Hardware and Software
ORACLE
Engineered to Work Together

**Oracle® Communications**

Software Installation

# Policy Management 12.5.0/12.5.0.4 to 12.6 Upgrade Procedure

**F45857-01**

September 2021

**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 12.5.0/12.5.0.4 to 12.6 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 12.5.0/12.5.0.4 to Release 12.6 when georedundancy is enabled.

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

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

### 1.1.2 Acronyms

| Acronym | Definition |
|---|---|
| CMP | Configuration Management Platform |
| DR-CMP | Configuration Management Platform for Disaster Recovery<br>**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 |
| PMAC | Platform Management and Configuration |
| TPD | Tekelec Platform Distribution |
| TVOE | Tekelec Virtualization Operating Environment |

### 1.1.3 Terminology

| Term | Description |
|---|---|
| Primary Site (Site1) | Site where the MPE/MRA Server-A and Server-B are deployed. |

| Term | Description |
|---|---|
| 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

- Firmware
  - Oracle: 3.1.5 or higher
  - HP Solutions Firmware Upgrade Pack: 2.2.10 or higher
- COMCOL: 6.5
- PMAC: 6.6.1
- TPD: 7.8.0
- TVOE: 3.8.0
- Policy Management release 12.6

## 1.2 Upgrade Overview

This section lists the required materials and information needed to run Policy Management release 12.6 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 paths:

- Policy Management 12.5.0 to 12.6 (Major Path)
- Policy Management 12.5.0.4 to 12.6 (Minor Path)

**NOTE:** 12.6.0 upgrade is only applicable for bare metal deployments and not applicable for virtual deployments.

### 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.

#### *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 are documented by an Oracle provided Maintenance Operation Procedure (MOP).

**NOTE:** TVOE, PMAC Server, and Firmware may be necessary prior to the Policy Management upgrade.

1. Upgrade PMAC Server at Site 1—Required if version is older than what is listed in Section 1.4.
2. Upgrade PMAC Server at Site 2—Required if version is older than what is listed in Section 1.4
3. Firmware upgrade—If needed (not covered in this document)
4. Upgrade Primary CMP
5. Upgrade Secondary CMP (if applicable)
6. Site 1 Segment 1—Upgrade non-CMP clusters (see note below)
7. Site 2 Segment 1—Upgrade non-CMP clusters (see note below)
8. Site 1 Segment 2—Upgrade non-CMP clusters (see note below)
9. Site 2 Segment 2—Upgrade non-CMP clusters (see note below)

**NOTE:** Up to 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-12.6 release and release 12.6 mixed configuration would support the performance and capacity of pre-12.6 release. The mixed version Policy Management configuration would support pre-12.6 release features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the release 12.6 CMP is managing servers in both the previous release and release 12.6. In this mixed version configuration, release 12.6 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 12.6 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 R12.6 | MRA R12.6 | MPE R12.6 |
|---|---|---|---|
| CMP 12.5.0, 12.5.0.4 | Yes | No | No |
| MRA 12.5.0, 12.5.0.4 | Yes | Yes | Yes |
| MPE 12.5.0, 12.5.0.4 | Yes | Yes | Yes |

**NOTE:** Replication between CMP and DR-CMP is automatically disabled during upgrade of the CMP and DR-CMP from the previous release to release 12.6. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to release 12.6.

### 1.2.4 Customer Impacts

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

### 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 ISO, and the TPD is upgraded to version 7.8.0 as part of this procedure.

In the case of an initial product manufacture (IPM) or clean install of a new server, the supported baseline TPD version 7.8.0 should be installed prior to upgrading to Policy Management release 12.6.

### 1.2.7 Server Hardware Platforms

The Policy Management release 12.6 software upgrade can be applied on any server that previously had Policy Management release 12.5.0, and 12.5.0.4.

### 1.2.8 Loading Application Software

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

**NOTE:** PMAC is not used during the upgrade and backout procedures.

### 1.2.9 Required Materials and Remote Access

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

- Policy Management 12.6 software ISO files and TPD software ISO
- Policy Management 12.6 software Release Notes.
- TVOE, PMAC upgrade/installation documentation, software ISO files and TPD ISO (if applicable).
- HP Solutions Firmware Upgrade Pack 2.2.10 (or higher) documentation and ISO files (if applicable).
- 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, and the PMAC GUI.

#### *1.2.9.1 Upgrade Media*

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

#### *1.2.9.2 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<br>**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 iLO | iLO Administrator Login User/Password |
| Target OA | OA Administrator Login User/Password |
| PMAC server | GUI Administrator Login User/Password |
| | admusr password |
| Software Upgrade Target Release[1] | Target Release Number |
| | Policy Management 12.6 software 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.

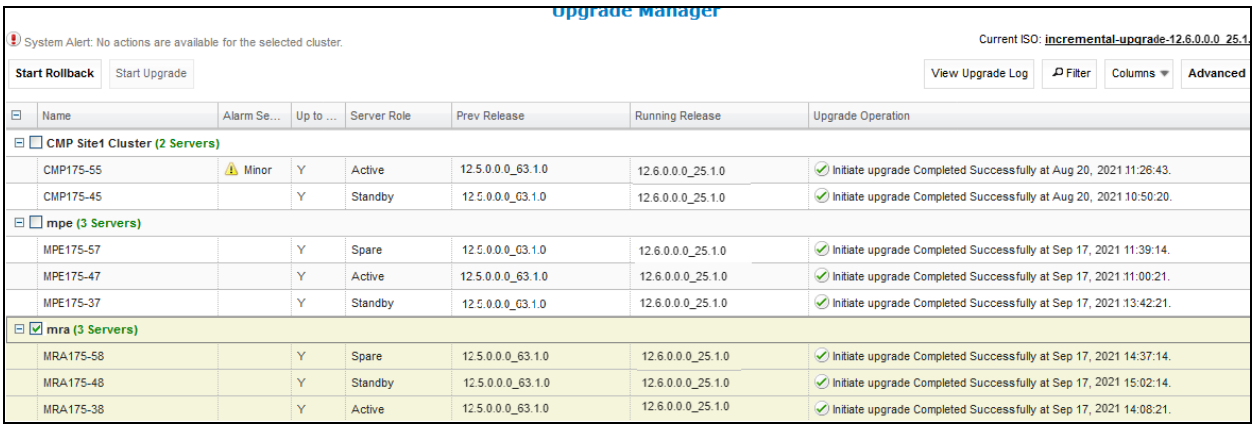



**Figure 1 Sample display of the Upgrade Manager page**

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.

Cluster Name: mpe
Last Update: 09/10/2018 10:21:21

Filter | Columns

| ID | Pare... | Action Name | Start Time | End Time | Durat... | Scope | Hostname | Result | Mode | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 327 | 325 | Modify the role/replication ... | 08/20/2018 11:59:43 | 08/20/2018 11:5... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |
| 328 | 325 | Wait for replication to syn... | 08/20/2018 12:20:03 | 08/20/2018 12:2... | 0:00:09 | Server | MPE175-37 | Success | Automatic | Automatic action w... |
| 329 | 325 | Modify the role/replication ... | 08/20/2018 12:20:03 | 08/20/2018 12:2... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |
| 345 | 0 | Backing out server upgrade | 09/06/2018 13:13:54 | 09/06/2018 13:2... | 0:15:24 | Server | MPE175-37 | Success | Manual | User initiated action:... |
| 346 | 345 | Modify the role/replication ... | 09/06/2018 13:13:54 | 09/06/2018 13:1... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |
| 347 | 345 | Waiting for replication to s... | 09/06/2018 13:29:19 | 09/06/2018 13:2... | 0:00:10 | Server | MPE175-37 | Success | Automatic | Automatic action w... |
| 348 | 0 | Backing out server upgrade | 09/06/2018 13:36:17 | 09/06/2018 14:0... | 0:33:02 | Server | MPE175-57 | Success | Manual | User initiated action:... |
| 349 | 348 | Modify the role/replication ... | 09/06/2018 13:36:17 | 09/06/2018 13:3... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |
| 353 | 348 | Waiting for replication to s... | 09/06/2018 14:09:19 | 09/06/2018 14:0... | 0:00:09 | Server | MPE175-57 | Success | Automatic | Automatic action w... |
| 354 | 0 | Preflight Check | 09/06/2018 14:35:26 | 09/06/2018 14:3... | 0:00:13 | Server | MPE175-57 | Success | Manual | User initiated action:... |
| 356 | 354 | Upgrading server | 09/06/2018 14:35:39 | 09/06/2018 14:5... | 0:21:33 | Server | MPE175-57 | Success | Automatic | Automatic action initi... |
| 357 | 354 | Modify the role/replication ... | 09/06/2018 14:35:39 | 09/06/2018 14:3... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |
| 362 | 354 | Wait for replication to syn... | 09/06/2018 14:57:12 | 09/06/2018 14:5... | 0:00:06 | Server | MPE175-57 | Success | Automatic | Automatic action w... |
| 363 | 354 | Modify the role/replication ... | 09/06/2018 14:57:12 | 09/06/2018 14:5... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |
| 364 | 0 | Preflight Check | 09/06/2018 15:44:54 | 09/06/2018 15:4... | 0:00:19 | Server | MPE175-37 | Success | Manual | User initiated action:... |
| 365 | 364 | Upgrading server | 09/06/2018 15:45:13 | 09/06/2018 16:0... | 0:19:59 | Server | MPE175-37 | Success | Automatic | Automatic action initi... |
| 366 | 364 | Modify the role/replication ... | 09/06/2018 15:45:13 | 09/06/2018 15:4... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |
| 367 | 364 | Wait for replication to syn... | 09/06/2018 16:05:13 | 09/06/2018 16:0... | 0:00:06 | Server | MPE175-37 | Success | Automatic | Automatic action w... |
| 368 | 364 | Modify the role/replication ... | 09/06/2018 16:05:13 | 09/06/2018 16:0... | 0:00:01 | Cluster | mpe | Success | Automatic | Automatic action for... |

**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.

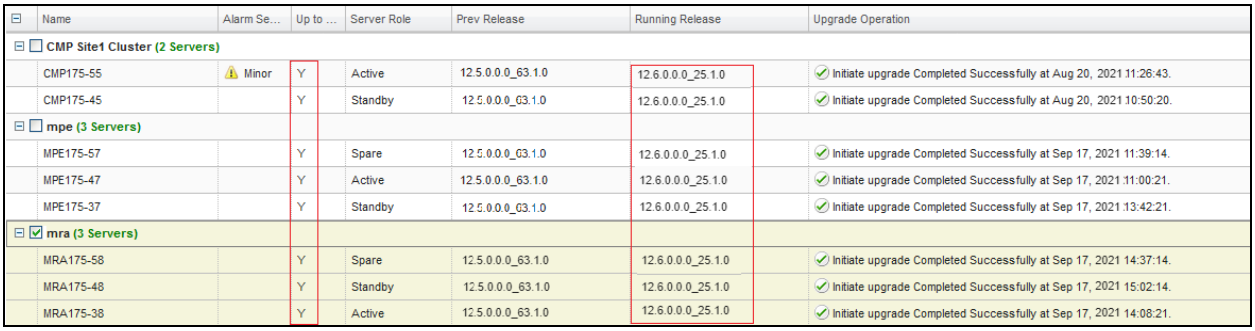



**Figure 3 Upgrade in Progress Showing Transient Alarms**

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 |
| 31283 | Critical | Lost Communication with server |
| 70001 | Critical | QP_procmgr failed |
| 70025 | Critical | QP Slave database is a different version than the master |
| 31233 | Major | HA Path Down |
| 70004 | Major | QP Processes down for maintenance |
| 31101 | Minor | DB replication to slave failure |
| 31106 | Minor | DB merge to parent failure |
| 31107 | Minor | DB merge from child failure |

| Alarm Number | Severity | Name |
|---|---|---|
| 31114 | Minor | DB replication over SOAP has failed |
| 31282 | Minor | HA Management Fault |
| 70500 | Minor | System Mixed Version |
| 70501 | Minor | Cluster Mixed Version |
| 70502 | Minor | Cluster Replication Inhibited |
| 70503 | Minor | Server Forced Standby |
| 70507 | Minor | Upgrade in Progress |

The Upgrade Manager 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 12.6, 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 TVOE PMAC Server at Site1 (if applicable)
2. Upgrade TVOE PMAC Server at Site2 (if applicable)
3. Firmware (if applicable)
4. Upgrade Primary (Site1) CMP
5. Upgrade Secondary (Site2) CMP (if applicable)
6. Segment 1 Site1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
7. Segment 1 Site2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters

8. Segment 2 Site1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
9. Segment 2 Site2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters

### 1.4.1 Prerequisites

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

TVOE, PMAC and Firmware might need to be upgraded prior to upgrade to Policy Management release 12.6.

**Procedure 1 Prerequisites**

| Step | Procedure | Details |
|---|---|---|
| 1. ☐ | Verify all required materials are present | As listed in section 1.2.9 Required Materials and Remote Access. |
| 2. ☐ | Review Release Notes | Review Policy Management 12.6 Release Notes for the following information:<br>• Individual software components and versions included in target release.<br>• New features included in target release.<br>• Issues (bugs) resolved in target release.<br>• Known issues with target release.<br>• Any further instructions that may be required to complete the software upgrade for the target release. In particular, the supported browsers: In release 12.6, only Mozilla Firefox and Google Chrome are fully supported. |
| **—End of Procedure—** | | |

### 1.4.2 TVOE and PMAC Server Upgrade

Policy Management release 12.6 requires PMAC Version 6.6.1 to support IPM of TPD 7.8.0 on c-Class servers.

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

See Appendix A to upgrade the TVOE and PMAC.

### 1.4.3 Firmware Upgrade

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

### 1.4.4 Plan and Track Upgrades

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

**Prerequisite:** TVOE and PMAC Server upgraded. Firmware upgrade deployed if necessary.

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 TVOE/PMAC | Site Names _____ and _____ | | 3 hrs |
| 3. ☐ | Upgrade Site1 and Site2 CMP clusters.<br>Each cluster takes approximately 1 and ½ hours to complete | Site Names _____ and _____ | | 3 hrs |
| 4. ☐ | Upgrade Site1 MPE/MRA clusters for Segment-1 | Site Names _____<br>Cluster List: | | 2 hrs |

| Step | Procedure | Result | Engineer | Time |
|---|---|---|---|---|
| 5. ☐ | Upgrade Site2 clusters for Segment-1 | Site Names _____<br>Cluster List: | | 2 hrs |
| 6. ☐ | Upgrade Site1 clusters for Segment-2 | Site Names _____<br>Cluster List: | | 2 hrs |
| 7. ☐ | Upgrade Site2 clusters for Segment-2 | Site Names _____<br>Cluster List: | | 2 hrs |
| **—End of Procedure—** | | | | |

### 1.4.5 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.<br>***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<br>**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.<br>2. Confirm that time is synchronized on each server using the following CLI shell command:<br>`$sudo ntpq -np`<br>3. Confirm that date is correct on each server.<br>4. Check that BIOS clock is synced with the clock using the following CLI shell command:<br>`$sudo hwclock` |
| **—End of Procedure—** | | |

## 1.4.6 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 ISO file, sufficient time should be planned to accomplish this step. For Policy Management release 12.6, each ISO image size is about 1.3 Gigabytes.

### *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.***

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

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

### *1.4.6.2 Copy ISO image files to Management Server (PMAC)*

**NOTE:** Not all Policy Management systems use a PMAC server. If that is the case, skip to the next section.

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

***IMPORTANT: PMAC is not used for upgrade activities. The purpose of Use this procedure to be prepared for server recovery activities in case a server must be re-installed with software.***

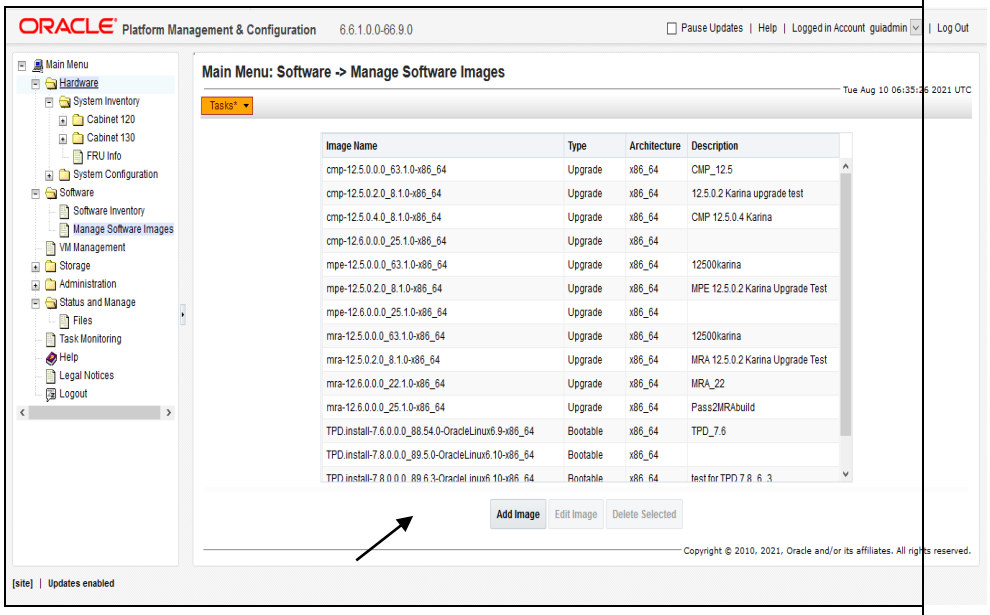
**NOTES:**

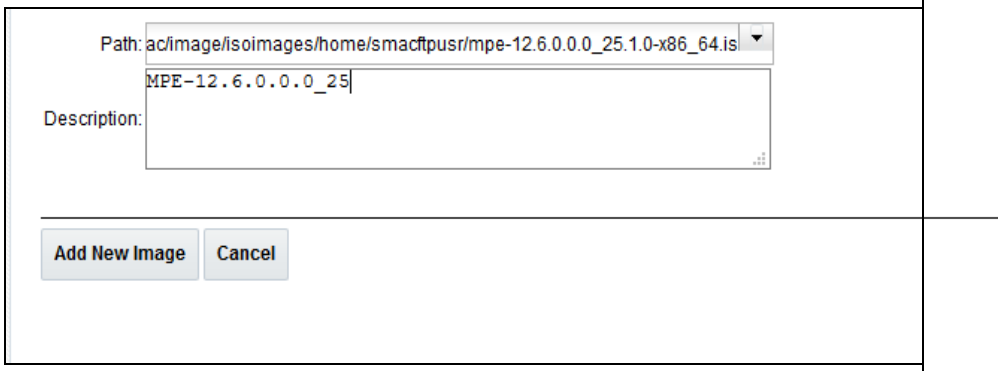
ISO file transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO file transfers to the target systems should be performed prior to and outside of the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.
Because the ISO files are large, the procedure includes instructions to check the space available in the `/var/TKLC/upgrade` directory before copying the ISO files to the directory. After the Add Image action on the PMAC, the ISO files are registered in PMAC, and stored in the `/var/TKLC/smac/image/repository` directory, which is very large.

**Procedure 3 Copy ISO image files to Management Server**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **PMAC GUI:** Verify that release 12.6 ISO files are not on the server | 1. Log on to the PMAC Server GUI<br>2. Navigate to **Software → Manage Software Images**.<br>3. Confirm that the release 12.6 ISO files do not exist. If there are files, remove them. |
| 2. ☐ | SSH to PMAC server as admusr | 1. Log on as admusr to the PMAC server.<br>2. Change Target directory to `/var/TKLC/upgrade` and ensure there is at least of 3.0 GB free disk space available.<br>`$cd /var/TKLC/upgrade`<br>`$df -h /var/TKLC`<br>**NOTE:** If there are ISO files in the `/var/TKLC/upgrade` directory, you can remove the files to free up disk space or add the files to the PMAC repository. |
| 3. ☐ | Copy release 12.6 ISO files to the target directory in the PMAC server | 1. Transfer all release 12.6 ISO files (CMP and non-CMP) into directory `/var/TKLC/upgrade` using one of the following methods:<br>2. SCP/WGET command in the following steps outline in this procedure<br>**USB drive**<br>**NOTE:** If the directory becomes full, you may have to use the scp command to transfer one ISO file at a time. Verify that the ISO file is in the directory before adding the next ISO file. You may also use the `/var/TKLC/smac/image/isoimages/home/smacftpusr` directory which has more available space. |

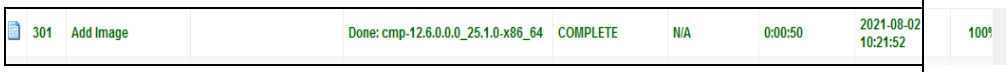
| Step | Procedure | Result |
|---|---|---|
| 4. ☐ | **PMAC GUI:** Adding the new release 12.6 ISO files | 1. Navigate to **Software → Manage Software Images**.<br>2. Click **Add Image** to select the ISO files that were transferred to the PMAC server. |




3. Click **Add New Image**.

| Image Name | Type | Architecture | Description |
|---|---|---|---|
| cmp-12.5.0.0.0_63.1.0-x86_64 | Upgrade | x86_64 | CMP_12.5 |
| cmp-12.5.0.2.0_8.1.0-x86_64 | Upgrade | x86_64 | 12.5.0.2 Karina upgrade test |
| cmp-12.5.0.4.0_8.1.0-x86_64 | Upgrade | x86_64 | CMP 12.5.0.4 Karina |
| cmp-12.6.0.0.0_25.1.0-x86_64 | Upgrade | x86_64 | |
| mpe-12.5.0.0.0_63.1.0-x86_64 | Upgrade | x86_64 | 12500karina |

| Step | Procedure | Result |
|---|---|---|
| 5. ☐ | **PMAC GUI:** Verify that the ISO files were added successfully | Navigate to **Software → Manage Software Images**.<br>The status of the image being added can be monitored using the Task Monitoring menu with the display as the following:<br>  <br>**NOTE:** The added ISO files are now stored in the `/var/TKLC/smac/image/repository` directory |
| **—End of Procedure—** | | |

### *1.4.6.3 Distribute Application ISO Image Files to Servers*

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

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

The distribution can be done in one of the following ways:

- Manual Distribution
- PMAC Distribution

#### Manual Distribution

**Procedure 4 Manual Distribution**

| Step | Procedure | Result |
|---|---|---|
| 1. | Transfer ISO files to Policy Management server. | 1. Transfer release 12.6 ISO files (CMP and non-CMP) into the `/var/TKLC/upgrade` directory on the respective server using one of the following methods:<br>- SCP/WGET command<br>- USB drive<br>2. If the images are on a server in the same network, **`scp`** the files using the CLI, for example, for CMP:<br>3. Copy CMP software ISO file to ONE of the other CMP servers:<br>`$sudo scp cmp-12.6.0.0_25.1.0-x86_64.iso user@remote_host.com:/var/TKLC/upgrade/`<br>4. Repeat for one server of all clusters.<br>**NOTE:** After copying the ISO to one of the respective servers, the ISO Maintenance is used to upload to the rest of the servers. |
| **—End of Procedure—** | | |

#### PMAC Distribution

The PMAC product is not used during Policy Management upgrade and backout procedures. However, if your topology is supported by PMAC servers, you should add the Policy Management ISO images to the PMAC image repository to support new installations and server field replacements.

Collect the following information and material beforehand:

- The URL of the PMAC server and the **`guiadmin`** password
- The Policy Management ISO files, loaded into the directory `/var/TKLC/upgrade` on the PMAC server

**NOTE:** You can instead add images from the following sources:

- Media mounted in the CD/DVD drive of the PMAC host
- USB media attached to the PMAC host
- External mounts (prefix the directory with `extfile://`)

  These local search paths:

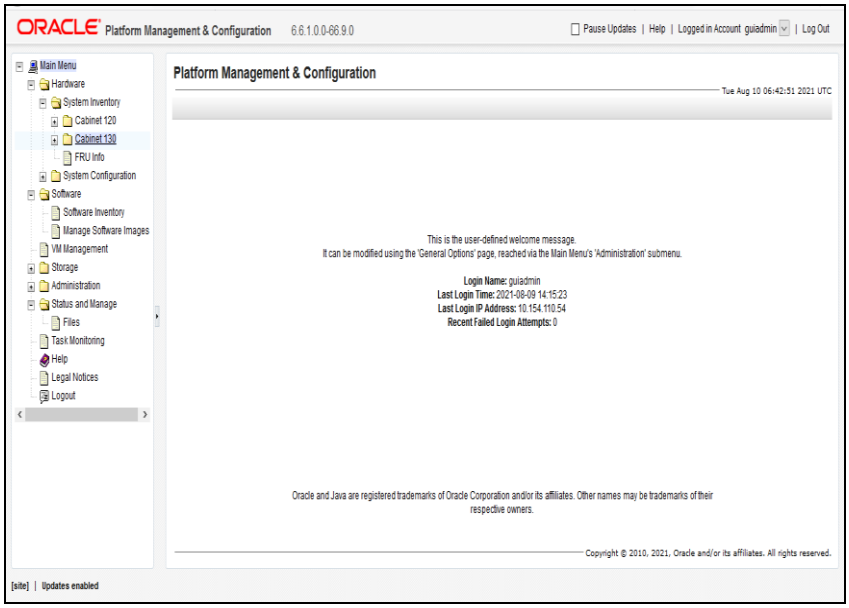
  `/var/TKLC/upgrade/`

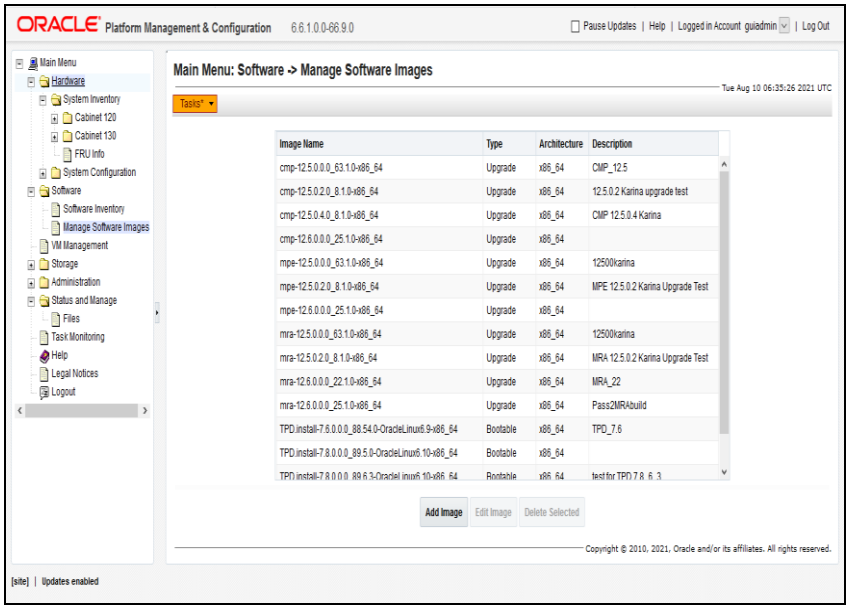
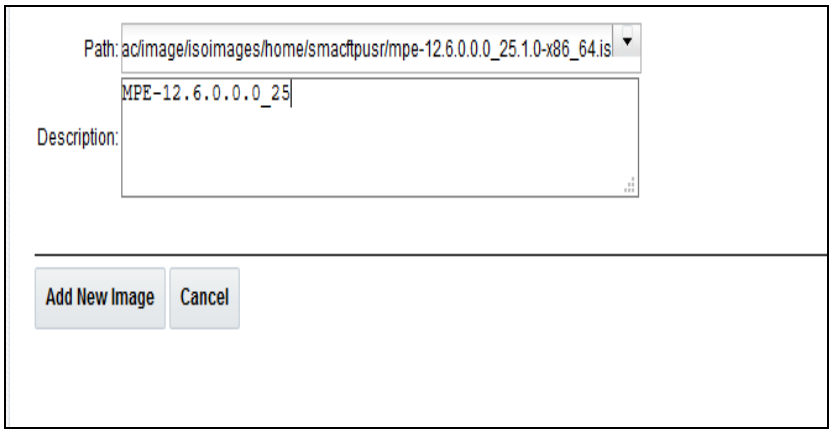
  `/var/TKLC/smac/image/isoimages/home/smacftpusr/`

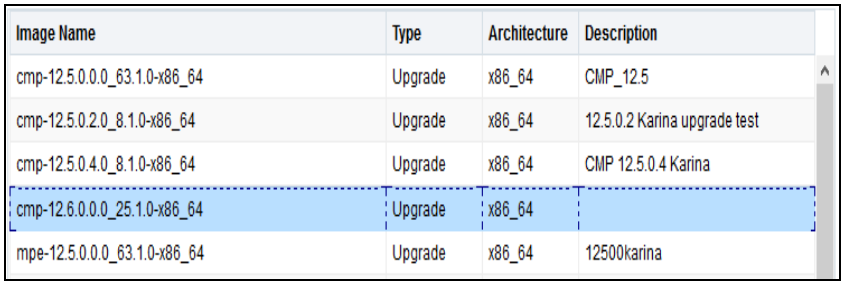
**NOTE:** CD, DVD, and USB images mounted on the PMAC VM host must be made accessible to the PMAC VM guest. To do this, go to the Media tab of the PMAC View VM Guest page on the PMAC VM Management page.

