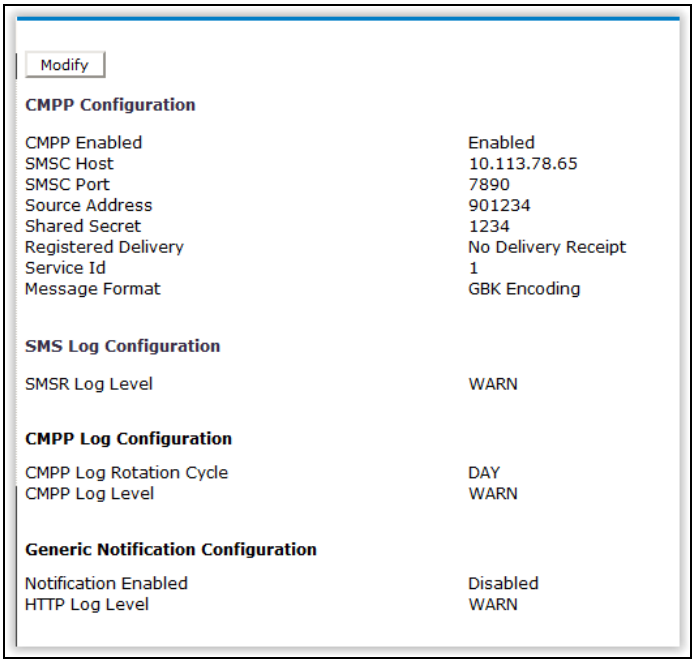
Upgrade Manager

Current ISO: incremental-upgrade-15.0.0.1.0_6.1.0

Start Rollback | Start Upgrade | View Upgrade Log | Filter | Columns | Advanced

Name	Alarm Sev...	Up to D...	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
WCMP2		Y	Active	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 13:04:49.
WCMP1		Y	Standby	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 14:56:02.
CMP Site2 Cluster (2 Servers)						
WCMP4		Y	Active	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 15:15:22.
WCMP3		Y	Standby	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 16:01:33.
MPE (3 Servers)						
WMPE1		Y	Standby	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 17:51:03.
WMPE2		Y	Active	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 17:00:43.
WMPE3		Y	Spare	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 17:30:53.
MRA (3 Servers)						
WMRA2		Y	Active	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 17:04:22.
WMRA3		Y	Spare	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 17:32:12.
WMRA1		Y	Standby	15.0.0.0.0_20.1.0	15.0.0.1.0_6.1.0	Initiate upgrade Completed Successfully at Jan 29, 2024 17:51:03.

Step	Procedure	Result
15. ☐	**CMP GUI:** Modify/save SMSR configuration	**System Administration → SMS Relay → Modify** **NOTE: This step is only for Wireless-C system. If you do not see SMS Relay under System Administration, skip this step.** Initial access into this configuration upon upgrade to release 15.0.x, the configuration shows as such with Config Mismatch.  1. Click **Modify.** The following is an example of the SMSR configuration. DO NOT change any of the configuration if it has been working in the past.  2. Click **Save** to save the configuration and continue as shown.

Step	Procedure	Result
		 **NOTE:** The Config Mismatch message is not there with the saved configuration.
—End of Procedure—		

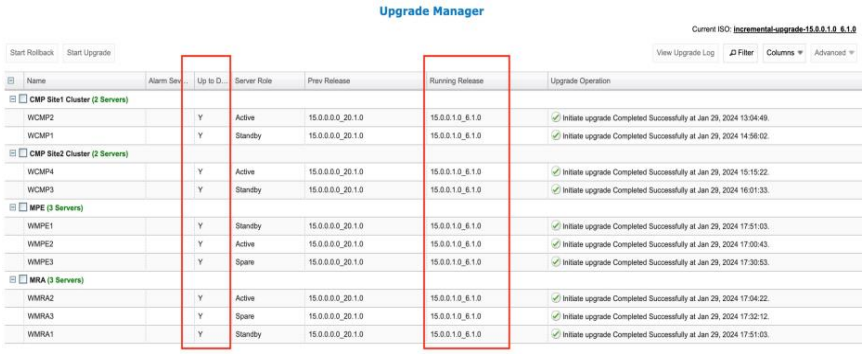
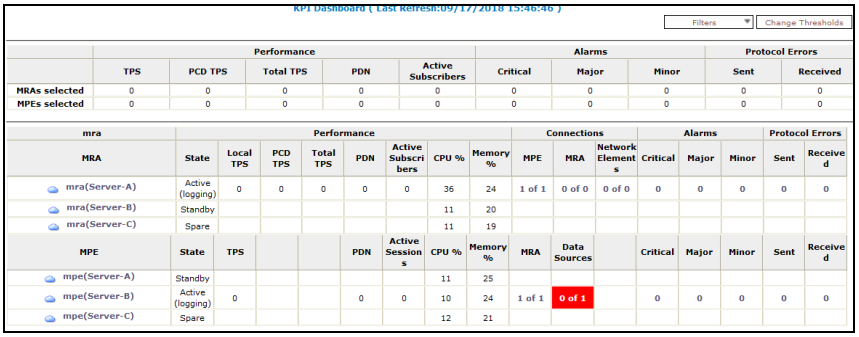
NOTE: A message "This system has been upgraded but the upgrade has not yet been accepted or rejected. Please accept or reject the upgrade soon." will be displayed after upgrade of each node in the terminal. This message is just a reminder to accept or reject the upgrade and can be ignored.

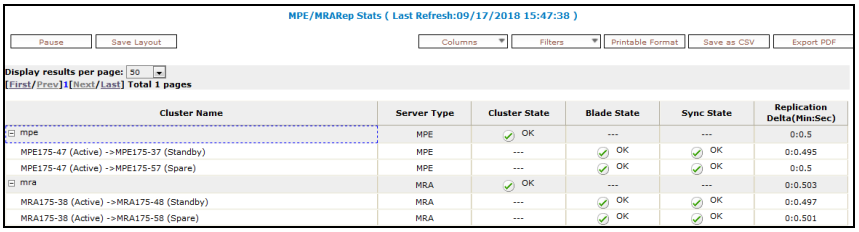
1.8 Post Upgrade health Check for wireless systems

NOTE: This section is used when the entire topology is running release 15.0.x

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

Procedure 9 Post Upgrade health Check for wireless systems

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the upgrade is successful on all CMP/MRA/MPE clusters.	1. Navigate to **Upgrade → Upgrade Manager**. 2. View the Up to Date, Running Release, and Upgrade Operation columns and verify they read Y, 15.0.x…, and Initiate upgrade completed successfully at… respectively, for all servers in all clusters. 
2. ☐	**CMP GUI:** View current alarms	1. Navigate to **System Wide Reports→Alarms→Active Alarms**. 2. Verify that all alarms due to the upgrade have been cleared. 
3. ☐	**CMP GUI:** View current KPIs	1. Navigate to **System Wide Reports→KPI Dashboard**. 2. Make sure everything looks normal. 

Step	Procedure	Result
4. ☐	**CMP GUI:** Replication stats	Navigate to System Wide Reports→Others→MPE/MRA Rep Stats (for a wireless system) **Wireless:** 
—End of Procedure—		

1.9 Backout (ROLLBACK) 15.0 wireless mode

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

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

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

1.9.1 Backout Sequence

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

1. Back out the non-CMP clusters (from both Site1 and Site2, if applicable)
2. Back out the Secondary CMP cluster (if applicable)
3. Back out the Primary CMP cluster

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

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

1.9.2 Pre-requisites

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

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

1.9.3 Backout of Fully Upgraded Cluster

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

Use this to backout a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster is on a pre-15.0.x release with Active, Standby, or Spare status.

Expected pre-conditions:

1. Primary Active CMP is on Release 15.0.x
2. Secondary CMP cluster is on Release 15.0.x
3. All MPE/MRA Clusters are on Release 15.0.x

1.10.3.1 Backout Sequence

This procedure applies to a cluster. The non-CMP cluster types (MRA, MPE) is in georedundant mode with active, standby, and spare servers. CMP clusters may be in Site1 or Site2. Each server backout will take about 20 minutes.

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

Overview on Backout/Rollback MRA/MPE cluster

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

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

Backout Secondary CMP (if applicable)

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

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

Backout Primary CMP

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

1. Back out of the Primary standby CMP cluster.
2. Failover to older version CMP cluster.
3. Log back into the Primary CMP VIP.
4. If needed, go to **Policy Server→ Configuration → Policy Server** and click **Reapply Configuration**.
5. Wait for 10-15 minutes before the rollback of secondary CMP (in Primary Site) to allow secondary site CMP nodes to sync with the new MySQL master.
6. Back out of the new standby server.

1.10.3.2 Back-out Partially Upgraded MPE/MRA Cluster

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

Expected Pre-conditions:

1. Primary Active CMP is on Release 15.0.x
2. Cluster is any of MPE or MRA
3. One server of target cluster is on Release 15.0.x
4. Other servers of target cluster are on Release 15.0

NOTES:

- This procedure must be performed within a maintenance window.

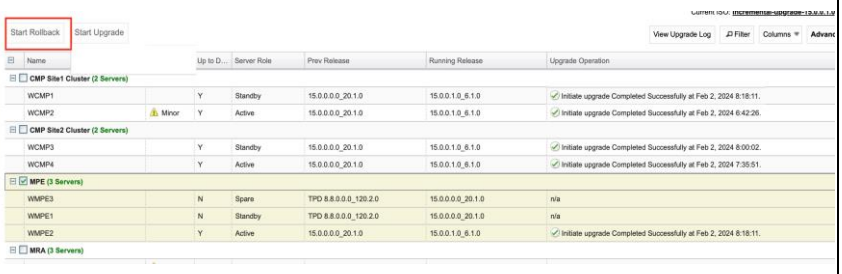
- This procedure takes approximately 15 minutes per blade.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

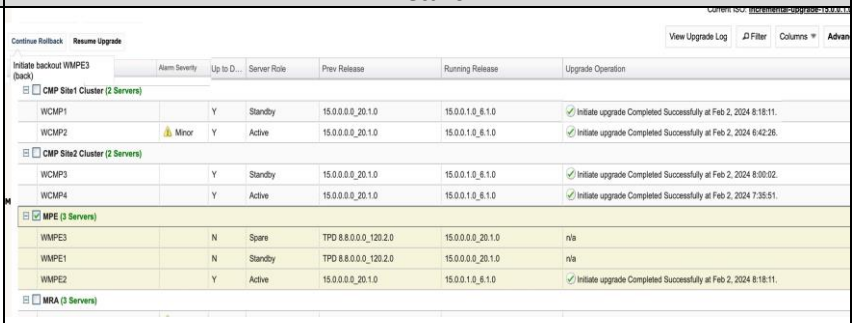
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 10: Back-out Partially Upgraded MPE/MRA Cluster

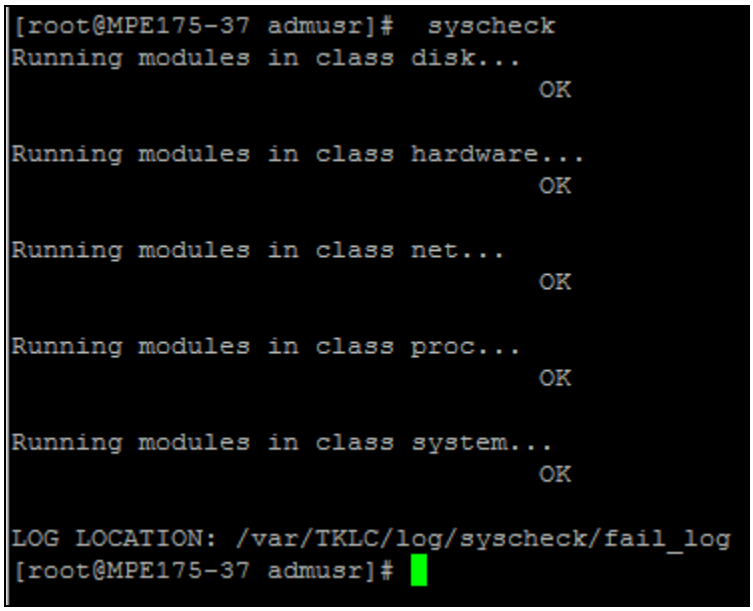
Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of affected Clusters	Navigate to **Upgrade → Upgrade Manager**. Confirm status of the cluster to be backed out: • Primary Active CMP is on Release 15.0.x • Target Cluster has 2 servers on Release 15.0, and 1 server on Release 15.0.x • Active server is on 15.0

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

3. ☐	**CMP GUI:** Verify the status of affected Clusters **NOTE:** This takes approximately 15 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the partially upgraded cluster to back-out. 3. Select the cluster (one cluster at a time) (can be an MRA or MPE) 4. Click Start Rollback. When hovering over the button, it indicates the server to get backed out. 

Step	Procedure	Details
		 5. Click **OK** to confirm and continue with the operation. It begins to back-out. Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message **31284** High availability remote subscriber has not received a heartbeat **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **70502** Cluster Replication Inhibited **31100** The DB replication process is impaired by a s/w fault

Step	Procedure	Details
		Back-out of the server is complete when the following message (Initiate Back-out Completed Successfully) 

4. ☐	**MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to back-out server and verify that there are not anyt any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		3. **NOTE:** Permissions should be the following,
		`drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following; otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

—End of Procedure—		

1.10.3.3 Back-out Fully Upgraded MPE/MRA Cluster

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

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

This procedure is used to back-out a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster is on Release 15.0 (MRA, MPE, CMP) with Active, Standby status.

Expected pre-conditions:

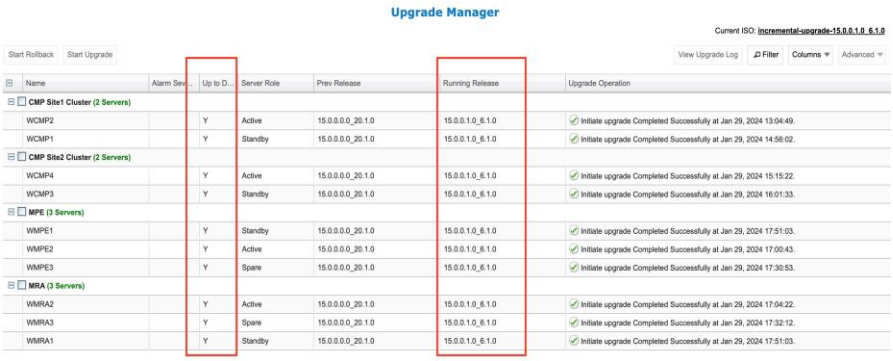
1. Primary Active CMP is on Release 15.0.x
2. Cluster is of MPE or MRA
3. Servers of target cluster are on Release 15.0.x in either in Active, Standby, Force Standby or Spare role

NOTES:

- This procedure must be performed within a maintenance window.
- This procedure takes approximately 45-60 minutes per MPE or MRA cluster.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

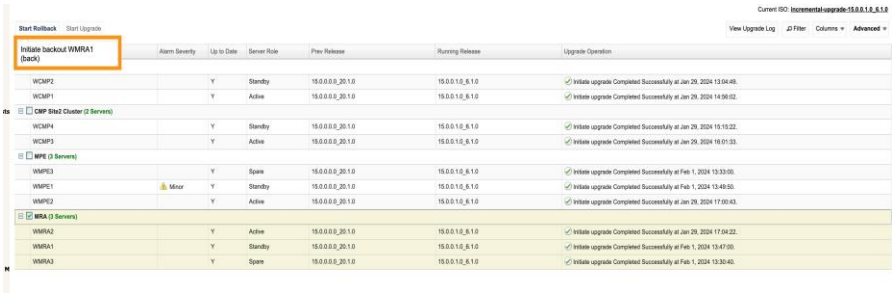
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

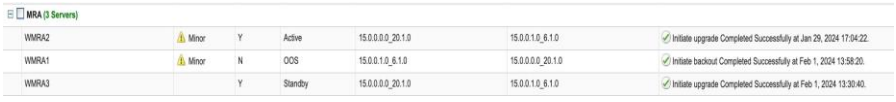
Procedure 11 Back-out Fully Upgraded MPE/MRA Cluster

Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of affected Clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm status of the cluster is backed out: - Primary Active CMP is on Release 15.0.x - MPE/MRA is on Release 15.0.x Up to Date column shows Y for all servers **EXAMPLE:** 
2. ☐	**MPE/MRA SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby and Spare servers to be backed out as admusr. 2. **NOTE:** Currently Active server is checked after the failover later on in this procedure.

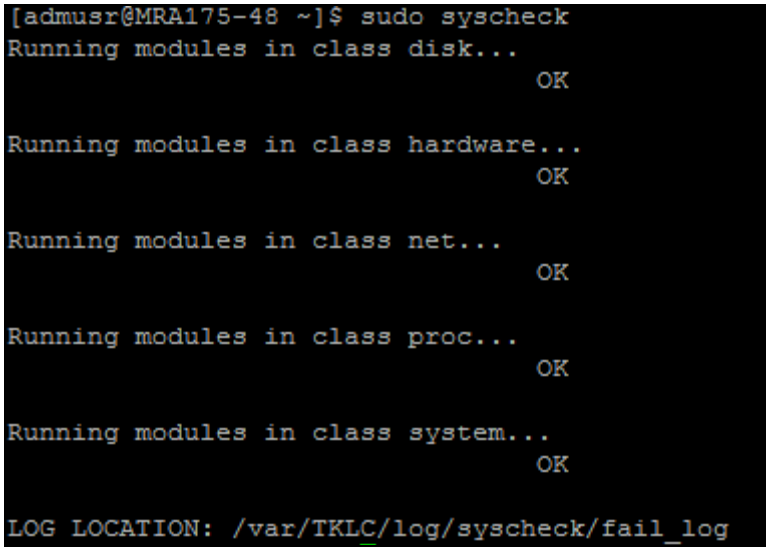
Step	Procedure	Details

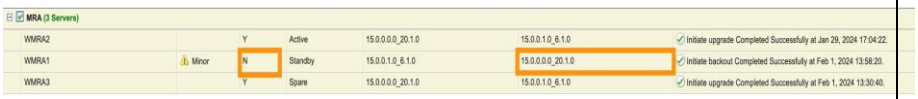
		`$ ls -lh /var/log/messages`
		3. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		4. Verify:
		`$ ls -lh /var/log/messages`

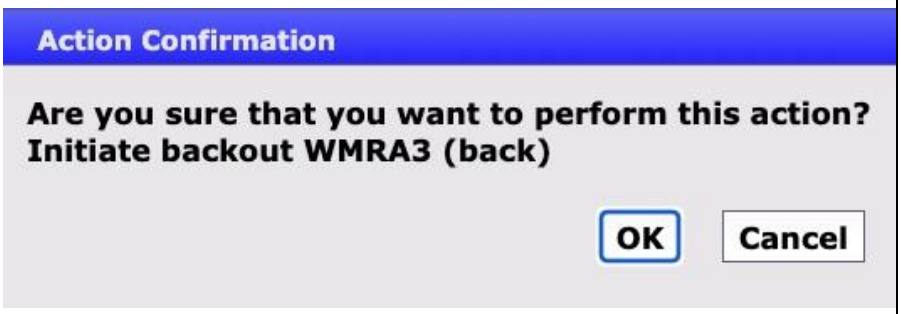
3. ☐	**CMP GUI:** Initiate Back-out **NOTE:** Each back-out of one blade server completes in approximately 15 minutes. **NOTE:** Up to 16 clusters can be backed out at the same time, selecting one at a time.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the cluster (one cluster at a time, can be an MRA or MPE). 3. Click **Start Rollback**. When hovering over the button, it indicates the server to be backed out. In this case it is the current standby server.  4. Click **OK** to confirm and continue with the operation. It begins to back-out.  Follow the progress status in the Upgrade Operation column. At this point, the server backing out goes into OOS state. Wait until the server goes to an OOS state before selecting the next cluster to back-out. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out.

Step	Procedure	Details
		Expected Critical Alarms **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message …. **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **70502** Cluster Replication Inhibited **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server shows running release of 15.0 and return to standby with an N in the Up To Date column. Note: first version column is Prev Release, and second version column is Running Release. 
4. ☐	**CMP GUI:** Verify the back-out is successful	1. Select the partially backed out cluster 2. Select the View Upgrade LOG 

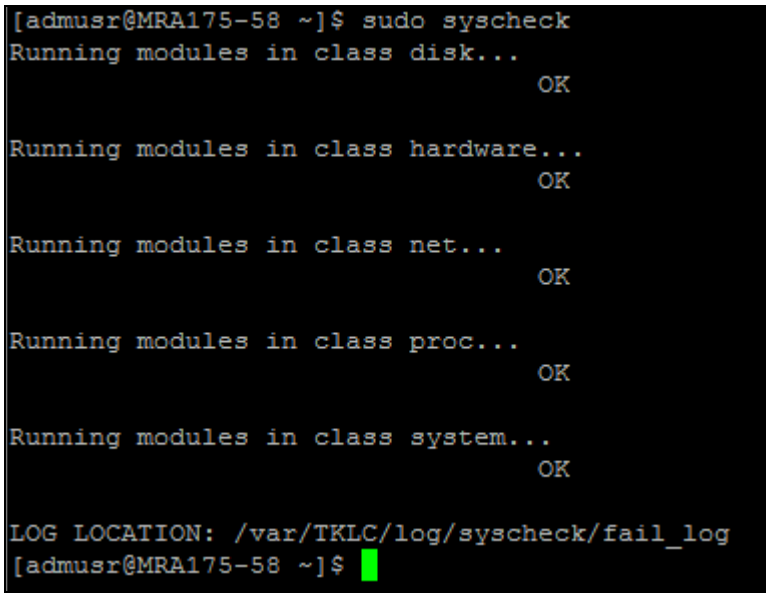
Step	Procedure	Details
		3. Check upgrade logs for the remainder of partially backed out clusters.

5. ☐	**MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Standby server and verify that there are not anyt any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		3. **NOTE:** Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

6. ☐	Confirm MPE/MRA server status	Ensure that the Active/Spare are on 15.0.x and the standby server shows running release of 15.0. Note: first version column is Prev Release, and second version column is Running Release. 

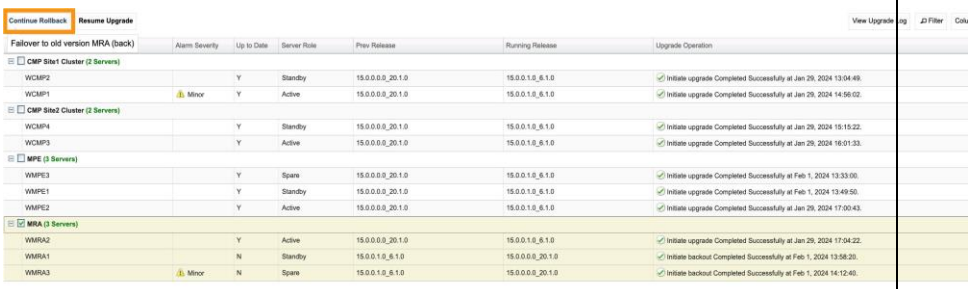
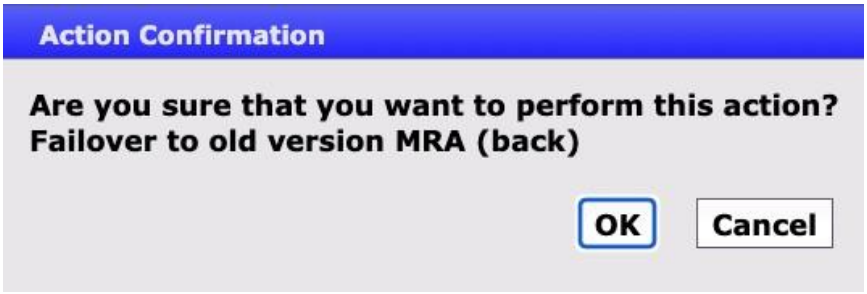
Step	Procedure	Details
7. ☐	**CMP GUI:** Continue the back-out of the MRA / MPE clusters. Next operation is Initiate Back-out on spare server **NOTE:** Up to 16 clusters can be backed out at the same time, selecting one at a time. **NOTE:** This takes approximately 15 minutes to complete.	1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click **Continue Rollback**. When hovering over the button, it indicates to initiate Back-out.  3. Click **OK** to confirm and continue with the operation.  Wait until the server goes to an OOS state before selecting the next cluster. Follow the progress status in the Server Role column. The Server shows OOS in the server role until the back-out completes. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress

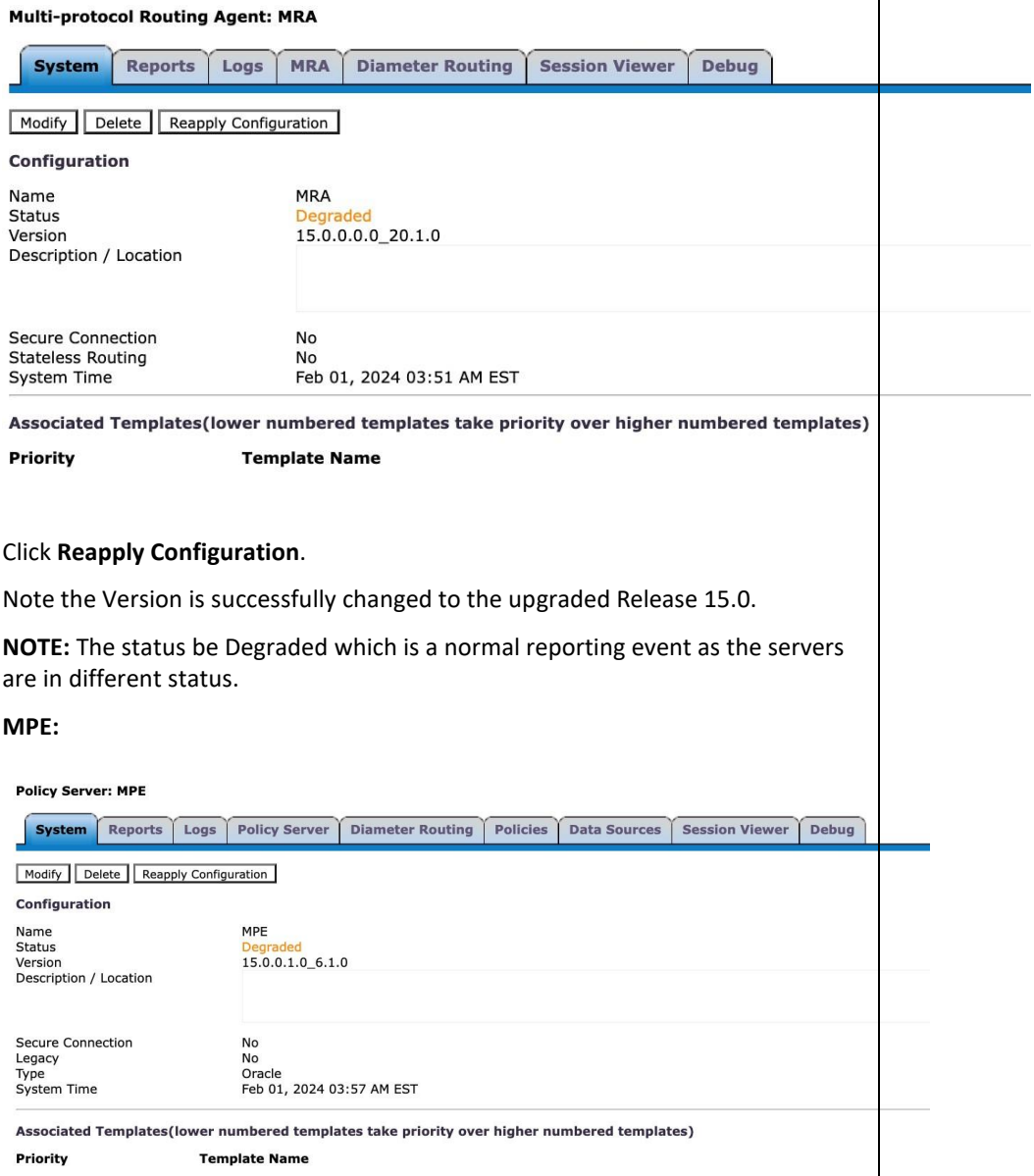
Step	Procedure	Details
		70501 The Cluster is running different versions of software **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message …. **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **70502** Cluster Replication Inhibited **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server goes back to running release of 15.0. Note: first version column is Prev Release, and second version column is Running Release. 