This procedure assumes the ISO file is located in the `/var/TKLC/upgrade` directory on the PMAC server.

**Procedure 5 PMAC Distribution**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | Log in to PMAC | Open a browser, enter the URL of the PMAC server, and log in as guiadmin.<br>The PMAC Main Menu opens. For example:<br>  |

| Step | Procedure | Result |
|---|---|---|
| 2. ☐ | Select the ISO image | 1. Navigate to **Main Menu → Software → Manage Software Images.**<br>2. The **Manage Software Images** page opens. For example:<br>  <br><br>3. Click **Add Image** (at the bottom of the page).The Manage Software Images [Add Image] page opens. For example:<br>  <br><br>4. Select the ISO file from the **Path** list and click **Add New Image**.<br>**Tip:** You can enter a description of the ISO file before adding it.<br>You are prompted: Click **OK** to remove the image from `/var/TKLC/upgrade` directory after it is added to the repository. Click Cancel to leave it there. |

| Step | Procedure | Result |
|---|---|---|
| 3. ☐ | Move the ISO file to the repository | Click **OK** to move the file (or **Cancel** to copy it).<br>The ISO file is loaded into the PMAC image repository in the background.<br>**Tip:** You can click **Tasks** to check the progress of the task.<br>When the upload is complete, the ISO file is in the list. For example:<br>  |
| 4. ☐ | Verify that the image is not in the directory | Enter the following command:<br>`$ sudo ls /var/TKLC/upgrade` |
| 5. ☐ | Load addition files | If you are loading multiple ISO files into the image repository, repeat steps 2 through 4 until all files are loaded. |
| 6. ☐ | Remove media | When you finish, remove the CD/DVD media or unmount the USB device. |
| **—End of Procedure—** | | |

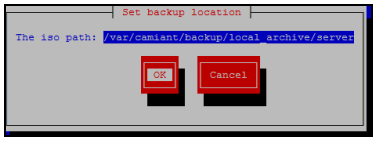
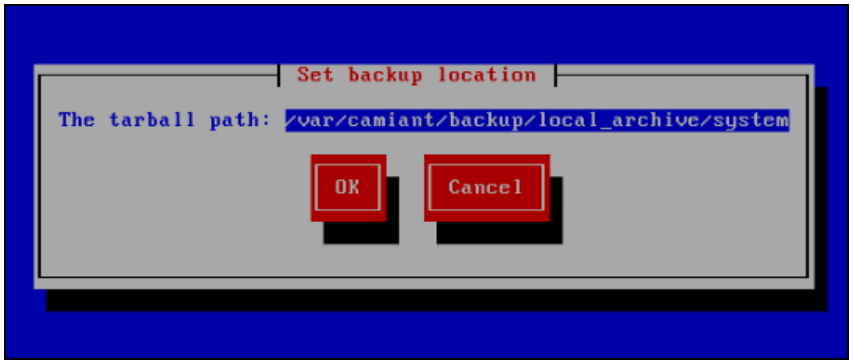


#### *1.4.6.4 Backups and Backup Locations*

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 6 Backups and Backup Locations**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **SSH CLI/iLO:** Access the server to be backed up<br><br>**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.***<br><br>1. Login into the active Primary CMP server.<br>2. Open the platcfg utility.<br>`$sudo su - platcfg`<br>3. Navigate to:<br>**Policy Configuration → Backup and Restore → Server Backup**<br>4. Provide (or use the suggested) ISO backup filename in the default backup location path of:<br>`/var/camiant/backup/local_archive/serverbackup/<filename>.iso`<br>  <br>5. Go back to the previous menu.<br>**Policy Configuration→Backup and Restore**<br>6. Select **System Backup**.<br>7. Provide (or use the suggested) tarball backup filename in the default backup location path of:<br>`/var/camiant/backup/local_archive/systembackup/<filename>.tar.gz`<br>  |

| Step | Procedure | Result |
|---|---|---|
| 2. ☐ | **SSH CLI/iLO:** Verify the backup ISO file | If default location is accepted in the previous step, change to the following directory and verify the file. For example for an MPE server backup:<br>`$ cd /var/camiant/backup/local_archive/serverbackup`<br>`$ ls <hostname>-mpe-_12.6-serverbackup-<yyyy><mm><dd><hhmm>.iso`<br>And for the system backup:<br>`$ cd /var/camiant/backup/local_archive/systembackup`<br>`$ ls <hostname>-cmp_12.6-systembackup-<yyyy><mm><dd><hhmm>.tar.gz` |
| 3. ☐ | Copy backup files. | 1. Copy the files to remote server or local workstation/laptop.<br>2. Example of a remote server copy.<br>`$ sudo scp /var/camiant/backup/local_archive/systembackup/xx_tar.gz <remoteserver_ipaddress>:<destinationpath>`<br>3. Remove the backup ISO file from the TPD Sever.<br>`$sudo rm <backup_filename>.iso` |
| 4. ☐ | Identify backup location | Backup location is:<br>_____<br>Instructions to access to backups are as follows:<br>_____<br>_____<br>_____ |
| **—End of Procedure—** | | |

## 1.5 Upgrade CMP clusters (12.5.0/12.5.0.4 to 12.6)

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 _____<br>Server-A IP Address _____<br>Server-A HA Status _____ | Server-B Hostname _____<br>Server-B IP Address _____<br>Server-B HA Status _____ |
| Secondary Site | | | Server-A Hostname _____<br>Server-A IP Address _____<br>Server-A HA Status _____ | Server-B Hostname _____<br>Server-B IP Address _____<br>Server-B HA Status _____ |

***IMPORTANT:***

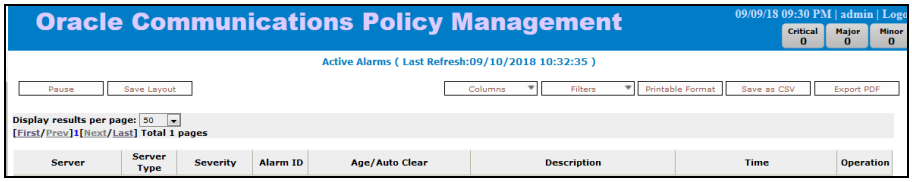
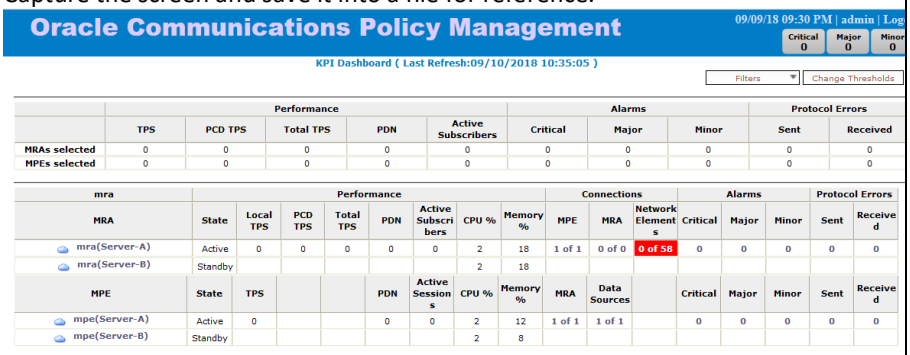
- Site1 CMP MUST be upgraded to the new release before the Site2 CMP
- CMP servers MUST be upgraded before the non-CMP clusters

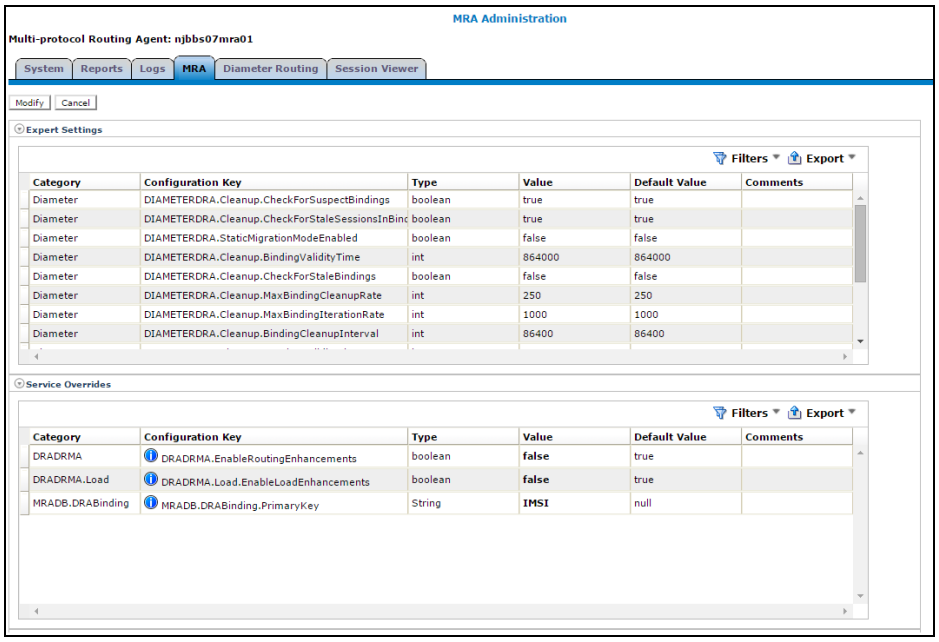
**NOTE:** The following steps use build 12.5.0.0.0_63.1.0 as example.

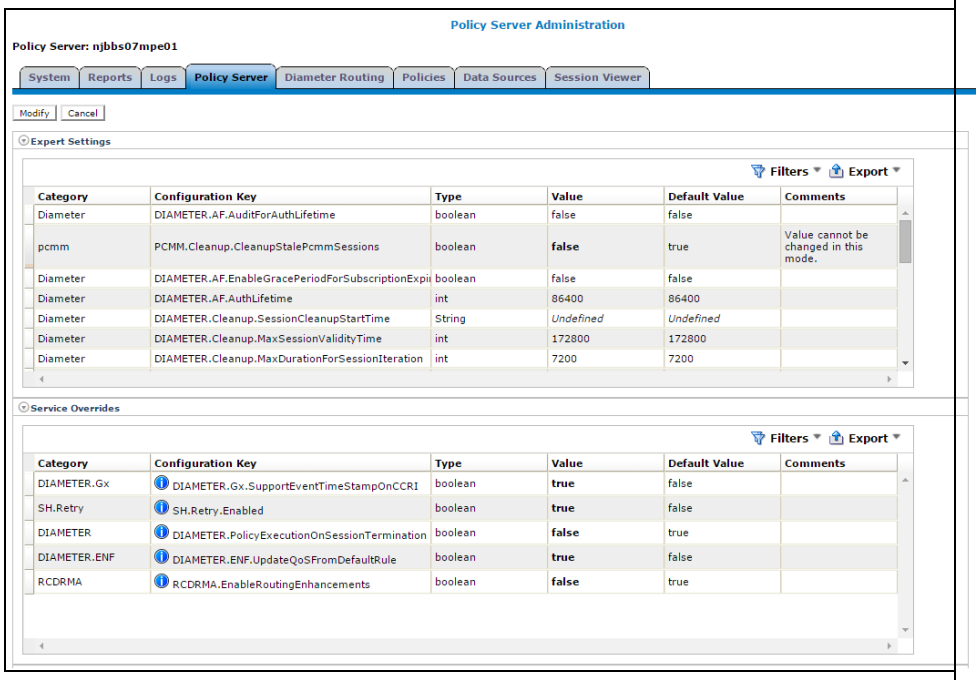
### 1.5.2 Upgrade Primary CMP cluster

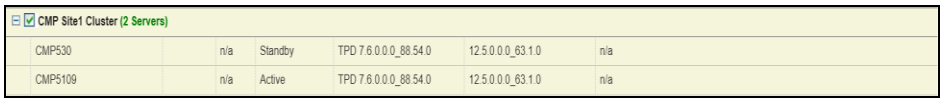
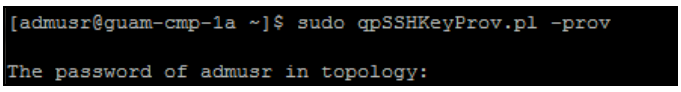
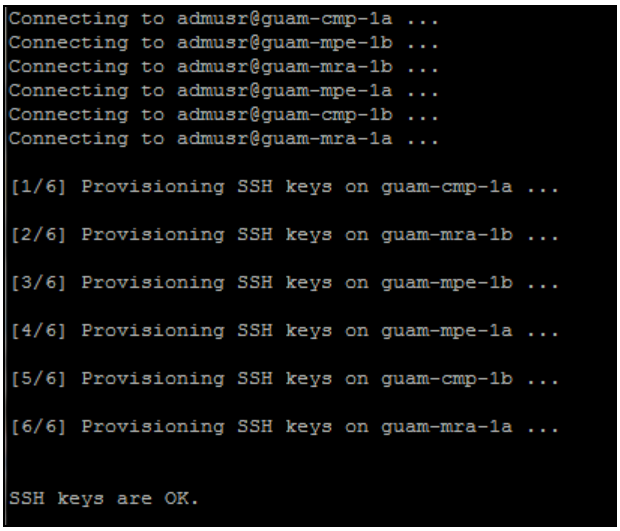
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

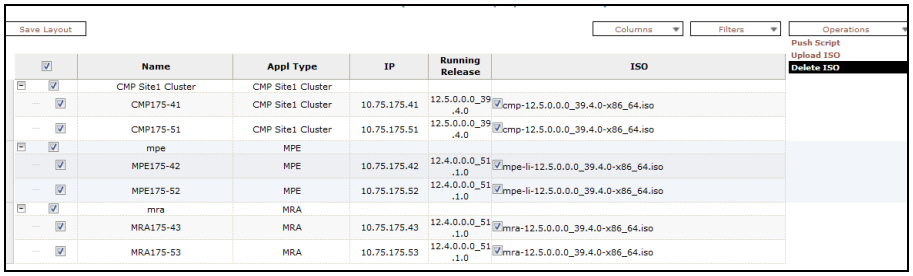
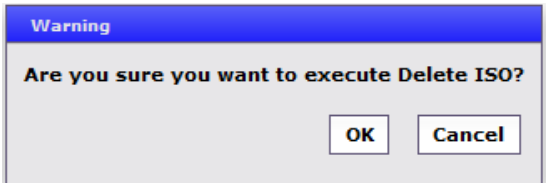
**Procedure 7 Upgrade Primary CMP cluster**

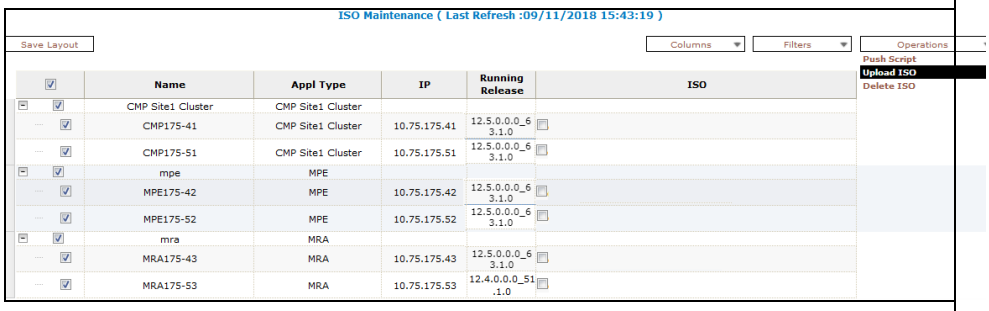
| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **CMP GUI:** Verify alarm status. | 1. Navigate to **System Wide Reports → Alarms→Active Alarms**.<br>2. Confirm that any existing alarm is understood and is not an impact to the upgrade procedure. If has critical alarm like 70020 (The current MYSQL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

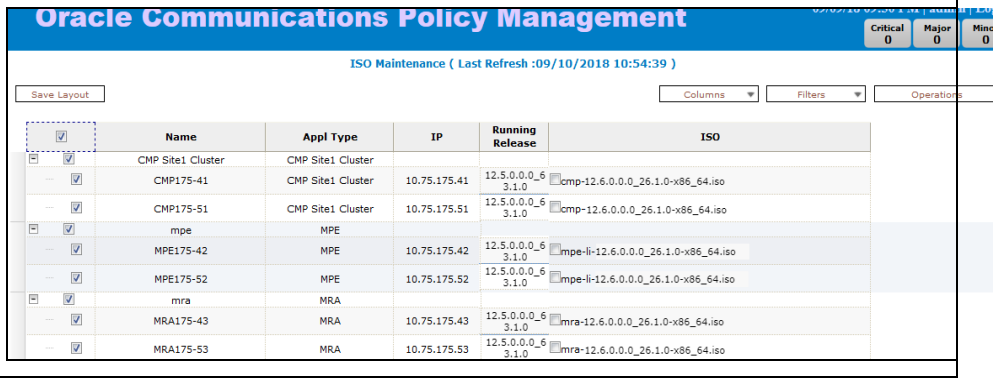
| Step | Procedure | Result |
|---|---|---|
| 3. ☐ | **CMP GUI:** Capture MRA Advanced Settings | 1. Capture screenshots of the advanced settings on the MRA prior to upgrading the CMP and save them into files for future reference check.<br>2. Navigate to **MRA → Configuration →** <*mra_cluster name*>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

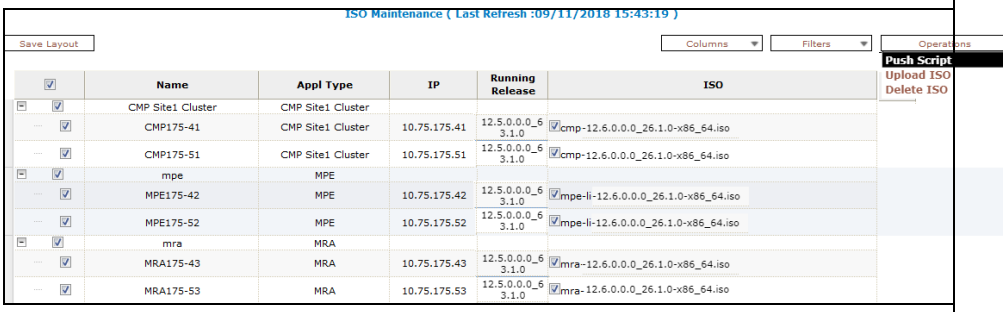
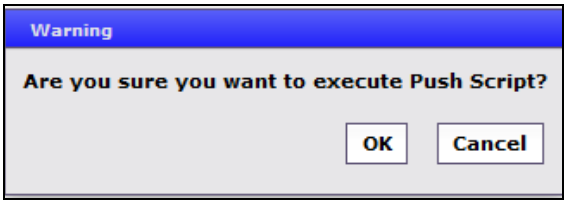
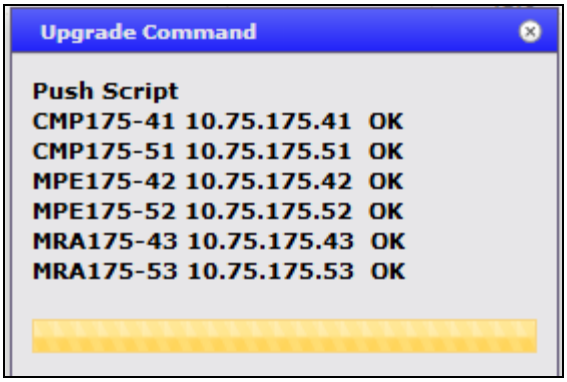
| Step | Procedure | Result |
|---|---|---|
| 4. ☐ | **CMP GUI:** Capture MPE Advanced Settings | 1. Capture screenshots of the advanced settings on the MPE prior to upgrading the CMP and save them into files for future reference check.<br>2. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ Policy Server**<br>3. Click **Advanced Settings**.<br>  <br>Policy Server Administration<br>Policy Server: njbbs07mpe01<br>System \| Reports \| Logs \| Policy Server \| Diameter Routing \| Policies \| Data Sources \| Session Viewer<br>Modify \| Cancel<br>Expert Settings<br>Filters Export<br>Category \| Configuration Key \| Type \| Value \| Default Value \| Comments<br>Diameter \| DIAMETER.AF.AuditForAuthLifetime \| boolean \| false \| false<br>pcmm \| PCMM.Cleanup.CleanupStalePcmmSessions \| boolean \| **false** \| true \| Value cannot be changed in this mode.<br>Diameter \| DIAMETER.AF.EnableGracePeriodForSubscriptionExpi \| boolean \| false \| false<br>Diameter \| DIAMETER.AF.AuthLifetime \| int \| 86400 \| 86400<br>Diameter \| DIAMETER.Cleanup.SessionCleanupStartTime \| String \| *Undefined* \| *Undefined*<br>Diameter \| DIAMETER.Cleanup.MaxSessionValidityTime \| int \| 172800 \| 172800<br>Diameter \| DIAMETER.Cleanup.MaxDurationForSessionIteration \| int \| 7200 \| 7200<br>Service Overrides<br>Filters Export<br>Category \| Configuration Key \| Type \| Value \| Default Value \| Comments<br>DIAMETER.Gx \| DIAMETER.Gx.SupportEventTimeStampOnCCRI \| boolean \| **true** \| false<br>SH.Retry \| SH.Retry.Enabled \| boolean \| **true** \| false<br>DIAMETER \| DIAMETER.PolicyExecutionOnSessionTermination \| boolean \| **false** \| true<br>DIAMETER.ENF \| DIAMETER.ENF.UpdateQoSFromDefaultRule \| boolean \| **true** \| false<br>RCDRMA \| RCDRMA.EnableRoutingEnhancements \| boolean \| **false** \| true<br>4. Alternatively, settings can be exported clicking **Export** 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**.<br>Cluster Settings<br>Name \| Appl Type \| Site Preference \| OAM VIP \| Server-A \| Server-B \| Server-C \| Operation<br>CMP Site1 Cluster (P) \| CMP Site1 Cluster \| N/A \| 10.75.175.65/25 \| 10.75.175.45 \| 10.75.175.55 \| N/A \| View Demote<br>CMP Site2 Cluster (S) \| CMP Site2 Cluster \| N/A \| 10.75.175.66/25 \| 10.75.175.46 (FS) \| 10.75.175.56 \| N/A \| View Delete<br>mpe300 \| MPE \| Normal \| 10.75.175.67/25 (P) N/A (S) \| 10.75.175.37 \| 10.75.175.47 \| 10.75.175.57 \| View Delete<br>mra300 \| MRA \| Normal \| 10.75.175.68/25 (P) N/A (S) \| 10.75.175.38 \| 10.75.175.48 \| 10.75.175.58 \| View Delete<br>2. Note which cluster is the primary and which cluster is the secondary.<br>3. The Primary CMP is noted with a P in parenthesis and a Secondary CMP is noted with an S in parenthesis.<br>4. Save a screenshot for future reference. |

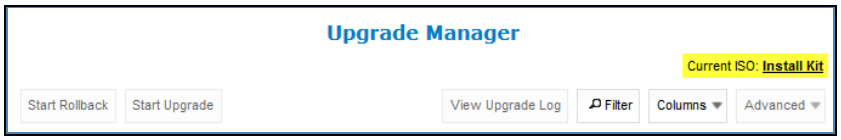
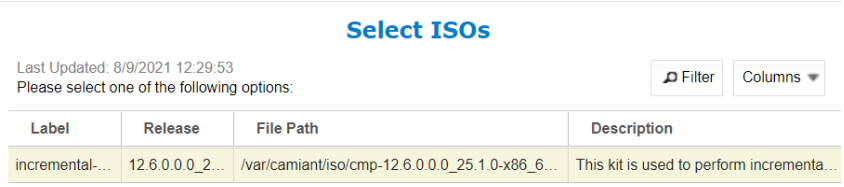
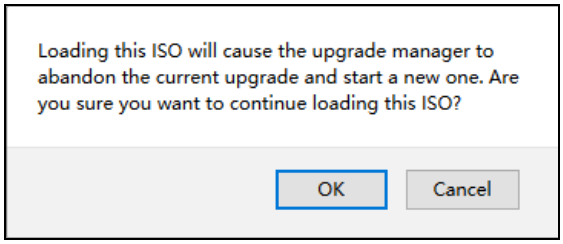
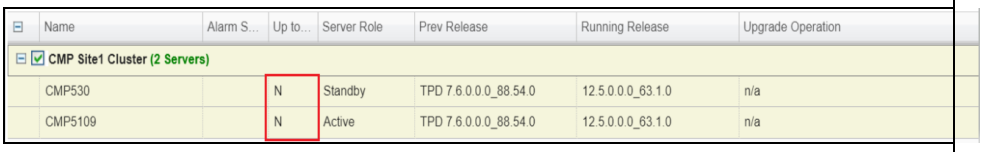
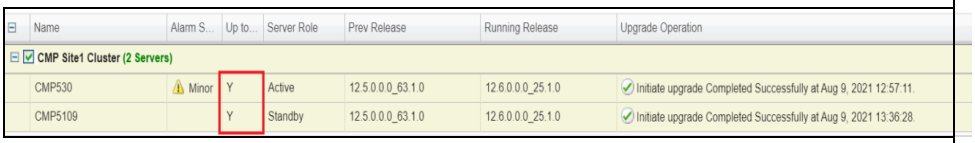
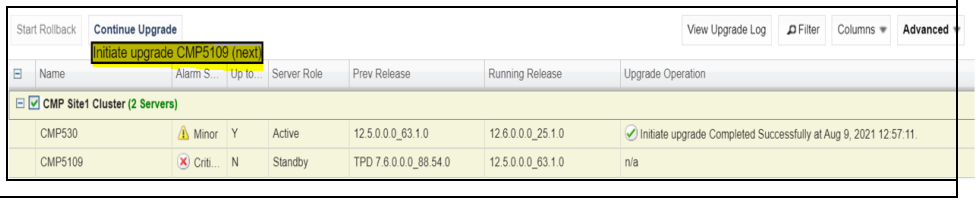
| Step | Procedure | Result |
|---|---|---|
| 6. ☐ | **CMP GUI:** Verify the status of the CMP clusters | 1. Navigate to **Upgrade → Upgrade Manager**.<br>  <br>2. Confirm the CMP clusters have the following:<br>- Active/Standby status<br>- Running release 12.5.0/12.5.0.4<br>  <br>3. Navigate to **Upgrade → ISO Maintenance**.<br>  <br>Release 12.6 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 |
| 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:<br>`$sudo qpSSHKeyProv.pl --prov`<br>  <br>2. Enter the password for admusr.<br>3. Ensure that the keys are exchanged successfully with all the server clusters:<br>  |

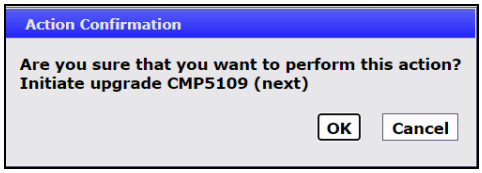
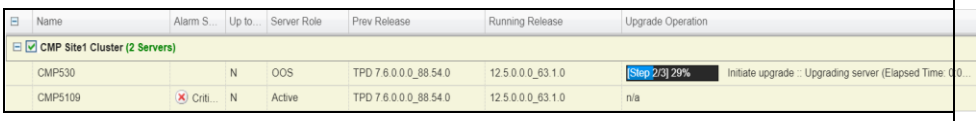
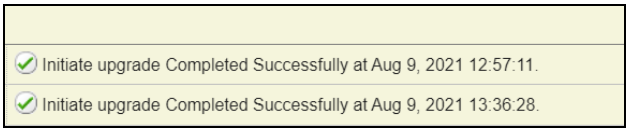
| Step | Procedure | Result |
|---|---|---|
| 8. ☐ | **CMP GUI:** Access into Primary CMP Server—Remove old ISO files from servers. | 1. Navigate to **Upgrade → ISO Maintenance**.<br>2. Select the servers that show old ISO files.<br>3. Select the server cluster.<br>4. Select **Operations → Delete ISO**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

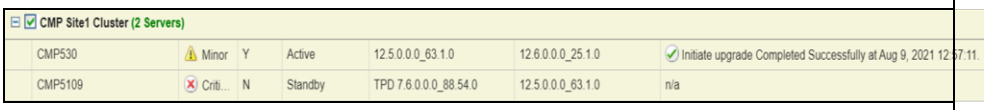
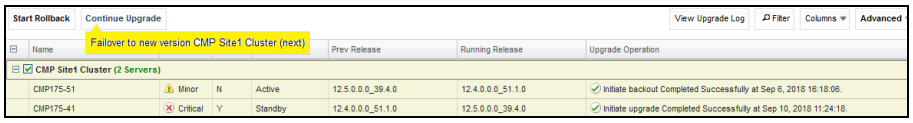
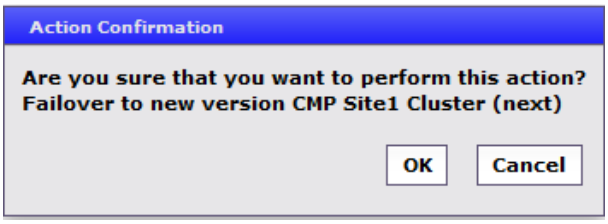
| Step | Procedure | Result |
|---|---|---|
| 9. ☐ | **CMP GUI:** Distribute ISO files to CMP/MPE/ MRA servers<br><br>**NOTE:** This step depends on the ISO file type. Distribute ISO files accordingly. | 1. Navigate to **Upgrade → ISO Maintenance**.<br>2. Filter by server type (optional, but preferred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

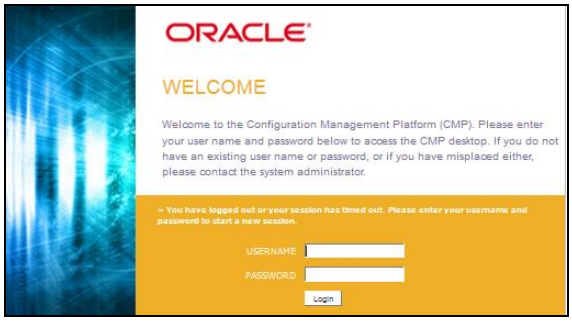
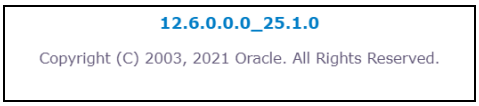
| Step | Procedure | Result |
|---|---|---|
| 10. ☐ | **CMP GUI:** Verify ISO distribution to all the server | 1. Navigate to **Upgrade → ISO Maintenance**.<br>2. Verify that the release 12.6 ISO file of the correct type is shown for each server.<br>3. When completed, the ISO column is populated with the ISO filename and a notification of [100%].<br>**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.<br>  |

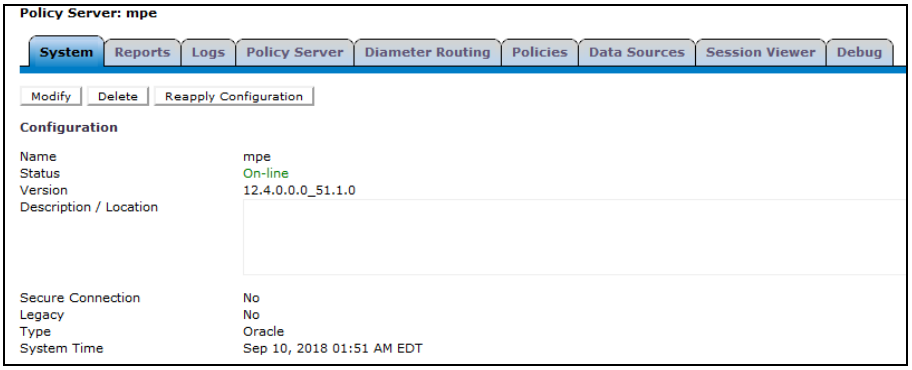
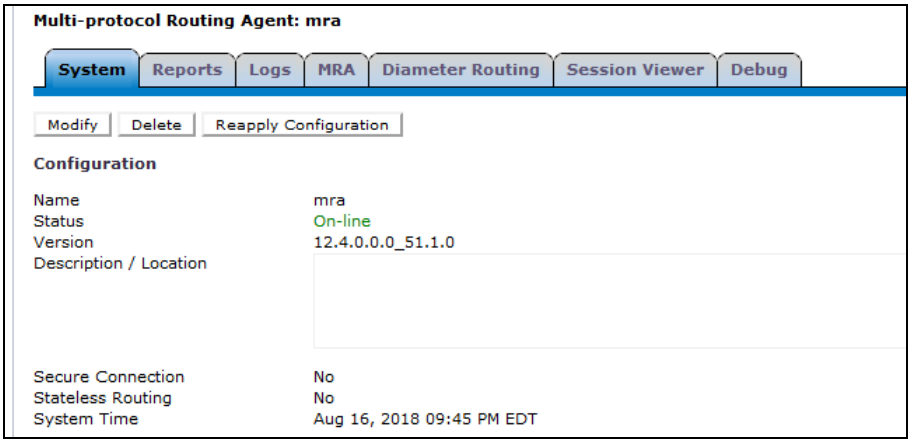
| Step | Procedure | Result |
|---|---|---|
| 11. ☐ | **CMP GUI:** Push the Release 12.6 upgrade scripts to all servers | 1. Navigate to **Upgrade → ISO Maintenance**.<br>  <br>2. Select all the servers in the topology as shown.<br>3. Select **Operations → Push Script** operation.<br>  <br>4. On the warning dialog, click **OK** to continue the operation.<br>  <br>After a minute or so, a successful popup window similar to this should appear:<br>  |
| 12. ☐ | **Primary Active CMP:** SSH to primary active CMP and copy ISO file to `/var/camiant/iso` directory | 1. Logon to the primary active CMP as admusr and copy the 12.6 ISO file to the `/var/camiant/iso` directory:<br>`$sudo cp /var/TKLC/upgrade/cmp-12.6.0.0.0_x.1.0-x86_64.iso/var/camiant/iso/`<br>2. Verify the copy by using the following command:<br>`$ ls /var/camiant/iso/` |

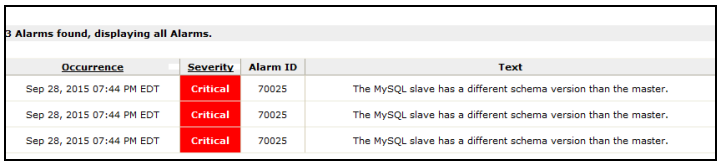
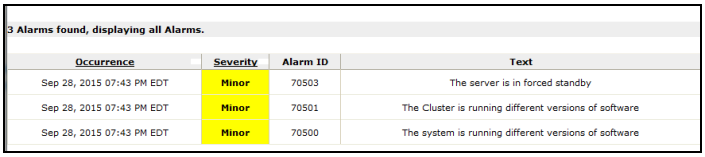
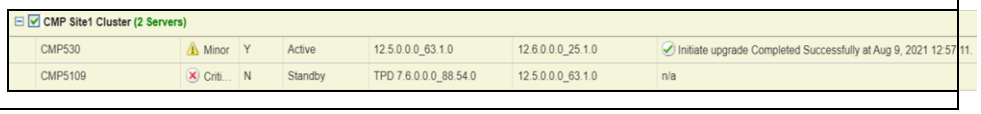
| Step | Procedure | Result |
|---|---|---|
| 13. ☐ | **CMP GUI:** Locate the new 12.6 upgrade manual | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the **Current ISO**. In this case it is labeled Install Kit.<br>  <br>A dialog box with a description of the ISO file that was copied into the `/var/camiant/iso` directory opens.<br>3. Highlight the ISO file and click **Select incremental-upgrade-12.6…** located in the bottom right-hand corner of the window.<br>  <br>4. When the confirmations message displays, click **OK**.<br>  <br>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.<br>  |
| 14. ☐ | **CMP GUI:** Upgrade Primary CMP cluster<br>**NOTE:** This takes approximately 30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. **NOTE:** Click **Filter** and enter `CMP` in the Name field to show the CMP servers only.<br>  <br>3. Select the Primary CMP Server cluster<br>4. Click **Continue Upgrade**.<br>  |

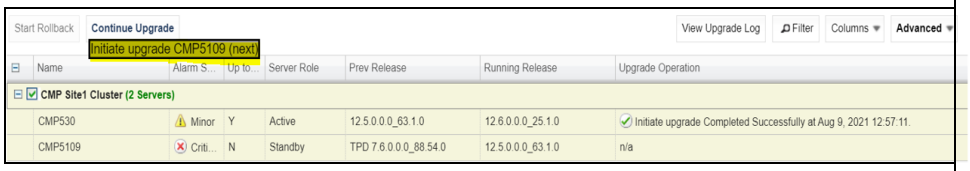
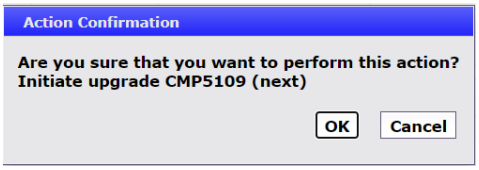
| Step | Procedure | Result |
|---|---|---|
| | | 5. Click **OK** to confirm and continue with the operation.<br>  <br><br>This continues to upgrade the standby server only in the CMP cluster<br>The Upgrade Operation column shows a progress bar along with the upgrade activities.<br>  <br><br>Upgrade Operation column indicates to completed when done.<br>During the upgrade activities, the following alarms may be generated and are considered normal reporting events.<br>**Expected Critical alarm**<br>**31283** Lost Communication with server<br>**31227** HA availability status failed<br>**70025** QP Slave database is a different version than the master<br>**70001** QP_procmgr failed<br>**Expected Major Alarm**<br>**70004** QP Processes down for maintenance<br>**Expected Minor Database replication Alarms**<br>**70503** Server Forced Standby<br>**70507** Upgrade In Progress<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**31106** Database merge to parent failure<br>**31107** Database merge from child failure<br>**31101** Database replication to slave failure<br>**31114** DB replication over SOAP has failed<br>**31282** HA Management Fault<br>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.<br>  <br> |

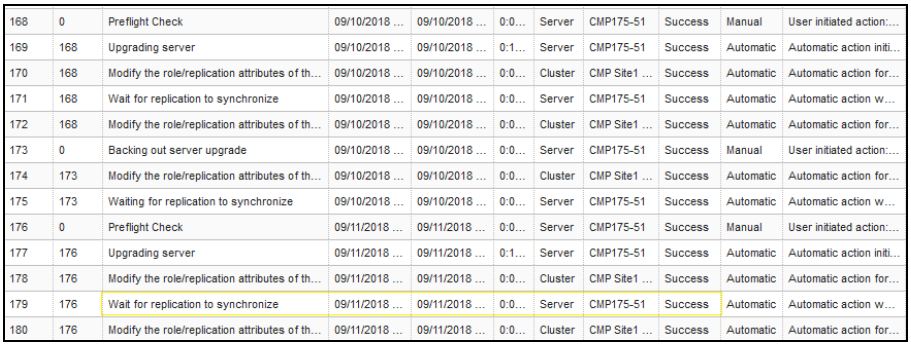
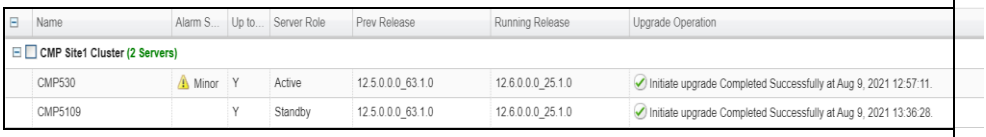
| Step | Procedure | Result |
|---|---|---|
| 15. ☐ | **CMP GUI:** Verify that the upgrade is successful | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. View the cluster.<br>3. Verify the following information:<br>- The standby server is on 12.6<br>- The other server in the cluster is on 12.5.0/12.5.0.4<br>- The Up to Date column shows Y for the 12.6 server and N for the 12.5.0/12.5.0.4 server.<br>- Has alarm:<br>70025 – QP Slave database is a different version than the master<br>70501 – Cluster Mixed Version<br>70503 – Server Forced Standby<br>  |
| 16. ☐ | **CMP GUI:** Continue to upgrade CMP cluster | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Primary CMP Server cluster.<br>3. Click **Continue Upgrade**. Notice the Failover to new version CMP Site1 Cluster message.<br>  <br>4. Click **OK** to confirm and continue with the operation.<br>  <br>The specific action takes a minute to complete.<br>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.<br><br>The Policy Management release 12.6 CMP GUI login page opens as shown—login and password credentials are the same as the pre-upgrade.<br>  |
| 18. ☐ | **CMP GUI:** Verify new Policy Management release | Navigate to **Help→About**. Verify the release displayed is 12.6.<br>  |

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

| Step | Procedure | Result |
|---|---|---|
| 20. ☐ | **CMP GUI:** Critical alarms | Critical alarm 70025, QP Slave database is a different version than the master, is seen until the SQL Database matches the master (12.6). This alarm is expected and remains until all CMP servers are upgraded to the same version.<br><br>**Current Critical Alarms**<br><br>**70025** QP Slave database is a different version than the master:<br>  <br>3 Alarms found, displaying all Alarms.<br>Occurrence \| Severity \| Alarm ID \| Text<br>Sep 28, 2015 07:44 PM EDT \| Critical \| 70025 \| The MySQL slave has a different schema version than the master.<br>Sep 28, 2015 07:44 PM EDT \| Critical \| 70025 \| The MySQL slave has a different schema version than the master.<br>Sep 28, 2015 07:44 PM EDT \| Critical \| 70025 \| The MySQL slave has a different schema version than the master.<br><br>**Current Minor Alarms**<br><br>**70503** Server Forced Standby<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>  <br>3 Alarms found, displaying all Alarms.<br>Occurrence \| Severity \| Alarm ID \| Text<br>Sep 28, 2015 07:43 PM EDT \| Minor \| 70503 \| The server is in forced standby<br>Sep 28, 2015 07:43 PM EDT \| Minor \| 70501 \| The Cluster is running different versions of software<br>Sep 28, 2015 07:43 PM EDT \| Minor \| 70500 \| The system is running different versions of software<br><br>**NOTE:** The Upgrade Manager shows alarms as well. |
| 21. ☐ | **CMP GUI:** Verify the Policy Management release 12.6 CMP is Active | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Verify the following<br>- Active server is running release12.6<br>- Standby server is on the previous release<br>  <br>CMP Site1 Cluster (2 Servers)<br>CMP530 \| Minor \| Y \| Active \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Aug 9, 2021 12:57:11.<br>CMP5109 \| Criti... \| N \| Standby \| TPD 7.6.0.0.0_88.54.0 \| 12.5.0.0.0_63.1.0 \| n/a |

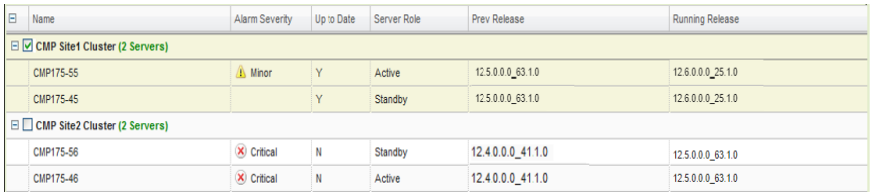
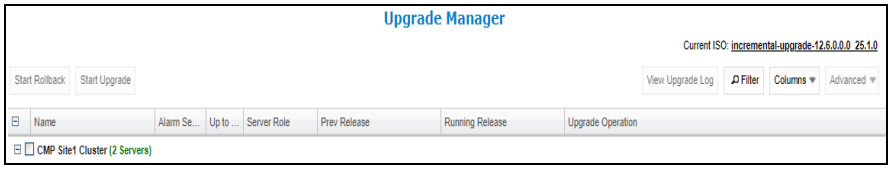
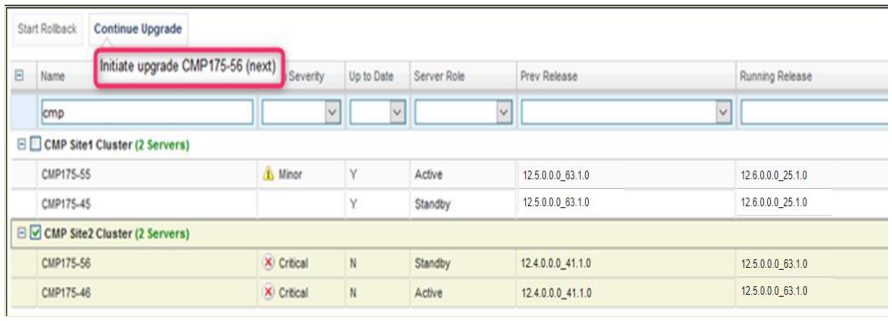
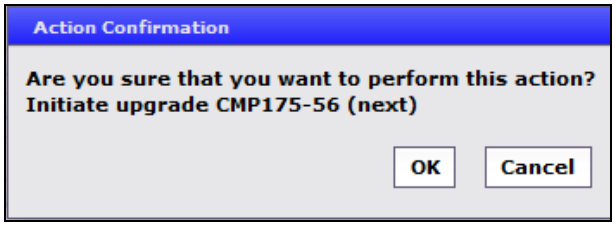
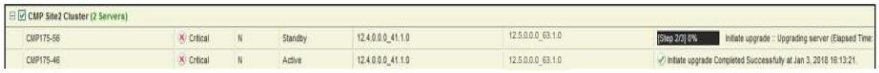
| Step | Procedure | Result |
|---|---|---|
| 22. ☐ | **CMP GUI:** Complete the upgrade of the Primary CMP cluster<br><br>**NOTE:** Remaining CMP server takes approximately 30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Primary CMP Server cluster<br>3. Click **Continue Upgrade**. Notice the Initiate upgrade <*standbyserver*> (next) message when hovering over the button.<br>  <br><br>4. Click **OK** to continue the upgrade on the remaining server in the CMP cluster.<br>  <br><br>**NOTE:** The server that is being upgraded goes into an OOS state.<br><br>**Expected Critical Alarms**<br><br>**31227** HA availability status failed<br>**31283** Lost Communication with server<br>**70001** QP_procmgr failed<br>**70025** QP Slave database is a different version than the master<br><br>**Expected Major Alarm**<br><br>**70004** QP Processes down for maintenance<br><br>**Expected Minor Alarms**<br><br>**70503** Server Forced Standby<br>**70507** Upgrade In Progress<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**31114** DB replication over SOAP has failed<br>**31106** Database merge to parent failure<br>**31107** Database merge from child failure<br>**31101** Database replication to slave failure<br>**31282** HA Management Fault |

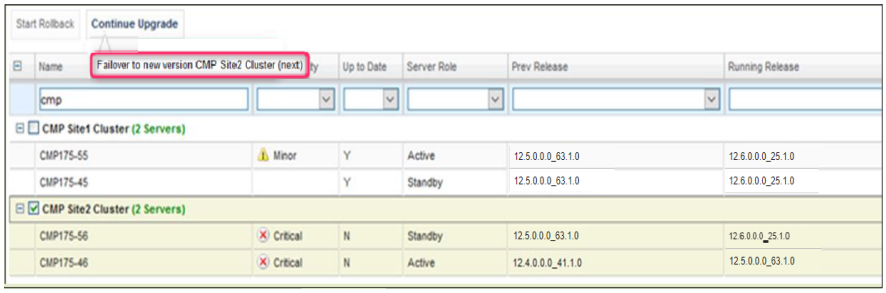
| Step | Procedure | Result |
|---|---|---|
| 23. ☐ | **CMP GUI:** Tracking the upgrade complete | Navigate to **Upgrade → Upgrade Manager**.<br>The last step of the upgrade for the first CMP cluster is to wait for replication to complete.<br>With the CMP cluster selected, click **View Upgrade Log** to open a window where you can verify that synchronization has taken place:<br>  |
| 24. ☐ | **CMP GUI:** Verify the status of upgraded CMP server. | Navigate to **Upgrade Manager → Upgrade Manager**.<br>  <br>Successful upgrade status shows the following for both servers in the Primary CMP cluster:<br>• 12.6 in the Running Release column for both servers<br>• A Y in the Up to Date column<br>• Active or Standby state for both servers in the Primary CMP cluster. |
| 25. ☐ | Proceed to next upgrade procedure | Verify the following information:<br>• Primary Site1 is running release 12.6<br>• Secondary Site is on release 12.5.0/12.5.0.4<br>• Proceed to the next procedure to upgrade the secondary CMP cluster. |
| **—End of Procedure—** | | |

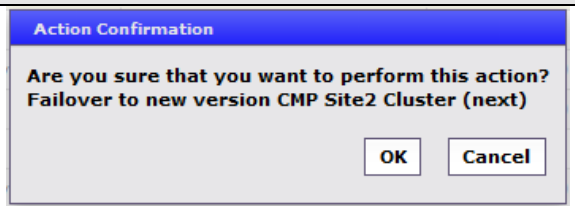
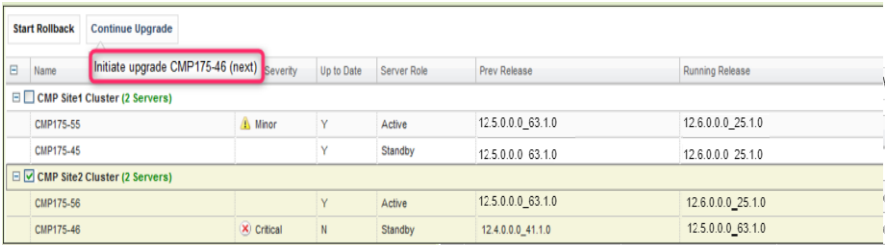
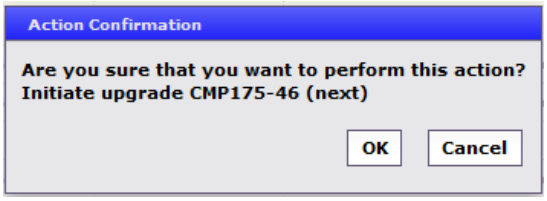
## 1.6 Upgrade Secondary CMP cluster

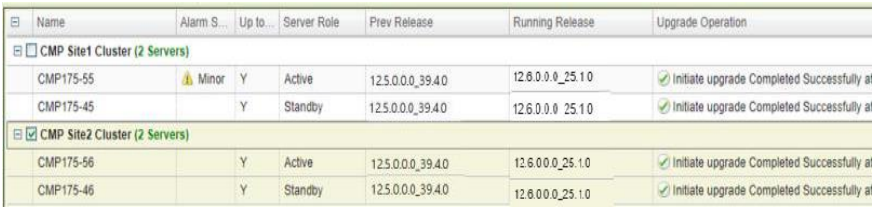
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