8. ☐	**MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Spare server as admusr.
		2. Verify that there are not anyt any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		4. **NOTE:** Permissions should be the following,

Step	Procedure	Details

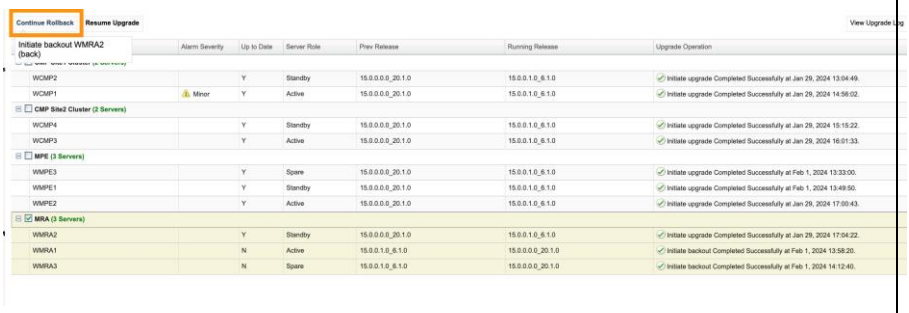
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		5. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		6. Verify:
		`$ ls -l /`
		7. Perform **`syscheck`**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

Step	Procedure	Details
9.	**CMP GUI:** Continue the back-out of the MRA / MPE clusters. Next operation is failover to the 15.0 server. **NOTE:** Up to 16 clusters can be backed out at the same time, selecting one at a time.	Current state of the cluster must be as follows. - Active Server is on Release 15.0 - Standby Server is on Previous release - Spare Server is on Previous release 1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click **Continue Rollback**. When hovering over the button, it informs you to failover to old version, which is 15.0  3. Click **OK** to confirm and continue with the operation. It begins to failover.  Wait until the server fails over before selecting the next cluster. This takes approximately 2 minutes **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **Expected Major Alarms** **74603** The number of failed MPE primary cluster reaches the threshold **Expected Minor Alarms** **70503** The server is in forced standby **31102** DB replication from a master DB has failed **71402** Diameter Connectivity Lost **31101** DB replication to a slave DB has failed **78001** Transfer of Policy jar files failed State of the cluster looks like the following when the failover completes. Note: first version column is Prev Release, and second version column is Running Release. 

Step	Procedure	Details
10. ☐	**CMP GUI:** Reapply Configuration on MPE/MRA cluster that competed the failover successfully	• MPE Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ System** • MRA: Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ System** The selected Cluster status is Degraded as expected as shown:  **Multi-protocol Routing Agent: MRA** System | Reports | Logs | MRA | Diameter Routing | Session Viewer | Debug Modify | Delete | Reapply Configuration **Configuration** Name: MRA Status: Degraded Version: 15.0.0.0.0_20.1.0 Description / Location: Secure Connection: No Stateless Routing: No System Time: Feb 01, 2024 03:51 AM EST **Associated Templates(lower numbered templates take priority over higher numbered templates)** **Priority** **Template Name** Click **Reapply Configuration**. Note the Version is successfully changed to the upgraded Release 15.0. **NOTE:** The status be Degraded which is a normal reporting event as the servers are in different status. **MPE:** **Policy Server: MPE** System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sources | Session Viewer | Debug Modify | Delete | Reapply Configuration **Configuration** Name: MPE Status: Degraded Version: 15.0.0.1.0_6.1.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Feb 01, 2024 03:57 AM EST **Associated Templates(lower numbered templates take priority over higher numbered templates)** **Priority** **Template Name**
11. ☐	**MPE/MRA SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr. `$ ls -lh /var/log/messages` 2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the

Step	Procedure	Details

		following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`
		`$ sudo cat /dev/null > /var/log/messages`
		`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`
		3. Verify:
		`$ ls -lh /var/log/messages`

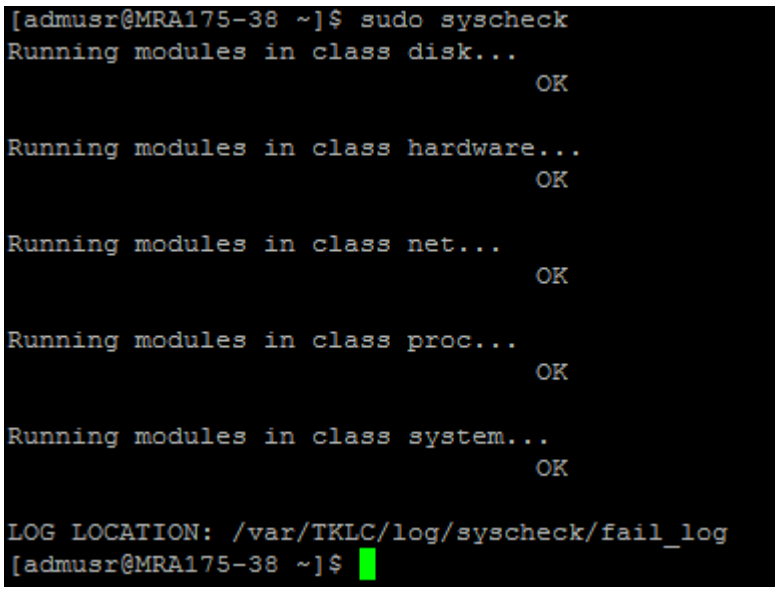
12. ☐	**CMP GUI:** Complete Back-out of cluster(s) **NOTE:** Up to 16 clusters can be backed out at the same time, selecting one at a time. **NOTE:** Each back-out of a one blade server completes in approximately 15 minutes.	1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click **Continue Rollback**. When hovering over the button, it indicates the back-out server.  3. Click **OK** to confirm and continue with the operation. It begins to back-out. Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited

Step	Procedure	Details
		31101 DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message **31284** High availability remote subscriber has not received a heartbeat **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. Verify in Upgrade Log that that back-out was successful:  All of the servers is on Release 15.0 at this point and show active/standby/spare. Note: first version column is Prev Release, and second version column is Running Release. 

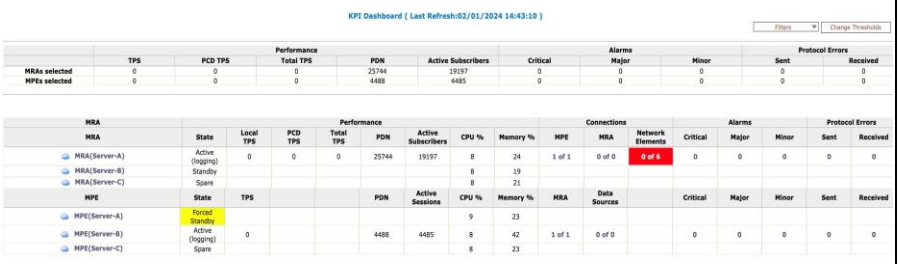
171	0	Backing out server upgrade	02/01/2024 13:52:24	02/01/2024 13:54:36	0:02:12	Server	WMRA1	Success	Manual	User initiated action: initiateBac...
172	171	Modify the role/replication attributes of th...	02/01/2024 13:52:24	02/01/2024 13:52:25	0:00:01	Cluster	MRA	Success	Automatic	Automatic action for managing ...
173	171	Waiting for replication to synchronize	02/01/2024 13:54:36	02/01/2024 13:58:20	0:03:44	Server	WMRA1	Success	Automatic	Automatic action waitForReplic...
174	0	Backing out server upgrade	02/01/2024 14:06:53	02/01/2024 14:09:14	0:02:20	Server	WMRA3	Success	Manual	User initiated action: initiateBac...
175	174	Modify the role/replication attributes of th...	02/01/2024 14:06:53	02/01/2024 14:06:54	0:00:01	Cluster	MRA	Success	Automatic	Automatic action for managing ...
176	174	Waiting for replication to synchronize	02/01/2024 14:09:14	02/01/2024 14:12:40	0:03:26	Server	WMRA3	Success	Automatic	Automatic action waitForReplic...
177	0	Failover to old version	02/01/2024 14:18:31	02/01/2024 14:18:31	0:00:00	Cluster	MRA	Success	Manual	User initiated action: FailoverTo...
178	0	Backing out server upgrade	02/01/2024 14:29:21	02/01/2024 14:31:44	0:02:22	Server	WMRA2	Success	Manual	User initiated action: initiateBac...
179	178	Modify the role/replication attributes of th...	02/01/2024 14:29:21	02/01/2024 14:29:23	0:00:01	Cluster	MRA	Success	Automatic	Automatic action for managing ...
180	178	Waiting for replication to synchronize	02/01/2024 14:31:44	02/01/2024 14:35:20	0:03:36	Server	WMRA2	Success	Automatic	Automatic action waitForReplic...
181	178	Modify the role/replication attributes of th...	02/01/2024 14:31:44	02/01/2024 14:31:45	0:00:01	Cluster	MRA	Success	Automatic	Automatic action for managing ...

MRA (3 Servers)					
WMRA2	N	Standby	15.0.0.1.0_6.1.0	15.0.0.0.0_20.1.0	Initiate backout Completed Successfully at Feb 1, 2024 14:35:20.
WMRA1	N	Active	15.0.0.1.0_6.1.0	15.0.0.0.0_20.1.0	Initiate backout Completed Successfully at Feb 1, 2024 13:58:20.
WMRA3	N	Spare	15.0.0.1.0_6.1.0	15.0.0.0.0_20.1.0	Initiate backout Completed Successfully at Feb 1, 2024 14:12:40.

Step	Procedure	Details

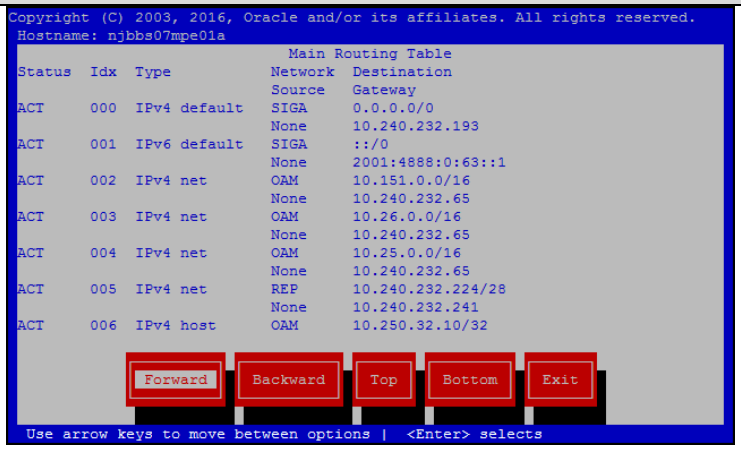
13. ☐	**MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Standby server as admusr.
		2. Verify that there are not any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		4. **NOTE:** Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		5. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		6. Verify:
		`$ ls -l /`
		7. Perform **`syscheck`** again:
		`$ sudo syscheck`

14. ☐	**CMP GUI:** Verify that backed out cluster is processing traffic normally.	Verify Cluster is processing traffic normally: Navigate to **System Wide Reports → KPI Dashboard**.

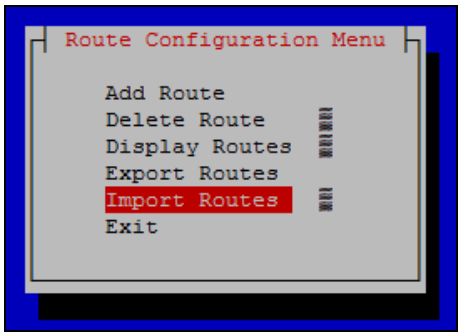
Step	Procedure	Details
		
15. ☐	**CMP GUI:** Verify alarms	1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Verify that there are not any unexpected active alarms present. **NOTE:** Some Alarms take approximately 30 minutes to 1 hour to auto clear. ***NOTE: After the backout of the clusters, if Critical Alarm 31283 (High availability server is offline) does not clear, then REP route might be missing from the backed-out server. Therefore Routes need to be verified and added. In this case, proceed to next step, otherwise, skip to step 20.***

16. ☐	**MPE/MRA SSH:** Verify routes	1. Login into MPE/MRA server as admusr
		2. Copy routes_output.txt from /home/admusr to /tmp
		`$ sudo cp routes_output.txt /tmp`
		`$ cd /tmp`
		`$ ls`
		`routes_output.txt`
		WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance Engineering.
		3. Run the platcfg utility:
		`$ sudo su - platcfg`
		4. Navigate to **Policy Configuration → Routing Config → Display Routes**.
		5. Verify that all routes are present.
		6. Click **Forward** to view all the routes.
		Example:

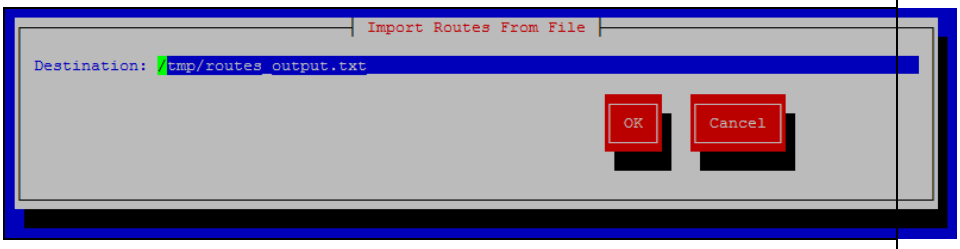
Step	Procedure	Details



7. If any of the routes are missing then perform the following otherwise skip to step 20
8. Navigate back to **Route Configuration Menu** and select **Import Routes**.

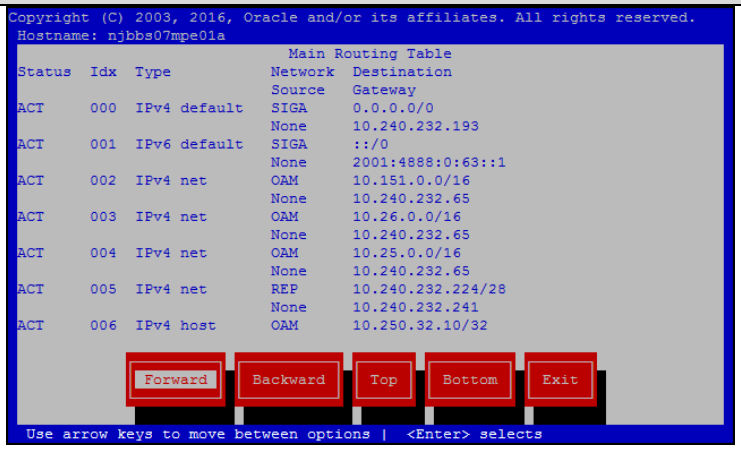


9. Click **OK**.



10. Routes is imported from `/tmp/routes_output.txt` file and **Route Configuration Menu** is displayed again.
11. Select **Display Routes**.
12. Verify that all routes are present.
13. Click **Forward** to view all the routes.

Example:

Step	Procedure	Details
		 14. Exit the platcfg utility **WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance Engineering.**
17. ☐	Repeat for other clusters as needed	Repeat this procedure for remainder of MPE/MRA servers, if not fully backed out yet.
18. ☐	Perform **`syscheck`** and verify that alarms are clear.	Another **`syscheck`** on all the back-out servers can be performed to ensure all modules are still operationally OK before progressing to the next procedure. 1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Verify that there are not any unexpected active alarms present. **NOTE:** Some Alarms take appoximately 30 minutes to 1 hour to auto clear.
—End of Procedure—		

1.10.3.4 Back-out Fully Upgraded Secondary CMP cluster

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

Expected Pre-conditions:

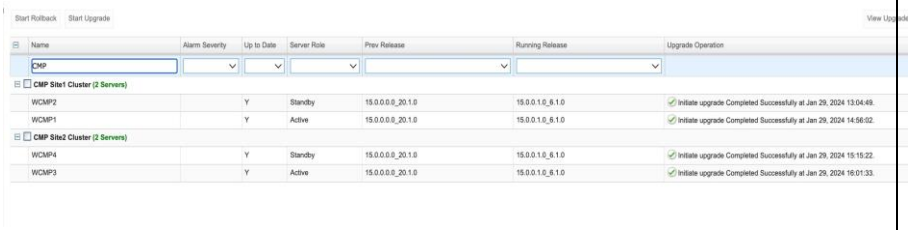
1. Primary Active CMP is on Release 15.0.x
2. Secondary CMP cluster is on Release 15.0.x
3. All MPE/MRA Clusters are on Release 15.0

NOTES:

- This procedure must be performed within a maintenance window.
- This procedure takes approximately 45-60 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

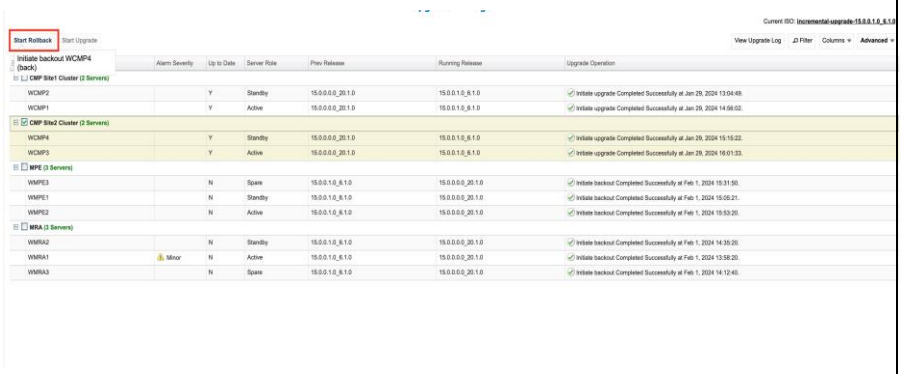
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

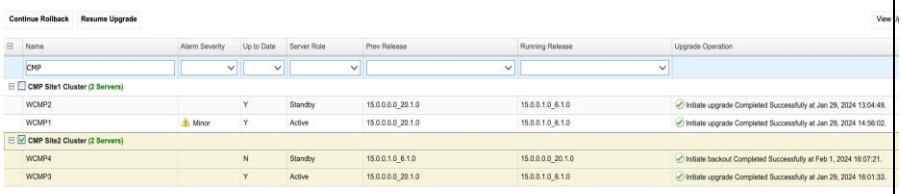
Procedure 12: Back-out Fully Upgraded Secondary CMP cluster

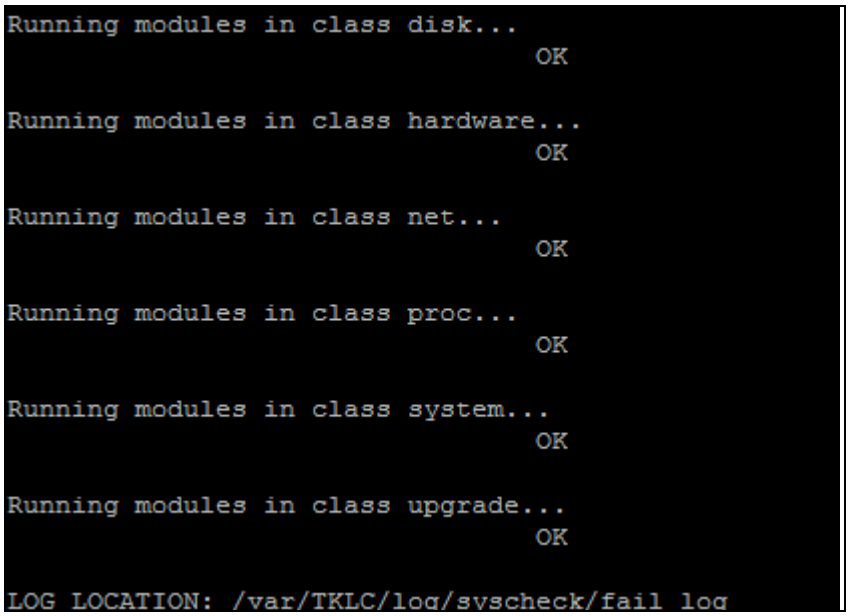
Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of CMP clusters	1. Navigate to **Upgrade → Upgrade Manager**. 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 15.0.x - Secondary CMP cluster is on Release 15.0.x - Up to Date column shows Y for all servers 3. Click **Filter** and enter `cmp` in the **Name** field. **Example:** 

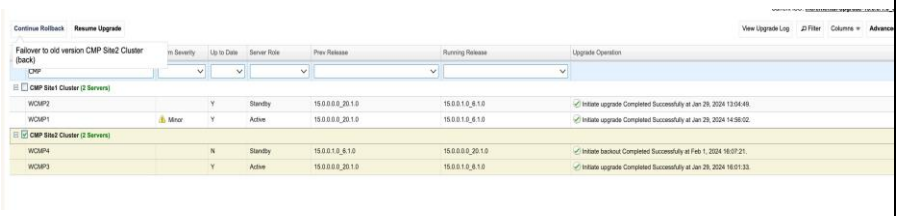
2. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages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

3. ☐	**CMP GUI:** Back-out clusters **NOTE:** Each back-out of one server takes about 20 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP cluster 3. Click **Start Rollback**. When hovering over the button, it indicates the back-out server.

Step	Procedure	Details
		 4. Click **OK** to confirm and continue with the operation. It begins to back-out. Server goes into an OOS server Role Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server

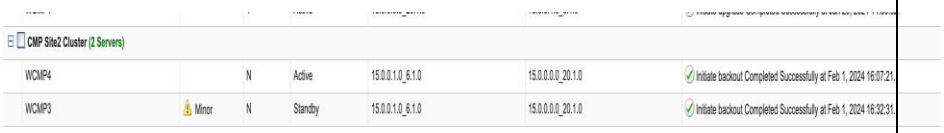
Step	Procedure	Details
		goes back to standby state and show running release of 15.0. 

4. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server and verify that there are not any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		
		2. Verify `/tmp` directory permissions:
		`$ ls -l /`
		3. **NOTE:** Permissions should be the following:
		`drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

Step	Procedure	Details
5. ☐	**CMP GUI:** Continue the back-out. Next operation is failover.	1. Select Secondary CMP cluster. 2. Navigate to **Upgrade → Upgrade Manager**. 3. Select the Secondary CMP cluster 4. Click **Continue Rollback**. When hovering over the button, it informs you to failover.  5. Click **OK** to confirm and continue with the operation. It begins to failover. Follow the progress status in the Server Role column. Wait for the server to show standby. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **74604** Policy cluster is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software

Step	Procedure	Details

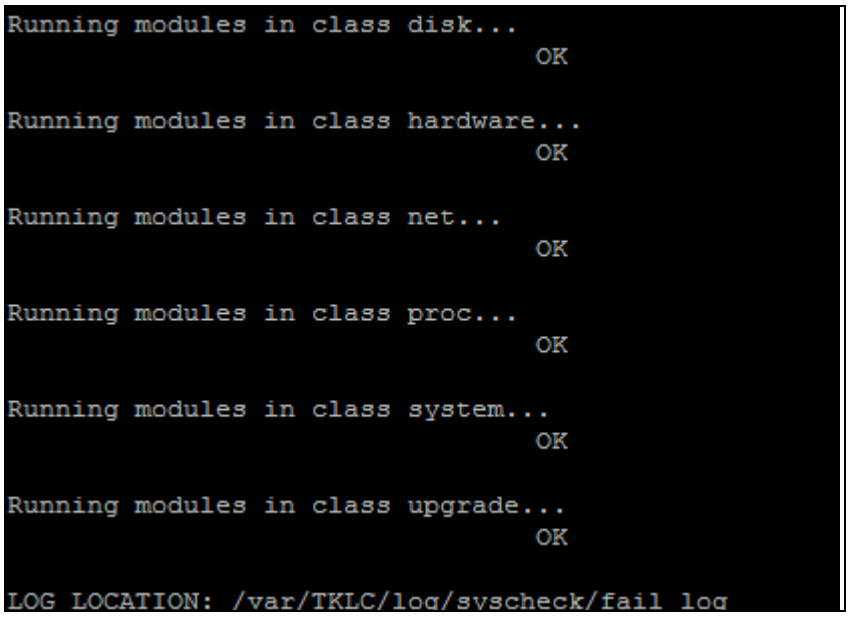
6. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages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

7. ☐	**CMP GUI:** Continue the backed-out. Next operation is Initiate Back-out **NOTE:** Each back-out of one server takes about 20 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Secondary CMP cluster. 3. Click **Continue Rollback**. When hovering over the button, it informs you to rollback.  4. Click **OK** to confirm and continue with the operation. It begins to failover. 5. Follow the progress status in the Server Role column. Wait until the server to back-out comes to Standby state before continuing. 6. Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column.  **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance

Step	Procedure	Details
		31236 High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **<u>Expected Minor Alarms</u>** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software 7. Verify in Upgrade Log that that back-out was successful: 8. All Secondary CMP servers is on Release 15.0 at this point and show active/standby

193	0	Backing out server upgrade	02/01/2024 16:00:21	02/01/2024 16:03:29	0:03:08	Server	WCMP4	Success	Manual	User initiated action: initiat...
194	193	Modify the role/replication attributes ...	02/01/2024 16:00:21	02/01/2024 16:00:22	0:00:01	Cluster	CMP Site2 Clu...	Success	Automatic	Automatic action for mana...
195	193	Waiting for replication to synchronize	02/01/2024 16:03:29	02/01/2024 16:07:21	0:03:51	Server	WCMP4	Success	Automatic	Automatic action waitForR...
196	0	Failover to old version	02/01/2024 16:23:15	02/01/2024 16:23:15	0:00:00	Cluster	CMP Site2 Clu...	Success	Manual	User initiated action: Failo...
197	0	Backing out server upgrade	02/01/2024 16:25:29	02/01/2024 16:27:57	0:02:27	Server	WCMP3	Success	Manual	User initiated action: initiat...
198	197	Modify the role/replication attributes ...	02/01/2024 16:25:29	02/01/2024 16:25:30	0:00:01	Cluster	CMP Site2 Clu...	Success	Automatic	Automatic action for mana...
199	197	Waiting for replication to synchronize	02/01/2024 16:27:57	02/01/2024 16:32:31	0:04:33	Server	WCMP3	Success	Automatic	Automatic action waitForR...
200	197	Modify the role/replication attributes ...	02/01/2024 16:27:57	02/01/2024 16:27:58	0:00:01	Cluster	CMP Site2 Clu...	Success	Automatic	Automatic action for mana...

Step	Procedure	Details

8. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server as admusr.
		2. Verify that there are not any failures in **`syscheck`**.
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		9. **NOTE:** Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

—End of Procedure—		

1.10.3.5 Back-out Fully Upgraded Primary CMP cluster

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

Expected Pre-conditions:

1. Primary Active CMP cluster is on Release 15.0.x.
2. Secondary CMP, MPE and MRA Clusters are on Release 15.0.

NOTES:

- This procedure must be performed within a maintenance window.
- This procedure takes approximately 45-60 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

Procedure 13: Back-out Fully Upgraded Primary CMP cluster

Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of CMP clusters	1. Navigate to **Upgrade → Upgrade Manager** 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 15.0.x - Secondary CMP, MPE and MRA Clusters are on Release 15.0 - Up to Date column shows Y for all servers in Primary CMP cluster - Click Filter and enter cmp in the Name field. **Example:** 

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

3. ☐	**CMP GUI:** Back-out standby server of Primary CMP cluster **NOTE:** Back-out of one server takes about 20 minutes to complete.	1. Select the Primary CMP cluster 2. Click **Start Rollback**. When hovering over the button, it indicates the server to back out.

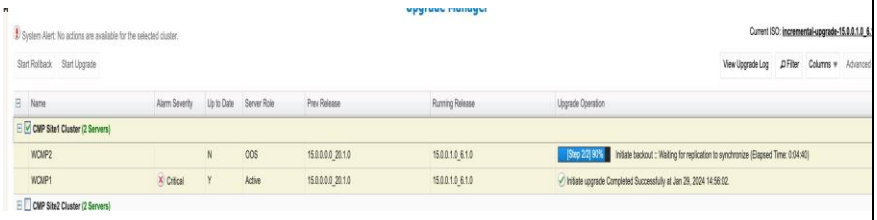
Step	Procedure	Details

3. Click **OK** to confirm and continue with the operation. It begins to back-out.

Server goes into an OOS server Role

Follow the progress status in the Upgrade Operation column.

During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out.



Expected Critical Alarms

70001 The qp_procmgr process has failed.

31227 The high availability status is failed due to raised alarms

31283 High availability server is offline

70007 Not all QP resources are ready

70025 The MySQL slave has a different schema version than the master

Expected Major Alarms

70004 The QP processes have been brought down for maintenance

31236 High availability TCP link is down

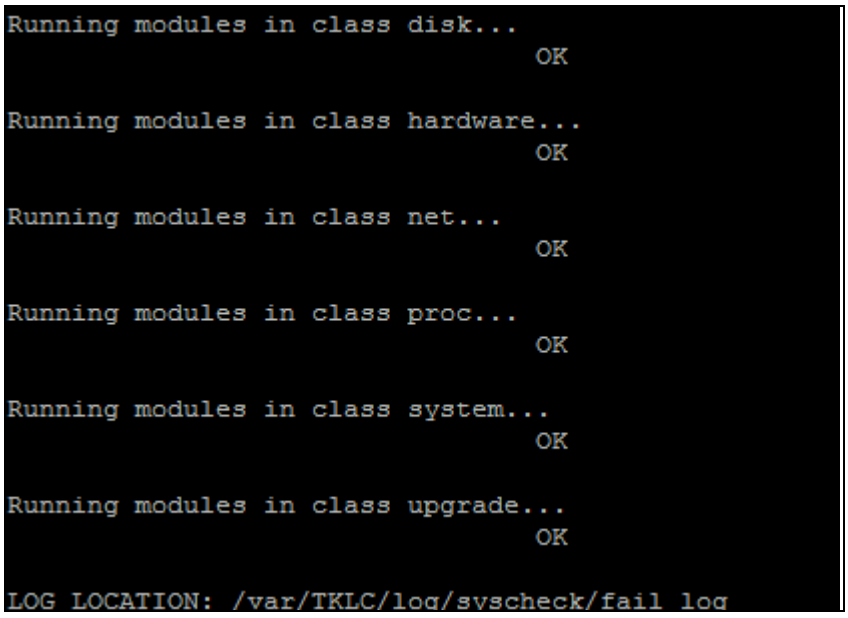
31233 High availability path loss of connectivity

70021 The MySQL slave is not connected to the master

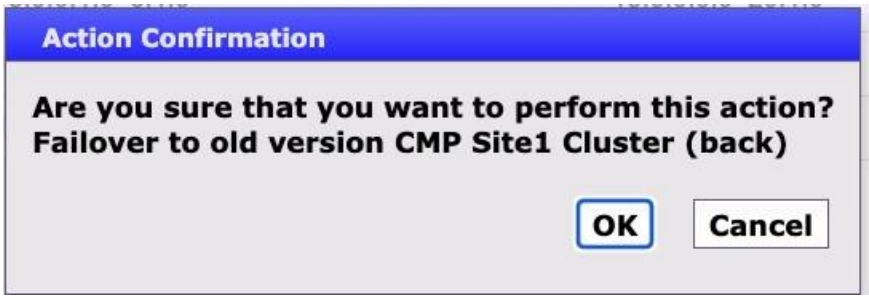
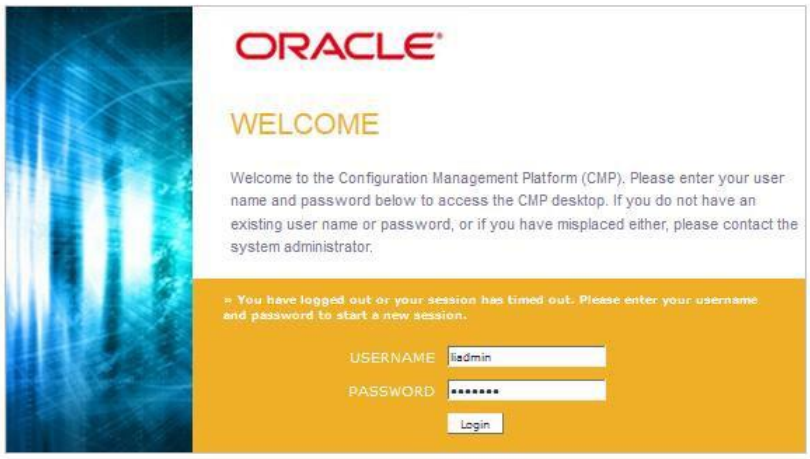
Expected Minor Alarms

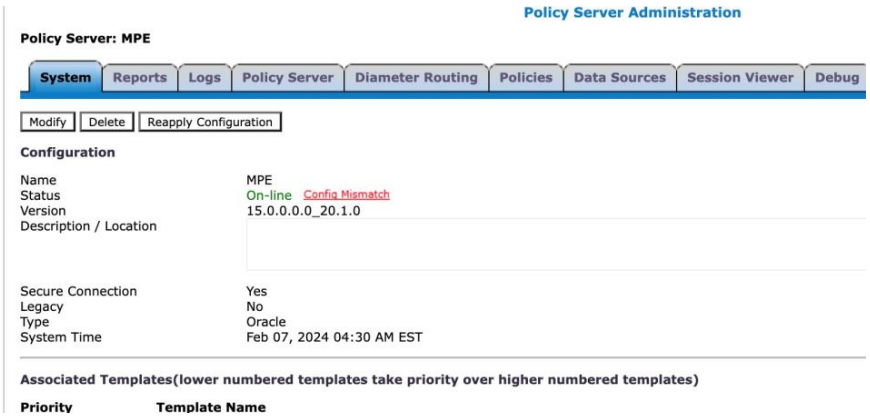
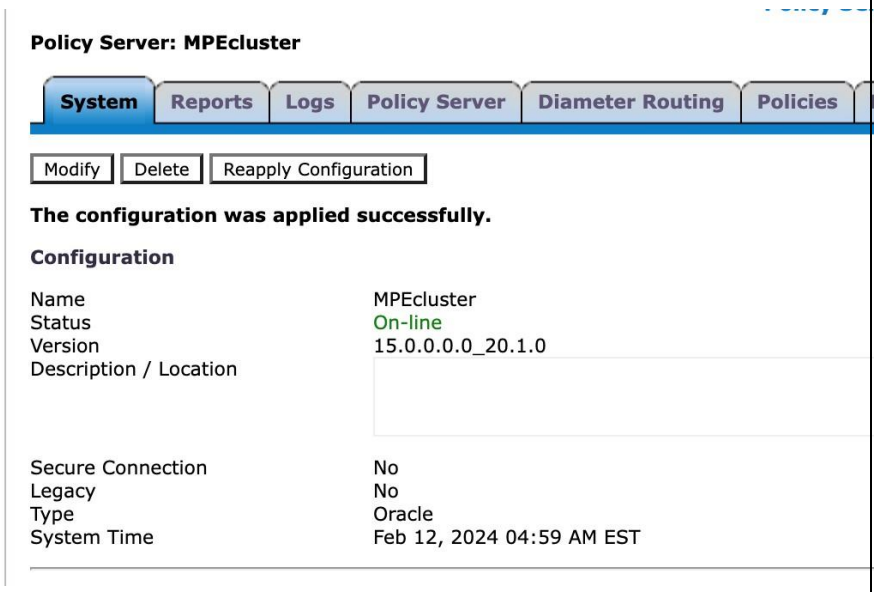
Step	Procedure	Details
		70503 The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software Back-out of the server is complete when the initiate Back-out completed successfully message displays in the Upgrade Operation column. The server goes back to standby state and show running release of 15.0  Name Alarm Severity Up to Date Server Role Prev Release Running Release Upgrade Operation CMP Site1 Cluster (2 Servers) WCMP2 Minor N Standby 15.0.0.1.0_6.1.0 15.0.0.0.0_20.1.0 Initiate backout Completed Successfully at Feb 1, 2024 16:45:21. WCMP1 Minor Y Active 15.0.0.0.0_20.1.0 15.0.0.1.0_6.1.0 Initiate upgrade Completed Successfully at Jan 29, 2024 14:56:02.

Step	Procedure	Details

4. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server as admusr.
		2. Verify that there are not any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		10. **NOTE:** Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

5. ☐	**CMP GUI:** Continue the back-out. Next operation is failover.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP cluster. 3. Click **Continue Rollback**. When hovering over the button, it informs you to failover.

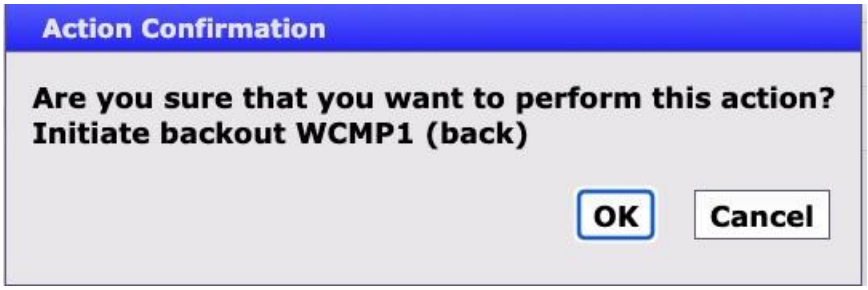
Step	Procedure	Details
		 4. Click **OK** to confirm and continue with the operation. It begins to failover. The failover takes couple of minutes.  After a minute, you are required to log back in.
6. ☐	**CMP GUI:** Log back into the Primary CMP VIP	After failover, you are required to log back in to the CMP GUI using the Primary CMP VIP. 
7. ☐	CMP GUI: Verify previous Policy Management Release	1. Navigate to **Help → About**. 2. Verify the release displayed is 15.0 **15.0.0.0.0_20.1.0** Copyright (C) 2003, 2024 Oracle. All Rights Reserved.

Step	Procedure	Details
8. ☐	**CMP GUI:** If a Config Mismatch is observed on MPE or MRA	**MPE:** Navigate to **Policy → Configuration →** <*mpe_cluster name*> **→ System** **MRA:** Navigate to **MRA → Configuration →** <*MRA Cluster*> **→ System**  Click **Reapply Configuration**. Config Mismatch is resolves: 

9. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Using SSH, log into the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of /var/log/messages is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`