**Procedure 8 Upgrade Secondary CMP cluster**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **CMP GUI:** Verify status of CMP cluster | Navigate to **Upgrade → Upgrade Manager**.<br>• Primary CMP is completely upgraded to 12.6<br>• Secondary CMP cluster is on 12.5.0/12.5.0.4<br>  |
| 2. ☐ | **CMP GUI:** Upgrade Secondary CMP cluster<br>**NOTE:** This takes approximately 30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. **NOTE:** Click **Filter** and enter CMP in the Name field to see only the CMP servers.<br>  <br>3. Select the Secondary CMP Server cluster at Site2<br>4. Click **Continue Upgrade**. When hovering over the button, it reads Initiate upgrade <*site2_standbyserver*> (next).<br>  <br>5. Click **OK** to confirm and continue with the operation.<br>  <br>This continues to upgrade the standby server only in the CMP cluster<br>The Upgrade Operation column shows a progress bar along with the upgrade activities. Note: first version column is Prev Release, and second version column is Running Release.<br>  |

| Step | Procedure | Result |
|---|---|---|
| | | During the upgrade activities, the following alarms may be generated and are considered normal reporting events:<br><br>**Expected Critical alarm**<br><br>**31283** Lost Communication with server<br>**70001** QP_procmgr failed<br>**70025** QP Slave database is a different version than the master<br><br>**Expected Major Alarm**<br><br>**70004** QP Processes down for maintenance<br><br>**Expected Minor Alarms**<br><br>**70503** Server Forced Standby<br>**70507** Upgrade In Progress<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**31114** DB replication over SOAP has failed<br>**31106** Database merge to parent failure<br>**31107** Database merge from child failure<br>**31101** Database replication to slave failure<br>**31282** HA Management Fault<br>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.<br>  |
| 3. ☐ | **CMP GUI:**<br>Failover of the Secondary CMP cluster | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Secondary CMP Server cluster at Site2.<br>3. Click **Continue Upgrade**. Notice the Failover to new version CMP Site2 Cluster message<br>  <br>4. Click **OK** to confirm and continue with the operation. |

| Step | Procedure | Result |
|---|---|---|
| | |  <br>5. The failover takes about a minute to complete. Wait until the upgraded server is active, running 12.6 as shown below. Note: first version column is Prev Release, and second version column is Running Release.<br>  |
| 4. ☐ | **CMP GUI:** Continue upgrade of the Secondary CMP cluster | 1. Select the Secondary CMP Server cluster at Site2<br>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 12. 5.0/12.5.0.4.<br>  <br>3. Click **OK** to confirm and continue with the operation.<br>  <br>During the upgrade activities, the following alarms may be generated and are considered normal reporting events.<br><br>**<u>Expected Critical alarm</u>**<br><br>**31283** Lost Communication with server<br>**70001** QP_procmgr failed<br>**70025** QP Slave database is a different version than the master<br><br>**<u>Expected Major Alarm</u>**<br><br>**70004** QP Processes down for maintenance<br><br>**<u>Expected Minor Alarms</u>**<br><br>**70503** Server Forced Standby<br>**70507** Upgrade In Progress<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version |

| Step | Procedure | Result |
|---|---|---|
| | | **31114** DB replication over SOAP has failed<br>**31106** Database merge to parent failure<br>**31107** Database merge from child failure<br>**31101** Database replication to slave failure<br>**31282** HA Management Fault |
| 5. ☐ | **CMP GUI:** Verify that the upgrade completed successfully. | Navigate to **Upgrade → Upgrade Manager**.<br>Successful upgrade status shows release 12.6 in the Running Release column and the Upgrade Operation.<br>The Upgrade Operation column shows:<br>• Initiate Upgrade Completed Successfully at message<br>• The correct date and time.<br>  |
| 6. ☐ | **CMP GUI:** Verify alarms | Navigate to **System Wide Reports → Alarms → Active Alarms**.<br>**Expected Minor Alarms**<br>**70500** System Mixed Version |
| 7. ☐ | Procedure is complete. | Verify the following information:<br>• All CMP clusters upgrades are complete and running release 12.6<br>• All MRA and MPE clusters are running release 12.5.0/12.5.0.4<br>The Policy Management system is running in mixed-version mode. |
| **—End of Procedure—** | | |

## 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 12.5.0.0.0_63.1.0 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 9: Configuration Preparation**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **CMP GUI:** Access into CMP server | Use the supported browser to login as the admin user or as a user with administrative privileges. |
| 2. ☐ | **CMP GUI:** Verify current Upgrade Manager status and software release 12.6 ISO files | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Verify that all CMP clusters have both Active, Standby status.<br>3. Verify that all MPE and MRA clusters have an Active, Standby, and Spare server.<br>4. Verify that Policy Management release 12.6 ISO files are available on `/var/TKLC/upgrade` for all MPE, and MRA clusters. One ISO per server<br>5. Verify that the CMP cluster is upgraded successfully and running Policy Management release 12.6 |
| **—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 12.5.0/12.5.0.4 upgrade to 12.6

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

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

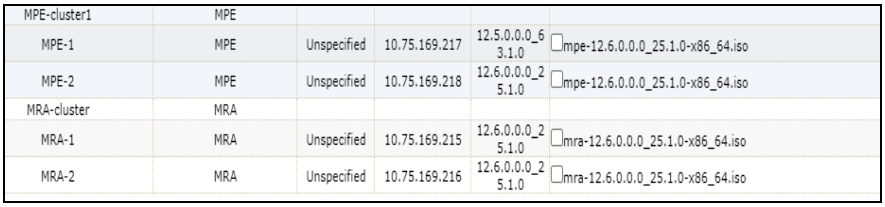
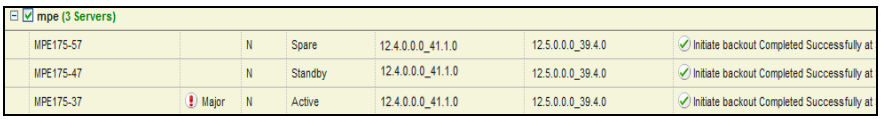
1. Select and start upgrade on the standby server
2. Failover
3. Re-apply configuration
4. Continue to upgrade the spare server
5. Continue upgrade on remaining server
6. (MPE only) Re-apply configuration one MPE cluster at a time

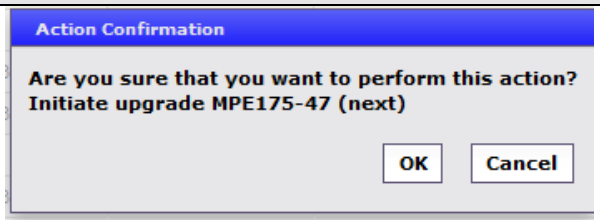
**NOTES:**

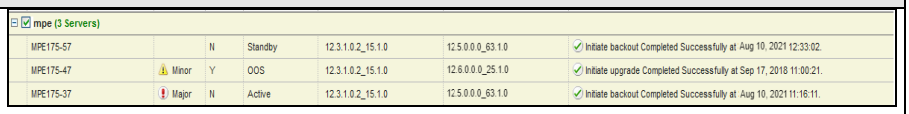
- All CMP clusters must be upgraded to Policy Management release 12.6 prior to performing the following procedures.
- Four (4) clusters (8 for 12.5.0/12.5.0.4) can be running the upgrade at one time.
- Only ONE cluster can be selected for upgrade activity, bulk selection of servers is not supported in release 12.6.

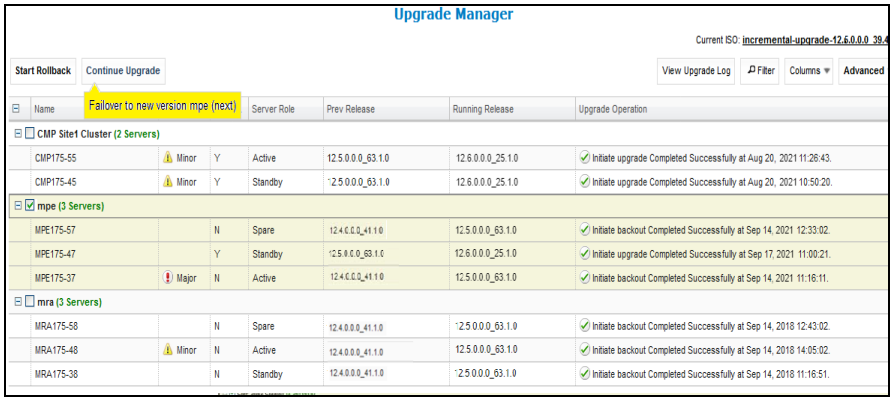
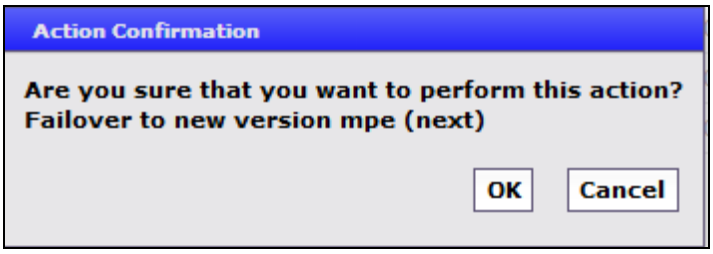
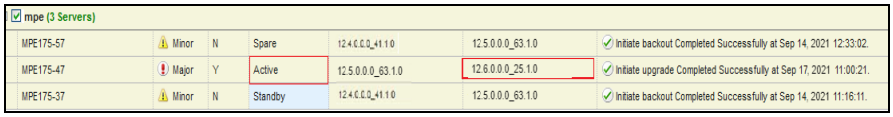
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

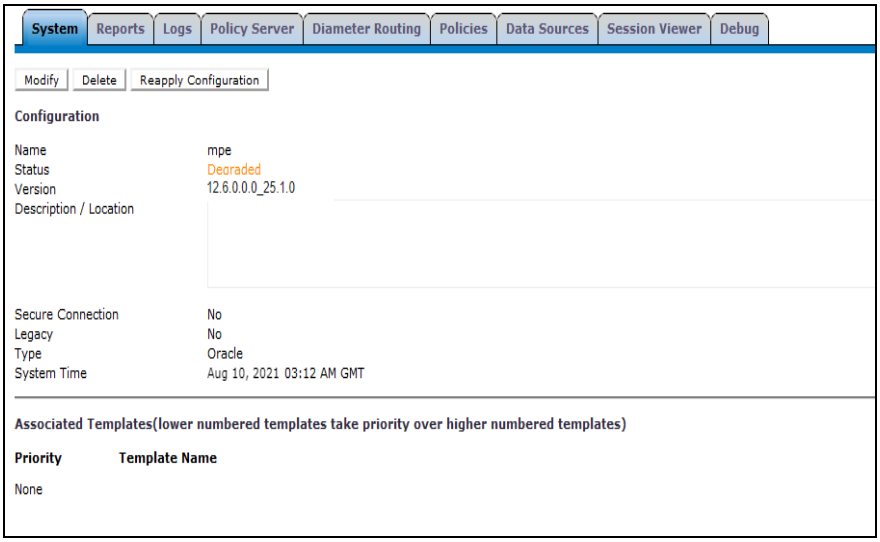
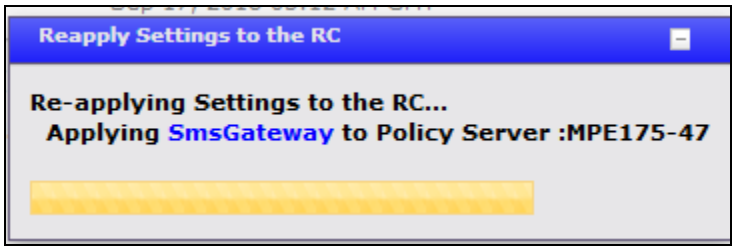
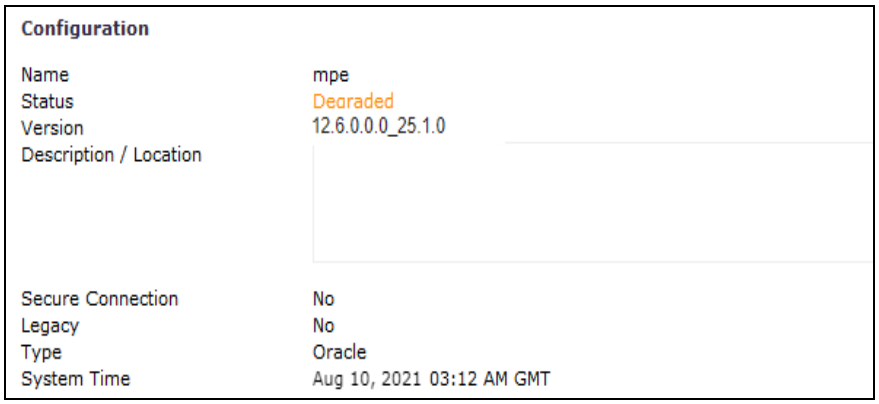
**Procedure 10: Upgrade MRA and MPE Servers**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **CMP GUI:** Health checks on the MPE/MRA servers to be upgraded | Perform the following:<br>1. Check for current active alarms<br>2. Reset MPE/MRA counters to make a baseline<br>- For the MPE: **Policy Server → Configuration →** <*server_name*> **→ Reports → Reset Counters**<br>- For the MRA: **MRA → Configuration →** <*server_name*> **→ Reports → Reset Counters**<br>3. Go to the KPI Dashboard and capture a screenshot.<br>4. **System Wide Reports → KPI Dashboard** |
| 2. ☐ | **CMP GUI:** Verify upgrade status of selected MPE/MRA site/segment | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Verify information for the MRA/MPE servers:<br>- Current release 12.5.0, or 12.5.0.4 installed<br>- Active/Standby/Spare status<br>- ISO version to be deployed is 12.6 (verify the current ISO files are 12.6 by going to **Upgrade → ISO Maintenance**) Note: first version column is Prev Release, and second version column is Running Release.<br>  |
| 3. ☐ | **CMP GUI:** Upgrade clusters<br>**NOTE:** The upgrade of a single server takes approximately 40 minutes to complete. | **NOTE:** Start the upgrade on ONE cluster. Wait until the cluster shows OOS, and then continue with the next cluster and so on. Up to 16 clusters may be running upgrade at any time.<br>1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the cluster to be upgraded, it can be an MRA or MPE<br>3. Click **Continue Upgrade**.<br>  <br>4. Click **OK** to confirm and continue with the operation. It begins to upgrade the standby server of that cluster. |

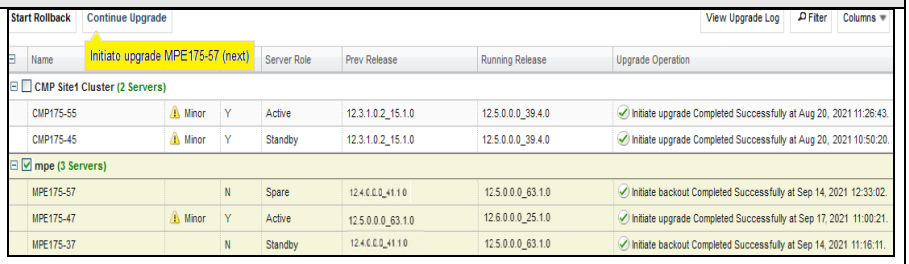
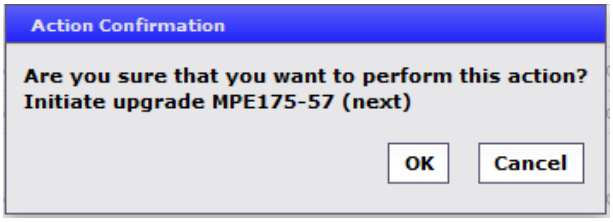
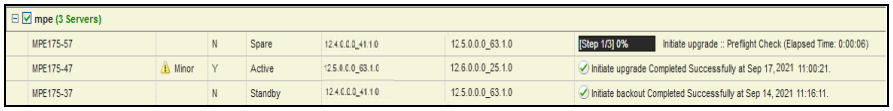
| Step | Procedure | Result |
|---|---|---|
| | |  <br>Wait until the cluster reports OOS before selecting the next cluster.<br>Follow the progress in the Upgrade Operation column.<br>  <br>During the upgrade activities, the following alarms may be generated and are considered normal reporting events.<br>**Expected Critical Alarms**<br>**31283** HA Server Offline / Lost Communication with server<br>**70001** QP_procmgr failed<br>**31227** HA availability status failed<br>**Expected Major Alarm**<br>**31233** High availability path loss of connectivity<br>**70004** QP Processes down for maintenance<br>**Expected Minor Alarms**<br>**70503** Server Forced Standby<br>**70507** Upgrade In Progress<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**31114** DB replication over SOAP has failed<br>**31106** Database merge to parent failure<br>**31107** Database merge from child failure<br>**31101** Database replication to slave failure<br>**31282** HA Management Fault<br>**78001** Rsync Failed<br>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. |

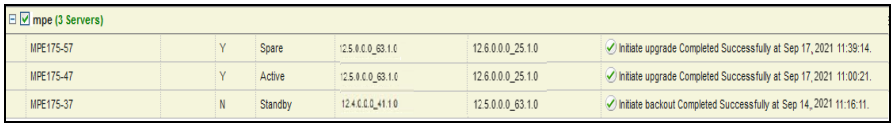
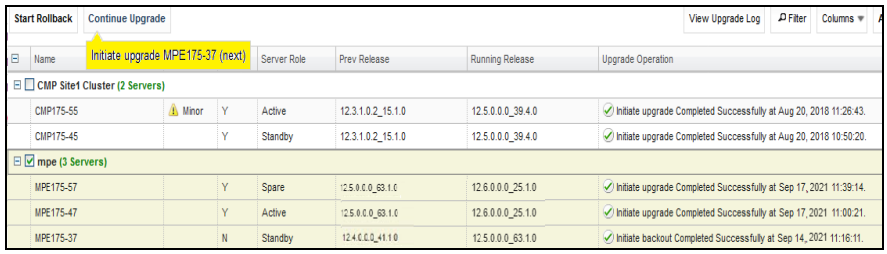
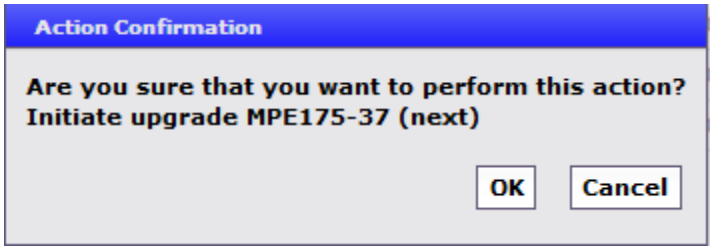
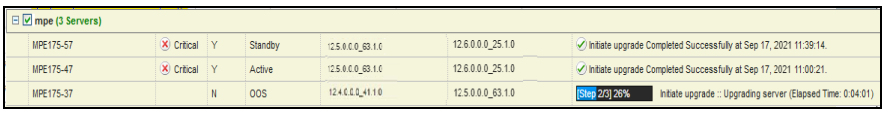
| Step | Procedure | Result |
|---|---|---|
| | |  <br>During the upgrade activities, the following alarms may be generated and are considered normal reporting events.<br>Alarm 31224—HA configuration error (major) is raised noting that there is a configuration error. This clears a few minutes after the upgrade completes on the first server. The following minor alarms may be present:<br>**Expected Minor Alarms**<br>**78001** Rsync Failed<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**70503** Server Forced Standby |

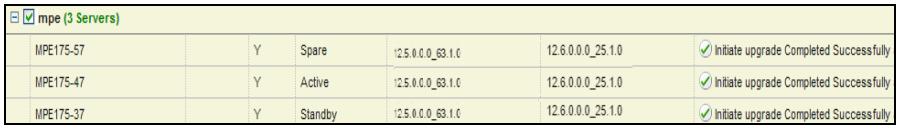
| Step | Procedure | Result |
|---|---|---|
| 4. ☐ | **CMP GUI:** Continue to upgrade the MRA/MPE clusters. Next operation is a failover.<br><br>**NOTE:** 4 clusters (8 for 12.5.0/12.5.0.4) can be running the upgrade process at one time. | Fail over ONE cluster at a time and wait until the upgraded server becomes active before moving on to the next cluster.<br><br>1. Navigate to **Upgrade → Upgrade Manager**.<br><br>2. Select the cluster being upgraded (it can be an MRA or MPE)<br><br>3. Click **Continue Upgrade**. When hovering over the button, it says Failover to new version<br><br>  <br><br>4. Click **OK** to confirm and continue with the operation. It starts to failover the cluster.<br><br>  <br><br>Wait until failover completes before failing over the next cluster, This takes a minute or two to complete. Verify the 12.6 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.<br><br>  |

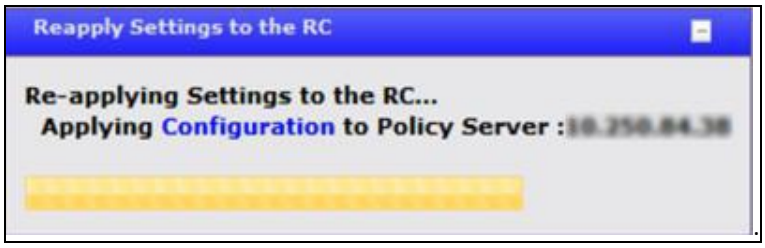
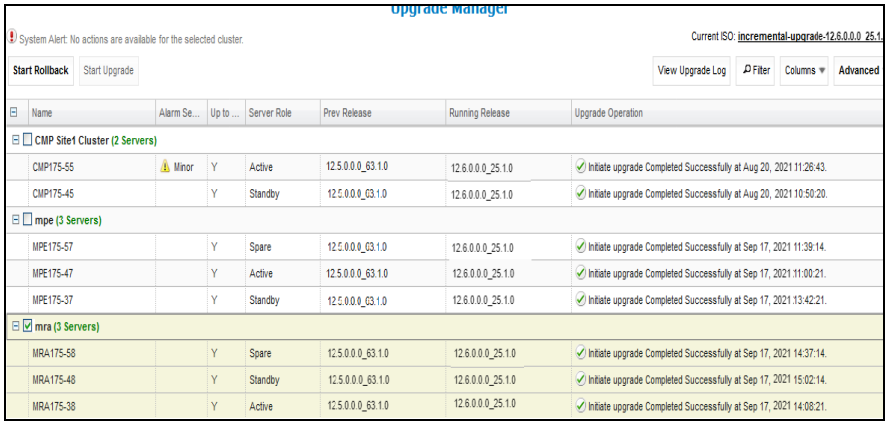
| Step | Procedure | Result |
|---|---|---|
| 5. ☐ | **CMP GUI:** Reapply configuration on MPE/MRA cluster that completed the upgrade successfully. | • For MPE: **PolicyServer → Configuration →** <*mpe_cluster name*> **→ System**<br>• For MRA: **MRA → Configuration →** <*mra_cluster name*> **→ System**<br>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.<br>1. Click **Reapply Configuration**.<br>  <br>**NOTE:** A progress bar displays for the MPE reapply configuration only. The MRA reapply configuration does not display the progress bar.<br>  <br>2. Note the version is successfully changed to the upgraded release 12.6.<br>**NOTE:** The status shows Degraded because the servers are still in different releases.<br>  |

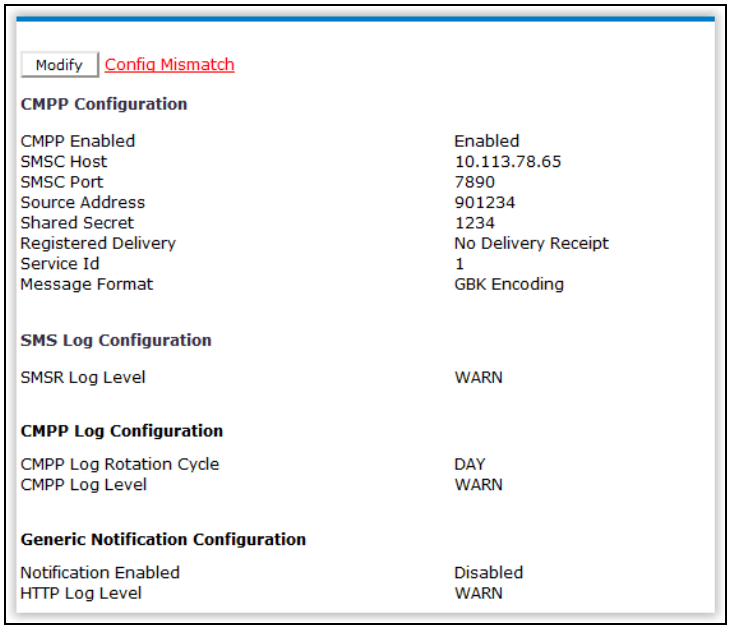
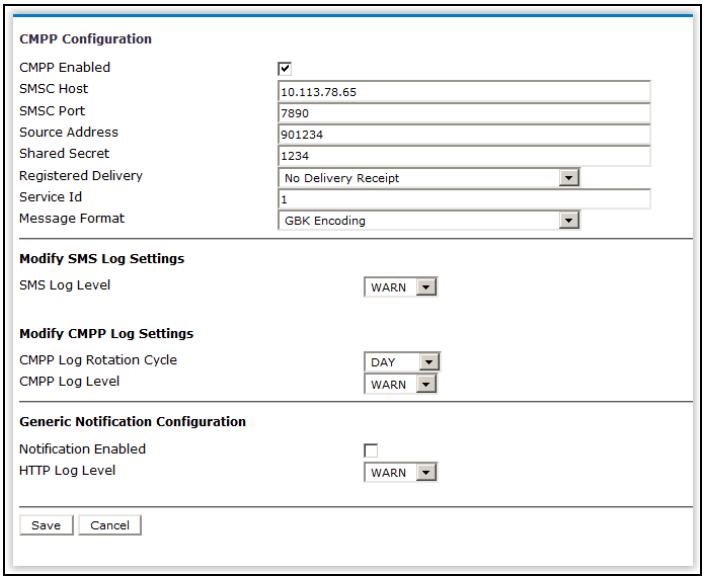
| Step | Procedure | Result |
|---|---|---|
| 6. ☐ | **CMP GUI:** Current alarms | During the upgrade activities, the following alarms may be generated and are considered normal reporting events.<br><br>**Expected Critical alarm**<br><br>None<br><br>**Expected Major Alarm**<br><br>**78001** Rsync Failed<br><br>**Expected Minor Alarms**<br><br>**70503** Server Forced Standby<br>**70502** Cluster Replication Inhibited<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**71402** Connectivity Lost<br>**31101** Database replication to slave failure |
| 7. ☐ | **CMP GUI:** Verify traffic becomes active within 90 seconds | 1. Navigate to Upgrade Manager → System Maintenance.<br>- If traffic is active, go to step 9.<br>- If traffic does not become active within 90 seconds:<br>2. Select the Partially upgraded cluster, and select **Operations → Rollback**.<br><br>The pre-12.3 MPE server should become active and resume handling traffic. |
| 8. ☐ | **CMP GUI:** Reapply configuration | • For MPE: **Policy Server → Configuration → <***mpe_cluster name***> → System**<br>• For MRA: **MRA → Configuration → <***mra_cluster name***> → System**<br>1. Click Reapply Configuration<br>2. Verify that the version is changed back to 12.5.0 or 12.5.0.4, and the action report success.<br><br>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.<br><br>**NOTE:** Up to 16 clusters can be running the upgrade process at one time.<br><br>1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the checkbox for a cluster.<br>- Select one cluster at a time<br>- Can be an either an MRA or MPE cluster<br>3. Click **Continue Upgrade**. When hovering over the button, it reads Initiate upgrade… on the spare server |

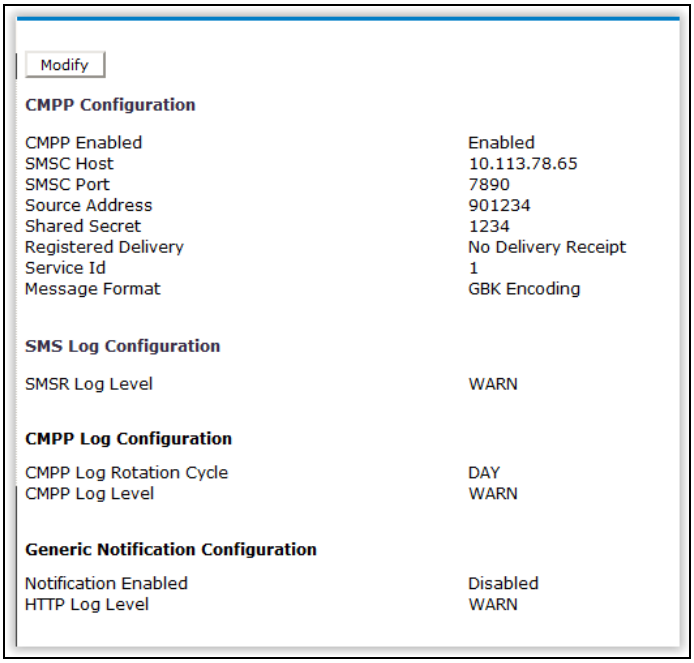
| Step | Procedure | Result |
|---|---|---|
| | |  <br>4. Click **OK** to confirm and continue with the operation.<br>  <br>Wait until the cluster reports OOS before selecting the next cluster<br>Follow the progress in the Upgrade Operation column.<br>  <br>During the upgrade activities, the following alarms may be generated and are considered normal reporting events—these is cleared after the MPE cluster is completely upgraded.<br><br>**Expected Critical Alarms**<br><br>**31283** HA Server Offline / Lost Communication with server<br>**31227** HA availability status failed<br>**70001** QP_procmgr failed<br><br>**Expected Major Alarm**<br><br>**70004** QP Processes down for maintenance<br><br>**Expected Minor Alarms**<br><br>**70503** Server Forced Standby<br>**70507** Upgrade In Progress<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**70502** Cluster Replication Inhibited<br>Upgrade is complete on the spare server in the georedundant cluster when:<br>• 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. |

| Step | Procedure | Result |
|---|---|---|
| | |  <br>• The server goes back to the Spare state.<br>• The Up to Date column shows a Y (YES).<br>The Active and Spare servers are on release 12.6 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.<br>1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the checkbox for a cluster:<br>- Select one cluster at a time<br>- Can be an either an MRA or MPE cluster<br>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.<br>  <br>4. Click **OK** to confirm and continue with the operation. It begins the final server upgrade of the cluster.<br>  <br>Wait until the cluster reports OOS before selecting the next cluster<br>Follow the progress in the Upgrade Operation column.<br>  <br>During the upgrade activities, the following alarms may be generated and are considered normal reporting events—these is cleared after the MPE cluster is |

| Step | Procedure | Result |
|---|---|---|
| | | completely upgraded.<br><br>**Expected Critical Alarms**<br><br>**31283** HA Server Offline / Lost Communication with server<br>**31227** HA availability status failed<br>**70001** QP_procmgr failed<br><br>**Expected Major Alarm**<br><br>**70004** QP Processes down for maintenance<br><br>**Expected Minor Alarms**<br><br>**70503** Server Forced Standby<br>**70507** Upgrade In Progress<br>**70500** System Mixed Version<br>**70501** Cluster Mixed Version<br>**70502** Cluster Replication Inhibited<br>**31114** DB replication over SOAP has failed<br>**31106** Database merge to parent failure<br>**31107** Database merge from child failure<br>**31101** Database replication to slave failure<br>**31102** Database replication from master failure<br>**31113** DB replication manually disabled<br>Upgrade is complete on the third server in the georedundant cluster when:<br>• The completed successfully message shows in the Upgrade Operation column.<br>• The server goes back to the Standby state.<br>• The Up to Date column shows a Y (YES). Note: first version column is Prev Release, and second version column is Running Release.<br>  <br>mpe (3 Servers)<br>MPE175-57 Y Spare 12.5.0.0.0_63.1.0 12.6.0.0.0_25.1.0 Initiate upgrade Completed Successfully<br>MPE175-47 Y Active 12.5.0.0.0_63.1.0 12.6.0.0.0_25.1.0 Initiate upgrade Completed Successfully<br>MPE175-37 Y Standby 12.5.0.0.0_63.1.0 12.6.0.0.0_25.1.0 Initiate upgrade Completed Successfully<br><br>All servers are now running release 12.6. |
| 11. ☐ | Exchange SSH Keys | 1. Enter the following command: $ sudo qpSSHKeyProv.pl--prov<br><br>You are prompted: The password of admusr in topology<br><br>**Note**: The above command to exchange SSH keys needs to be run on the active CMP only.<br><br>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 | 1. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ System** |

| Step | Procedure | Result |
|---|---|---|
| | the fully upgraded MPE clusters. | 2. Click **Reapply Configuration**.<br>**NOTE:** A progress bar displays for the MPE reapply configuration.<br>  |
| 13. ☐ | Repeat steps 1 through 14 for the next MPE or MRA clusters | Proceed with next cluster(s) |
| 14. ☐ | Upgrade Completed | At this point all servers have been upgraded.<br>  |

| Step | Procedure | Result |
|---|---|---|
| 15. ☐ | **CMP GUI:** Modify/save SMSR configuration | **System Administration → SMS Relay → Modify**<br><br>**NOTE: This step is only for Wireless-C system. If you do not see SMS Relay under System Administration, skip this step.**<br><br>Initial access into this configuration upon upgrade to release 12.6, the configuration shows as such with Config Mismatch.<br><br>  <br><br><br>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.<br><br>  <br><br><br>2. Click **Save** to save the configuration and continue as shown. |

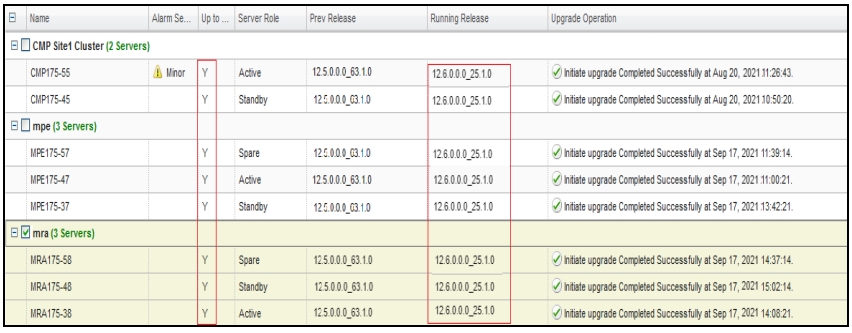
| Step | Procedure | Result |
|---|---|---|
| | |  <br>Modify<br>**CMPP Configuration**<br>CMPP Enabled: Enabled<br>SMSC Host: 10.113.78.65<br>SMSC Port: 7890<br>Source Address: 901234<br>Shared Secret: 1234<br>Registered Delivery: No Delivery Receipt<br>Service Id: 1<br>Message Format: GBK Encoding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

## 1.8 Post Upgrade health Check for wireless systems

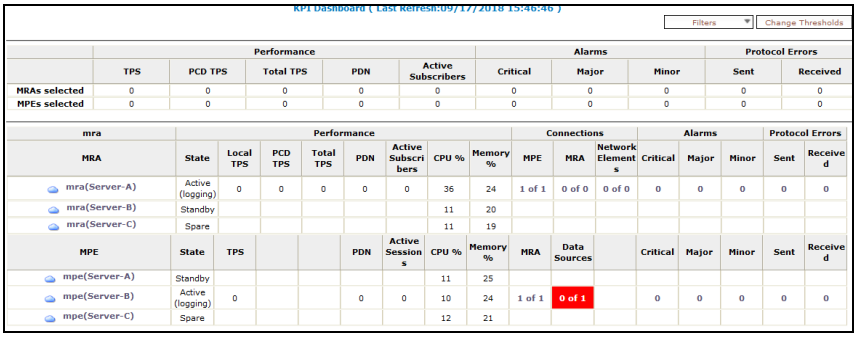
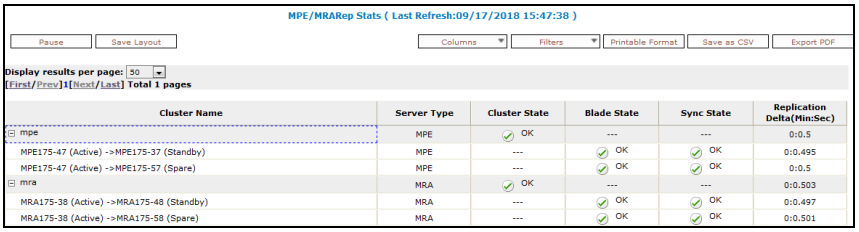
**NOTE:** This section is used when the entire topology is running release 12.6

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

**Procedure 11 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**.<br>2. View the Up to Date, Running Release, and Upgrade Operation columns and verify they read Y, 12.6…, and Initiate upgrade completed successfully at… respectively, for all servers in all clusters.<br>  |

| Name | Alarm Se... | Up to ... | Server Role | Prev Release | Running Release | Upgrade Operation |
|---|---|---|---|---|---|---|
| CMP Site1 Cluster (2 Servers) | | | | | | |
| CMP175-55 | Minor | Y | Active | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Aug 20, 2021 11:26:43. |
| CMP175-45 | | Y | Standby | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Aug 20, 2021 10:50:20. |
| mpe (3 Servers) | | | | | | |
| MPE175-57 | | Y | Spare | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Sep 17, 2021 11:39:14. |
| MPE175-47 | | Y | Active | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Sep 17, 2021 11:00:21. |
| MPE175-37 | | Y | Standby | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Sep 17, 2021 13:42:21. |
| mra (3 Servers) | | | | | | |
| MRA175-58 | | Y | Spare | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Sep 17, 2021 14:37:14. |
| MRA175-48 | | Y | Standby | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Sep 17, 2021 15:02:14. |
| MRA175-38 | | Y | Active | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate upgrade Completed Successfully at Sep 17, 2021 14:08:21. |

| Step | Procedure | Result |
|---|---|---|
| 2. ☐ | **CMP GUI:** View current alarms | 1. Navigate to **System Wide Reports→Alarms→Active Alarms**.<br>2. Verify that all alarms due to the upgrade have been cleared.<br>  |
| 3. ☐ | **CMP GUI:** View current KPIs | 1. Navigate to **System Wide Reports→KPI Dashboard**.<br>2. Make sure everything looks normal.<br>  |
| 4. ☐ | **CMP GUI:** Replication stats | Navigate to System Wide Reports→Others→MPE/MRA Rep Stats (for a wireless system)<br>**Wireless:**<br>  |
| **—End of Procedure—** | | |

## 1.9 Workaround for Netbackup Client Installation after Upgrading to 12.6

If you were on R12.3.1 CMP with netbackup client R7.1 installed, then upgrade the CMP to R12.6 and install R7.7 netbackup client, perform the following steps if the installation fails:

1. Force standby the CMP server to install or upgrade netbackup client:
   `Vim /etc/fstab` to make the **/tmp** mount options back to defaults
   Find the below line:
   `/dev/mapper/vgroot-plat_tmp /tmp ext4 noexec,nosuid,nodev 1 2`

update to:
```
/dev/mapper/vgroot-plat_tmp /tmp  ext4 defaults  1 2
```

2. Reboot the server for re-mount the **/tmp** with defaults.
3. Perform the netbackup client following installation steps. The netbackup client must be installed successfully on the CMP server.
4. Back the **/etc/fstab** for **/tmp** to the original value.
5. Reboot the server.
6. The netbackup server could retrieve the backup content from the CMP server.

## 1.10 Backout (ROLLBACK) 12.5.0/12.5.0.4 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.

### 1.10.1 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.

### 1.10.2 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.

### 1.10.3 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-12.6 release with Active, Standby, or Spare status.

Expected pre-conditions:

1. Primary Active CMP is on Release 12.6
2. Secondary CMP cluster is on Release 12.6
3. All MPE/MRA Clusters are on Release 12.6

#### *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 in to the Primary CMP VIP.
4. If needed, go to **Policy Server→ Configuration → Policy Server** and click **Reapply Configuration**.
5. 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:

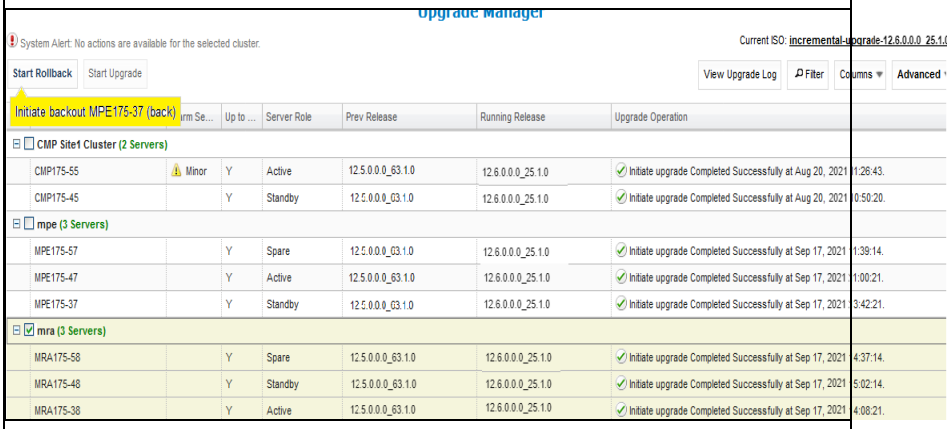
1. Primary Active CMP is on Release 12.6
2. Cluster is any of MPE or MRA
3. One server of target cluster is on Release 12.6
4. Other servers of target cluster are on Release 12.5.0/12.5.0.4

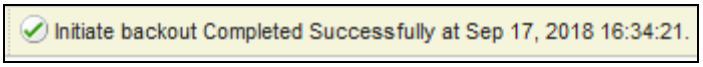
**NOTES:**

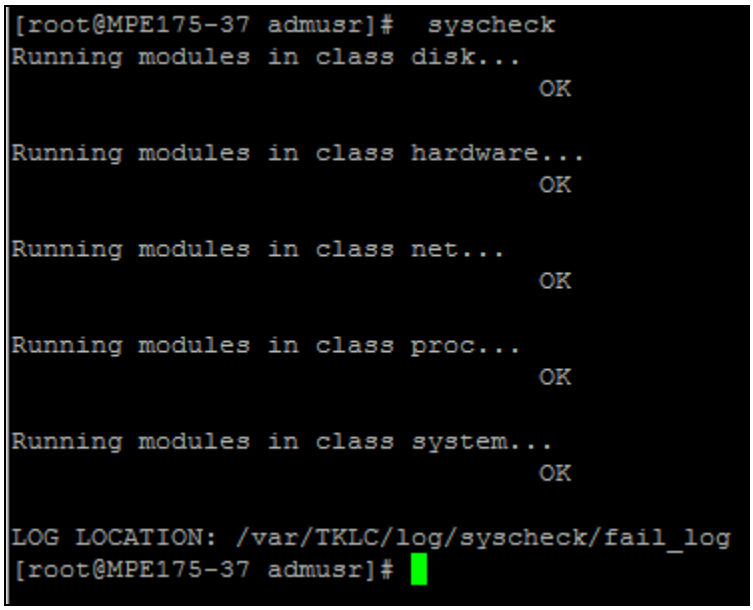
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 45 minutes per blade.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

**Procedure 12: Back-out Partially Upgraded MPE/MRA Cluster**

| Step | Procedure | Details |
|---|---|---|
| 1. ☐ | **CMP GUI:** Verify the status of affected Clusters | Navigate to **Upgrade → Upgrade Manager**.<br>Confirm status of the cluster to be backed out:<br>• Primary Active CMP is on Release 12.6<br>• Target Cluster has 2 servers on Release 12.5.0/12.5.0.4, and 1 server on Release 12.6<br>• Active server is on 12.5.0/12.5.0.4 |
| 2. ☐ | **MPE/MRA SSH:** Verify `/var/log/messages` file size | 1. Using SSH, log into the Standby server to be backed out as admusr.<br>`$ ls -lh /var/log/messages`<br>2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |
| 3. ☐ | **CMP GUI:** Verify the status of affected Clusters<br>**NOTE:** This takes approximately30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the partially upgraded cluster to back-out.<br>3. Select the cluster (one cluster at a time) (can be an MRA or MPE)<br>4. Click Start Rollback. When hovering over the button, it indicates the server to get backed out.<br>  <br>5. Click **OK** to confirm and continue with the operation. It begins to back-out.<br>Follow the progress status in the Upgrade Operation column.<br>During the back-out activities, the following alarms may be generated and are |

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

| Step | Procedure | Details |
|---|---|---|
| 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`**:<br>`$ sudo syscheck`<br>  <br>2. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>3. **NOTE:** Permissions should be the following,<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>4. If the permissions are not as listed above then perform the following; otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>5. Verify:<br>`$ ls -l /`<br>6. Perform **`syscheck`** again:<br>`$ sudo syscheck` |

| Step | Procedure | Details |
|---|---|---|
| 5. ☐ | **MPE/MRA CLI:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the upgrade is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.<br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>4. Find eth02.<br>5. Change from `primary=eth02` to `primary=eth01`<br>6. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| **—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 12.5.0/12.5.0.4 (MRA, MPE, CMP) with Active, Standby status.

Expected pre-conditions:

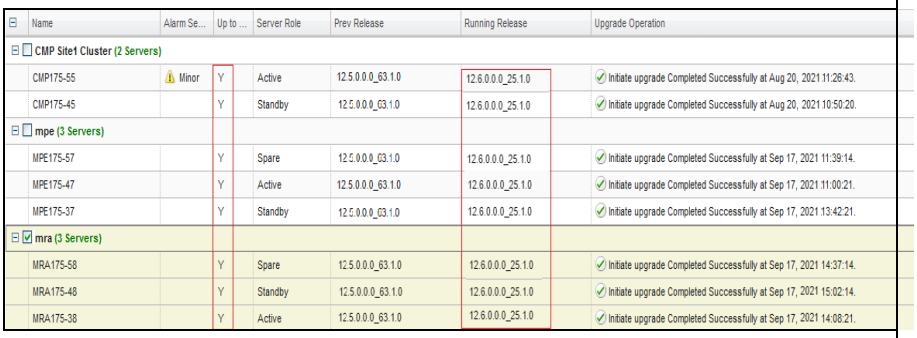
1. Primary Active CMP is on Release 12.6
2. Cluster is of MPE or MRA
3. Servers of target cluster are on Release 12.6 in either in Active, Standby, Force Standby or Spare role

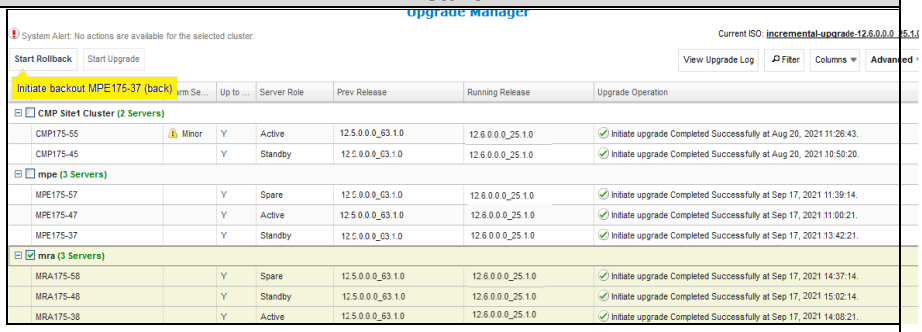
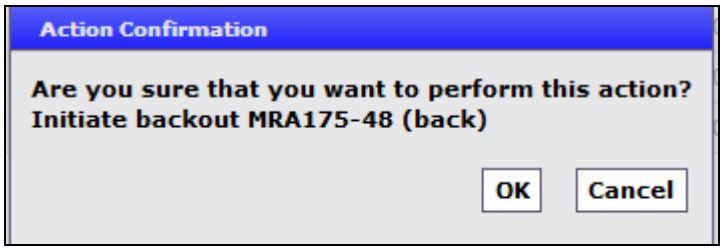
**NOTES:**

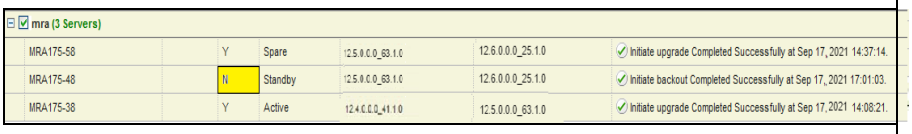
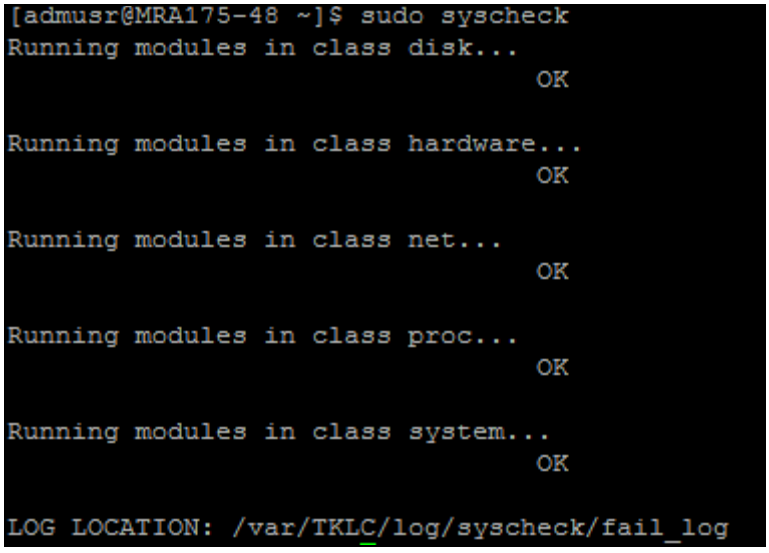
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes per MPE or MRA cluster.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

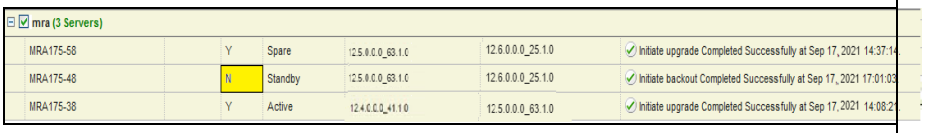
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

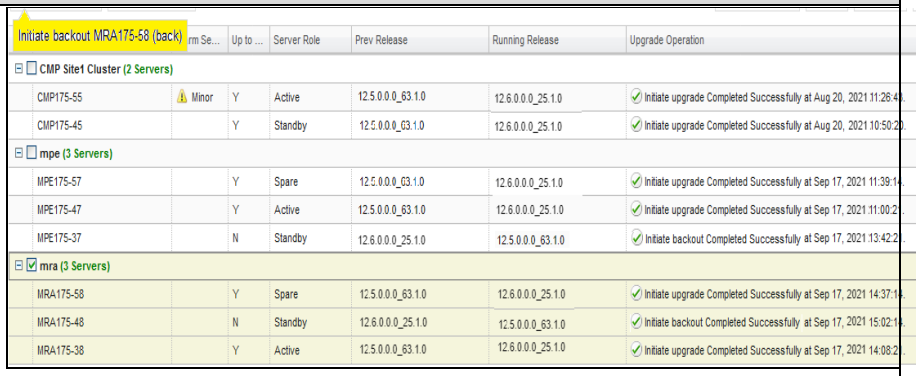
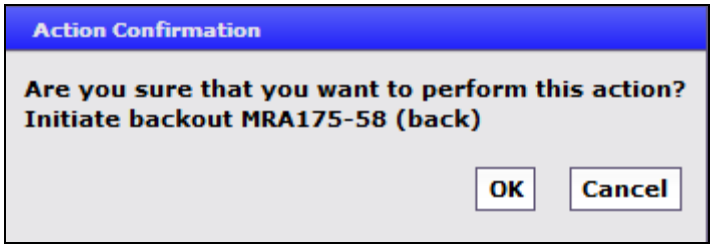
**Procedure 13 Back-out Fully Upgraded MPE/MRA Cluster**