Step	Procedure	Details

		```$ sudo cat /dev/null > /var/log/messages```
		 ```$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"```
		 3. Verify:
		 ```$ ls -lh /var/log/messages```

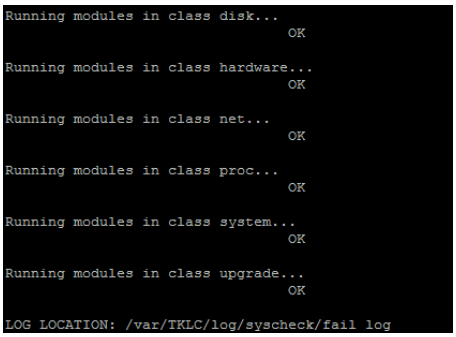
10. ☐	**CMP GUI:** Continue the back-out of the Primary CMP cluster **NOTE:** Back-out of one server takes about 15 minutes to complete. **Note: Wait for approximately 10 minutes to allow the secondary CMP Cluster to identify and change its (MySQL) master, that is, the new active CMP node. Alarms will appear and go automatically after the process happens.**	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP cluster. 3. Click Continue Rollback. When hovering over the button, it indicates the server to get backed out. At this point it is the remaining standby server.  4. Click OK to confirm and continue with the operation. It begins to back-out. Server goes into an OOS server Role  Follow the progress status In the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master

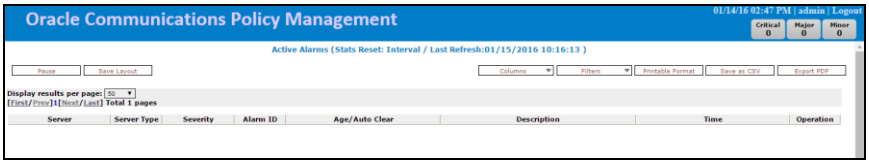
Step	Procedure	Details
		Expected Minor Alarms **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server goes back to standby state and show the previous release.  **Note**: Post primary and secondary CMP clusters rollback, few alarms maybe reported that might not be cleared (70501, 70500 and 70503), these are false alarms. To clear these alarms run *sudo service qp_procmgr restart* on the affected server. (If active CMP qp_procmgr is restarted, switchover will happen). Verify in Upgrade Log that that backout was successful:  All Primary CMP servers is on Release 15.0 at this point and show active/standby.

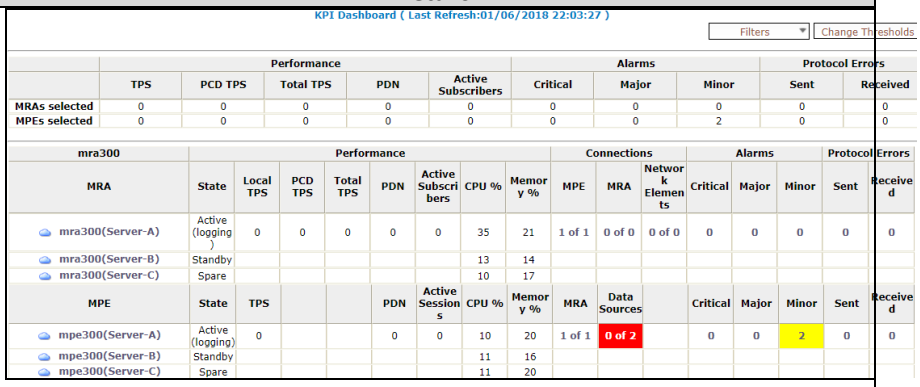
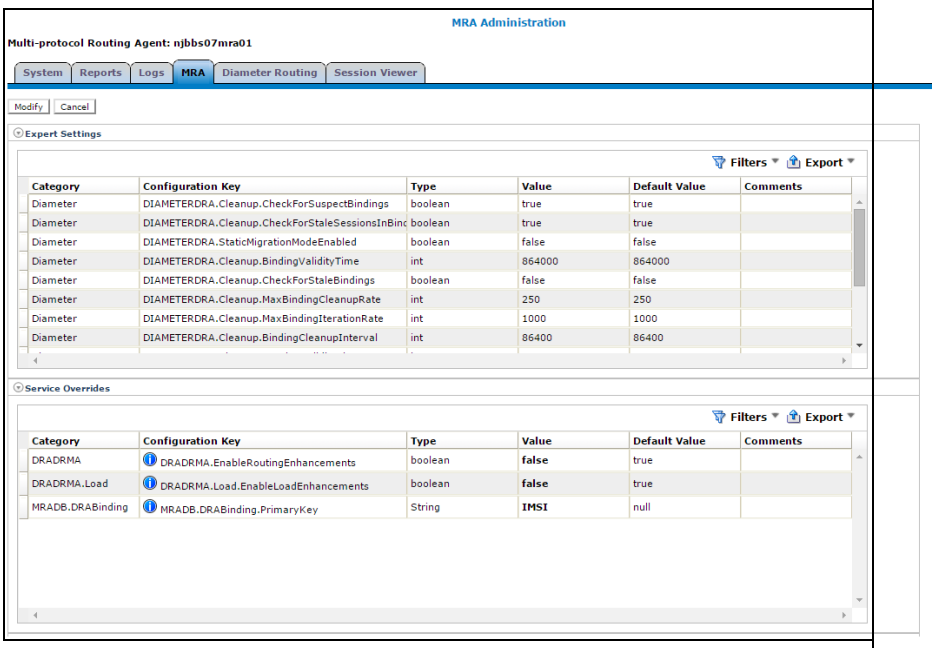
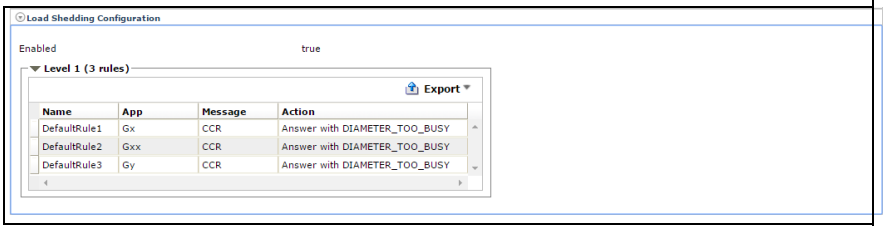
Name	Alarm Severity	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
WCMP2	Minor	N	Active	15.0.0.1.0_6.1.0	15.0.0.0.0_20.1.0	Initiate backout Completed Successfully at Feb 1, 2024 16:49:24
WCMP1		N	Standby	15.0.0.1.0_6.1.0	15.0.0.0.0_20.1.0	Initiate backout Completed Successfully at Feb 1, 2024 17:09:34

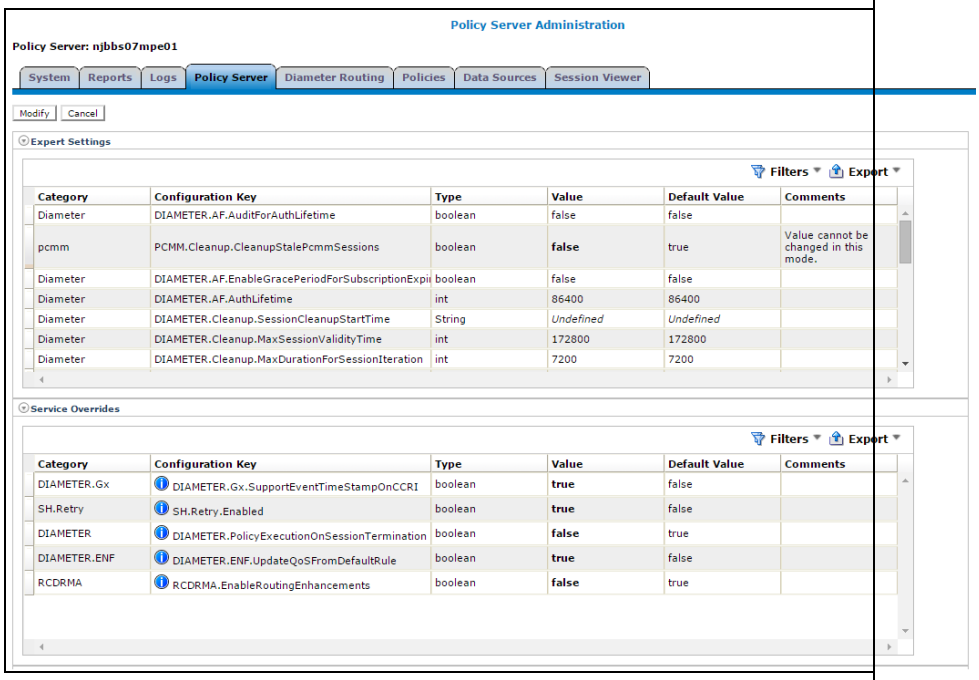
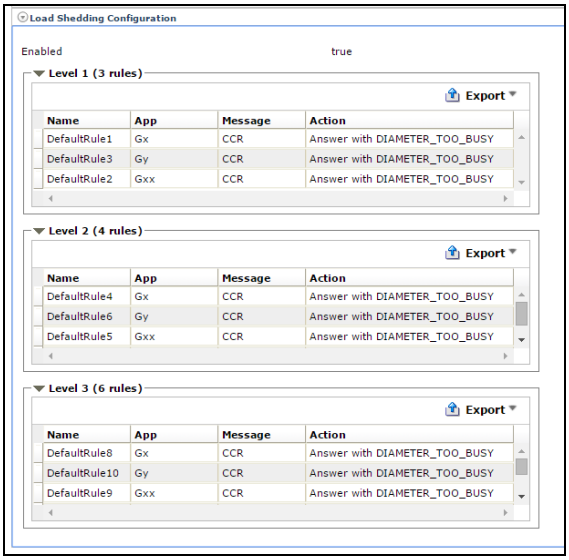
201	0	Backing out server upgrade	02/01/2024 16:38:21	02/01/2024 16:49:24	0:11:03	Server	WCMP2	Success	Manual	User initiated action: i...
202	201	Modify the role/replication attribu...	02/01/2024 16:38:21	02/01/2024 16:38:22	0:00:01	Cluster	CMP Site1 Cl...	Success	Automatic	Automatic action for ...
203	0	Backing out server upgrade	02/01/2024 17:02:41	02/01/2024 17:05:17	0:02:36	Server	WCMP1	Success	Manual	User initiated action: i...
204	203	Modify the role/replication attribu...	02/01/2024 17:02:41	02/01/2024 17:02:42	0:00:01	Cluster	CMP Site1 Cl...	Success	Automatic	Automatic action for ...
205	203	Waiting for replication to synchro...	02/01/2024 17:05:17	02/01/2024 17:09:34	0:04:17	Server	WCMP1	Success	Automatic	Automatic action wait...

Step	Procedure	Details

11. ☐	**CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission	1. Login to the backed-out Server as admusr
		2. Verify that there are not any failures in **`syscheck`**:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		NOTE: Permissions should be the following,
		`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`
		4. If the permissions are not as listed above then perform the following otherwise skip to next step:
		`$ sudo chmod 777 /tmp`
		`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`
		`$ sudo chmod +t /tmp`
		5. Verify:
		`$ ls -l /`
		6. Perform **`syscheck`** again:
		`$ sudo syscheck`

12. ☐	**CMP GUI:** Verify Alarm Status.	1. Navigate to **System Wide Reports → Alarms → Active Alarms**. 2. Confirm that any existing alarm is understood. 
13. ☐	**CMP GUI:** Verify Traffic Status - KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Confirm that all Connections and Traffic status are as expected. Observe it for a few screen refresh updates.

Step	Procedure	Details
		
14. ☐	**CMP GUI:** Verify Advanced Settings on the MRA	1. Capture screenshots of the advanced settings on the MRA and compare it with prior to upgrade screen captures. 2. Verify that there are not any differences. 3. Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ MRA**. 4. Click **Advanced**.  
15. ☐	**CMP GUI:** Verify Advanced Settings on the MPE	1. Capture screenshots of the advanced settings on the MPE and compare it with prior to upgrade screen captures. 2. Verify that there are not any difference 3. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→**

Step	Procedure	Details
		Policy Server. 4. Click **Advanced**.   Alternately, settings can be exported clicking **Export** on the right within each setting.
—End of Procedure—		

2 GEOREDUNDANCY DISABLED

2.1 Introduction

2.1.1 Purpose and Scope

This document describes methods utilized and procedures to perform a software upgrade of Oracle Communications Policy Management Release 15.0 to Release 15.0.x when georedundancy on non-CMP components (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 can 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 and standby resides on Site1 while the secondary MRA/MPE cluster of active and standby resides on Site2 for disaster recovery.

2.1.2 Acronyms

Table 5: Acronyms

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

Acronym	Meaning
IPM	Initial product manufacture

2.1.3 Terminology

Table 6: Terminology

Term	Description
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 secondary cluster exists with co-located Active and Standby servers for disaster recovery.
Spare Server or Server-C	Server that is ready to take over from the Active server if both the Active and Standby servers fail. It is generally in a different location than the Active and Standby servers.

2.1.4 Software Release Numbering

- TPD: 8.x
- COMCOL: 6.6
- Policy Management Release 15.0

2.1.5 Upgrade Overview

This section lists the required materials and information needed to perform Policy Management Release 15.0 software upgrades.

2.1.6 Upgrade Status Values

Table 7: 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.

2.1.7 Upgrade Path

This upgrade document supports the following upgrade path:

- Policy Management 15.0 (fresh install) to 15.0.x (full DIU ISO) (Major Path)

NOTE:

- If the official upgrade paths mentioned in the release documents of each supported version is not followed, please contact Oracle Support before upgrading to 15.0.x. (Refer to individual patch release document to see the supported upgrade paths.)
- 15.0 to 15.0.x upgrade is only applicable for VM based environments.

2.1.8 Upgrade Information

2.1.8.1 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 deployment may consist of multiple clusters.

Required Cluster Upgrade Sequence

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

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

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

1. Upgrade 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. (upgrades from 12.5.0 where 8 clusters can be upgraded in parallel, and from 12.6 where 16 clusters can be upgraded in parallel).

2.1.8.2 Policy Management Release Mixed-Version Operation and Limitation

The general expectation is that a system that is running in a mixed version configuration should support features and perform at a level of the previous version. Thus, a system that is running pre-15.0.x release and 15.0.x release in mixed configuration would support the performance and capacity of the pre-15.0 release. The mixed version Policy Management configuration would also support pre-15.0.x features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the Release 15.0.x CMP manages MRA/MPE servers in a pre-15.0.x release. In this mixed version configuration, a Release 15.0.x CMP does not prevent an operator from configuring anything that can be configured in a previous release and all configuration items from the previous release are still available. However, the configuration changes during the upgrade of Policy Management system are discouraged and have limited support.

In the mixed version, a Release 15.0.x CMP has the following limitations while running in a mixed version environment:

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

Table 8: Mixed-version configurations supported

Policy Management system components on	CMP R15.0.x	MRA R15.0.x	MPE R15.0.x
CMP 15.0	Yes	No	No
MRA 15.0	Yes	Yes	Yes
MPE 15.0	Yes	Yes	Yes

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP to Release 15.0.x. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to Release 15.0.x.

2.1.9 Customer Impacts

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

2.1.10 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.

2.1.11 TPD Version

The Tekelec Product Distribution (TPD) version needed for this release is included in the Policy Application Software Upgrade DUI ISO, and TPD is upgraded to version 8.x as part of this procedure.

2.1.12 Loading Application software

For upgrade of server application software, the recommended method is to copy the application DIU ISO images to the servers using scp or ftp.

2.1.13 Required Materials and Remote Access

1. Policy Management 15.0.x software DIU-ISO files
2. Policy Management 15.0.x software Release Notes
3. The capability to remote login to the target server as admusr.

   NOTE: The remote login can be done through SSH, local console. Ensure the 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 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 Management GUI.

2.1.14 Upgrade Media

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

2.1.14.1 Logins, Passwords and Server IP Addresses

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

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

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

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

Table-9: Logins, Passwords and Server IP Addresses

Item	Value
CMP servers	GUI Administrator Login User/Password:
	admusr password:
MRA/MPE servers	admusr password:
Target OA	OA Administrator Login: User/Password
Software Upgrade Target Release[2]	Target Release Number:
	Policy Management 15.0 software DIU ISO image filenames.

2.2 Theory of Operation

2.2.1 Upgrade Manager Page

The Upgrade Manager represents a significant shift from some of the previous upgrade pages. In the past it was up to the operator, with assistance from a MOP, to know the correct sequence of server selects and menu selects. The new upgrade manager takes a different approach. It determines the next course of action to either:

1. Begin/continue upgrading a cluster
2. Begin/continue backing out a cluster.

There is an important point implicit in the list above:

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

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

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

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

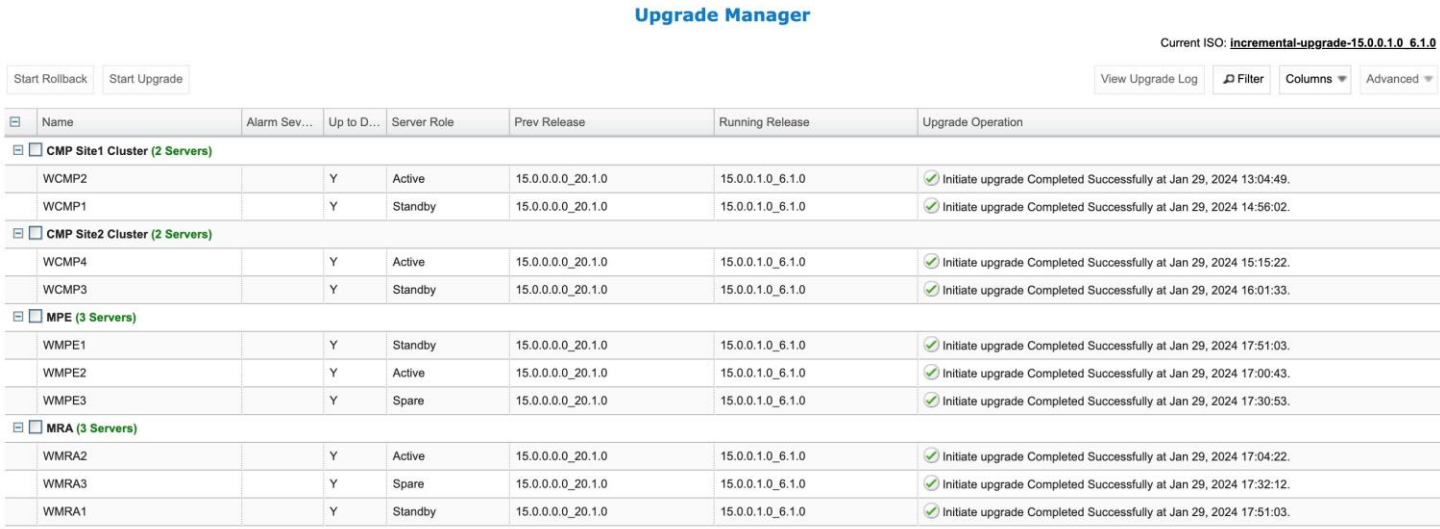


Figure 4: Sample display of the upgrade manager page.

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

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

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

- Alarm Severity

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

  - The CMP raises alarms simply to indicate that it is initiating upgrade activity.
  - Servers report alarms to indicate that their mate servers are offline.

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

- Up to Date

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

  - N

    The server is running old code and must be upgraded

  - Y

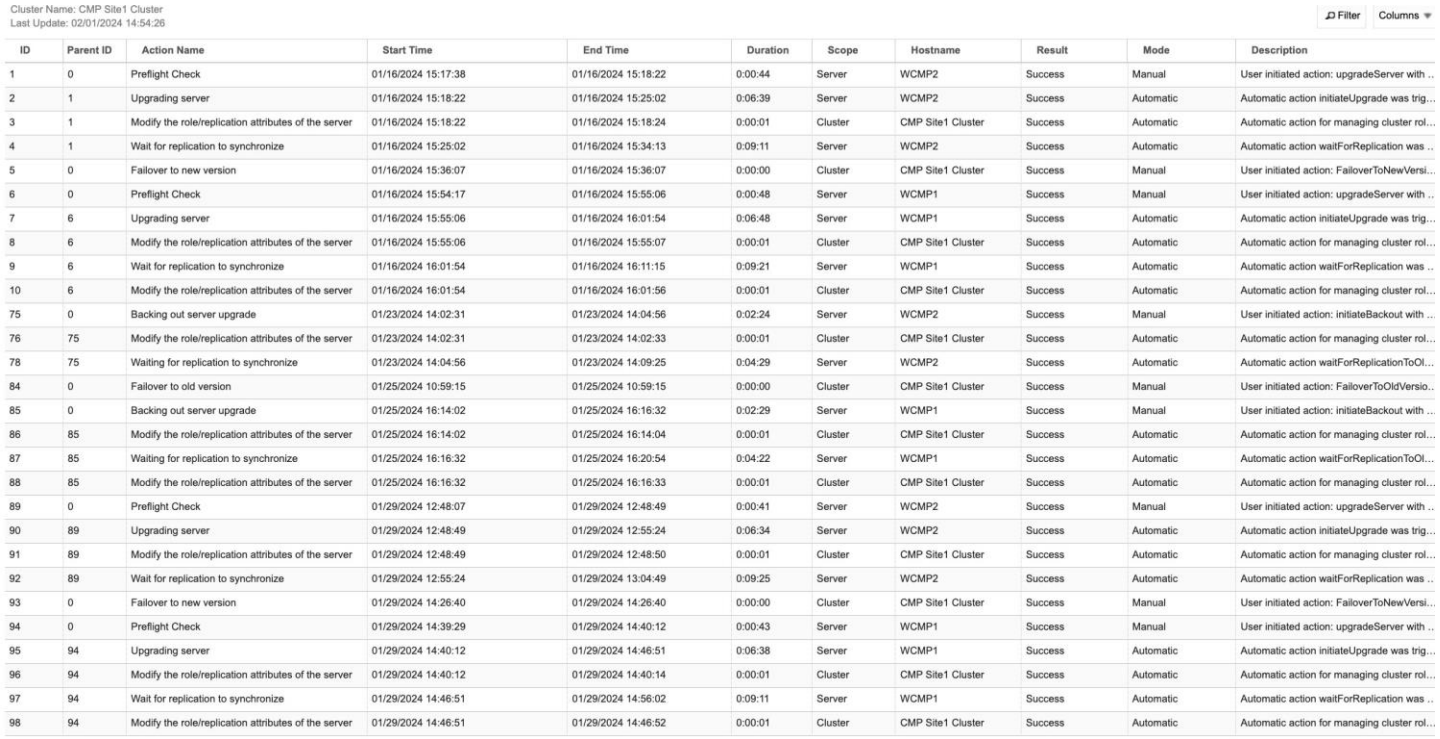
    The server is running new code.

- N/A

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

2.2.2 The Upgrade Log

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



Cluster Name: CMP Site1 Cluster
Last Update: 02/01/2024 14:54:26

Filter | Columns

ID	Parent ID	Action Name	Start Time	End Time	Duration	Scope	Hostname	Result	Mode	Description
1	0	Preflight Check	01/16/2024 15:17:38	01/16/2024 15:18:22	0:00:44	Server	WCMP2	Success	Manual	User initiated action: upgradeServer with ...
2	1	Upgrading server	01/16/2024 15:18:22	01/16/2024 15:25:02	0:06:39	Server	WCMP2	Success	Automatic	Automatic action initiateUpgrade was trig...
3	1	Modify the role/replication attributes of the server	01/16/2024 15:18:22	01/16/2024 15:18:24	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
4	1	Wait for replication to synchronize	01/16/2024 15:25:02	01/16/2024 15:34:13	0:09:11	Server	WCMP2	Success	Automatic	Automatic action waitForReplication was ...
5	0	Failover to new version	01/16/2024 15:36:07	01/16/2024 15:36:07	0:00:00	Cluster	CMP Site1 Cluster	Success	Manual	User initiated action: FailoverToNewVersi...
6	0	Preflight Check	01/16/2024 15:54:17	01/16/2024 15:55:06	0:00:48	Server	WCMP1	Success	Manual	User initiated action: upgradeServer with ...
7	6	Upgrading server	01/16/2024 15:55:06	01/16/2024 16:01:54	0:06:48	Server	WCMP1	Success	Automatic	Automatic action initiateUpgrade was trig...
8	6	Modify the role/replication attributes of the server	01/16/2024 15:55:06	01/16/2024 15:55:07	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
9	6	Wait for replication to synchronize	01/16/2024 16:01:54	01/16/2024 16:11:15	0:09:21	Server	WCMP1	Success	Automatic	Automatic action waitForReplication was ...
10	6	Modify the role/replication attributes of the server	01/16/2024 16:01:54	01/16/2024 16:01:56	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
75	0	Backing out server upgrade	01/23/2024 14:02:31	01/23/2024 14:04:56	0:02:24	Server	WCMP2	Success	Manual	User initiated action: initiateBackout with ...
76	75	Modify the role/replication attributes of the server	01/23/2024 14:02:31	01/23/2024 14:02:33	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
78	75	Waiting for replication to synchronize	01/23/2024 14:04:56	01/23/2024 14:09:25	0:04:29	Server	WCMP2	Success	Automatic	Automatic action waitForReplicationToOl...
84	0	Failover to old version	01/25/2024 10:59:15	01/25/2024 10:59:15	0:00:00	Cluster	CMP Site1 Cluster	Success	Manual	User initiated action: FailoverToOldVersio...
85	0	Backing out server upgrade	01/25/2024 16:14:02	01/25/2024 16:16:32	0:02:29	Server	WCMP1	Success	Manual	User initiated action: initiateBackout with ...
86	85	Modify the role/replication attributes of the server	01/25/2024 16:14:02	01/25/2024 16:14:04	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
87	85	Waiting for replication to synchronize	01/25/2024 16:16:32	01/25/2024 16:20:54	0:04:22	Server	WCMP1	Success	Automatic	Automatic action waitForReplicationToOl...
88	85	Modify the role/replication attributes of the server	01/25/2024 16:16:32	01/25/2024 16:16:33	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
89	0	Preflight Check	01/29/2024 12:48:07	01/29/2024 12:48:49	0:00:41	Server	WCMP2	Success	Manual	User initiated action: upgradeServer with ...
90	89	Upgrading server	01/29/2024 12:48:49	01/29/2024 12:55:24	0:06:34	Server	WCMP2	Success	Automatic	Automatic action initiateUpgrade was trig...
91	89	Modify the role/replication attributes of the server	01/29/2024 12:48:49	01/29/2024 12:48:50	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
92	89	Wait for replication to synchronize	01/29/2024 12:55:24	01/29/2024 13:04:49	0:09:25	Server	WCMP2	Success	Automatic	Automatic action waitForReplication was ...
93	0	Failover to new version	01/29/2024 14:26:40	01/29/2024 14:26:40	0:00:00	Cluster	CMP Site1 Cluster	Success	Manual	User initiated action: FailoverToNewVersi...
94	0	Preflight Check	01/29/2024 14:39:29	01/29/2024 14:40:12	0:00:43	Server	WCMP1	Success	Manual	User initiated action: upgradeServer with ...
95	94	Upgrading server	01/29/2024 14:40:12	01/29/2024 14:46:51	0:06:38	Server	WCMP1	Success	Automatic	Automatic action initiateUpgrade was trig...
96	94	Modify the role/replication attributes of the server	01/29/2024 14:40:12	01/29/2024 14:40:14	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...
97	94	Wait for replication to synchronize	01/29/2024 14:46:51	01/29/2024 14:56:02	0:09:11	Server	WCMP1	Success	Automatic	Automatic action waitForReplication was ...
98	94	Modify the role/replication attributes of the server	01/29/2024 14:46:51	01/29/2024 14:46:52	0:00:01	Cluster	CMP Site1 Cluster	Success	Automatic	Automatic action for managing cluster rol...

Figure 5: Upgrade Log

2.2.2.1 Optional Actions

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

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

2.2.2.2 The DIU ISO Select

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

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

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

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

2.2.2.3 Upgrade Director Behavior

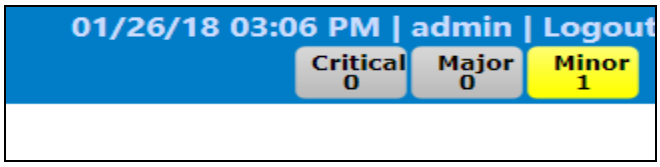
The Upgrade Director (UD) is a component that tracks the state of the servers, cluster, and system during an upgrade. The UD is hidden. However, there are conventions and operating principles that are visible.

Alarm Philosophy

NOTE: During an upgrade, the Upgrade Manager asserts (that is, generates) and displays alarms. An upgrade typically triggers multiple minor, major, and critical alarms as servers are taken out of service, go into forced standby, or fail over. This is normal and to be expected.

In general, the Upgrade Director raises alarms if:

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



The table summarizes the alarms that can be raised during a 15.0.x upgrade.

Table 5 Alarm summary

Alarm ID	Severity	Name	Description
70500	Minor	SYSTEM_MIXED_VERSION	The servers in the topology are running different versions of software. Upgrade of the

Alarm ID	Severity	Name	Description
			system is not complete.
70501	Minor	CLUSTER_MIXED_VERSION	The servers in the specified cluster are running different versions of software. The upgrade of the cluster is not complete.
70502	Minor	REPLICATION_INHIBITED	Replication is inhibited to the specified server. It is not receiving session information.
70503	Minor	SERVER_FORCED_STANDBY	The specified server has been placed in forced standby and cannot provide service.
70506	Minor	UPGRADE_OPERATION_FAILED	An upgrade operation failed on the specified server.
70507	Minor	UPGRADE_IN_PROGRESS	An upgrade/backout is currently in progress on the server. It may leave the cluster, become unreachable or even reboot.
70508	Critical	ZOMBIE_SERVER	The server is in an indeterminate state and must be repaired by support.

General Upgrade Procedure

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

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

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

Unreachable Servers

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

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

Mixed Version and Forced Standby

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

Failure Handling and Recovery

Failures fall into two categories:

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

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

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

2.3 Upgrade Preparation

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

Overview:

1. Upgrade Primary (Site1) CMP
2. Upgrade Secondary (Site2) CMP (if applicable)
3. Segment 1 Site 1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
4. Segment 1 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
5. Segment 2 Site 1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
6. Segment 2 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters

2.3.1 Prerequisites

The following Procedure 16 table verifies that all required prerequisite steps needed to be performed before the upgrade procedure begins.

Procedure 14 Prerequisites

Step	Procedure	Details
1. ☐	Review Release Notes	Review Policy Management Release 15.0.x 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 15.0.x, only Mozilla Firefox and Google Chrome are fully supported.**
—End of Procedure—		

2.3.2 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:

1. Policy changes or configuration changes should NOT be made while the system is in mixed-version operation.
2. Time estimates are for upgrade procedures without backout procedure. Backout procedure time is typically same as, or less than the upgrade procedure.

Step	Procedure	Result	Engineer	Time
1. ☐	Use the following checklist to plan the cluster upgrades for the entire system.	Maintenance windows are planned		
2. ☐	Upgrade Site1 and Site2 CMP clusters	Site Names _____ & _____		3 hrs

Step	Procedure	Result	Engineer	Time
3. ☐	Upgrade Site1 non-CMP clusters for Segment-1	Site Names _____ Cluster List:		2 hrs
4. ☐	Upgrade Site2 clusters for Segment-1	Site Names _____ Cluster List:		2 hrs
5. ☐	Upgrade Site1 clusters for Segment-2	Site Names _____ Cluster List:		2 hrs
6. ☐	Upgrade Site2 clusters for Segment-2	Site Names _____ Cluster List:		2 hrs

2.3.3 Perform System Health Check

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

Procedure 15 Perform System Heath Check

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

4. ☐	Confirm NTP servers reachable from all the servers (CMP and non-CMP) to be upgraded
	NOTE: If the time across the servers is out of synch, fix it first and re-validate this step, before starting the upgrade procedures.
		1. Validate the IP connectivity between the server and NTP servers with the **`ping`** command.
		2. Confirm that time is synchronized on each server with CLI shell command of:
		`[admusr@CMP1194 ~]$ sudo chronyc tracking`
		3. Confirm the date is correct on each server.
		4. Check that the BIOS clock is synced with the clock using the shell **`hwclock`** command:
		`[admusr@CMP1194 ~]$ sudo hwclock`

—End of Procedure—		

2.3.4 Deploy Policy Management Upgrade Software

Software should be deployed to each policy server `/var/TKLC/upgrade` directory, before the actual upgrade activities. This is typically done with utilities such as SCP, WGET, SFTP, or the Upgrade Manager. Because of the large size of the software ISO files, sufficient time should be planned to accomplish this step. For Policy Management Release 15.0.x, each DIU ISO image size is about 8GB for CMP and about 7GB for non-CMP servers.

2.3.4.1 Deploying Policy Management 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 `/var/TKLC/upgrade` directory of each server to be upgraded, where the image is the correct type for that server. Therefore, the CMP software image must be deployed to the CMP servers, the MPE image deployed to the MPE servers, the MRA image deployed to the MRA servers and so on.

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

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

2.3.4.2 Distribute Application ISO Image Files to Servers

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

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

Procedure 16 Distribute Application ISO Image Files to Servers

Step	Procedure	Result

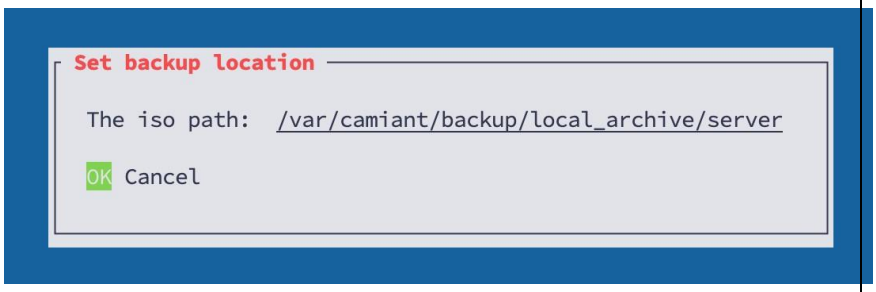
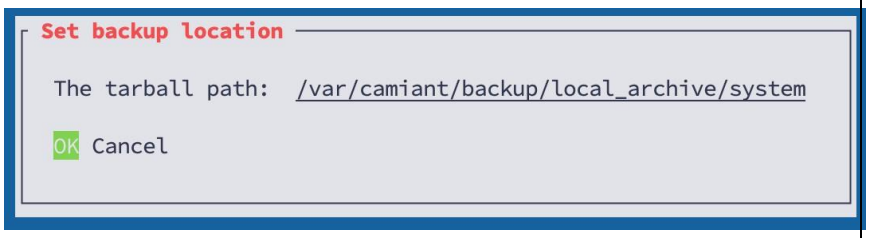
1. ☐	Transfer ISO files to Policy Management Servers.	Transfer release 15.0.x ISO files (CMP and non-CMP) into the `/var/TKLC/upgrade` directory on the respective server using one of the following methods
		• SCP/WGET command
		• USB drive
		OR, if the images are on a server on the same network, scp via CLI.
		Copy CMP software ISO to ONE of the other CMP servers:
		`$sudo scp 872-* <cmp-15.0.x>:/var/TKLC/upgrade/`
		Copy MPE software ISO to ONE of the other MPE servers:
		`$sudo scp 872-* <mpe-15.0.x >:/var/TKLC/upgrade/`
		Copy MPE-Li software ISO to ONE of the other MPE-Li servers:
		`$sudo scp 872-* <mpe-li-15.0.x >:/var/TKLC/upgrade/`
		Copy MRA software ISO to ONE of the other MRA servers:
		`$sudo scp 872-* <mra-15.0.x >:/var/TKLC/upgrade/`
		NOTE: After copying the ISO to one of the respective servers, the ISO Maintenance option is used to upload to the rest of the servers.

—End of Procedure—		

2.3.4.3 Backups and Backup Locations

Procedure 17 Backup servers before upgrading servers

Step	Procedure	Result

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

Step	Procedure	Result

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

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

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

2.4 Upgrade CMP Clusters (15.0 to 15.0.x) wireless mode

2.4.1 Upgrade CMP Clusters Overview

The following is an overview of CMP Cluster upgrade.

1. Upgrade Primary CMP cluster

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

   a. Start Upgrade

   b. Failover

   c. Log back into the CMP GUI

   d. Continue Upgrade

2. Upgrade The Secondary CMP cluster

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

a. Start Upgrade

b. Failover

c. Continue Upgrade

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

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

Note the Information on this CMP cluster:

Cluster Name_____

Server-A Hostname _____

Server-A IP Address _____

Server-A Status _____

Server-B Hostname _____

Server-B IP Address _____

Server-B Status _____

IMPORTANT:

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

2.4.1.1 Upgrade CMP Cluster

Use this procedure to upgrade a Primary CMP Cluster.

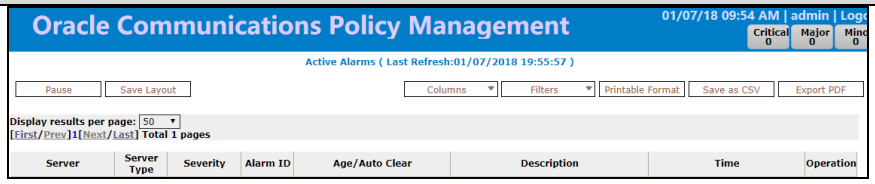
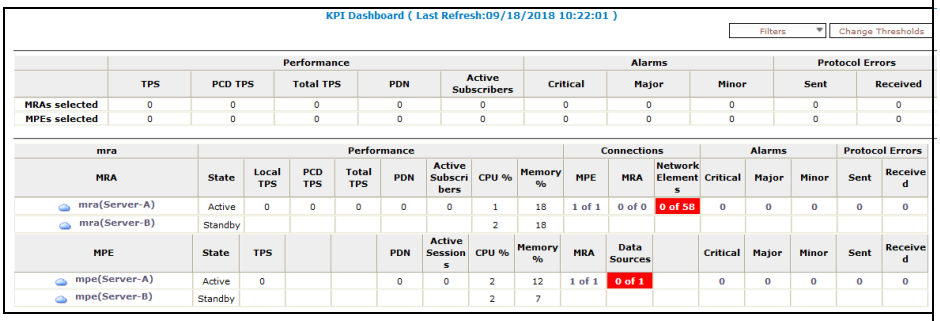
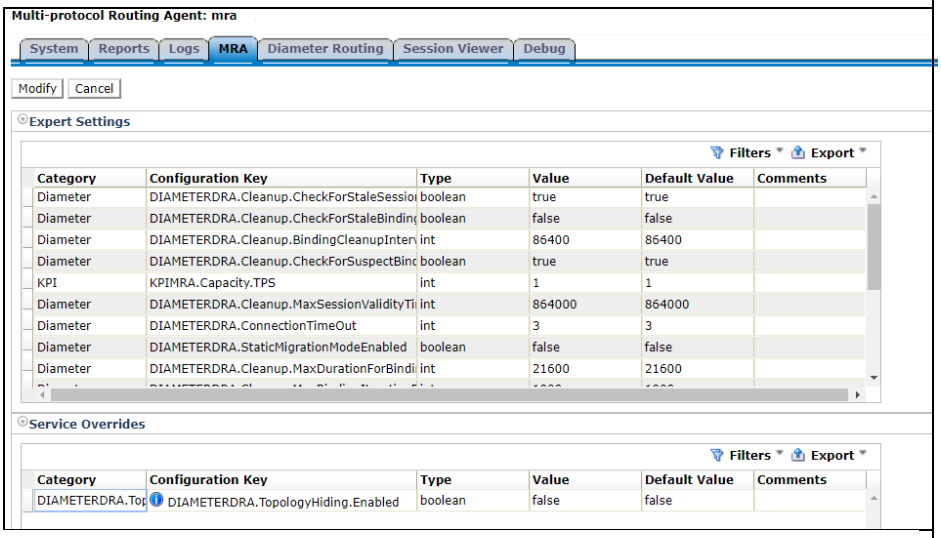
NOTES:

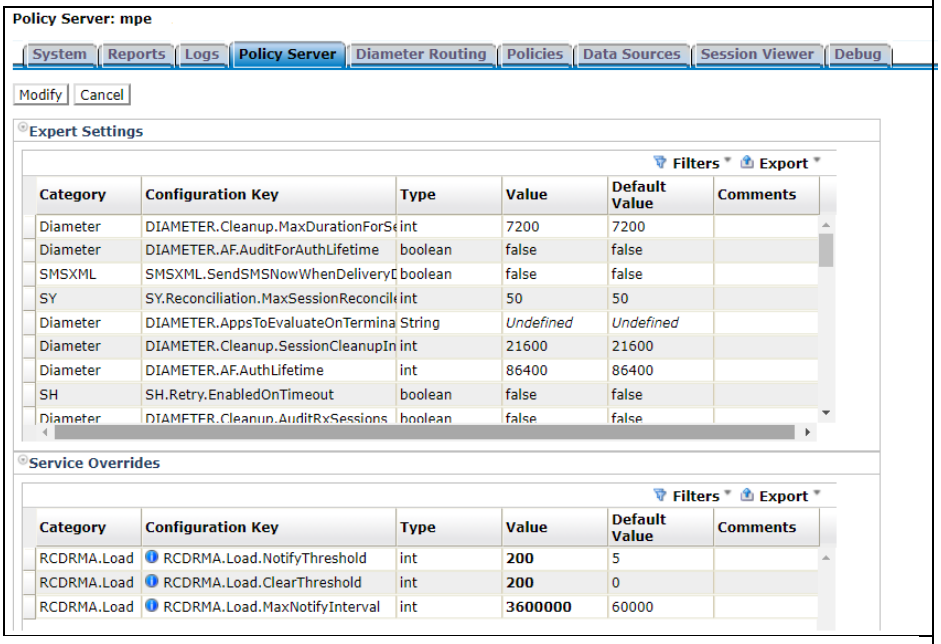
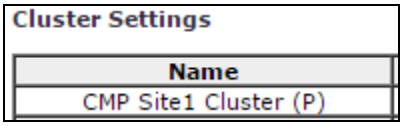
- This procedure must be performed in a maintenance window.
- This procedure takes approximately 60-75 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

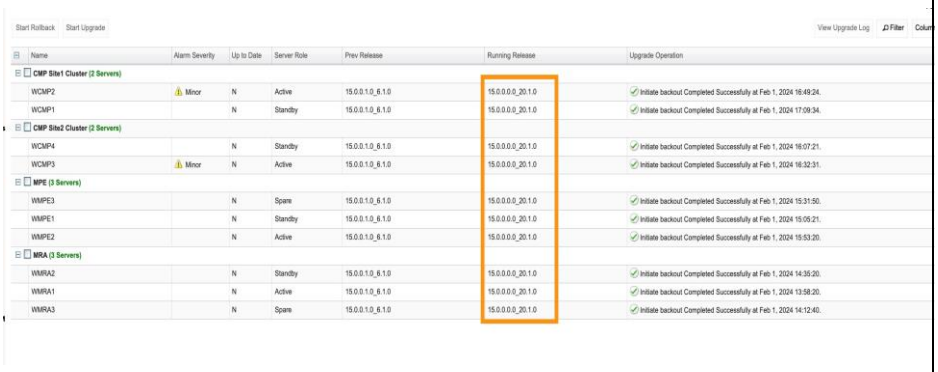
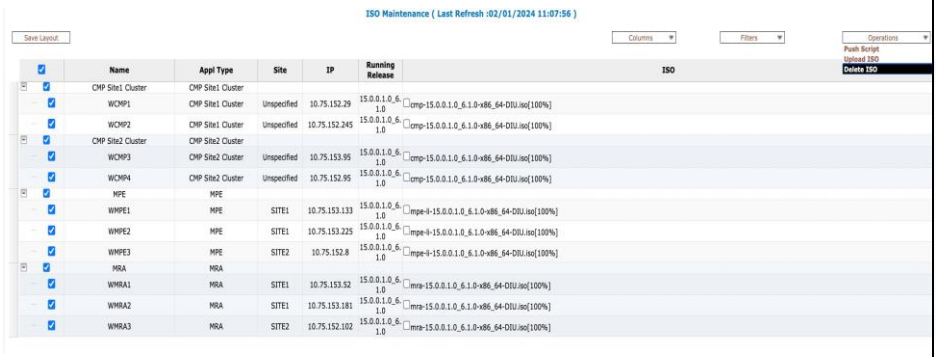
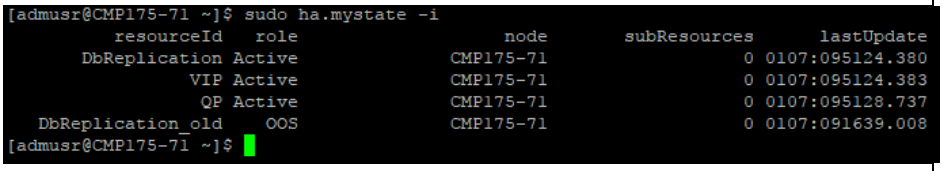
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 18 Upgrade CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Alarm Status.	1. Navigate to **System Wide Reports → Alarms → Active Alarms** 2. Confirm that any existing alarm is understood and there is not any impact to the Upgrade procedure. 3. Capture a screenshot and save it into a file for reference.

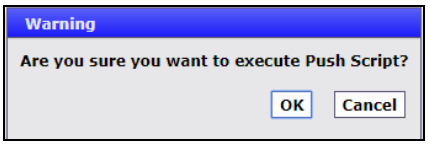
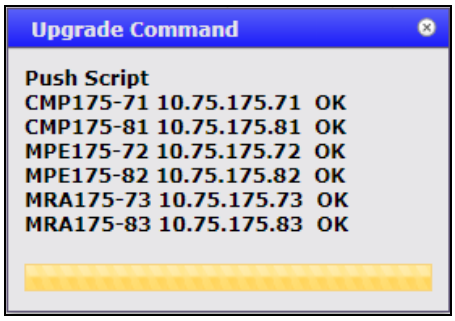
Step	Procedure	Result
		
2. ☐	**CMP GUI:** Verify Traffic Status - KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard** 2. Confirm that all Connections and Traffic status are as expected. Observe it for a few refresh updates. 3. Capture a screenshot and save it into a file for reference. 
3. ☐	**CMP GUI:** Capture MRA Advanced Settings	1. Capture screenshots of the advanced settings on the MRA prior to upgrading the CMP and save them into files for future reference check. 2. Navigate to **MRA → Configuration →** <*MRA*> **→ MRA** 3. Click **Advanced Settings**.  Alternatively, settings can be exported using the **Export** button on the right within each setting.

Step	Procedure	Result
4. ☐	**CMP GUI:** Capture MPE Advanced Settings	1. Capture screenshots of the advanced settings on the MPE prior to upgrading the CMP and save them for future reference. 2. Navigate to **Policy Server → Configuration →** <*MPE*> **→ Policy Server** 3. Click **Advanced Settings**.  Alternatively, settings can be exported using the **Export** button on the right within each setting.
5. ☐	**CMP GUI:** Identify and Record the CMP Cluster(s)	1. Navigate to **Platform Setting → Topology Settings → All Clusters**. 2. Note which cluster is the primary and which cluster is the secondary. 3. Save a screenshot for future reference. The primary CMP is noted with a P 

Step	Procedure	Result
6. ☐	**CMP GUI**: Verify Status of CMP clusters and ISO files are copied to each server	1. Navigate to **Upgrade → Upgrade Manage**r. 2. Verify that the CMP clusters have the following: - Server Role: Active/Standby status. - Running Release: 15.0 version.  3. Navigate to **Upgrade → ISO Maintenance**. 4. Corresponding Release 15.0.x ISO files copied to each of the servers (CMP/MRA/MPE) 
7. ☐	**SSH Primary Active CMP:** SSH CLI Primary Active CMP and verify the Primary Active CMP Role	1. SSH into the Primary Active CMP with its VIP address. Login: admusr Password: <*provided password*> 2. Run the **`sudo ha.mystate -i`** command to confirm the role is Active. `$ sudo ha.mystate -i`  **NOTE:** DbReplication_old_OOS is a non-issue status event.

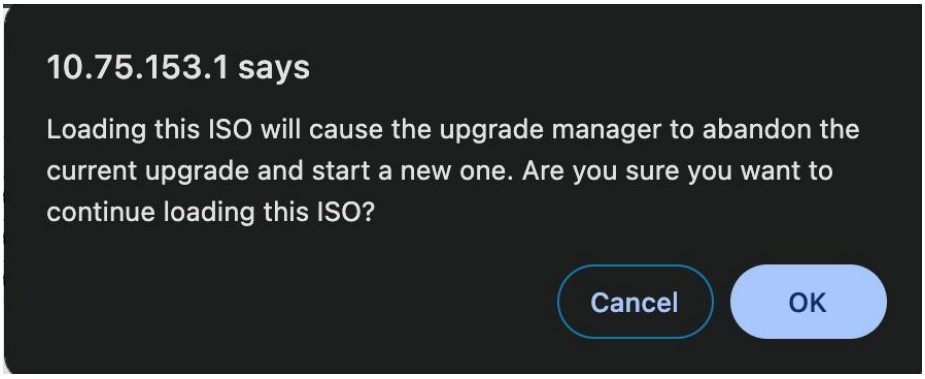
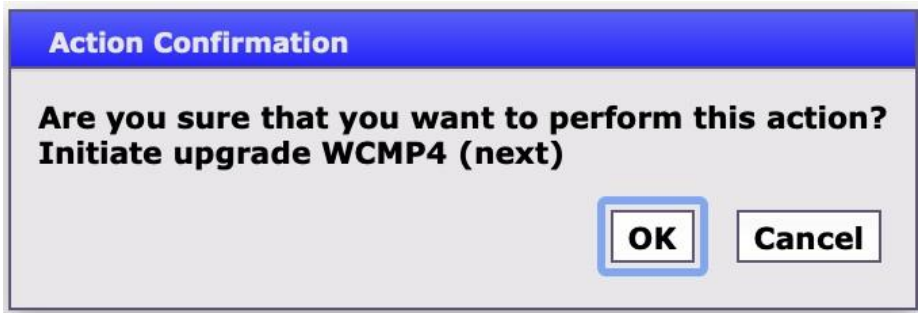
Step	Procedure	Result

8. ☐	**SSH Primary Active CMP:** exchange keys	1. Exchange keys to all servers from the SITE 1 Active Primary CMP.
		2. Login as admusr user.
		3. Notes: This step could be skipped if your system was fresh installed in R15.0.
		`$ sudo mount -o loop /var/TKLC/upgrade/cmp-15.0.0.1.0_x.x.0-x86_64-DIU.iso/mnt/upgrade/`
		`$ sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`
		NOTE: If prompted, answer Yes to all.
		`$ sudo umount /mnt/upgrade`
		`$ sudo qpSSHKeyProv.pl --prov`
		• Required to enter the PASSWORD for admusr user.
		• Ensure that the Keys are exchanged successfully with all the server clusters
		For example:
		`$ sudo qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:<admusr password>`
		`Connecting to admusr@njbbs07cmp01b ...`
		`Connecting to admusr@njbbs07cmp01a ...`
		`Connecting to admusr@txsls07mra01b ...`
		`Connecting to admusr@njbbs07mpe02a ...`
		`Connecting to admusr@txsls07mpe01b ...`
		`Connecting to admusr@njbbs07mra01a`
		`[16/17] Provisioning SSH keys on txsls07mpe02b ...`
		`[17/17] Provisioning SSH keys on njbbs07mra01b ...`
		`SSH keys are OK.`

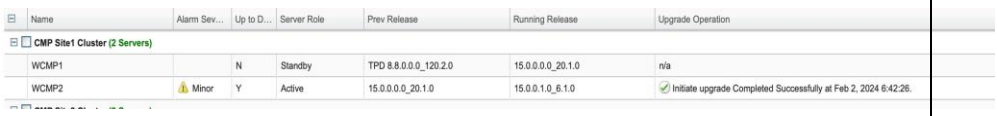
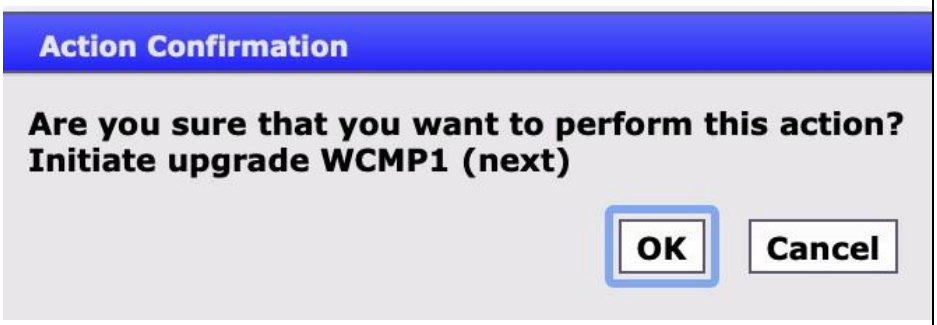
Step	Procedure	Result
9. ☐	**CMP GUI**: Push the Release 15.0.x upgrade Scripts to all servers in the segment topology	1. Navigate to **Upgrade → ISO Maintenanc**e. 2. Select all the servers in the Topology. 3. Select **Operations → Push Script**s. (It is safe to run the push script multiple times as needed). 4. Click **OK** to continue the operation.  5. Verify that operation was successful with OK for every server.  **NOTE:** It may take up to couple minutes to complete

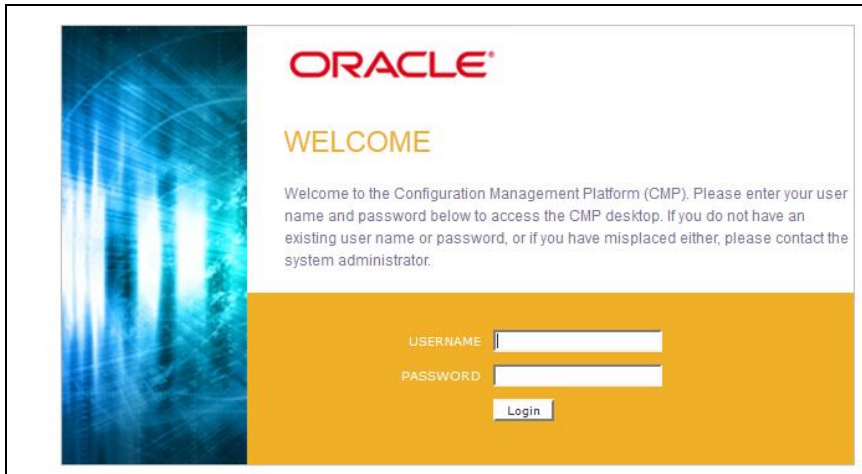
10. ☐	**Primary Active CMP:** ssh to primary active CMP and copy ISO to `/var/camiant/iso`	1. Logon to the primary active CMP as admusr.
		2. Copy the 15.0.x ISO to the `/var/camiant/iso` directory:
		`$ sudo cp /var/TKLC/upgrade/cmp-15.0.0.1.0_x.x.0-x86_64-DIU.iso /var/camiant/iso/`
		3. Verify:
		`$ ls /var/camiant/iso`

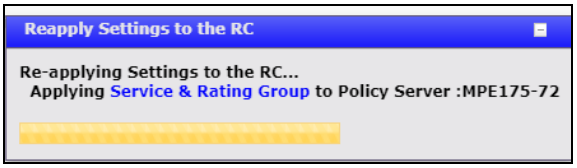
11. ☐	**CMP GUI:** Select the 15.0.x Upgrade release	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Current DIU ISO. 3. This opens a dialog box with a description of the DIU ISO that was copied into the `/var/camiant/iso` directory. 4. Highlight the available 15.0.x DIU ISO. 5. Click **Select incremental-upgrade-15.0.x DIU ISO** on the bottom right hand corner of the window.  6. Click **OK**.

Step	Procedure	Result
		 Within a few seconds, the Up to date column changes from Y (meaning up-to-date) to N (meaning needs upgrade).
12. ☐	**CMP GUI**: Upgrade Primary CMP cluster **NOTE:** This takes approximately 20 minutes at most to complete. **NOTE:** Up to 8 clusters can be upgraded at the same time, selecting one at a time.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Click **Filter** and enter `CMP` in the **Name** field. 3. Select the Primary CMP Server Cluster. 4. Click **Continue Upgrade**.  5. Click **OK** to confirm and continue with the operation.  The specific action taken is determined by the Upgrade Manager and based on the specific version change being performed. This continues to upgrade the standby server only in the CMP Cluster In the Upgrade Operation column, the In Progress status along with the upgrade activities cdisplays.

Step	Procedure	Result
		 Upgrade Status changes to Completed Successfully when done. During the Upgrade activities, the following alarms may be generated and are considered normal reporting events: **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault Upgrade is complete on the first CMP server in the cluster when the following message (completed successfully) displays in the Upgrade Operation column. 
13. ☐	**CMP GUI:** Verify the upgrade is	1. Navigate to **Upgrade → Upgrade Manager**. 2. View the cluster. At this point, one server is on 15.0.x and the other server in the cluster is on 15.0. The Up To Date column shows Y for the 15.0.x server and

Step	Procedure	Result
	successful	N for the 15.0 server. 
14. ☐	**CMP GUI:** Verify System Wide Reports—KPI Dashboard Report	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Verify that report shows all normal traffic processing for the MPEs/MRAs. Observe it for a few refresh updates.
15. ☐	**CMP GUI:** Continue Upgrade CMP cluster	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server cluster. 3. Click **Continue Upgrade**. Notice the failover to new version message. 4. **NOTE:** This causes a failover of the Primary CMP cluster  5. Click **OK** to confirm and continue with the operation.  The action takes less than a minute to complete.

Step	Procedure	Result
16. ☐	**CMP GUI:** Re-login to the CMP server VIP	Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. The Policy Management Release 15.0.x CMP GUI Login displays as shown. Login and password credentials are the same as the pre-upgrade. 
17. ☐	**CMP GUI:** Verify Policy Management Release	1. Navigate to **Help→About**. 2. Verify the release displayed is 15.0.x. **NOTE:** Any '15.0.0.1.0_x.y.z' is correct **15.0.0.1.0_6.1.0** Copyright (C) 2003, 2024 Oracle. All Rights Reserved.
18. ☐	**CMP GUI:** Reapply Configuration to MPE/MRA	• For MPE: **Policy Server → Configuration →** <*MPE cluster*> **→ System** • For MRA: **MRA→Configuration→**<*MRA cluster*>**→System** The selected cluster has the status shown as Degraded and still shows the old release version. Config mismatch may be displayed as well. 1. Click the **Reapply Configuration** operation.

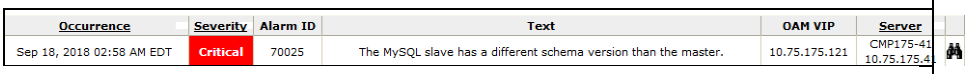
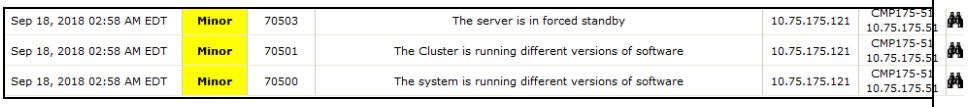
Step	Procedure	Result
		Policy Server: MPE System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sour Modify | Delete | Reapply Configuration **The configuration was applied successfully.** **Configuration** Name: MPE Status: On-line Version: 15.0.0.1.0_6.1.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Feb 01, 2024 10:35 PM EST **Associated Templates(lower numbered templates take priority over higher numbered tem** **Priority** **Template Name** None **NOTE:** A progress banner displays for the MPE reapply configuration. A progress banner DOES NOT display for the MRA reapply configuration.  2. Verify that the Reapply Configuration is successfully:

Step	Procedure	Result
		Policy Server: MPE System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sourc Modify | Delete | Reapply Configuration **The configuration was applied successfully.** **Configuration** Name: MPE Status: On-line Version: 15.0.0.1.0_6.1.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Feb 01, 2024 10:35 PM EST **Associated Templates(lower numbered templates take priority over higher numbered temp** **Priority** **Template Name** None
19. ☐	**CMP GUI:** Verify traffic	1. Navigate to **System Wide Reports → KPI Dashboard**. 2. Verify that report shows all normal traffic processing for the MPEs/MRAs. Observe it for few updates refresh.

	Performance					Alarms			Protocol Errors	
	TPS	PCD TPS	Total TPS	PDN	Active Subscribers	Critical	Major	Minor	Sent	Received
MRAs selected	0	0	0	0	0	0	0	0	0	0
MPEs selected	0	0	0	0	0	0	0	1	0	0

mra		Performance							Connections			Alarms			Protocol Errors	
MRA	State	Local TPS	PCD TPS	Total TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra(Server-A)	Active	0	0	0	0	0	1	18	1 of 1	0 of 0	0 of 58	0	0	0	0	0
mra(Server-B)	Standby						2	18								

MPE	State	TPS			PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
mpe(Server-A)	Active	0			0	0	2	9	1 of 1	0 of 1		0	0	1	0	0
mpe(Server-B)	Standby						2	6								

Step	Procedure	Result
20. ☐	**CMP GUI:** Critical Alarms	Multiple critical alarms (70025) are seen until the SQL Database matches the master (15.0.x). These alarms are expected and remain until all CMPs have been upgraded to the same version.  **Current Minor Alarms** **70503** Server Forced Standby **70501** Cluster Mixed Version **70500** System Mixed Version  **NOTE:** The Upgrade Manager also displays alarms.
21. ☐	**CMP GUI:** Verify the Policy Management Release 15.0 CMP is Active	1. Navigate to **Upgrade→ Upgrade Manager** 2. Verify the following - - Active server is on Running Release 15.0.x - Standby server is on the previous Release  As noted, the Active CMP server is now on the Running Release of 15.0.x.

Step	Procedure	Result