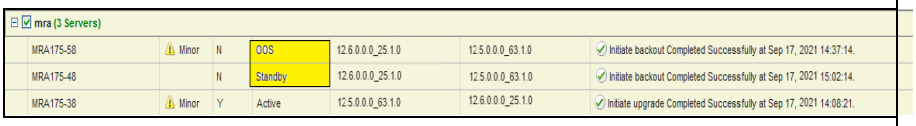
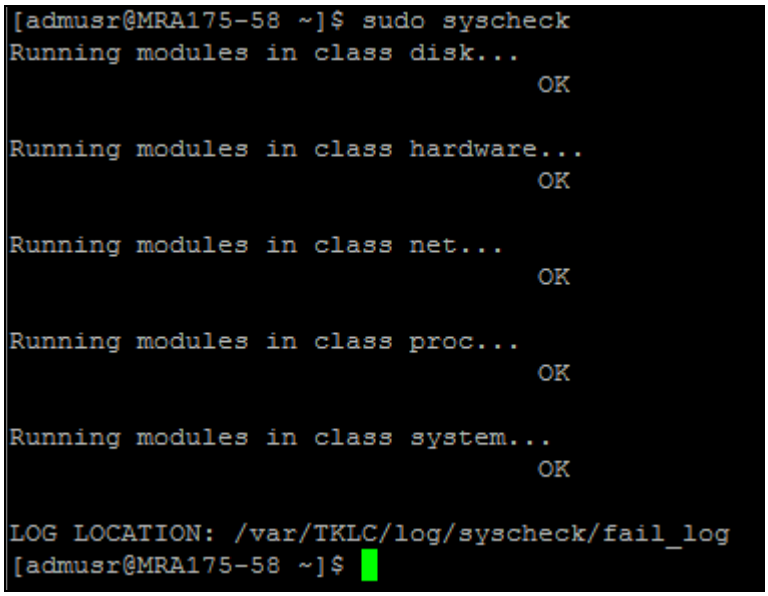
| Step | Procedure | Details |
|---|---|---|
| 1. ☐ | **CMP GUI:** Verify the status of affected Clusters | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Confirm status of the cluster is backed out:<br>- Primary Active CMP is on Release 12.6<br>- MPE/MRA is on Release 12.6 Up to Date column shows Y for all servers<br>**EXAMPLE:**<br>  |
| 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.<br>2. **NOTE:** Currently Active server is checked after the failover later on in this procedure.<br>`$ ls -lh /var/log/messages`<br>3. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>4. Verify:<br>`$ ls -lh /var/log/messages` |
| 3. ☐ | **CMP GUI:** Initiate Back-out<br>**NOTE:** Each back-out of one blade server completes in approximately30 minutes.<br>**NOTE:** Up to 16 clusters can be backed out at the same time, selecting one at | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the cluster (one cluster at a time, can be an MRA or MPE).<br>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. |

| Step | Procedure | Details |
|---|---|---|
| | a time. |  <br>4. Click **OK** to confirm and continue with the operation. It begins to back-out.<br>  <br>Follow the progress status in the Upgrade Operation column.<br>At this point, the server backing out goes into OOS state.<br>Wait until the server goes to an OOS state before selecting the next cluster to back-out.<br>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.<br>**Expected Critical Alarms**<br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br>**70028** Signaling bonded interface is down<br>**31283** High availability server is offline<br>**Expected Major Alarms**<br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br>**Expected Minor Alarms**<br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31282** The HA manager (cmha) is impaired by a s/w fault<br>**31232** High availability server has not received a message …. |

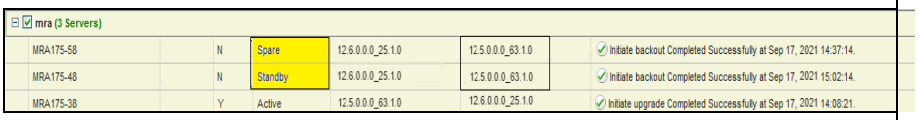
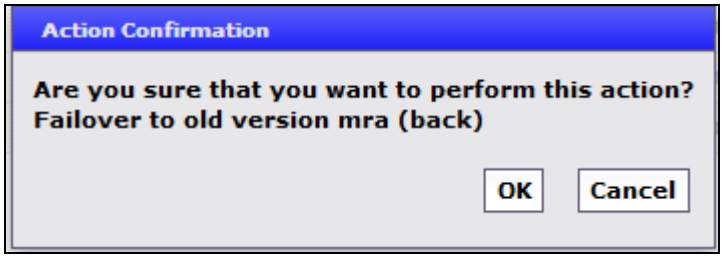
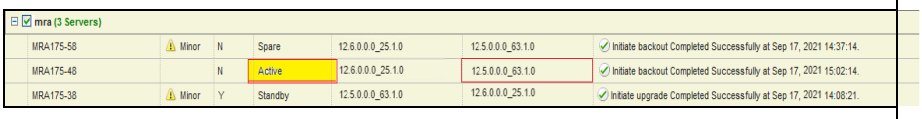
| Step | Procedure | Details |
|---|---|---|
| | | **31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31104** DB Replication latency has exceeded thresholds<br>**78001** Transfer of Policy jar files failed<br>**70500** The system is running difference versions of software<br>**31100** The DB replication process is impaired by a s/w fault<br>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 12.5.0/12.5.0.4 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.<br>  |
| 4. ☐ | **CMP GUI:** Verify the back-out is successful | 1. Select the partially backed out cluster<br>2. Select the View Upgrade LOG<br>  <br>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`**:<br>`$ sudo syscheck`<br>  <br>2. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>3. **NOTE:** Permissions should be the following,<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>4. If the permissions are not as listed above then perform the following |

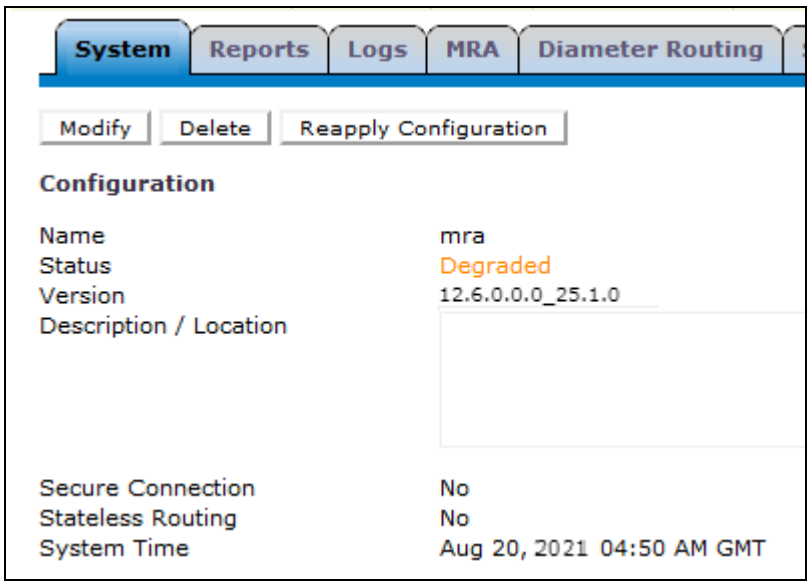
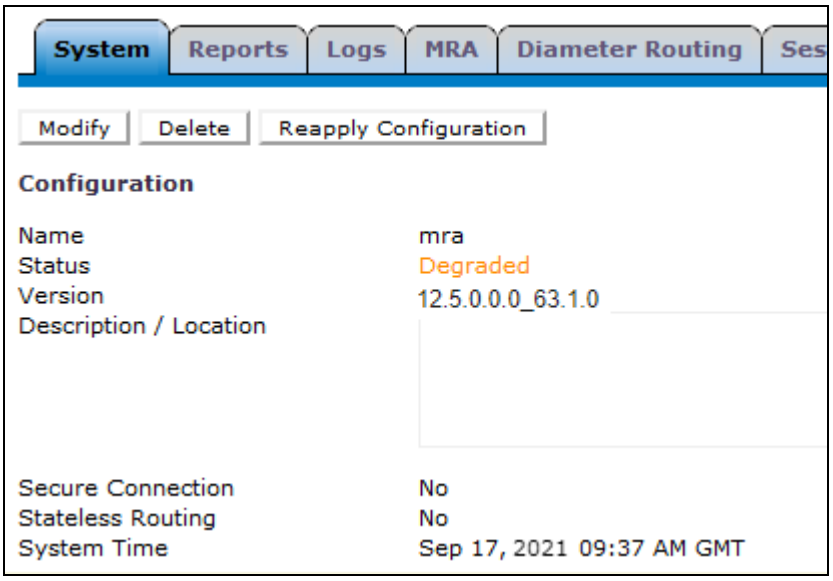
| Step | Procedure | Details |
|---|---|---|
| | | otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>5. Verify:<br>`$ ls -l /`<br>6. Perform **syscheck** again:<br>`$ sudo syscheck` |
| 6. ☐ | **MPE/MRA CLI:** Verify eth01 is primary device interface | This step only applies if the backed-out Standby server has a condition in which after the upgrade is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.<br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>4. Find eth02.<br>5. Change from primary=eth02 to primary=eth01<br>6. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 7. ☐ | Confirm MPE/MRA server status | Ensure that the Active/Spare are on 12.6 and the standby server shows running release of 12.5.0/12.5.0.4. Note: first version column is Prev Release, and second version column is Running Release.<br>  |
| 8. ☐ | **CMP GUI:** Continue the back-out of the MRA / MPE clusters. Next operation is Initiate Back-out on spare server<br>**NOTE:** Up to 16 clusters can be backed out at the same time, | 1. Select the cluster (one cluster at a time) (can be an MRA or MPE)<br>2. Click **Continue Rollback**. When hovering over the button, it indicates to initiate Back-out. |

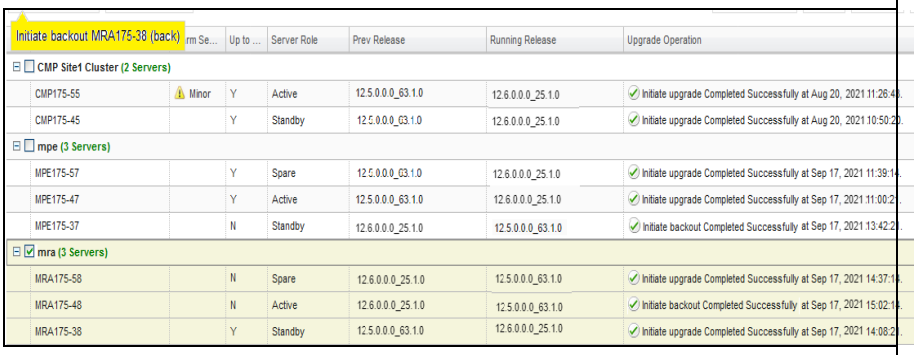
| Step | Procedure | Details |
|---|---|---|
| | selecting one at a time.<br><br>**NOTE:** This takes approximately 30 minutes to complete. |  <br>3. Click **OK** to confirm and continue with the operation.<br>  <br>Wait until the server goes to an OOS state before selecting the next cluster.<br><br>Follow the progress status in the Server Role column. The Server shows OOS in the server role until the back-out completes.<br><br>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.<br><br>**Expected Critical Alarms**<br><br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br>**70028** Signaling bonded interface is down<br>**31283** High availability server is offline<br><br>**Expected Major Alarms**<br><br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31282** The HA manager (cmha) is impaired by a s/w fault<br>**31232** High availability server has not received a message …. |

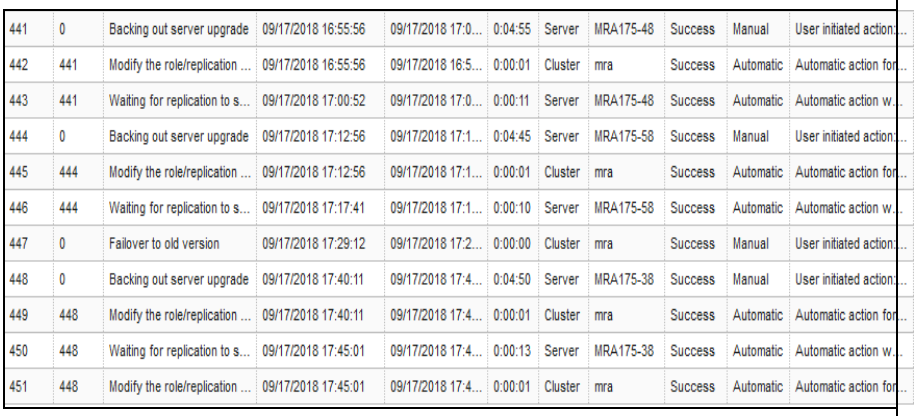
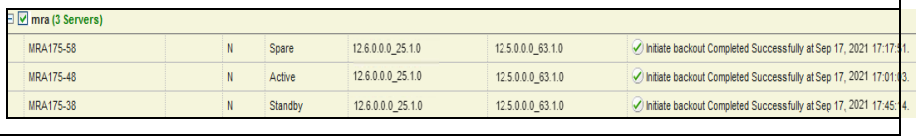
| Step | Procedure | Details |
|---|---|---|
| | | **31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31104** DB Replication latency has exceeded thresholds<br>**78001** Transfer of Policy jar files failed<br>**70500** The system is running difference versions of software<br>**31100** The DB replication process is impaired by a s/w fault<br>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 12.5.0/12.5.0.4. Note: first version column is Prev Release, and second version column is Running Release.<br>  |
| 9. ☐ | **MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission | 1. Login to the backed-out Spare server as admusr.<br>2. Verify that there are not anyt any failures in **`syscheck`**:<br>`$ sudo syscheck`<br>  <br>3. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>4. **NOTE:** Permissions should be the following,<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>5. If the permissions are not as listed above then perform the following otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>6. Verify: |

| Step | Procedure | Details |
|---|---|---|
| | | `$ ls -l /`<br>7. Perform **syscheck** again:<br>`$ sudo syscheck` |
| 10. ☐ | **MPE/MRA CLI:** Verify eth01 is primary device interface | This step only applies if the backed-out Spare server has a condition in which after the back-out is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.<br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>4. Find eth02.<br>5. Change from `primary=eth02` to `primary=eth01`<br>6. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |

| Step | Procedure | Details |
|---|---|---|
| 11. ☐ | **CMP GUI:** Continue the back-out of the MRA / MPE clusters. Next operation is failover to the 12.5.0/12.5.0.4 server.<br><br>**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.<br>- Active Server is on Release 12.5.0/12.5.0.4<br>- Standby Server is on Previous release<br>- Spare Server is on Previous release<br>1. Select the cluster (one cluster at a time) (can be an MRA or MPE)<br>2. Click **Continue Rollback**. When hovering over the button, it informs you to failover to old version, which is 12.5.0/12.5.0.4<br>  <br>3. Click **OK** to confirm and continue with the operation. It begins to failover.<br>  <br>Wait until the server fails over before selecting the next cluster. This takes approximately 2 minutes<br><br>**Expected Critical Alarms**<br><br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br><br>**Expected Major Alarms**<br><br>**74603** The number of failed MPE primary cluster reaches the threshold<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**31102** DB replication from a master DB has failed<br>**71402** Diameter Connectivity Lost<br>**31101** DB replication to a slave DB has failed<br>**78001** Transfer of Policy jar files failed<br>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.<br>  |
| 12. ☐ | **CMP GUI:** Reapply Configuration on MPE/MRA | • MPE<br>Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ System** |

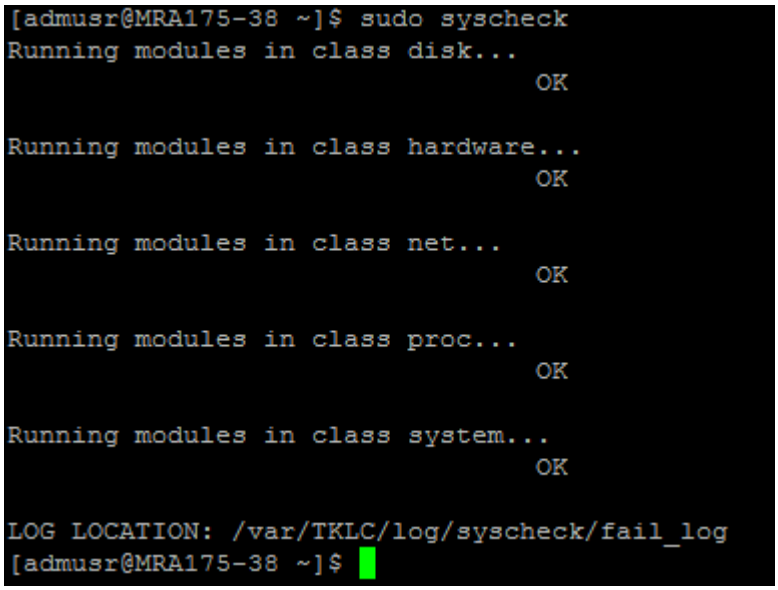
| Step | Procedure | Details |
|---|---|---|
| | cluster that competed the failover successfully | • MRA:<br>Navigate to **MRA → Configuration → <*mra_cluster name*> → System**<br>The selected Cluster status is Degraded as expected as shown:<br>  <br>Click **Reapply Configuration**.<br>Note the Version is successfully changed to the upgraded Release 12.5.0/12.5.0.4.<br>**NOTE:** The status be Degraded which is a normal reporting event as the servers are in different status.<br>**MPE:**<br>  |
| 13. ☐ | **MPE/MRA SSH:** Verify `/var/log/messa` | 1. Using SSH, log into the Standby server to be backed out as admusr.<br>`$ ls -lh /var/log/messages` |

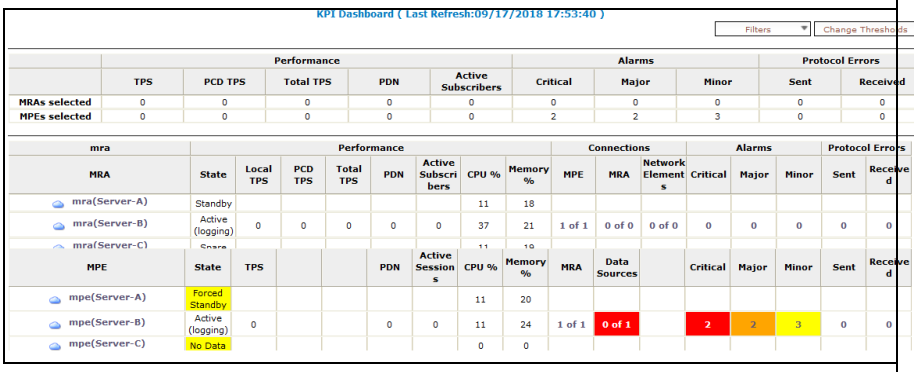
| Step | Procedure | Details |
|---|---|---|
| | `ges` file size | 2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |
| 14. ☐ | **CMP GUI:** Complete Back-out of cluster(s)<br>**NOTE:** Up to 16 clusters can be backed out at the same time, selecting one at a time.<br>**NOTE:** Each back-out of a one blade server completes in approximately 30 minutes | 1. Select the cluster (one cluster at a time) (can be an MRA or MPE)<br>2. Click **Continue Rollback**. When hovering over the button, it indicates the back-out server.<br>  <br>3. Click **OK** to confirm and continue with the operation. It begins to back-out.<br>Follow the progress status in the Upgrade Operation column.<br>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.<br>**Expected Critical Alarms**<br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br>**70028** Signaling bonded interface is down<br>**31283** High availability server is offline<br>**Expected Major Alarms**<br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br>**Expected Minor Alarms**<br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31101** DB replication to a slave DB has failed |

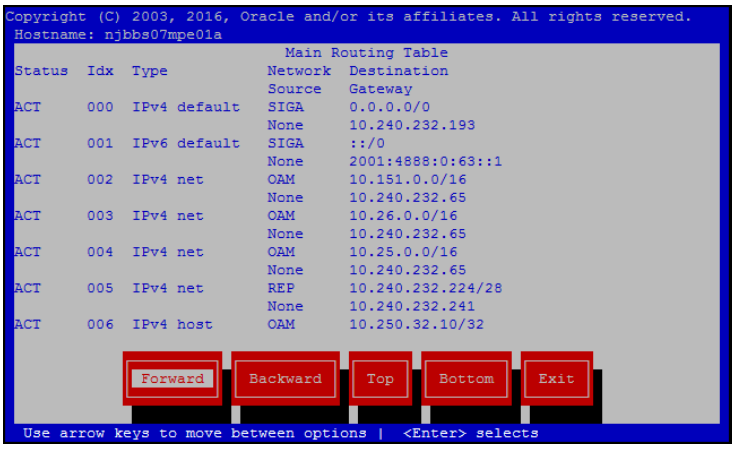
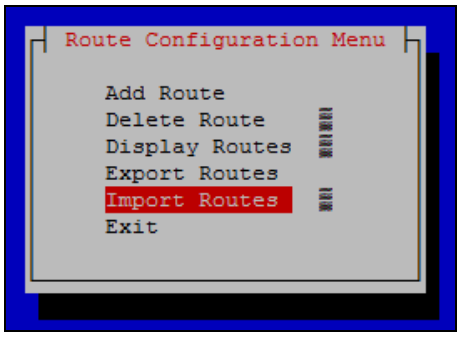
| Step | Procedure | Details |
|---|---|---|
| | | **31102** DB replication from a master DB has failed<br>**31282** The HA manager (cmha) is impaired by a s/w fault<br>**31232** High availability server has not received a message<br>**31284** High availability remote subscriber has not received a heartbeat<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31104** DB Replication latency has exceeded thresholds<br>**78001** Transfer of Policy jar files failed<br>**70500** The system is running difference versions of software<br>**31100** The DB replication process is impaired by a s/w fault<br>Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column.<br>Verify in Upgrade Log that that back-out was successful:<br>  <br>All of the servers is on Release 12.5.0/12.5.0.4 at this point and show active/standby/spare. Note: first version column is Prev Release, and second version column is Running Release.<br>  |

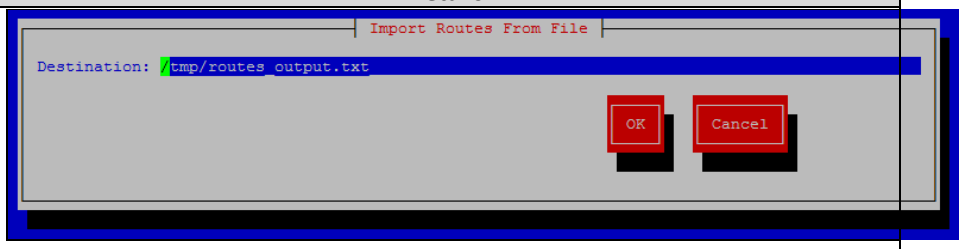
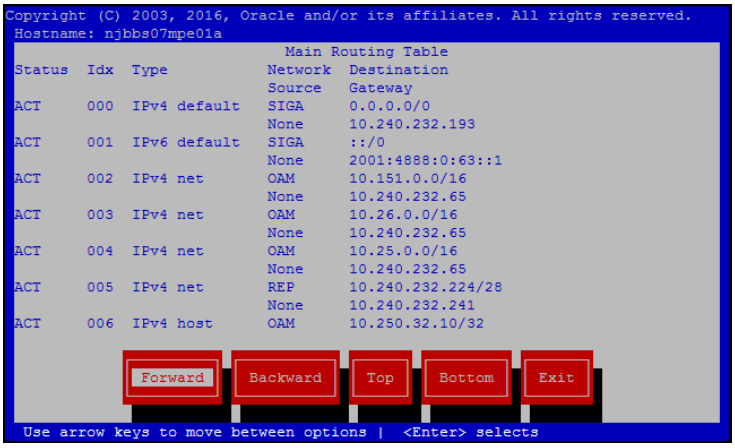
| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 441 | 0 | Backing out server upgrade | 09/17/2018 16:55:56 | 09/17/2018 17:0... | 0:04:55 | Server | MRA175-48 | Success | Manual | User initiated action:... |
| 442 | 441 | Modify the role/replication ... | 09/17/2018 16:55:56 | 09/17/2018 16:5... | 0:00:01 | Cluster | mra | Success | Automatic | Automatic action for... |
| 443 | 441 | Waiting for replication to s... | 09/17/2018 17:00:52 | 09/17/2018 17:0... | 0:00:11 | Server | MRA175-48 | Success | Automatic | Automatic action w... |
| 444 | 0 | Backing out server upgrade | 09/17/2018 17:12:56 | 09/17/2018 17:1... | 0:04:45 | Server | MRA175-58 | Success | Manual | User initiated action:... |
| 445 | 444 | Modify the role/replication ... | 09/17/2018 17:12:56 | 09/17/2018 17:1... | 0:00:01 | Cluster | mra | Success | Automatic | Automatic action for... |
| 446 | 444 | Waiting for replication to s... | 09/17/2018 17:17:41 | 09/17/2018 17:1... | 0:00:10 | Server | MRA175-58 | Success | Automatic | Automatic action w... |
| 447 | 0 | Failover to old version | 09/17/2018 17:29:12 | 09/17/2018 17:2... | 0:00:00 | Cluster | mra | Success | Manual | User initiated action:... |
| 448 | 0 | Backing out server upgrade | 09/17/2018 17:40:11 | 09/17/2018 17:4... | 0:04:50 | Server | MRA175-38 | Success | Manual | User initiated action:... |
| 449 | 448 | Modify the role/replication ... | 09/17/2018 17:40:11 | 09/17/2018 17:4... | 0:00:01 | Cluster | mra | Success | Automatic | Automatic action for... |
| 450 | 448 | Waiting for replication to s... | 09/17/2018 17:45:01 | 09/17/2018 17:4... | 0:00:13 | Server | MRA175-38 | Success | Automatic | Automatic action w... |
| 451 | 448 | Modify the role/replication ... | 09/17/2018 17:45:01 | 09/17/2018 17:4... | 0:00:01 | Cluster | mra | Success | Automatic | Automatic action for... |

| | | | | | |
|---|---|---|---|---|---|
| mra (3 Servers) | | | | | |
| MRA175-58 | N | Spare | 12.6.0.0.0_25.1.0 | 12.5.0.0.0_63.1.0 | Initiate backout Completed Successfully at Sep 17, 2021 17:17:51. |
| MRA175-48 | N | Active | 12.6.0.0.0_25.1.0 | 12.5.0.0.0_63.1.0 | Initiate backout Completed Successfully at Sep 17, 2021 17:01:03. |
| MRA175-38 | N | Standby | 12.6.0.0.0_25.1.0 | 12.5.0.0.0_63.1.0 | Initiate backout Completed Successfully at Sep 17, 2021 17:45:14. |

| Step | Procedure | Details |
|---|---|---|
| 15. ☐ | **MPE/MRA SSH:** Verify **`syscheck`** and `/tmp` directory permission | 1. Login to the backed-out Standby server as admusr.<br>2. Verify that there are not any failures in **`syscheck`**:<br>`$ sudo syscheck`<br>  <br>3. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>4. **NOTE:** Permissions should be the following,<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>5. If the permissions are not as listed above then perform the following otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>6. Verify:<br>`$ ls -l /`<br>7. Perform **`syscheck`** again:<br>`$ sudo syscheck` |

| Step | Procedure | Details |
|---|---|---|
| 16. ☐ | **MPE/MRA CLI:** Verify eth01 is primary device interface | This step only applies if the backed-out Standby server has a condition in which after the back-out is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable to the case where primary is set to eth02.<br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>4. Find eth02.<br>5. Change from primary=eth02 to primary=eth01<br>6. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 17. ☐ | **CMP GUI:** Verify that backed out cluster is processing traffic normally. | Verify Cluster is processing traffic normally:<br>Navigate to **System Wide Reports → KPI Dashboard**.<br>  |
| 18. ☐ | **CMP GUI:** Verify alarms | 1. Navigate to **System Wide Reports → Alarms → Active Alarms**.<br>2. Verify that there are not any unexpected active alarms present.<br>**NOTE:** Some Alarms take approximately 30 minutes to 1 hour to auto clear.<br>***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.*** |
| 19. ☐ | **MPE/MRA SSH:** Verify routes | 1. Login into MPE/MRA server as admusr<br>2. Copy routes_output.txt from /home/admusr to /tmp<br>`$ sudo cp routes_output.txt /tmp` |

| Step | Procedure | Details |
|---|---|---|
| | | `$ cd /tmp`<br>`$ ls`<br>`routes_output.txt`<br><br>**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.**<br><br>3. Run the platcfg utility:<br>`$ sudo su - platcfg`<br>4. Navigate to **Policy Configuration → Routing Config → Display Routes**.<br>5. Verify that all routes are present.<br>6. Click **Forward** to view all the routes.<br>**Example:**<br>  <br><br>7. If any of the routes are missing then perform the following otherwise skip to step 20<br>8. Navigate back to **Route Configuration Menu** and select **Import Routes**.<br>  <br><br>9. Click **OK**. |

| Step | Procedure | Details |
|---|---|---|
| | |  <br>10. Routes is imported from `/tmp/routes_output.txt` file and **Route Configuration Menu** is displayed again.<br>11. Select **Display Routes**.<br>12. Verify that all routes are present.<br>13. Click **Forward** to view all the routes.<br>**Example:**<br>  <br>14. Exit the platcfg utility<br>**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.** |
| 20. ☐ | Repeat for other clusters as needed | Repeat this procedure for remainder of MPE/MRA servers, if not fully backed out yet. |
| 21. ☐ | 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.<br>1. Navigate to **System Wide Reports → Alarms → Active Alarms**.<br>2. Verify that there are not any unexpected active alarms present.<br>**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:

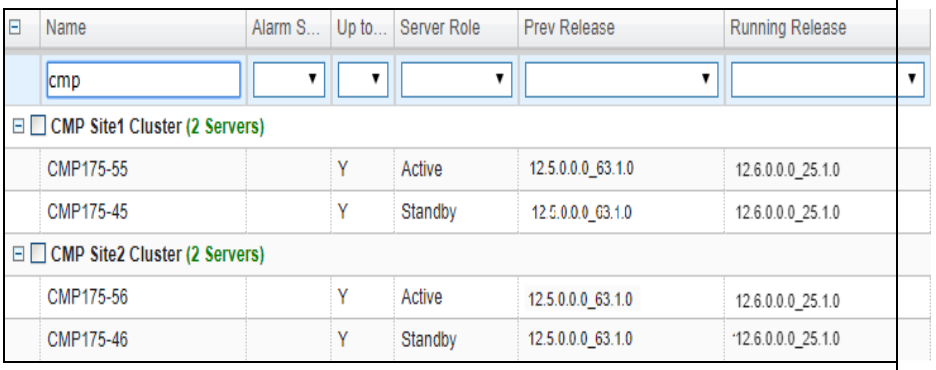
1. Primary Active CMP is on Release 12.6
2. Secondary CMP cluster is on Release 12.6
3. All MPE/MRA Clusters are on Release 12.5.0/12.5.0.4

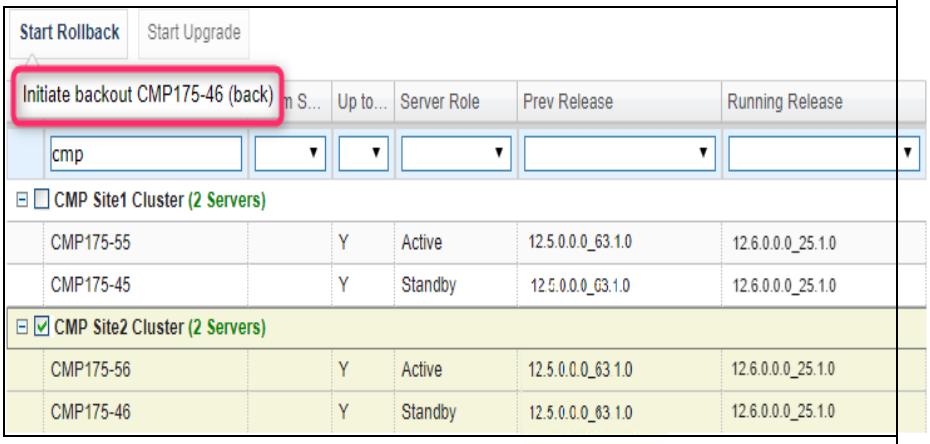
**NOTES:**

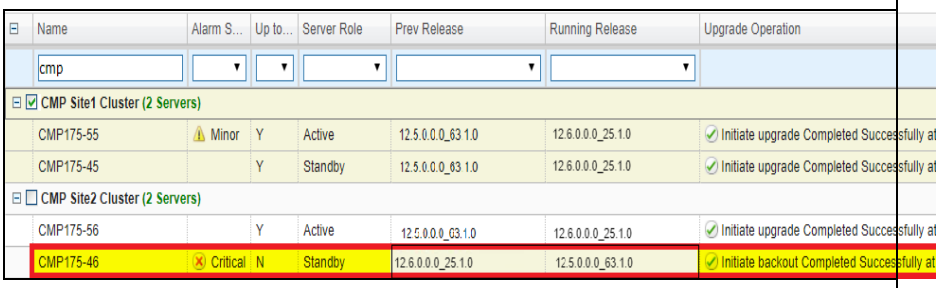
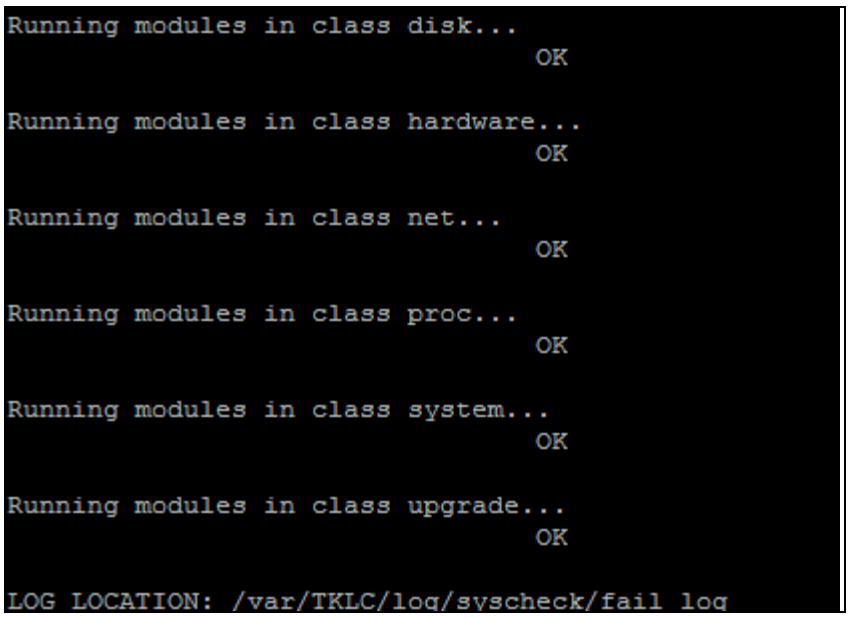
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

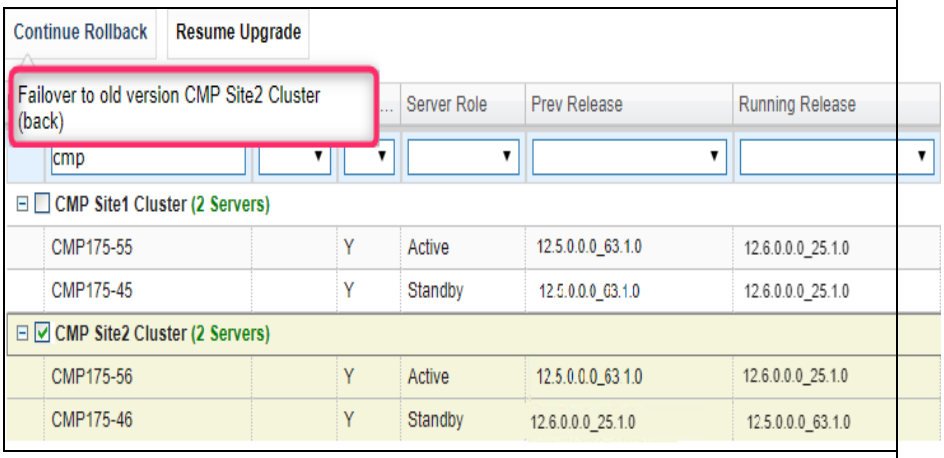
**Procedure 14: Back-out Fully Upgraded Secondary CMP cluster**

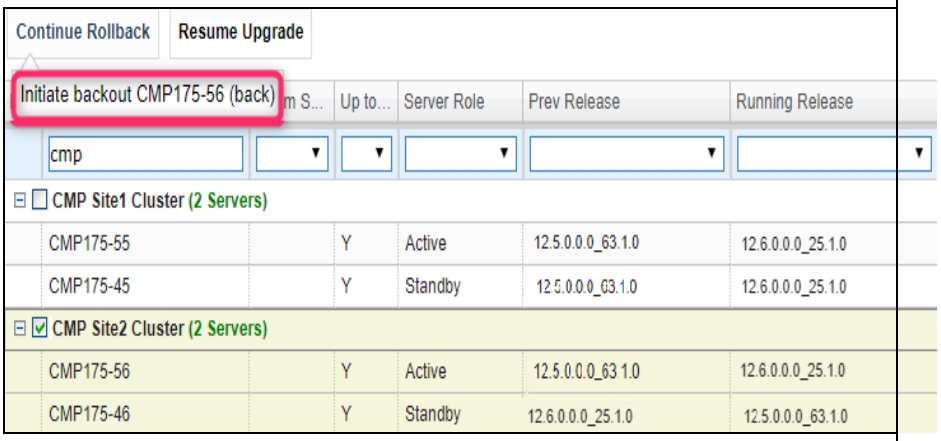
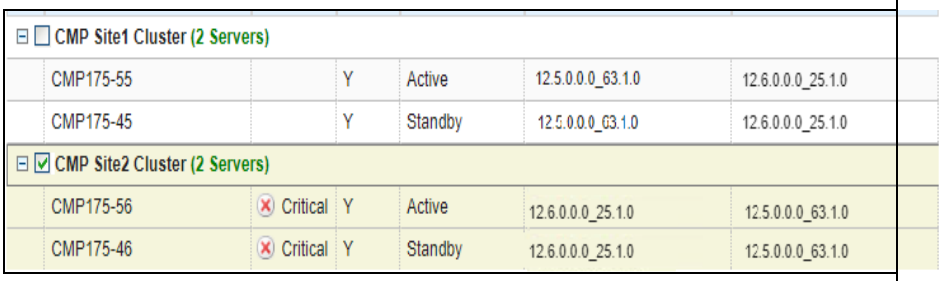
<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>1. ☐</td><td>CMP GUI: Verify the status of CMP clusters</td><td>1. Navigate to Upgrade → Upgrade Manager.<br>2. Confirm status of the cluster to be backed out:<br>- Primary Active CMP is on Release 12.6<br>- Secondary CMP cluster is on Release 12.6<br>- Up to Date column shows Y for all servers<br>3. Click Filter and enter <code>cmp</code> in the Name field.<br>Example:<br> 
</td></tr>
<tr><td>2. ☐</td><td>CMP SSH: Verify <code>/var/log/messages</code> file size</td><td>1. Using SSH, log into the Standby server to be backed out as admusr<br><code>$ ls -lh /var/log/messages</code><br>2. ONLY if the resulting size of <code>/var/log/messages</code> is above 20M, run the following, otherwise proceed to the next step.<br><code>$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out</code><br><code>$ sudo cat /dev/null > /var/log/messages</code><br><code>$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"</code><br>3. Verify:</td></tr>
</table>

| Step | Procedure | Details |
|---|---|---|
| | | `$ ls -lh /var/log/messages` |
| 3. ☐ | **CMP GUI:** Back-out clusters<br><br>**NOTE:** Each back-out of one server takes about 30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Secondary CMP cluster<br>3. Click **Start Rollback**. When hovering over the button, it indicates the back-out server.<br>  <br><br>4. Click **OK** to confirm and continue with the operation. It begins to back-out. Server goes into an OOS server Role<br><br>Follow the progress status in the Upgrade Operation column.<br><br>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.<br><br>**Expected Critical Alarms**<br><br>**70001** The qp_procmgr process has failed.<br>**31227** The high availability status is failed due to raised alarms<br>**31283** High availability server is offline<br>**70025** The MySQL slave has a different schema version than the master<br><br>**Expected Major Alarms**<br><br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br>**70021** The MySQL slave is not connected to the master<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31232** High availability server has not received a message<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed |

| Step | Procedure | Details |
|---|---|---|
| | | **31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31106** DB merging to the parent Merge Node has failed<br>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 running release of 12.5.0/12.5.0.4.<br>  |
| 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`**:<br>`$ sudo syscheck`<br>  <br>2. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>3. **NOTE:** Permissions should be the following:<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>4. If the permissions are not as listed above then perform the following otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>5. Verify: |

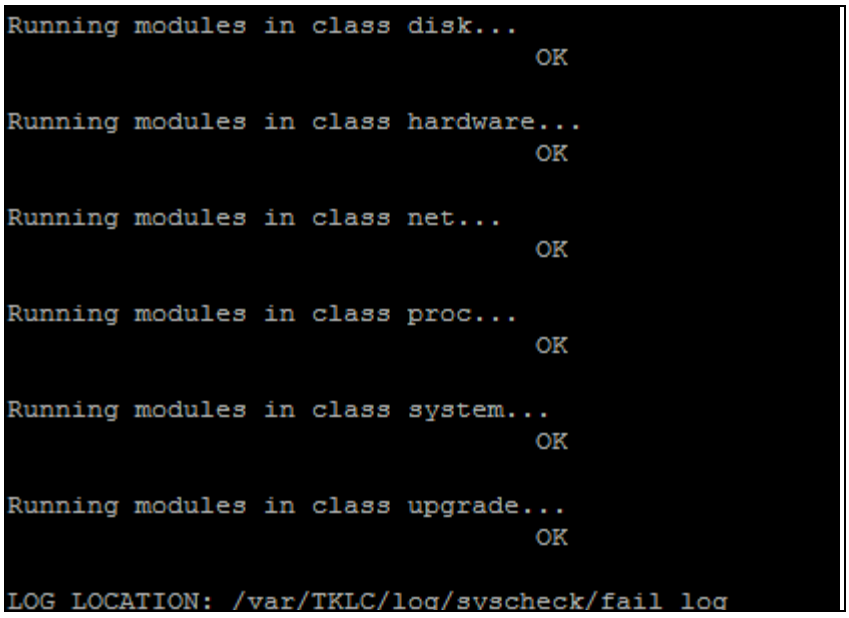
| Step | Procedure | Details |
|---|---|---|
| | | `$ ls -l /`<br>6. Perform **`syscheck`** again:<br>`$ sudo syscheck` |
| 5. ☐ | **CMP SSH:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary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

| Step | Procedure | Details |
|---|---|---|
| 6. ☐ | **CMP GUI:** Continue the back-out. Next operation is failover. | 1. Select Secondary CMP cluster.<br>2. Navigate to **Upgrade → Upgrade Manager**.<br>3. Select the Secondary CMP cluster<br>4. Click **Continue Rollback**. When hovering over the button, it informs you to failover.<br>  <br><br>5. Click **OK** to confirm and continue with the operation. It begins to failover.<br>Follow the progress status in the Server Role column. Wait for the server to show standby.<br>**Expected Critical Alarms**<br>**70001** The qp_procmgr process has failed.<br>**31227** The high availability status is failed due to raised alarms<br>**31283** High availability server is offline<br>**70025** The MySQL slave has a different schema version than the master<br>**74604** Policy cluster is offline<br>**Expected Major Alarms**<br>**70004** The QP processes have been brought down for maintenance<br>**31233** High availability path loss of connectivity<br>**70021** The MySQL slave is not connected to the master<br>**Expected Minor Alarms**<br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31232** High availability server has not received a message<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31106** DB merging to the parent Merge Node has failed<br>**70500** The system is running different versions of software |

| Step | Procedure | Details |
|---|---|---|
| 7. ☐ | **CMP SSH:** Verify `/var/log/messages` file size | 1. Using SSH, log into the Standby server to be backed out as admusr.<br>`$ ls -lh /var/log/messages`<br>2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |
| 8. ☐ | **CMP GUI:** Continue the backed-out. Next operation is Initiate Back-out<br>**NOTE:** Each back-out of one server takes about 30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Secondary CMP cluster.<br>3. Click **Continue Rollback**. When hovering over the button, it informs you to rollback.<br>  <br>4. Click **OK** to confirm and continue with the operation. It begins to failover.<br>5. Follow the progress status in the Server Role column. Wait until the server to back-out comes to Standby state before continuing.<br>6. Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column.<br>  <br>**Expected Critical Alarms**<br>**70001** The qp_procmgr process has failed. |

| Step | Procedure | Details |
|---|---|---|
| | | **31227** The high availability status is failed due to raised alarms<br>**31283** High availability server is offline<br>**70025** The MySQL slave has a different schema version than the master<br><br>**Expected Major Alarms**<br><br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br>**70021** The MySQL slave is not connected to the master<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31232** High availability server has not received a message<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31106** DB merging to the parent Merge Node has failed<br>**70500** The system is running different versions of software<br>7. Verify in Upgrade Log that that back-out was successful:<br>8. All Secondary CMP servers is on Release 12.5.0/12.5.0.4 at this point and show active/standby |

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

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

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

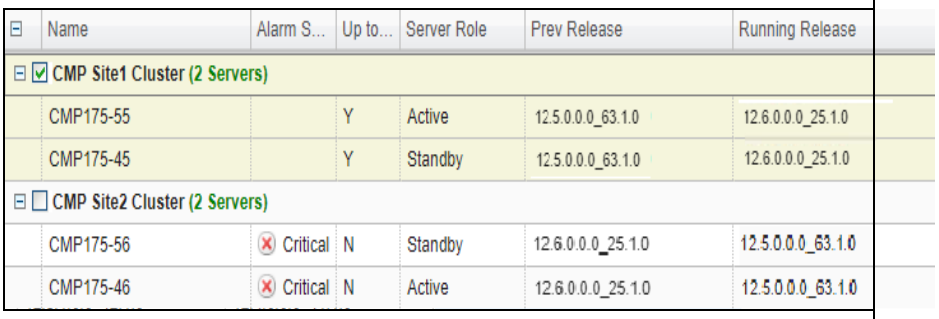
1. Primary Active CMP cluster is on Release 12.6.
2. Secondary CMP, MPE and MRA Clusters are on Release 12.5.0/12.5.0.4.

**NOTES:**

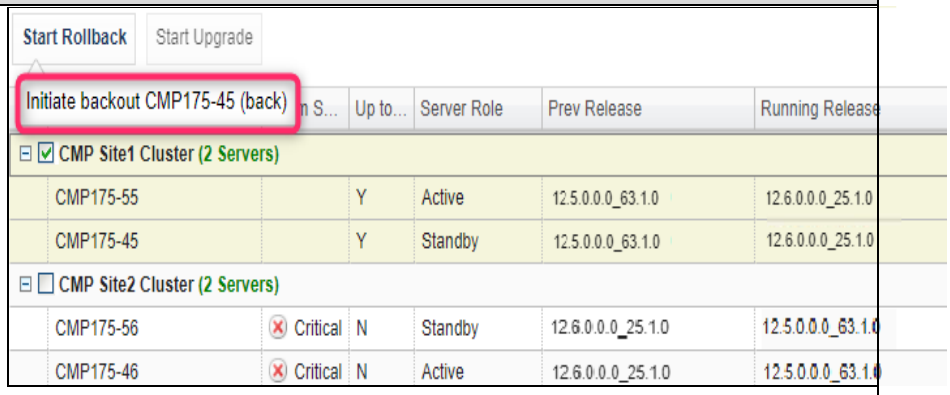
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

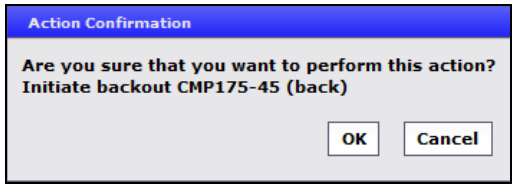
**Procedure 15: Back-out Fully Upgraded Primary CMP cluster**

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>1. ☐</td><td>CMP GUI: Verify the status of CMP clusters</td><td>1. Navigate to Upgrade → Upgrade Manager<br>2. Confirm status of the cluster to be backed out:<br>- Primary Active CMP is on Release 12.6<br>- Secondary CMP, MPE and MRA Clusters are on Release 12.5.0/12.5.0.4<br>- Up to Date column shows Y for all servers in Primary CMP cluster<br>- Click Filter and enter cmp in the Name field.<br>Example:<br> 
<table>
<tr><th></th><th>Name</th><th>Alarm S...</th><th>Up to...</th><th>Server Role</th><th>Prev Release</th><th>Running Release</th></tr>
<tr><td colspan="7">CMP Site1 Cluster (2 Servers)</td></tr>
<tr><td></td><td>CMP175-55</td><td></td><td>Y</td><td>Active</td><td>12.5.0.0.0_63.1.0</td><td>12.6.0.0.0_25.1.0</td></tr>
<tr><td></td><td>CMP175-45</td><td></td><td>Y</td><td>Standby</td><td>12.5.0.0.0_63.1.0</td><td>12.6.0.0.0_25.1.0</td></tr>
<tr><td colspan="7">CMP Site2 Cluster (2 Servers)</td></tr>
<tr><td></td><td>CMP175-56</td><td>Critical</td><td>N</td><td>Standby</td><td>12.6.0.0.0_25.1.0</td><td>12.5.0.0.0_63.1.0</td></tr>
<tr><td></td><td>CMP175-46</td><td>Critical</td><td>N</td><td>Active</td><td>12.6.0.0.0_25.1.0</td><td>12.5.0.0.0_63.1.0</td></tr>
</table></td></tr>
<tr><td>2. ☐</td><td>CMP SSH: Verify <code>/var/log/messages</code> file size</td><td>1. Using SSH, log into the Standby server to be backed out as admusr.<br><code>$ ls -lh /var/log/messages</code><br>2. ONLY if the resulting size of <code>/var/log/messages</code> is above 20M, run the following, otherwise proceed to the next step.<br><code>$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out</code><br><code>$ sudo cat /dev/null > /var/log/messages</code><br><code>$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"</code><br>3. Verify:<br><code>$ ls -lh /var/log/messages</code></td></tr>
<tr><td>3. ☐</td><td>CMP GUI: Back-out standby server of Primary CMP cluster<br>NOTE: Back-out of one server takes about 30 minutes to complete.</td><td>1. Select the Primary CMP cluster<br>2. Click Start Rollback. When hovering over the button, it indicates the server to back out.</td></tr>
</table>

| Step | Procedure | Details |
|---|---|---|



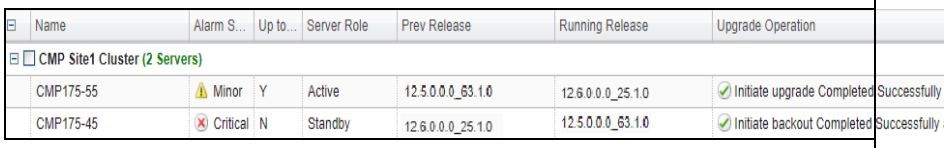

3. Click **OK** to confirm and continue with the operation. It begins to back-out.




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

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

**Expected Major Alarms**

**70004** The QP processes have been brought down for maintenance

**31236** High availability TCP link is down

**31233** High availability path loss of connectivity

**70021** The MySQL slave is not connected to the master

**Expected Minor Alarms**

**70503** The server is in forced standby

**70507** An upgrade/backout action on a server is in progress

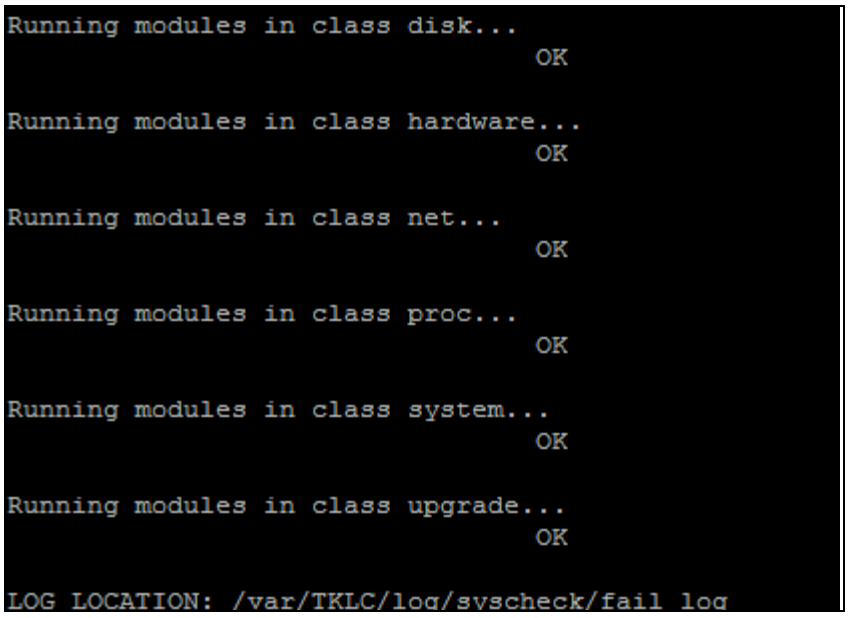
**70501** The Cluster is running different versions of software

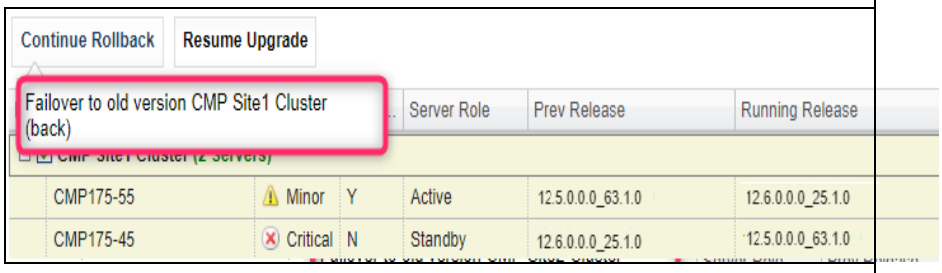
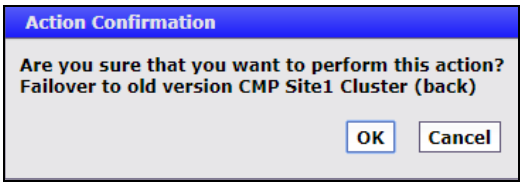
**31232** High availability server has not received a message