22. ☐	**CMP GUI:** Complete the Upgrade of the Primary CMP Cluster **NOTE:** This takes approximately 20 minutes to complete.	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP Server Cluster. 3. Click **Continue Upgrade**. Notice the message Initiate upgrade.  4. Click **OK** in the dialog to continue the upgrade on the remaining server in the CMP cluster.  **NOTE:** The remaining CMP server takes approximately 20 minutes to complete. Server getting upgraded goes into OOS state. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **70022** The MySQL slave failed synchronizing with the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **70500** The system is running difference versions of software **31101** DB replication to a slave DB has failed **31106** DB merging to the parent Merge Node has failed **31107** DB merging from a child Source Node has failed **31102** DB replication from a master DB has failed **31114** DB Replication of configuration data via SOAP has failed **31105** The DB merge process (inetmerge) is impaired by a s/w fault

Step	Procedure	Result
23. ☐	**CMP GUI:** Tracking the upgrade complete	1. Navigate to **Upgrade → Upgrade Manager**. 2. The last step in the upgrade for the first CMP cluster is to wait for replication to complete. 3. Select the upgraded CMP cluster. 4. Click **View Upgrade** Log.  Cluster Name: CMP Site2 Cluster Last Update: 02/02/2024 9:10:39 Filter Columns ID | Paren… | Action Name | Start Time | End Time | Durat… | Scope | Hostname | Result | Mode | Description 10 | 0 | Preflight Check | 02/02/2024 7:19:26 | 02/02/2024 7:20… | 0:00:45 | Server | WCMP4 | Success | Manual | User initiated action: … 11 | 10 | Upgrading server | 02/02/2024 7:20:11 | 02/02/2024 7:26… | 0:05:49 | Server | WCMP4 | Success | Automatic | Automatic action initi… 12 | 10 | Modify the role/replication … | 02/02/2024 7:20:11 | 02/02/2024 7:20… | 0:00:01 | Cluster | CMP Site2… | Success | Automatic | Automatic action for … 13 | 10 | Wait for replication to sync… | 02/02/2024 7:26:01 | 02/02/2024 7:35… | 0:09:50 | Server | WCMP4 | Success | Automatic | Automatic action wait… 14 | 0 | Failover to new version | 02/02/2024 7:37:16 | 02/02/2024 7:37… | 0:00:00 | Cluster | CMP Site2… | Success | Manual | User initiated action: … 15 | 0 | Failover to old version | 02/02/2024 7:39:12 | 02/02/2024 7:39… | 0:00:00 | Cluster | CMP Site2… | Success | Manual | User initiated action: … 16 | 0 | Preflight Check | 02/02/2024 7:43:48 | 02/02/2024 7:44… | 0:00:43 | Server | WCMP3 | Success | Manual | User initiated action: … 17 | 16 | Upgrading server | 02/02/2024 7:44:31 | 02/02/2024 7:50… | 0:06:18 | Server | WCMP3 | Success | Automatic | Automatic action initi… 18 | 16 | Modify the role/replication … | 02/02/2024 7:44:31 | 02/02/2024 7:44… | 0:00:01 | Cluster | CMP Site2… | Success | Automatic | Automatic action for … 19 | 16 | Wait for replication to sync… | 02/02/2024 7:50:50 | 02/02/2024 8:00… | 0:09:11 | Server | WCMP3 | Success | Automatic | Automatic action wait…
24. ☐	**CMP GUI:** Verify the status of the upgraded CMP server.	Navigate to **Upgrade Manager → Upgrade Manager**.  Name | Alarm Sev… | Up to D… | Server Role | Prev Release | Running Release | Upgrade Operation CMP Site1 Cluster (2 Servers) WCMP2 | Y | Active | 15.0.0.0.0_20.1.0 | 15.0.0.1.0_6.1.0 | Initiate upgrade Completed Successfully at Jan 29, 2024 13:04:49. WCMP1 | Y | Standby | 15.0.0.0.0_20.1.0 | 15.0.0.1.0_6.1.0 | Initiate upgrade Completed Successfully at Jan 29, 2024 14:56:02. CMP Site2 Cluster (2 Servers) • Successful upgrade status shows both servers running the Release 15.0.x in the Running Release column and Y for both servers in the Up To Date column • Active/standby state for both servers in the Primary CMP Cluster.
25. ☐	Proceed to next upgrade procedure	At this point, the Primary Site-1 is running Release 15.0.x • Secondary SITE is on 15.0. • Proceed to the next procedure to upgrade the non-CMP servers.
—End of Procedure—		

NOTE: A message "This system has been upgraded but the upgrade has not yet been accepted or rejected. Please accept or reject the upgrade soon." will be displayed after upgrade of each node in the terminal. This message is just a reminder to accept or reject the upgrade and can be ignored.

2.5 Upgrade non-cmp clusters 15.0 to 15.0.x

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

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

2.5.1 Site/Segment Upgrade Preparation

2.5.1.1 Configuration Preparation

Procedure 19 Preparation for NON-CMP Upgrade

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into CMP server	Use the supported browser to login as admin user or as a user with administrative privileges.
2. ☐	**CMP GUI:** Verify current Upgrade Manager status and Software Release 15.0.x DIU ISO files	**Upgrade → Upgrade Manager** • Verify that all CMP clusters have both Active and Standby status. • Verify that all MPE & MRA clusters have both Active and Standby status. • Verify that the CMP cluster is upgraded successfully and running Policy Management Release 15.0.x **Upgrade → ISO Maintenance** • Verify that Policy Management release 15.0.x DIU ISO files are available for all clusters. One DIU ISO per server
—End of Procedure—		

2.5.2 Upgrade Non-CMP Clusters (MPE or MRA)

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

This procedure is applicable for a 15.0 upgrade to 15.0.x

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

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

1. Upgrade MRAs
2. Upgrade MPEs after MRA upgrade is done

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

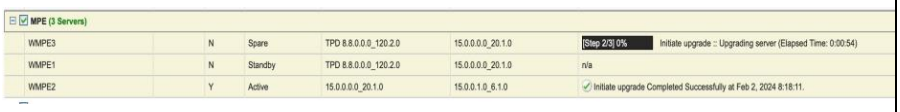
1. Select and start upgrade on the Standby server
2. Failover
3. Continue upgrade on remaining server
4. Re-apply configuration

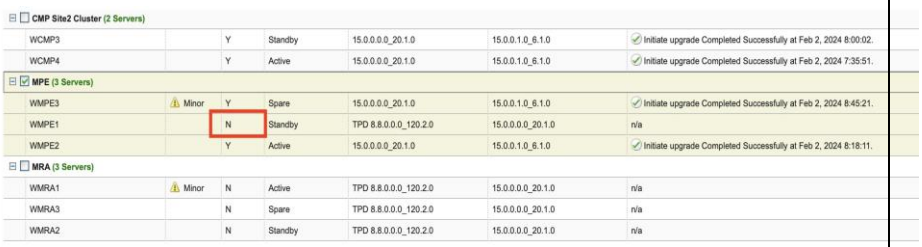
NOTES:

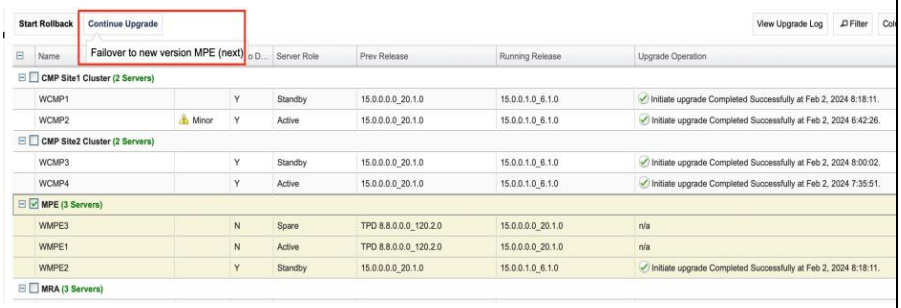
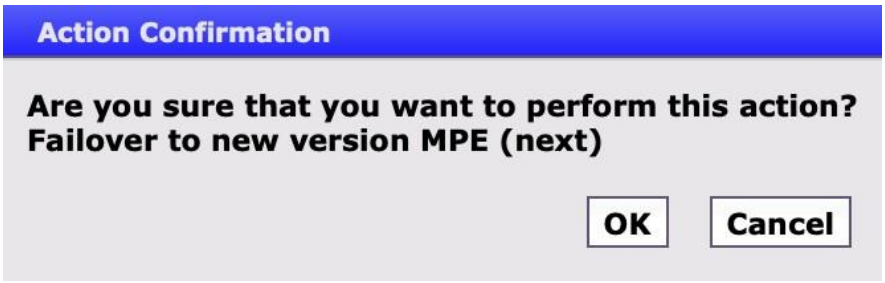
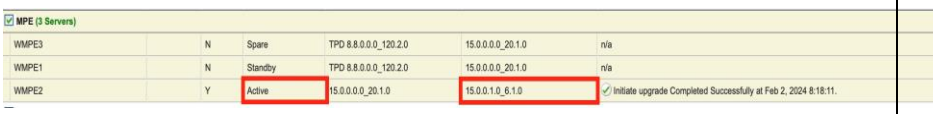
- All CMP clusters must have been upgraded to Policy Management release 15.0.x before performing the following procedures.
- The maximum clusters to be running the upgrade at one time is 16.

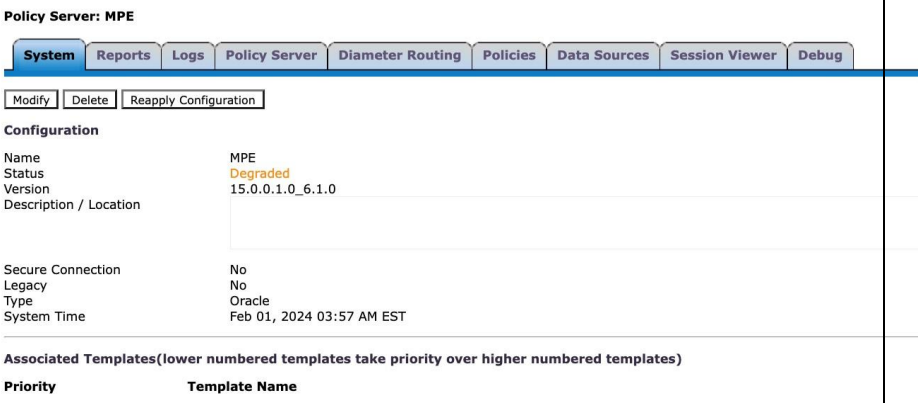
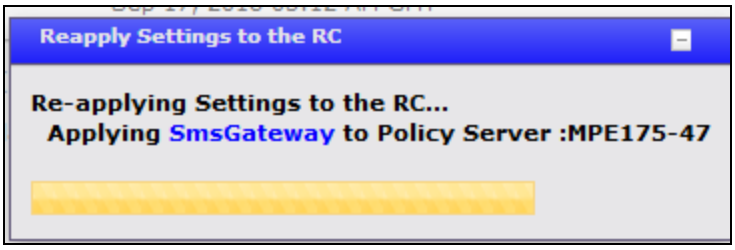
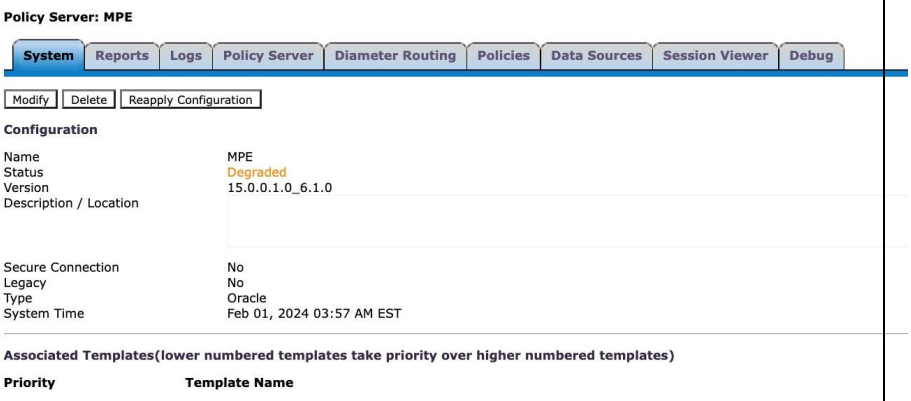
Procedure 20 Upgrade NON-CMP Servers

Step	Procedure	Result
1. ☐	**CMP GUI:** Health checks on the servers to be upgraded	1. Check for current active alarms - For the MPE: **Policy Server→Configuration→Reports → Reset Counters** - For the MRA: **MRA→Configuration→Reports → Reset Counters** 2. Check KPI Dashboard (capture and save screenshot to a file)
2. ☐	**CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment	1. Navigate to **Upgrade → Upgrade Manager**. 2. Verify information for the MRAs/MPEs: - Current Release 15.0 installed - Running with Active/Standby status 3. Navigate to **Upgrade → ISO Maintenance** 4. Verify the ISO version to be deployed is 15.0.x 
3. ☐	**CMP GUI:** Upgrade clusters **NOTE:** The upgrade of one server takes approximately 20 minutes to complete.	Start the upgrade on ONE cluster. Wait until the cluster shows OOS state, then continue with the next cluster and so on. Up to 16 clusters may be running upgrade at any one time. 1. Navigate to **Upgrade → Upgrade Manager** 2. Click the checkbox for the desired cluster (one cluster at a time.) It can be an MRA or an MPE. 3. Click **Continue Upgrade** or **Resume Upgrade**  4. Click **OK** to confirm and continue with the operation. It begins the upgrade of the standby server for that cluster.

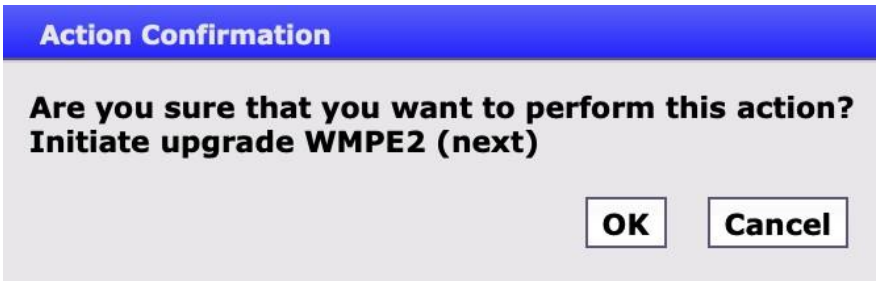
Step	Procedure	Result
		 5. Wait until the standby server reports OOS before selecting the next cluster 6. Follow the progress status in the Upgrade Operation column. 7. During the upgrade activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the clusters are completely upgraded. **Expected Critical Alarms** **31283** High availability server is offline **70001** QP_procmgr failed **31227** High availability status failed **70007** Not all QP resources are ready **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 **70502** Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31102** DB replication from a master DB has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault **78001** RSYNC Failed Upgrade is complete on the first server of the cluster when the Initiate upgrade completed successfully at… message displays in the Upgrade Operation column. The server goes back to standby state when the upgrade completes.

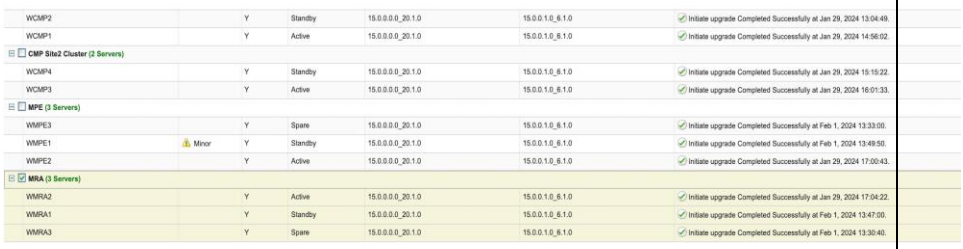
Step	Procedure	Result
		 A number of different alarms may be raised at this point: **Expected Minor Alarms** **78001** RSYNC Failed **70500** The system is running different versions of software **70501** The Cluster is running different versions of software **70503** The server is in forced standby

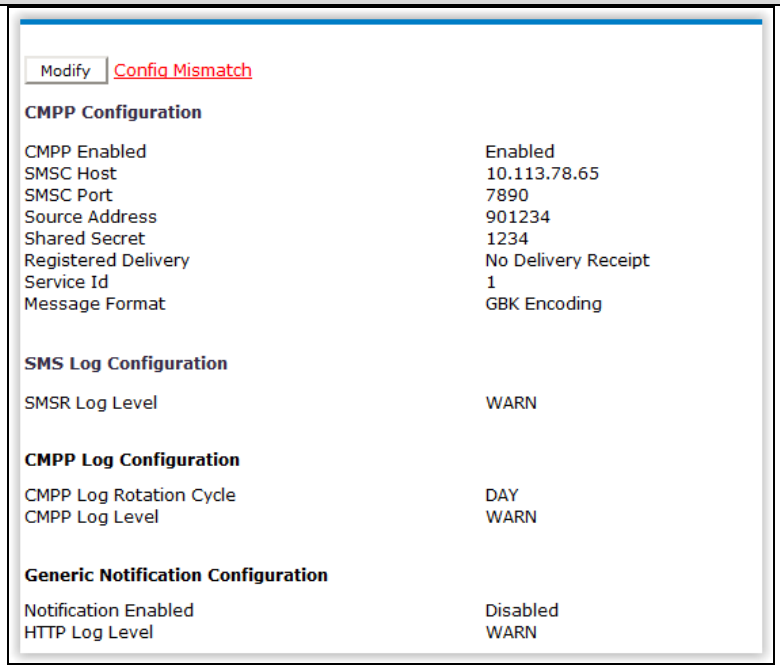
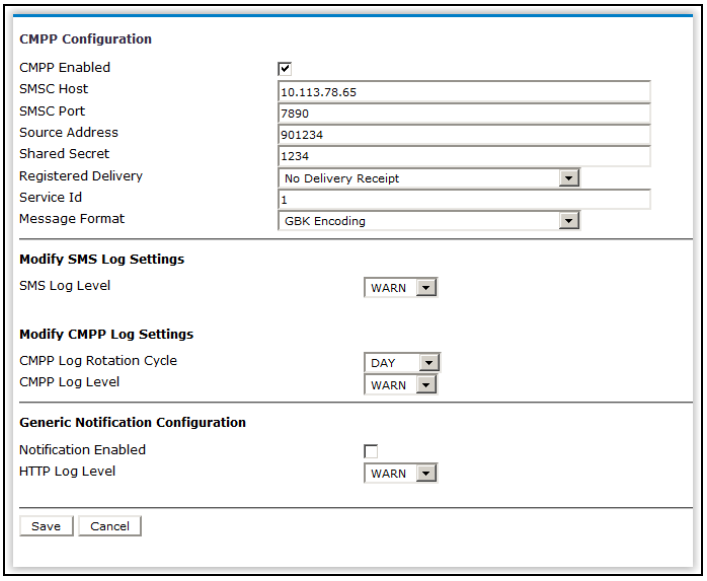
Step	Procedure	Result
4. ☐	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Next operation is a failover. **NOTE:** 16 clusters can be running the upgrade process at one time.	Failover ONE cluster at a time. Wait for a minute, before moving on to the next cluster. 1. Navigate to **Upgrade → Upgrade Manager** 2. Select the cluster (one cluster at a time). It can be an MRA or MPE. 3. Click **Continue Upgrade**. When hovering over the **Continue Upgrade** button, it displays the Failover to new version message.  4. Click **OK** to confirm and continue with the operation. It begins to failover the cluster.  5. Wait until failover completes, that is, the upgraded server becomes the active server before failing over the next cluster. 

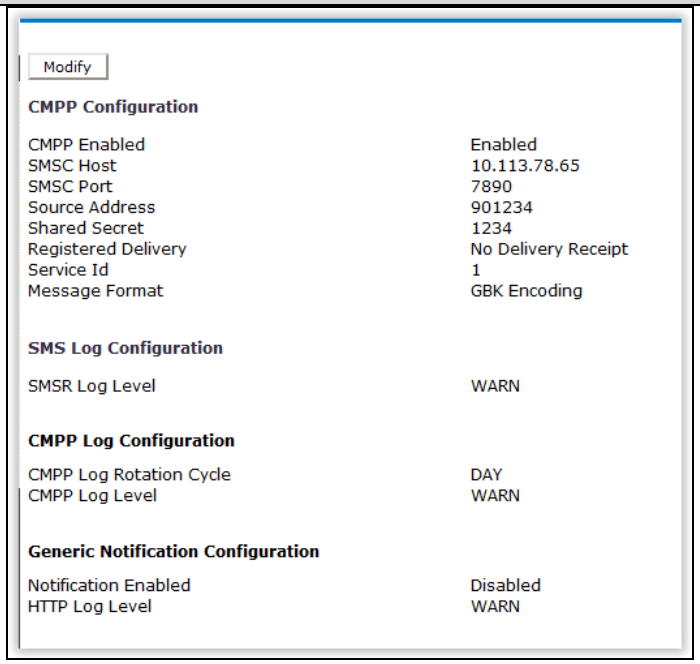
Step	Procedure	Result
5. ☐	**CMP GUI:** Reapply configuration on the MPE/MRA cluster that failed over successfully.	• For MPE: **Policy Server → Configuration → <***MPE cluster***> → System** • For MRA: **MRA→Configuration→<***MRA cluster***>→System** The selected cluster has the status shown as Degraded and still shows the old release version. Config mismatch may be displayed as well. 1. Click the **Reapply Configuration** operation.  **NOTE:** A progress banner displays for the MPE reapply configuration. A progress banner DOES NOT display for the MRA reapply configuration.  2. Verify that the Version is changed to the upgraded Release 15.0.x 3. The cluster still shows the Degraded status: 

Step	Procedure	Result
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 **31101** DB Replication To Slave Failure **31113** DB Replication Manually Disabled
7. ☐	**CMP GUI:** Verify traffic becomes active within 90 seconds	1. Navigate to **Upgrade Manager → System Maintenance** - If traffic is active, go to step 9. - If traffic does not become active within 90 seconds: 2. Select the checkbox for the partially upgraded cluster, and select **Operations → Rollback**. 3. The pre-15.0.x MPE server should become active and resume handling traffic.
8. ☐	**CMP GUI:** Reapply configuration	1. Navigate to **Policy Server → Configuration →** *<mpe_cluster name>* **→ System** or **MRA → Configuration →** *<mra_cluster name>* **→ System** 2. Click **Reapply Configuration** • Verify that the version is changed back to 15.0, and the action report success. • If NOT, stop and contact Oracle support to back out of the partially upgraded cluster.
9. ☐	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Upgrade on the Standby server	Continue the upgrade on ONE cluster at a time and when the server goes into OOS, continue with the next cluster and so on. Up to 16 clusters may be running upgrade at one time. 1. Navigate to **Upgrade → Upgrade Manager**. 2. Select a cluster (one cluster at a time), it can be an MRA or an MPE. 3. Click **Continue Upgrade**. When hovering over the **Continue Upgrade** button, it displays the Initiate upgrade… on the standby server message.

Step	Procedure	Result
		 4. Click **OK** to confirm and continue with the operation. It begins the final server upgrade of the cluster  5. If you plan to perform the upgrade for several clusters in parallel (up to 16), wait until the server being upgraded changes to OOS before moving on to the next cluster. 6. Follow the progress status in the Upgrade Operation column. 7. During the upgrade activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely upgraded. **Expected Critical Alarms** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **70007** Not all QP resources are ready **Expected Major Alarm** **70004** QP Processes down for maintenance **Expected Minor Alarms** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure

Step	Procedure	Result
		31107 DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled Upgrade is complete when the `Initiate upgrade completed successfully at…` message displays in the Upgrade Operation column. The server goes back to Standby state and the Up to Date column shows a Y (YES). 
10. ☐	REPEAT steps 1 through 10 for next MPE/MRA cluster(s)	Proceed with the next clusters until all clusters have been upgraded 
11. ☐	**CMP GUI:** Modify/save SMSR configuration	**System Administration → SMS Relay → Modify** **NOTE: This step is only for Wireless-C system. If you do not see SMS Relay under System Administration, skip this step.** Initial access into this configuration upon upgrade to release 15.0.x, the configuration shows as such with Config Mismatch.

Step	Procedure	Result
		 1. Click **Modify.** The following is an example of the SMSR configuration. DO NOT change any of the configuration if it has been working in the past.  2. Click **Save** to save the configuration and continue as shown.

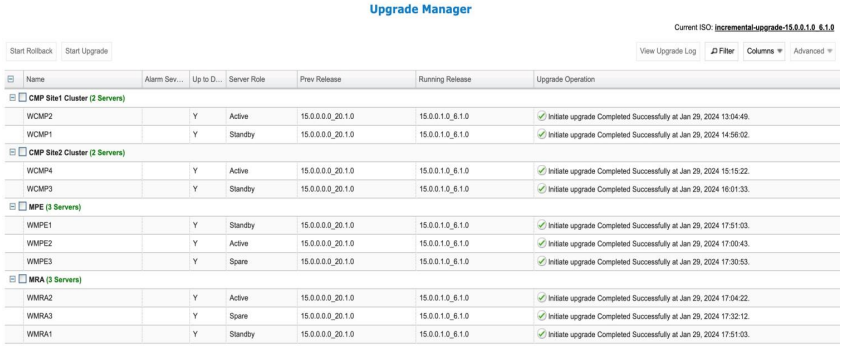
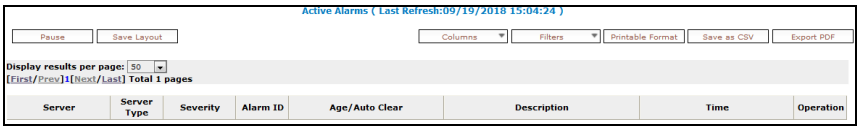
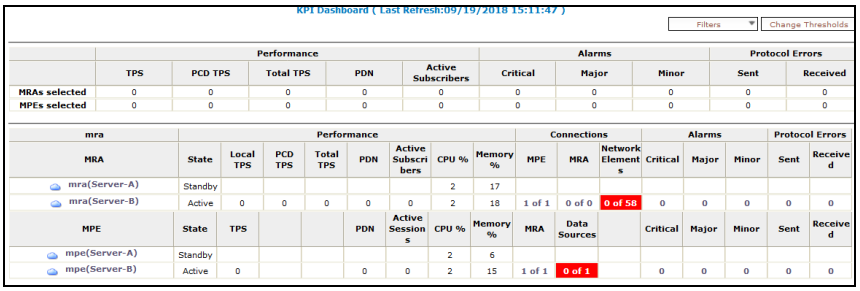
Step	Procedure	Result
		 Modify **CMPP Configuration** CMPP Enabled: Enabled SMSC Host: 10.113.78.65 SMSC Port: 7890 Source Address: 901234 Shared Secret: 1234 Registered Delivery: No Delivery Receipt Service Id: 1 Message Format: GBK Encoding **SMS Log Configuration** SMSR Log Level: WARN **CMPP Log Configuration** CMPP Log Rotation Cycle: DAY CMPP Log Level: WARN **Generic Notification Configuration** Notification Enabled: Disabled HTTP Log Level: WARN **NOTE:** The Config Mismatch message is not there with the saved configuration.
—End of Procedure—		

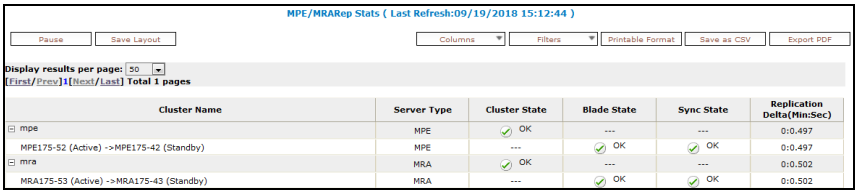
NOTE: A message "This system has been upgraded but the upgrade has not yet been accepted or rejected. Please accept or reject the upgrade soon." will be displayed after upgrade of each node in the terminal. This message is just a reminder to accept or reject the upgrade and can be ignored.

2.6 Post Upgrade health Check for wireless systems

NOTE: This section is used when the entire topology is running release 15.0.x.

Procedure 21 Health Check after upgrade completed

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the upgrade is successful on all clusters.	1. Navigate to **Upgrade → Upgrade Manager**. 2. View the Up to Date, Running Release, and Upgrade Operation columns and verify they read Y, 15.0.x…., and Initiate upgrade completed successfully at… respectively, for all servers in all clusters. 
2. ☐	**CMP GUI:** View current alarms	1. Navigate to **System Wide Reports→Alarms→Active Alarms**. 2. Verify that all alarms due to the upgrade have been cleared. 
3. ☐	**CMP GUI**: View current KPIs	1. Navigate to **System Wide Reports→KPI Dashbord.** 2. Make sure the counter stats are incrementing properly. 

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

3. ☐	Verify System Health	1. Use the **`sudo syscheck`** command on every server.
		2. Verify that each class test returns OK. For example:
		`$ sudo syscheck`
		`Running modules in class disk... OK`
		`Running modules in class hardware... OK`
		`Running modules in class net... OK`
		`Running modules in class proc... OK`
		`Running modules in class system...OK`
		LOG LOCATION: `/var/TKLC/log/syscheck/fail_log`

—End of Procedure—		

2.7 Backout (ROLLBACK) 15.0 wireless mode

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

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

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

2.7.1 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 must be maintained even if there are unexpected failures.

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

2.7.1.1 Pre-requisites

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

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

2.7.1.2 Backout of Fully Upgraded Cluster

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

Use this procedure to backout a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster are on a pre-15.0 release with Active, Standby status.

Expected pre-conditions:

- The primary active CMP is on release 15.0.x
- The cluster servers to be backed out are on release 15.0

2.7.1.3 Backout Sequence

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

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

Overview on Backout/Rollback MRA/MPE cluster

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

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

Backout Secondary CMP (if applicable)

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

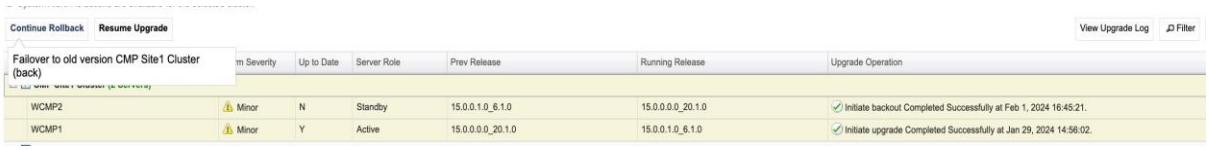
Use the CMP GUI (Upgrade Manager) to backout the Secondary CMP cluster.

Backout Primary CMP (From 15.0.x to 15.0)

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

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

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



4. Log in to the Primary CMP VIP.
5. Wait for 10-15 minutes before the rollback of secondary CMP (in Primary Site) to allow secondary site CMP nodes to sync with the new MySQL master.
6. Use the 15.0 Upgrade Manager to complete backout of the Primary CMP cluster.

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

2.7.1.4 Back-out Partially Upgraded MPE/MRA Cluster

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

Expected Pre-conditions:

1. Primary Active CMP is on Release 15.0.x
2. Cluster is any of MPE or MRA
3. One server of target cluster is on Release 15.0.x
4. Other servers of target cluster are on Release 15.0

NOTES:

- This procedure must be performed within a maintenance window.
- This procedure takes approximately 15 minutes at most per server.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

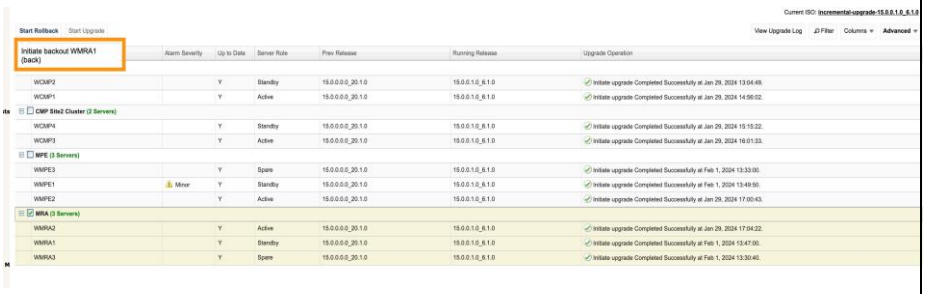
Procedure 22 Back-out Partially Upgraded MPE/MRA Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected Clusters	1. Navigate to **Upgrade → Upgrade Manager** 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 15.0.x - Target Cluster has 1 server on Release 15.0, and 1 server on Release 15.0.x - Active server is on 15.0

2. ☐	**MPE/MRA SSH:** Verify `/var/log/messages` file size	1. Using SSH, login to the Standby server to be backed out as admusr.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.
		`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`

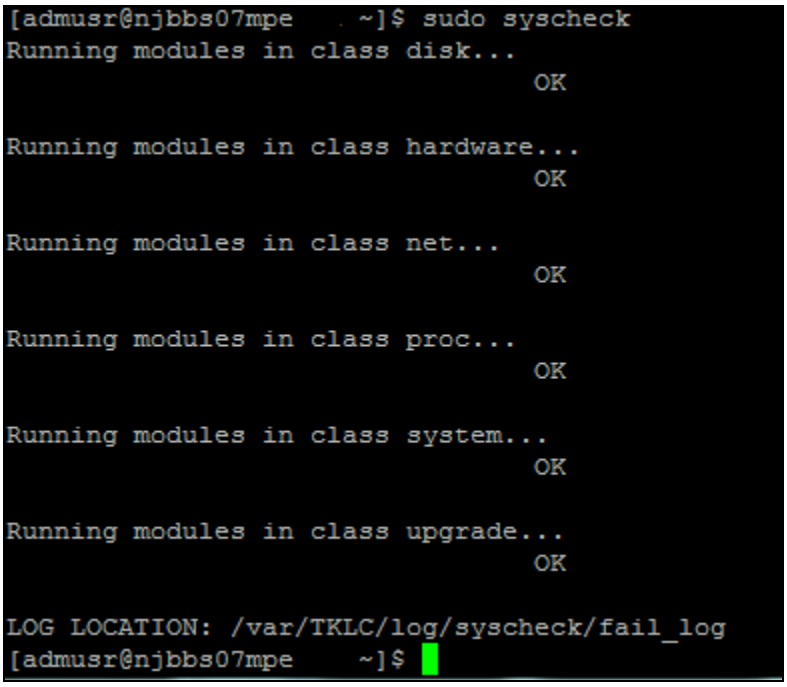
Step	Procedure	Result

		```$ sudo cat /dev/null > /var/log/messages```
		 ```$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"```
		 3. Verify:
		 ```$ ls -lh /var/log/messages```

3. ☐	**CMP GUI:** Verify the status of affected Clusters **NOTE:** This takes approximately 15 minutes to complete.	1. Select **Start Rollback** or **Continue Rollback**. When hovering over the button, it indicates the server to get backed out.  2. Click **OK** to confirm and continue with the operation. It begins to back-out. 3. Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message **31284** High availability remote subscriber has not received a heartbeat

Step	Procedure	Result
		31107 DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the successful completion message (Initiate Back-out Completed Successfully) 

Step	Procedure	Result

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

—End of Procedure—		

2.7.1.5 Back-out Fully Upgraded MPE/MRA Cluster

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

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

At the end of this procedure, all servers of the target cluster are on Release 15.0 (MRA, MPE, CMP) with Active, Standby status.

Expected pre-conditions:

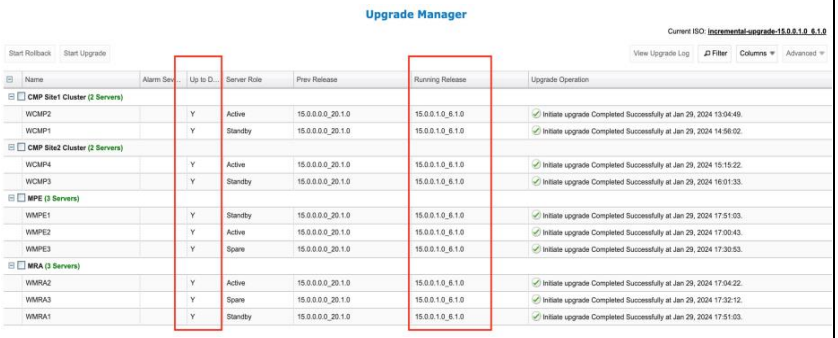
1. Primary Active CMP is on Release 15.0.x.
2. Cluster is of MPE or MRA.
3. Servers of target cluster are on Release 15.0.x in either in Active, Standby or Force Standby role.

NOTES:

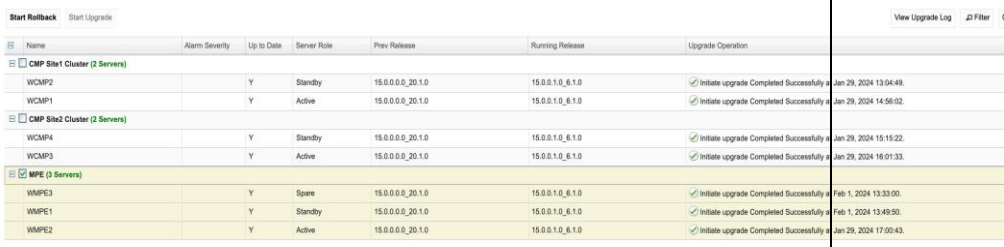
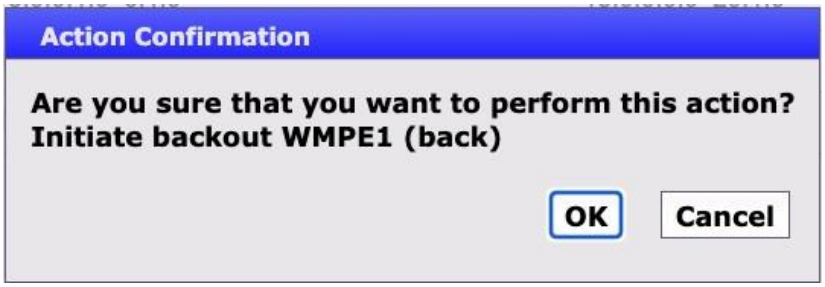
- This procedure must be performed within a maintenance window.
- This takes approximately 45-60 minutes per MPE or MRA cluster.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

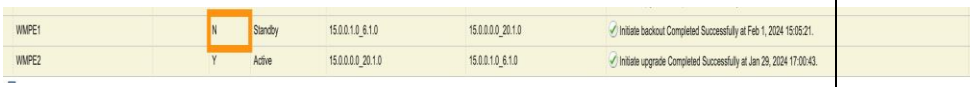
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure 23 Back-out Fully Upgraded MPE/MRA Cluster

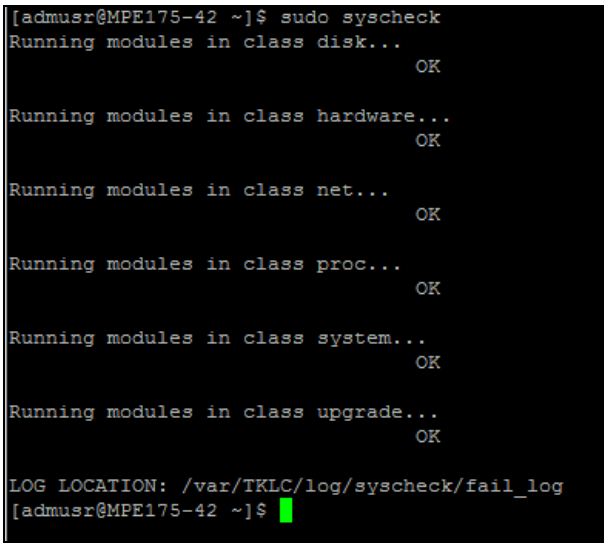
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the status of affected Clusters	1. Navigate to **Upgrade → Upgrade Manager** 2. Confirm status of the cluster is backed out: - Primary Active CMP is on Release 15.0.x - MPE/MRA is on Release 15.0.x Up to Date Column shows Y for all servers in this cluster **EXAMPLE** 

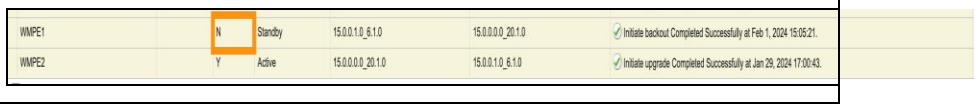
2. ☐	**MPE/MRA SSH:** Verify `/var/log/messages` file size	1. Use SSH to login to the Standby server to be backed out as admusr
		NOTE: The Active server is checked after the failover later on in this procedure.
		`$ ls -lh /var/log/messages`
		2. ONLY if the resulting size of `/var/log/messages` is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

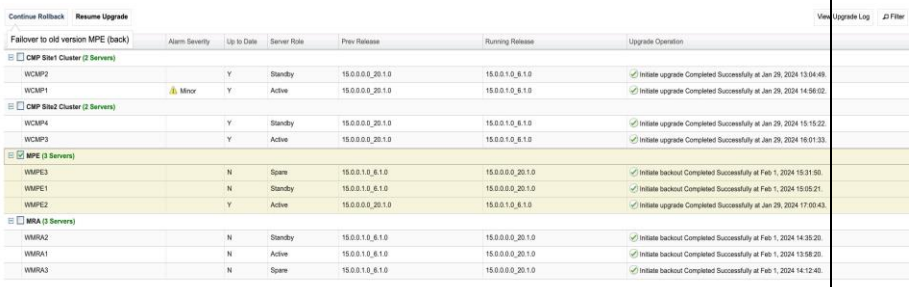
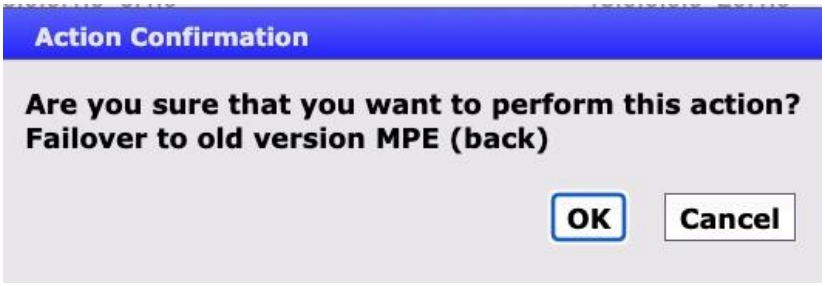
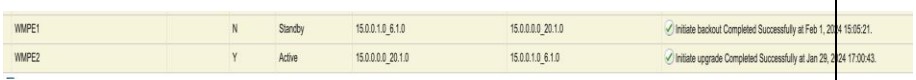
Step	Procedure	Result
		`$ ls -lh /var/log/messages`
3. ☐	**CMP GUI:** Initiate Back-out **NOTES:** Each back-out of one blade server completes in approximately 15 minutes. Up to 8 clusters can be backed out at the same time, selecting one at a time.	1. Navigate to **Upgrade → Upgrade Manager** 2. Select the cluster (one cluster at a time) (can be an MRA or MPE) 3. Click **Start Rollback**. When hovering over the button, it indicates the server to be backed out. In this case it is the current standby server.  4. Click **OK** to confirm and continue with the operation. It begins to back-out.  5. Follow the progress status in the Upgrade Operation column. 6. At this point, the server backing out goes into OOS state 7. Wait until the server goes to an OOS state before selecting the next cluster to back-out. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70028** Signaling bonded interface is down **31283** High availability server is offline **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance

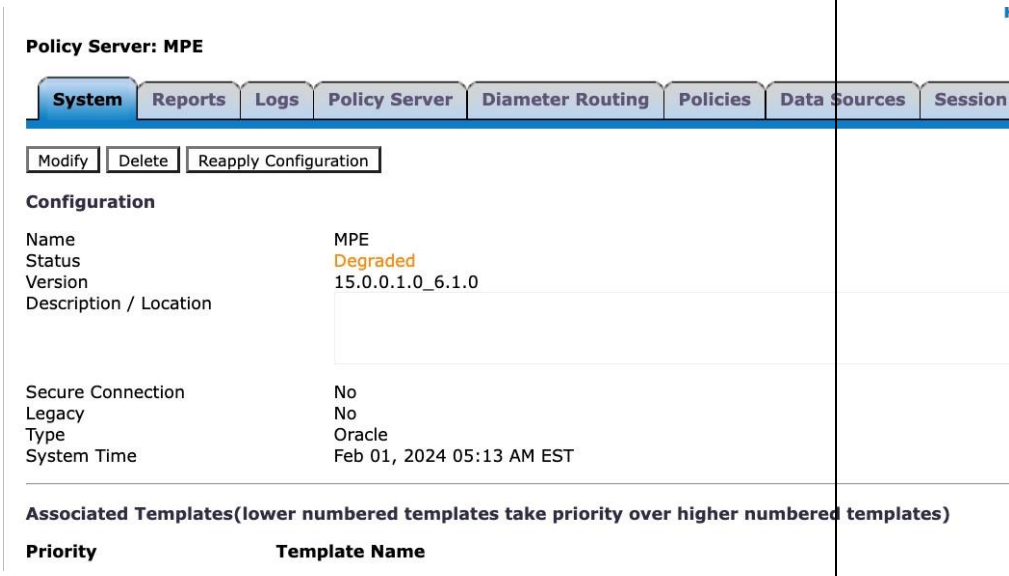
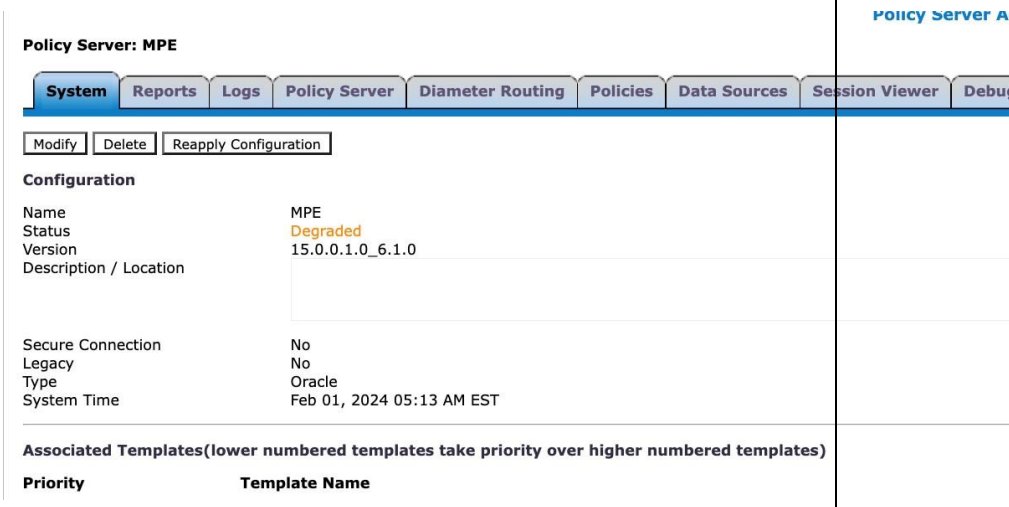
Step	Procedure	Result
		31236 High availability TCP link is down **31233** High availability path loss of connectivity **<u>Expected Minor Alarms</u>** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message …. **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault Back-out of the server is complete when the successful completion displays in the Upgrade Operation column. The server shows running release of 15.0 and return to standby with an N in the Up To Date Column.  ***Note:*** If the alarms 70501 and/or 70507 are not cleared, please follow the below steps: 1. Navigate to **Upgrade -> Upgrade Manager**. 2. In the **Current ISO** section, click **Select ISO** Button and select a previous iso. 3. Now the alarms should get cleared. 4. (optional) Revert the Step 2 and select the ISO of current version.
4. ☐	**CMP GUI** Verify the back-out is successful	1. Select the partially Backed out cluster 2. Select the View Upgrade LOG  3. Check upgrade logs for the remainder of partially Backed out clusters.

Step	Procedure	Result

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

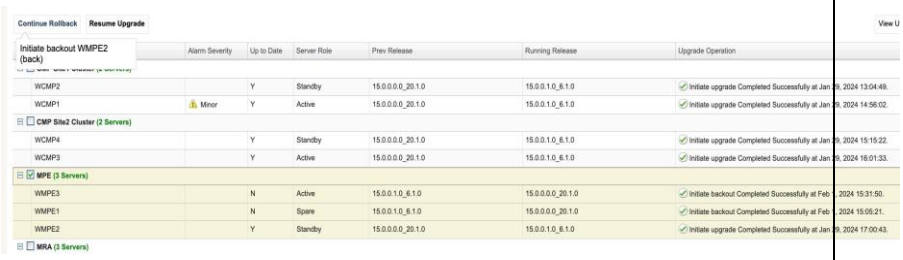
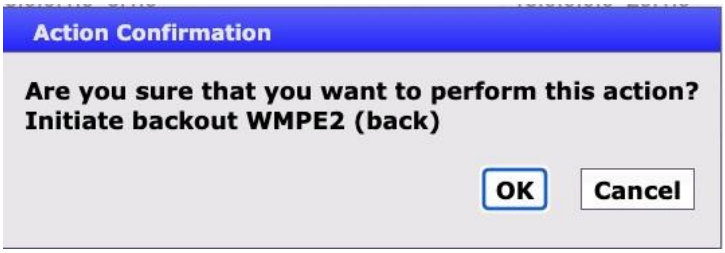
6. ☐	Confirm MPE/MRA server status	Ensure that the Active are on 15.0.x and the standby server shows running release of 15.0 

Step	Procedure	Result
7. ☐	**CMP GUI**: Continue the back-out of the MRA/MPE clusters. Next operation is failover to the 15.0 server. **NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time.	Current state of the cluster must be as follows. • Active Server is on Release 15.0.x • Standby Server is on Previous release 1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click Continue Rollback. When hovering over the button, it informs you to failover to old version, which is 15.0.  3. Click **OK** to confirm and continue with the operation. It begins to failover.  Wait until the server fails over before selecting the next cluster. This takes approximately 2 minutes. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **Expected Major Alarms** **74603** The number of failed MPE primary cluster reaches the threshold **Expected Minor Alarms** **70503** The server is in forced standby **31102** DB replication from a master DB has failed **71402** Diameter Connectivity Lost **31101** DB replication to a slave DB has failed **78001** Transfer of Policy jar files failed State of the cluster looks like the following when the failover completes. 

Step	Procedure	Result
8. ☐	**CMP GUI:** Reapply Configuration on MPE/MRA cluster that competed the failover successfully	• For MPE: Navigate to **Policy Server → Configuration →** <*MPE*> **→ System** • For MRA: Navigate to **MRA → Configuration →** <*MRA*> **→ System** The selected cluster status is Degraded as expected as shown:  Click **Reapply Configuration** operation. • The Version is successfully changed to the upgraded Release 15.0.x • The status is Degraded which is a normal reporting event as the servers are in different status. **MPE** 

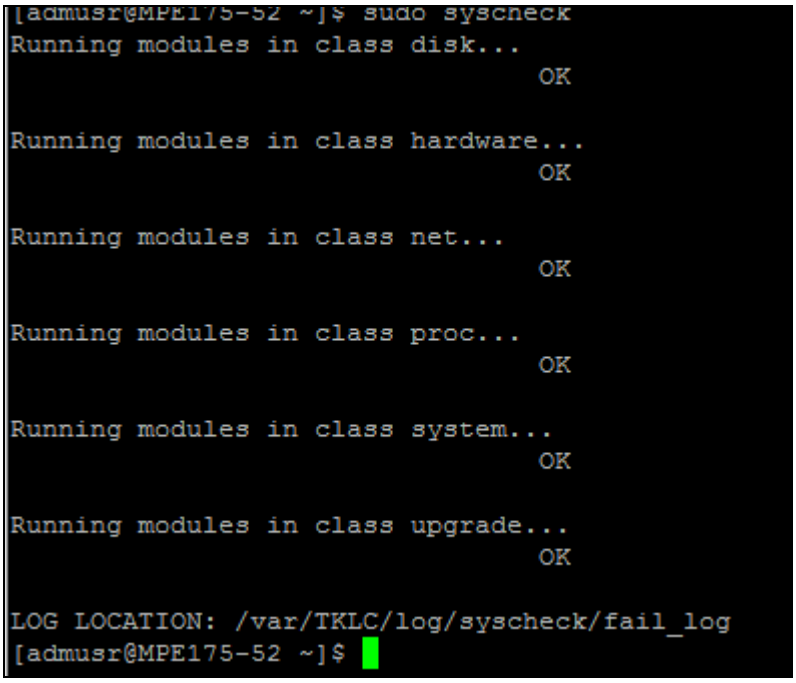
Step	Procedure	Result

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

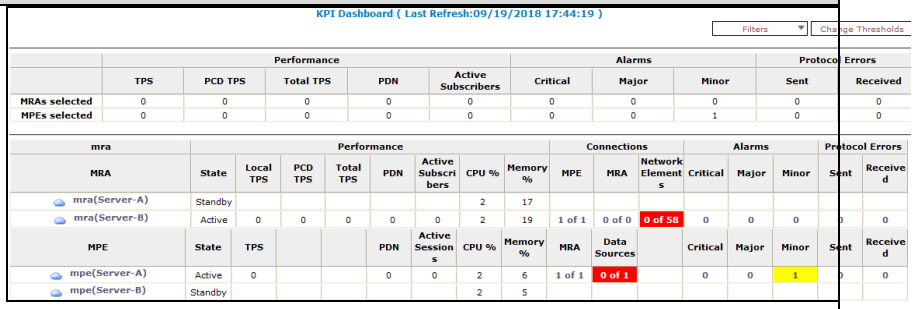
10. ☐	**CMP GUI:** Complete Back-out of cluster(s) **NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time. **NOTE:** Each back-out of one blade server completes in approximately 15 minutes	1. Select the cluster (one cluster at a time) (can be an MRA or MPE) 2. Click **Continue Rollback**. When hovering over the button, it indicates the back-out server.  3. Click **OK** to confirm and continue with the operation. It begins to back-out.  4. Follow the progress status in the Upgrade Operation column. 5. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed **31227** The high availability status is failed due to raised alarms **70007** Not all QP resources are ready **70028** Signaling bonded interface is down **31283** High availability server is offline

Step	Procedure	Result
		Expected Major Alarms **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31282** The HA manager (cmha) is impaired by a s/w fault **31232** High availability server has not received a message **31284** High availability remote subscriber has not received a heartbeat **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31104** DB Replication latency has exceeded thresholds **78001** Transfer of Policy jar files failed **70500** The system is running difference versions of software **31100** The DB replication process is impaired by a s/w fault 6. Back-out of the server is complete when the successful completion message (initiate Back-out completed successfully) displays in the Upgrade Operation column. 7. Verify in Upgrade Log that that back-out was successful: 8. All of the servers are on Release 15.0 at this point and show active/standby 

Step	Procedure	Result

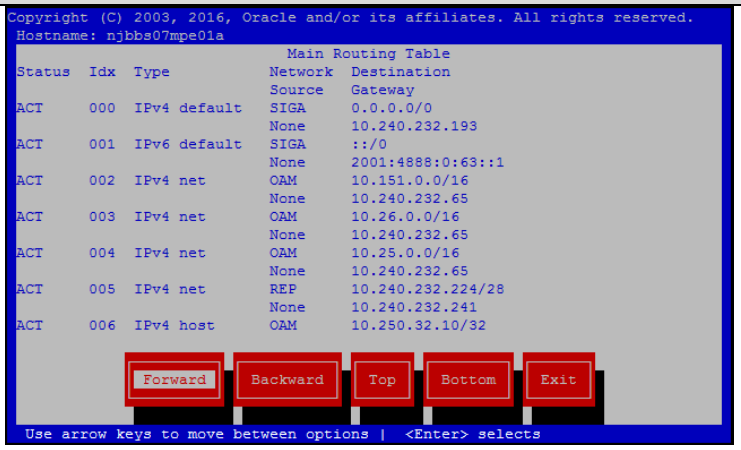
11. ☐	**MPE/MRA SSH:** Verify syscheck and `/tmp` directory permission	1. Login to the backed-out standby server as admusr.
		2. Verify that there are no failures in syscheck:
		`$ sudo syscheck`
		 
		3. Verify `/tmp` directory permissions:
		`$ ls -l /`
		4. **NOTE:** Permissions should be the following,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

12. ☐	**CMP GUI:** Verify that backed out cluster is processing traffic normally.	Verify Cluster is processing traffic normally. Navigate to **System Wide Reports → KPI Dashboard**.

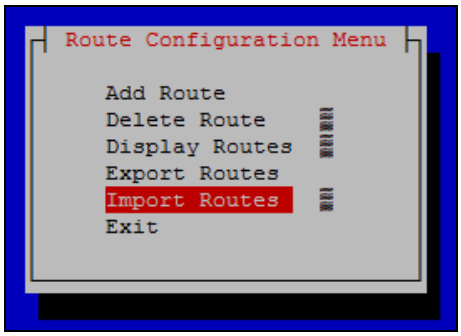
Step	Procedure	Result
		
13. ☐	**CMP GUI:** Verify alarms	1. Navigate to System Wide Reports → Alarms → Active Alarms 2. Verify that there are no unexpected active alarms present. **NOTE:** Some alarms may take 30 minutes to 1 hour for auto clearing time.

14. ☐	**MPE/MRA SSH:** Verify routes	1. Login into MPE/MRA server as admusr.
		2. Copy routes_output.txt from the `/home/admusr` directoy to the `/tmp` directory.
		`$ sudo cp routes_output.txt /tmp`
		`$ cd /tmp`
		`$ ls`
		`routes_output.txt`
		WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance Engineering.
		3. Start the platcfg utility.
		`$ sudo su - platcfg`
		4. Navigate to **Policy Configuration → Routing Config → Display Routes**
		5. Click **Forward** to view all the routes.
		6. Verify that all routes are present.
		Example

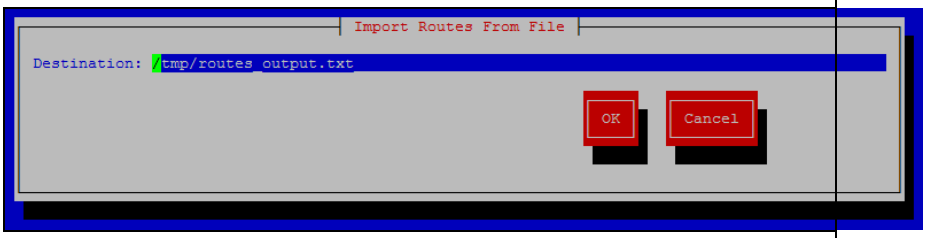
Step	Procedure	Result



7. If any of the routes are missing then perform the following otherwise skip to step 18
8. Navigate back to Route Configuration Menu and select **Import Routes**.

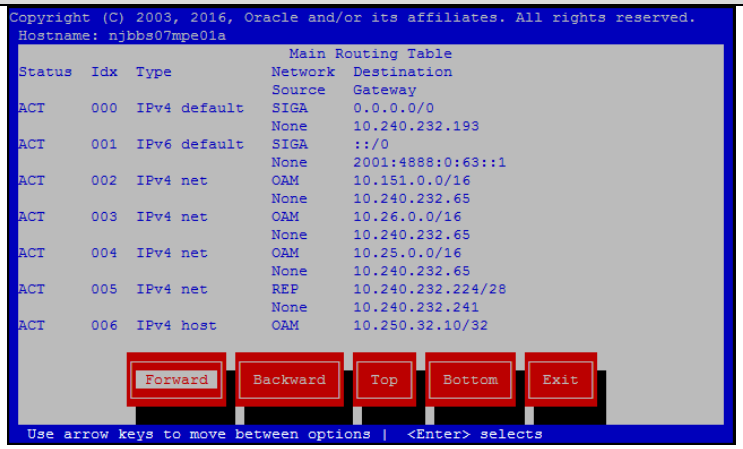


9. Click **OK**.



10. Routes are imported from `/tmp/routes_output.txt` file and Route Configuration menu displays.
11. Select Display Routes
12. Verify that all routes are present.
13. Click **Forward** to view all the routes.

Example

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

2.7.1.6 Back-out Fully Upgraded Primary CMP Cluster

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

Expected Pre-conditions:

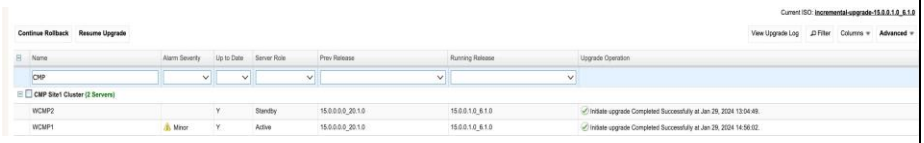
1. Primary Active CMP Cluster is on Release 15.0.x
2. Secondary CMP, MPE and MRA Clusters are on Release 15.0

NOTES:

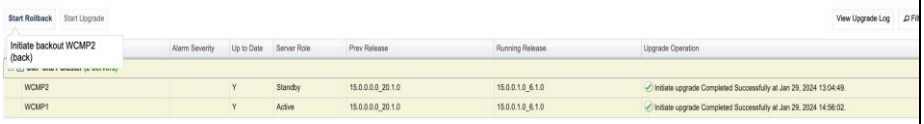
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 40 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

Procedure 24 Back-out Fully Upgraded Primary CMP Cluster

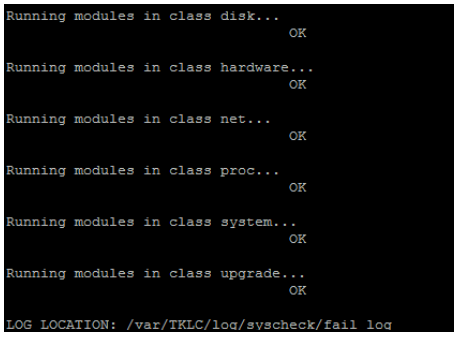
Step	Procedure	Details
1. ☐	**CMP GUI:** Verify the status of CMP Clusters	1. Navigate to **Upgrade → Upgrade Manager** 2. Confirm status of the cluster to be backed out: - Primary Active CMP is on Release 15.0.x - Secondary CMP, MPE and MRA Clusters are on Release 15.0 - Up to Date Column shows Y for all servers in Primary CMP Cluster 3. Click **Filter** and enter `CMP` in the **Name** field. **Example** 

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

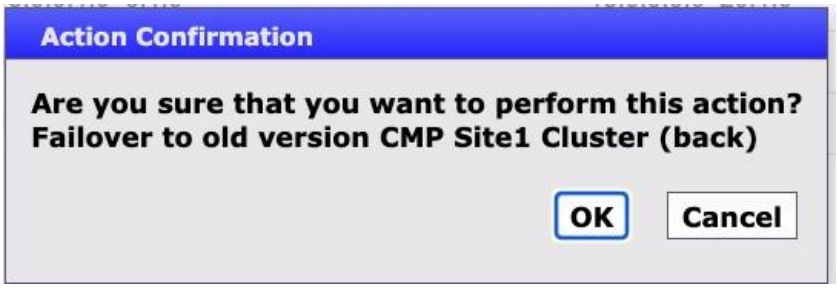
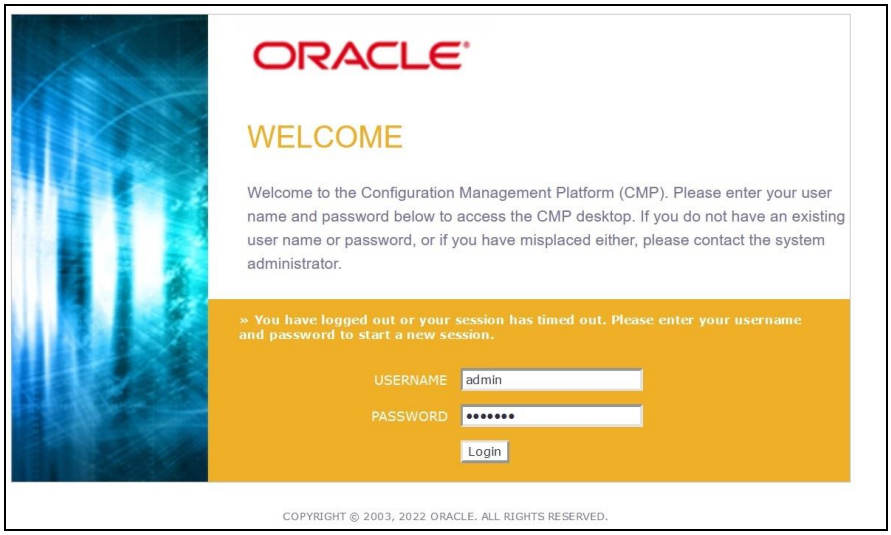
3. ☐	**CMP GUI:** Back-out standby server of Primary CMP cluster **NOTE:** Back-out of one server takes approximately 20 minutes to complete.	1. Select the Primary CMP Cluster 2. Click **Start Rollback**. When hovering over the button, it indicates the server to back out.  3. Click **OK** to confirm and continue with the operation. It begins to back-out.

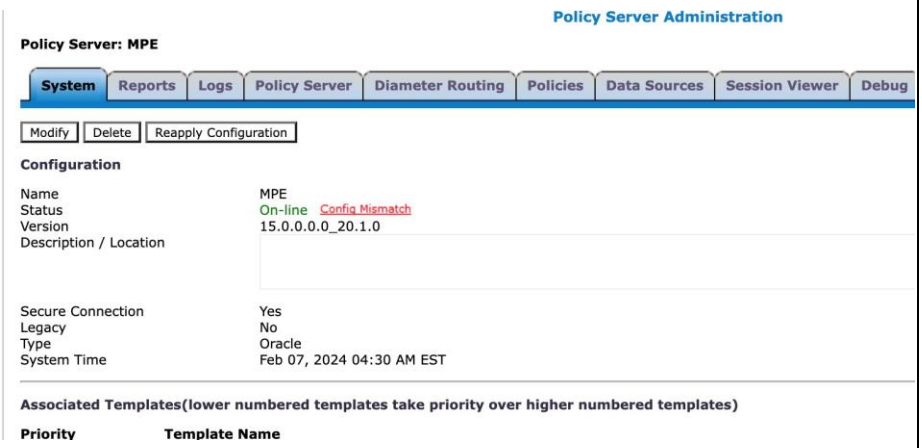
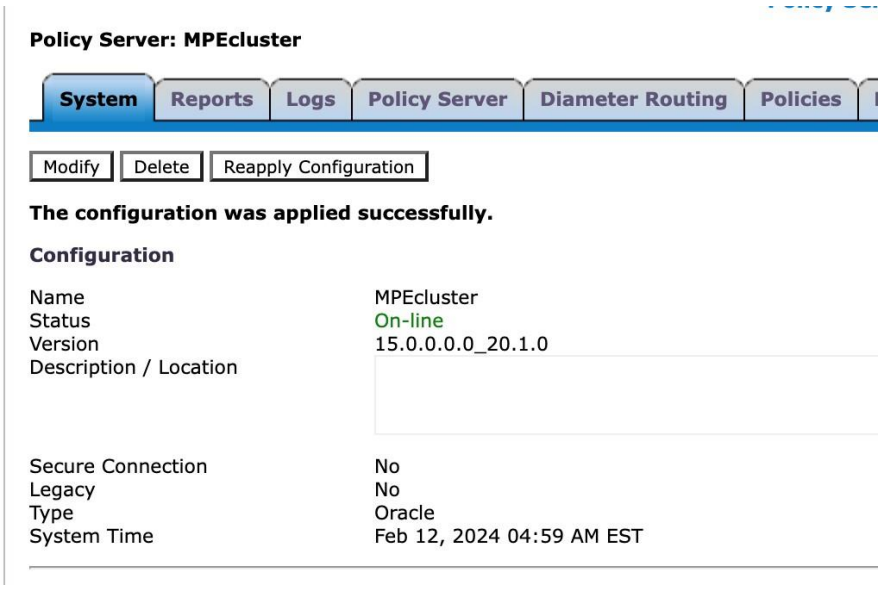
Step	Procedure	Details
		 4. Server goes into an OOS server role. 5. Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master **Expected Minor Alarms** **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software Back-out of the server is complete when the successful completion message displays in the Upgrade Operation column. The server goes back to standby state

Step	Procedure	Details
		and shows a running release of 15.0.x 

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

5. ☐	**CMP GUI**: Continue the back-out. Next operation is failover	1. Navigate to **Upgrade → Upgrade Manager**. 2. Select the Primary CMP cluster 3. Click **Continue Rollback**. When hovering over the button, it informs you of the failover.  4. Click **OK** to confirm and continue with the operation. It begins to failover and

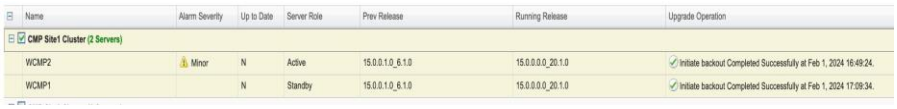
Step	Procedure	Details
		takes couple of minutes to complete.  After a minute, you are required to log back in.
6. ☐	**CMP GUI:** Log back into the Primary CMP VIP	After failover, you are required to log back in to the CMP GUI using the Primary CMP VIP. 
7. ☐	**CMP GUI:** Verify previous Policy Management release	1. Navigate to **Help → About**. 2. Verify the release displayed is 15.0.x. 

Step	Procedure	Details
8. ☐	**CMP GUI:** If a Config Mismatch is observed on MPE or MRA	**MPE:** Navigate to **Policy → Configuration →** <*MPE Cluster*> **→ System** **MRA:** Navigate to **MRA → Configuration →** *MRA Cluster*> **→ System**  Click **Reapply Configuration**. Config Mismatch is resolved: 
9. ☐	**CMP SSH:** Verify `/var/log/messages` file size	1. Use SSH to login to the Standby server to be backed out as admusr `$ ls -lh /var/log/messages` 2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.

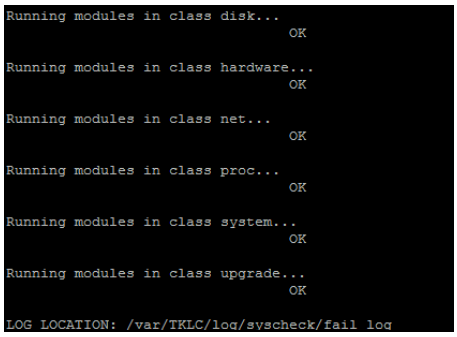
Step	Procedure	Details

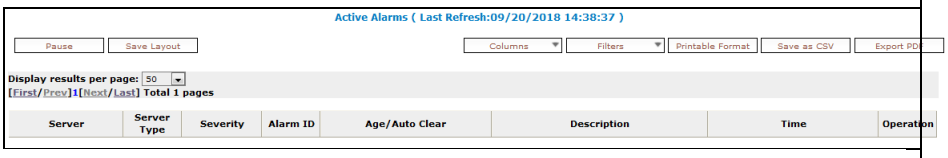
		```$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out```
		 ```$ sudo cat /dev/null > /var/log/messages```
		 ```$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"```
		 3. Verify:
		 ```$ ls -lh /var/log/messages```

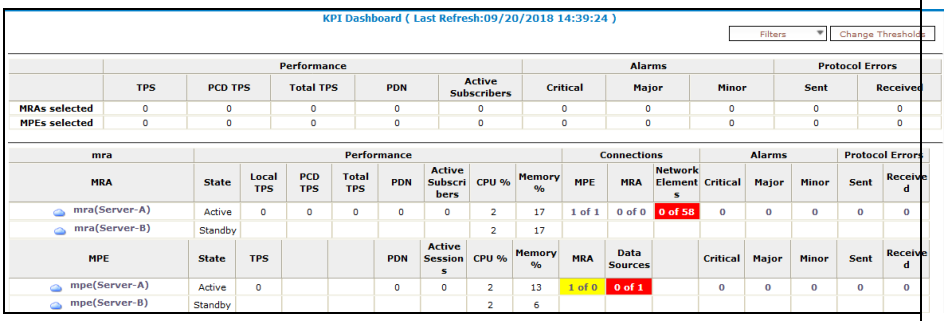
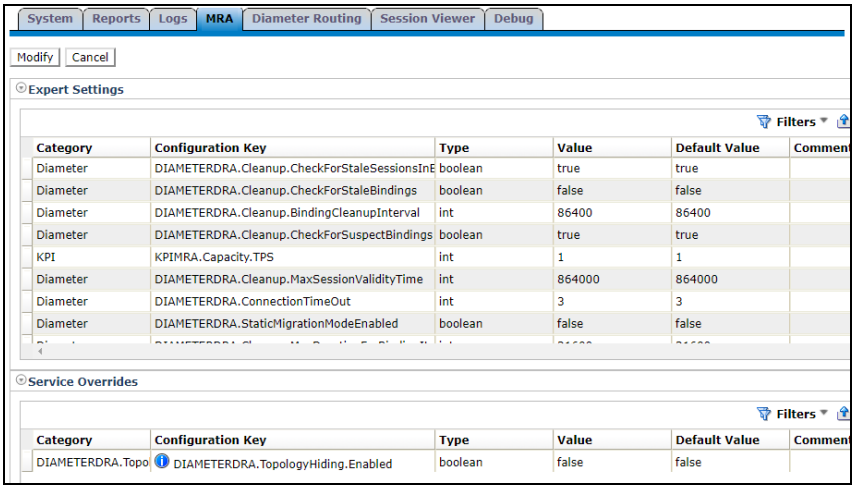
10. ☐	**CMP GUI:** Continue the back-out of the Primary CMP Cluster **NOTE:** Back-out of one server takes approximately 20 minutes to complete. **NOTE:** Wait for 10-15 minutes before the rollback of secondary CMP (in Primary Site) to allow secondary site CMP nodes to sync with the new MySQL master.	1. Navigate to **Upgrade → Upgrade Manager** 2. Select the Primary CMP Cluster. 3. Click **Continue Rollback**. When hovering over the button, it indicates the server to get backed out. At this point it is the remaining standby server.  4. Click **OK** to confirm and continue with the operation. It begins to back-out. The server goes in an OOS server role  Follow the progress status in the Upgrade Operation column. During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out. **Expected Critical Alarms** **70001** The qp_procmgr process has failed. **31227** The high availability status is failed due to raised alarms **31283** High availability server is offline **70007** Not all QP resources are ready **70025** The MySQL slave has a different schema version than the master **Expected Major Alarms** **70004** The QP processes have been brought down for maintenance **31236** High availability TCP link is down **31233** High availability path loss of connectivity **70021** The MySQL slave is not connected to the master

Step	Procedure	Details
		Expected Minor Alarms **70503** The server is in forced standby **70507** An upgrade/backout action on a server is in progress **70501** The Cluster is running different versions of software **70502** Cluster Replication Inhibited **31232** High availability server has not received a message **31101** DB replication to a slave DB has failed **31102** DB replication from a master DB has failed **31107** DB merging from a child Source Node has failed **31114** DB Replication of configuration data via SOAP has failed **31106** DB merging to the parent Merge Node has failed **70500** The system is running different versions of software Back-out of the server is complete when the successful completion message displays in the Upgrade Operation column. The server goes back to standby state and shows the previous release.  5. Verify in Upgrade Log that that back-out was successful:  All Primary CMP servers are on Release 15.0 at this point and show active/standby

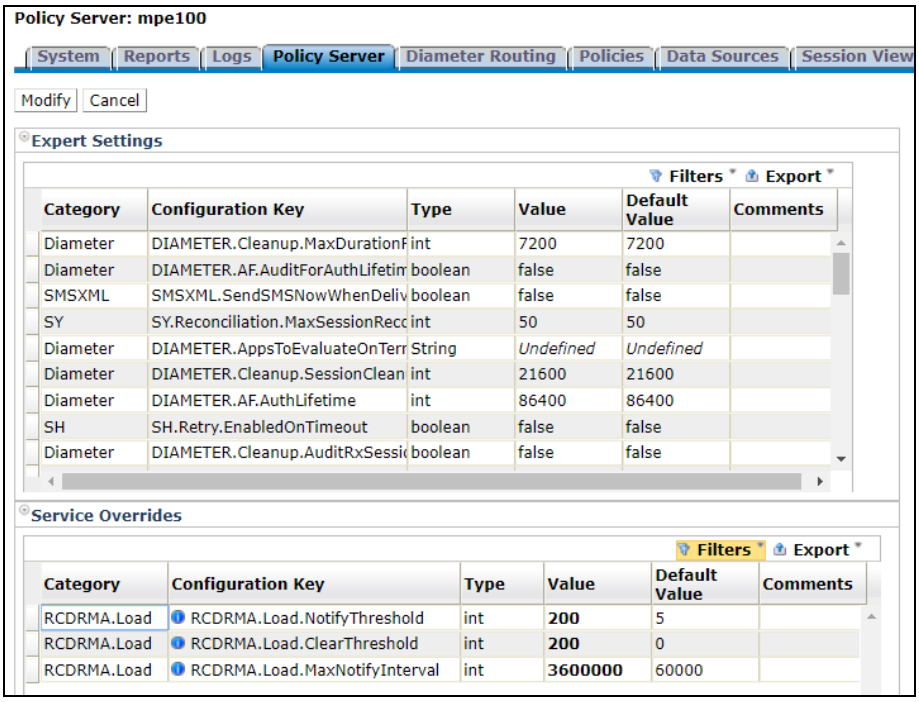
Step	Procedure	Details

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

12. ☐	**CMP GUI:** Verify Alarm Status.	Navigate to **System Wide Reports → Alarms → Active Alarms** Confirm that any existing alarm is understood. 

Step	Procedure	Details
13. ☐	**CMP GUI:** Verify Traffic Status—KPI Dashboard Report	**System Wide Reports → KPI Dashboard** Confirm that all Connections and Traffic status are as expected. Observe it for a few refresh updates. 
14. ☐	**CMP GUI:** Verify Advanced Settings on the MRA	1. Capture screenshots of the advanced settings on the MRA and compare it with prior to upgrade screen captures. 2. Verify that there are no differences. 3. Navigate to **MRA → Configuration →** <*MRA*> **→ MRA** 4. Click **Advanced**. 

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



Alternately, settings can be exported by clicking **Export** on the right within each setting.

—End of Procedure—

Appendix A. 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

   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