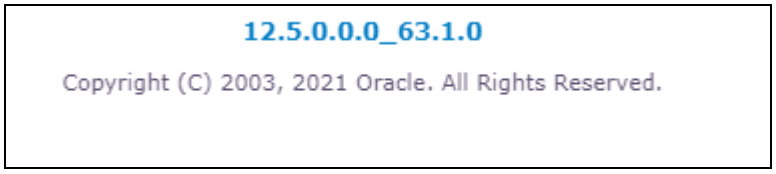
**31101** DB replication to a slave DB has failed

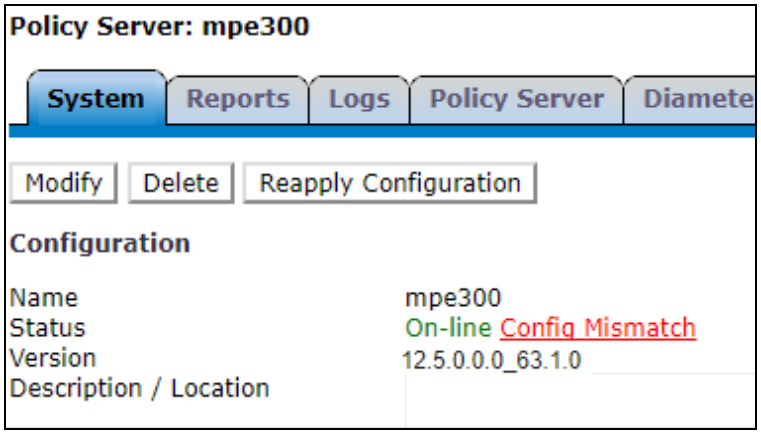
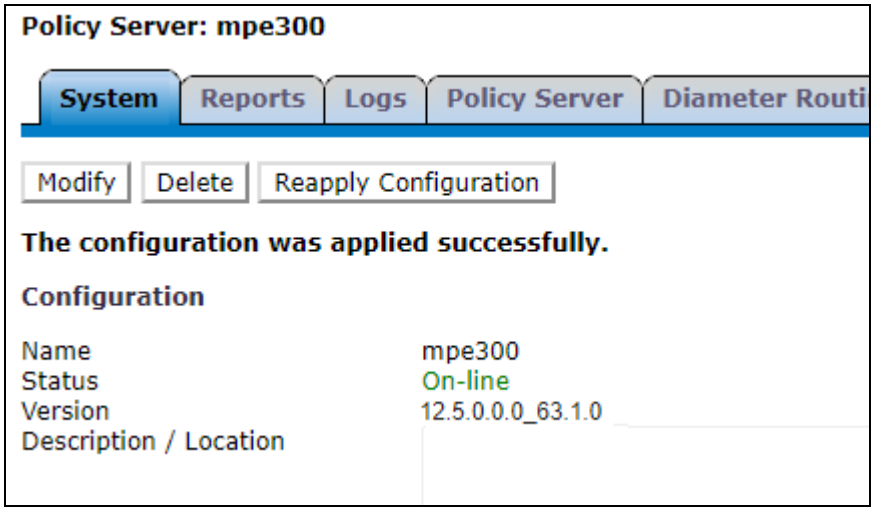
| Step | Procedure | Details |
|---|---|---|
| | | **31102** DB replication from a master DB has failed<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31106** DB merging to the parent Merge Node has failed<br>**70500** The system is running different versions of software<br>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 12.5.0/12.5.0.4 |

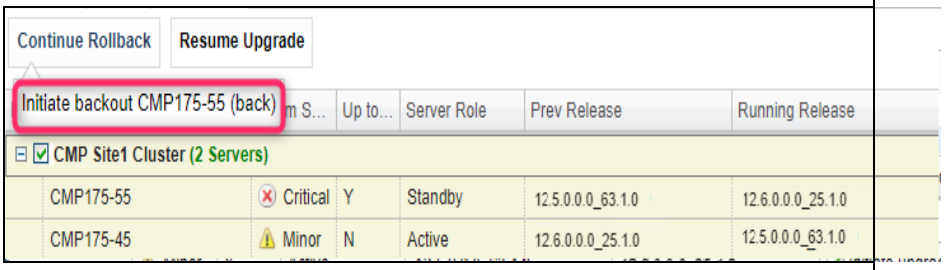
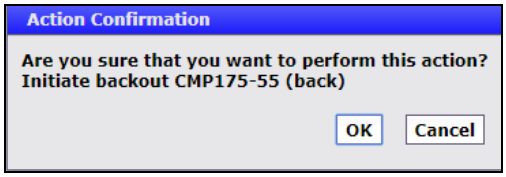
| Name | Alarm S... | Up to... | Server Role | Prev Release | Running Release | Upgrade O |
|---|---|---|---|---|---|---|
| CMP Site1 Cluster (2 Servers) | | | | | | |
| CMP175-55 | Minor | Y | Active | 12.5.0.0.0_63.1.0 | 12.6.0.0.0_25.1.0 | Initiate |
| CMP175-45 | Critical | N | Standby | 12.6.0.0.0_25.1.0 | 12.5.0.0.0_63.1.0 | Initiate |

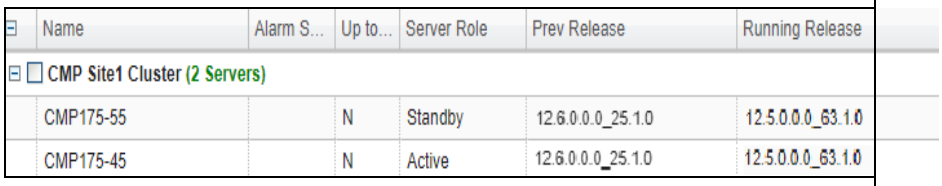
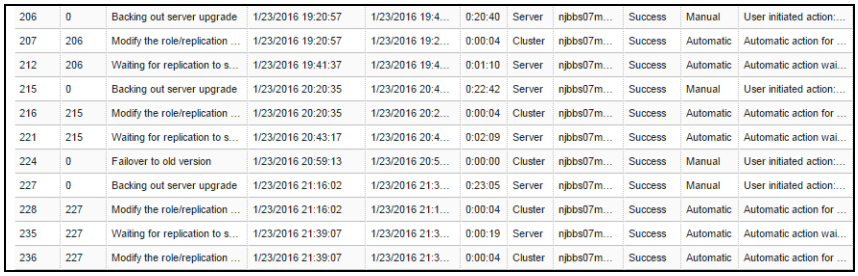
| Step | Procedure | Details |
|---|---|---|
| 4. ☐ | **CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission | 1. Login to the backed-out Server as admusr.<br>2. Verify that there are not any failures in **`syscheck`**:<br>`$ sudo syscheck`<br>  <br>3. Verify `/tmp` directory permissions: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

| Step | Procedure | Details |
|---|---|---|
| 5. ☐ | **CMP SSH:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br><br>To resolve this situation permanently, perform the following:<br><br>1. Login as admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.<br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>4. Find eth11.<br>5. Change from `primary=eth11` to `primary=eth01`<br>6. Save and exit (for example, vi uses ESC `:wq!`)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 6. ☐ | **CMP GUI:** Continue the back-out. Next operation is failover. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Primary CMP cluster.<br>3. Click **Continue Rollback**. When hovering over the button, it informs you to failover.<br>  <br>4. Click **OK** to confirm and continue with the operation. It begins to failover. The failover takes couple of minutes.<br>  <br>After a minute, you are required to log back in. |

| Step | Procedure | Details |
|---|---|---|
| 7. ☐ | **CMP GUI:** Log back into the Primary CMP VIP | After failover, you are required to log back in to the CMP GUI using the Primary CMP VIP.<br>  |
| 8. ☐ | CMP GUI: Verify previous Policy Management Release | 1. Navigate to **Help → About**.<br>2. Verify the release displayed is 12.5.0/12.5.0.4<br>  |

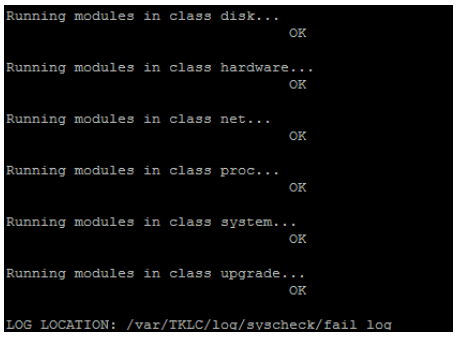
| Step | Procedure | Details |
|---|---|---|
| 9. ☐ | **CMP GUI:** If a Config Mismatch is observed on MPE or MRA | **MPE:**<br>Navigate to **Policy → Configuration →** <*mpe_cluster name*> **→ System**<br>**MRA:**<br>Navigate to **MRA → Configuration →** <*MRA Cluster*> **→ System**<br>  <br>Click **Reapply Configuration**.<br>Config Mismatch is resolves:<br>  |
| 10. ☐ | **CMP SSH:** Verify `/var/log/messages` file size | 1. Using SSH, log into the Standby server to be backed out as admusr.<br>`$ ls -lh /var/log/messages`<br>2. ONLY if the resulting size of /var/log/messages is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |

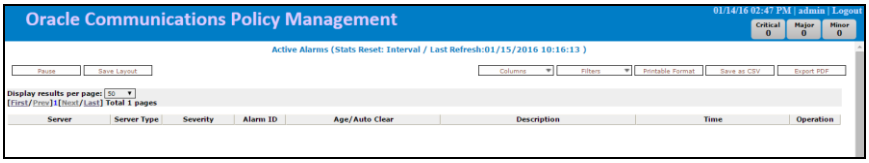
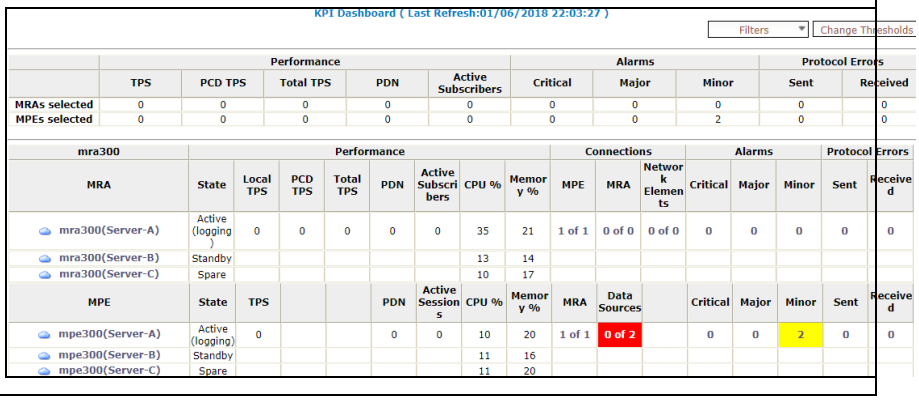
| Step | Procedure | Details |
|---|---|---|
| 11. ☐ | **CMP GUI:** Continue the back-out of the Primary CMP cluster<br><br>**NOTE:** Back-out of one server takes about 30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Primary CMP cluster.<br>3. Click Continue Rollback. When hovering over the button, it indicates the server to get backed out. At this point it is the remaining standby server.<br>  <br>4. Click OK to confirm and continue with the operation. It begins to back-out. Server goes into an OOS server Role<br>  <br>Follow the progress status In the Upgrade Operation column.<br><br>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.<br><br>**Expected Critical Alarms**<br><br>**70001** The qp_procmgr process has failed.<br>**31227** The high availability status is failed due to raised alarms<br>**31283** High availability server is offline<br>**70025** The MySQL slave has a different schema version than the master<br><br>**Expected Major Alarms**<br><br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br>**70021** The MySQL slave is not connected to the master<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31232** High availability server has not received a message<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed |

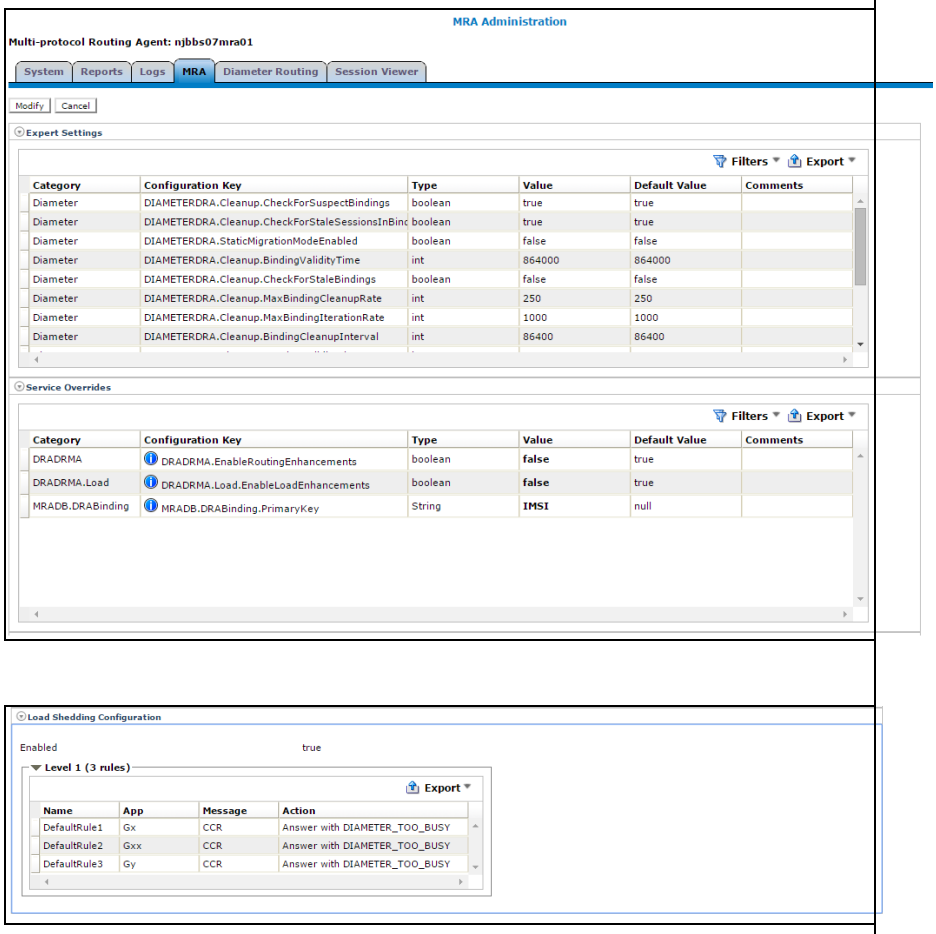
| Step | Procedure | Details |
|---|---|---|
| | | **31106** DB merging to the parent Merge Node has failed<br>**70500** The system is running different versions of software<br>Back-out of the server is complete when the following message (initiate Back-out completed successfully) displays in the Upgrade Operation column. The server goes back to standby state and show the previous release.<br>  <br>Verify in Upgrade Log that that back-out was successful:<br>  <br>All Primary CMP servers is on Release 12.5.0/12.5.0.4 at this point and show active/standby. |

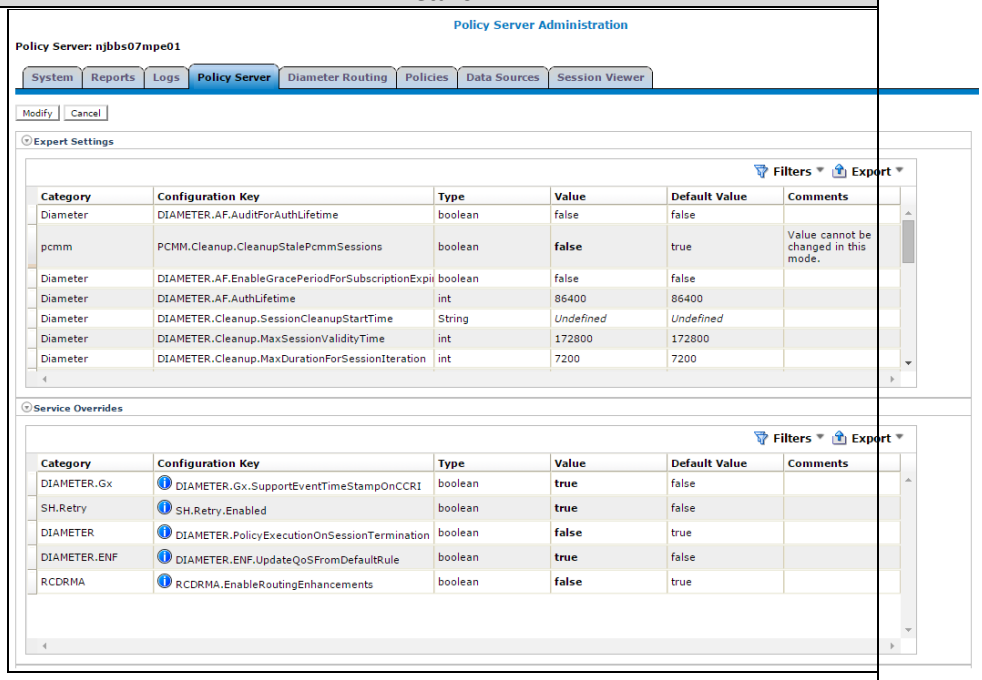
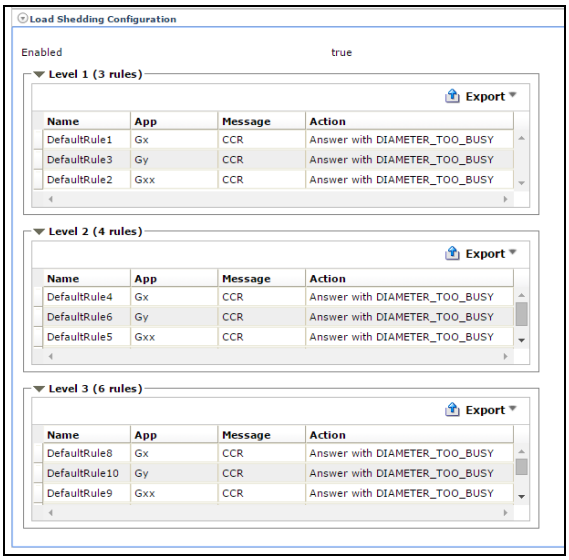
| Name | Alarm S... | Up to... | Server Role | Prev Release | Running Release |
|---|---|---|---|---|---|
| CMP Site1 Cluster (2 Servers) | | | | | |
| CMP175-55 | | N | Standby | 12.6.0.0.0_25.1.0 | 12.5.0.0.0_63.1.0 |
| CMP175-45 | | N | Active | 12.6.0.0.0_25.1.0 | 12.5.0.0.0_63.1.0 |

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

| Step | Procedure | Details |
|---|---|---|
| 12. ☐ | **CMP SSH:** Verify **`syscheck`** and `/tmp` directory permission | 1. Login to the backed-out Server as admusr<br>2. Verify that there are not any failures in **`syscheck`**:<br>`$ sudo syscheck`<br>  <br>3. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>**NOTE:** Permissions should be the following,<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>4. If the permissions are not as listed above then perform the following otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>5. Verify:<br>`$ ls -l /`<br>6. Perform **`syscheck`** again:<br>`$ sudo syscheck` |

| Step | Procedure | Details |
|---|---|---|
| 13. ☐ | **CMP SSH:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br><br>To resolve this situation permanently, perform the following:<br><br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable to the case where primary is set to eth11.<br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>4. Find eth11.<br>5. Change from `primary=eth11` to `primary=eth01`<br>6. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 14. ☐ | **CMP GUI:** Verify Alarm Status. | 1. Navigate to **System Wide Reports → Alarms → Active Alarms**.<br>2. Confirm that any existing alarm is understood.<br>  |
| 15. ☐ | **CMP GUI:** Verify Traffic Status - KPI Dashboard Report | 1. Navigate to **System Wide Reports → KPI Dashboard**.<br>2. Confirm that all Connections and Traffic status are as expected. Observe it for a few screen refresh updates.<br>  |

| Step | Procedure | Details |
|---|---|---|
| 16. ☐ | **CMP GUI:** Verify Advanced Settings on the MRA | 1. Capture screenshots of the advanced settings on the MRA and compare it with prior to upgrade screen captures.<br>2. Verify that there are not any differences.<br>3. Navigate to **MRA → Configuration →** <*mra_cluster name*> **→ MRA**.<br>4. Click **Advanced**.<br>  <br> |
| 17. ☐ | **CMP GUI:** Verify Advanced Settings on the MPE | 1. Capture screenshots of the advanced settings on the MPE and compare it with prior to upgrade screen captures.<br>2. Verify that there are not any difference<br>3. Navigate to **Policy Server → Configuration →** <*mpe_cluster name*> **→ Policy Server**.<br>4. Click **Advanced**. |

| Step | Procedure | Details |
|---|---|---|
| | |  <br>  <br>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 12.5.0/12.5.0.4 to Release 12.6 when georedundancy on non-CMP components (MPE/MRA) is disabled.

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

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<br>**NOTE:** It usually refers to the CMP on the primary site |
| DR-CMP | Configuration Management Platform for Disaster Recovery<br>**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 |
| PMAC | Platform Management and Configuration |
| TPD | Tekelec Platform Distribution |
| TVOE | Tekelec Virtualization Operating Environment |
| UE | User Equipment |
| UM | Upgrade Manager—The CMP GUI pages that the operator uses to perform an upgrade |

| Acronym | Meaning |
|---|---|
| VO | Verification Office |
| MOP | Method of Procedure |
| OOS | Out of Service |
| 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

- PMAC: 6.6.1
- TVOE: 3.8.0
- TPD: 7.8.0
- COMCOL: 6.5
- Policy Management Release 12.6
- Oracle Firmware: 3.1.5 as a minimum
- HP Firmware: Firmware Upgrade Pack Minimum: 2.2.10 or higher

### 2.1.5 Upgrade Overview

This section lists the required materials and information needed to perform Policy Management Release 12.6 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. |

| Status | Condition |
|---|---|
| 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 paths:

1. Policy Management 12.5.0 to 12.6 (Major Path)
2. Policy Management 12.5.0.4 to 12.6 (Minor Path)

### 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 PMAC Server at Site 1—Needed if version is older than what is listed in section 1.4
2. Upgrade PMAC Server at Site 2—Needed if version is older than what is listed in section 1.4
3. Firmware Upgrade—If needed (not covered in this document)
4. Upgrade Primary (Site1) CMP
5. Upgrade Secondary (Site2) CMP (if applicable)
6. Upgrade MPE/MRA (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-12.6 release and 12.6 release in mixed configuration would support the performance and capacity of the pre-12.6 release. The mixed version Policy Management configuration would also support pre-12.6 features.

Since the CMP is the first Policy Management system component that is upgraded to the new version, the Release 12.6 CMP manages MRA/MPE servers in a pre-12.6 release. In this mixed version configuration, a Release 12.6 CMP does not prevent an operator from configuring anything that can be configured in a previous release and all configuration items from the previous release are still available. However, the configuration changes during the upgrade of Policy Management system are discouraged and have limited support.

In the mixed version, a Release 12.6 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 R12.6 | MRA R12.6 | MPE R12.6 |
|---|---|---|---|
| CMP 12.5.0, 12.5.0.4 | Yes | No | No |
| MRA 12.5.0, 12.5.0.4 | Yes | Yes | Yes |
| MPE 12.5.0, 12.5.0.4 | Yes | Yes | Yes |

**NOTE:** Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP to Release 12.6. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to Release 12.6.

### 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 ISO, and TPD is upgraded to version 7.8 as part of this procedure.

In the case of IPM or clean install of a new server, the supported baseline TPD version 7.8 should be installed prior to upgrading to Policy Management Release 12.6.

### 2.1.12 Server Hardware Platforms

The Policy Management Release 12.6 software upgrade can be applied on any server that previously had Policy Management Release 12.5.0/12.5.0.4.

### 2.1.13 Loading Application software

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

**NOTE:** PMAC is not used during the Upgrade and Backout procedures.

### 2.1.14 Required Materials and Remote Access

1. Policy Management 12.6 software ISO files and TPD software ISO
2. Policy Management 12.6 software upgrade Release Notes.
3. TVOE, PMAC upgrade/installation documentation, software ISO files. (If applicable)
4. Firmware Upgrade Pack 2.2.10 (or higher) documentation and ISO files. (If applicable)
5. The capability to remote login to the target server as admusr.

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

6. The capability to secure copy (SCP) from the local workstation being used to perform this upgrade to the target server, or otherwise be able to transfer binary files to the target server.
7. User logins, passwords, IP addresses and other administration information.
8. VPN access to the network is required if that is the only method for remote logging into the target servers. It must be also possible to access the Policy Manager GUI, and the PMAC GUI.

### 2.1.15 Upgrade Media

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

#### *2.1.15.1 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 iLO | iLO Administrator Login: User/Password |
| Target OA | OA Administrator Login: User/Password |
| PMAC server | GUI Administrator Login User/Password: |
| | admusr password: |
| Software Upgrade Target Release[2] | Target Release Number: |
| | Policy Management 12.6 software ISO Image (.iso) 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.***

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

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.

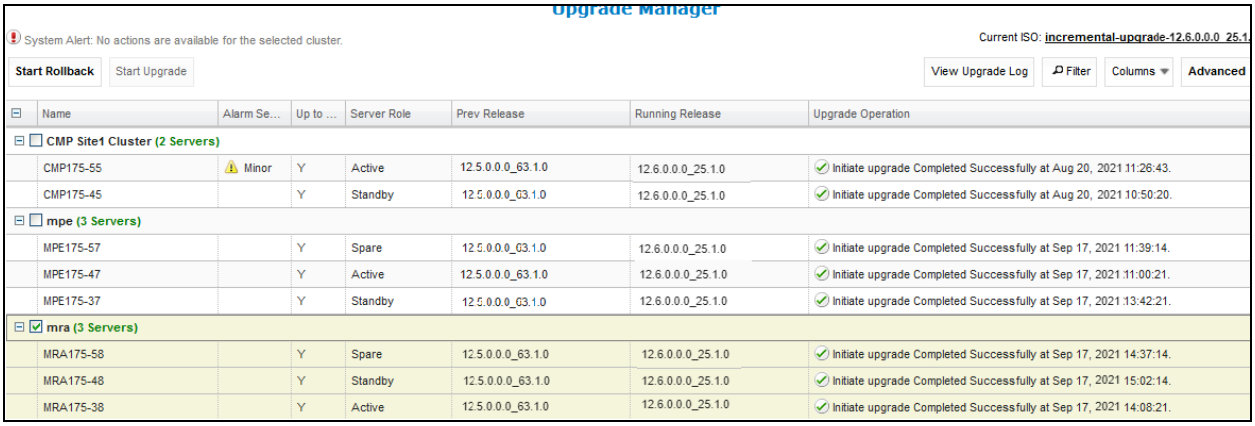



**Figure 4: Sample display of the upgrade manager page.**

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

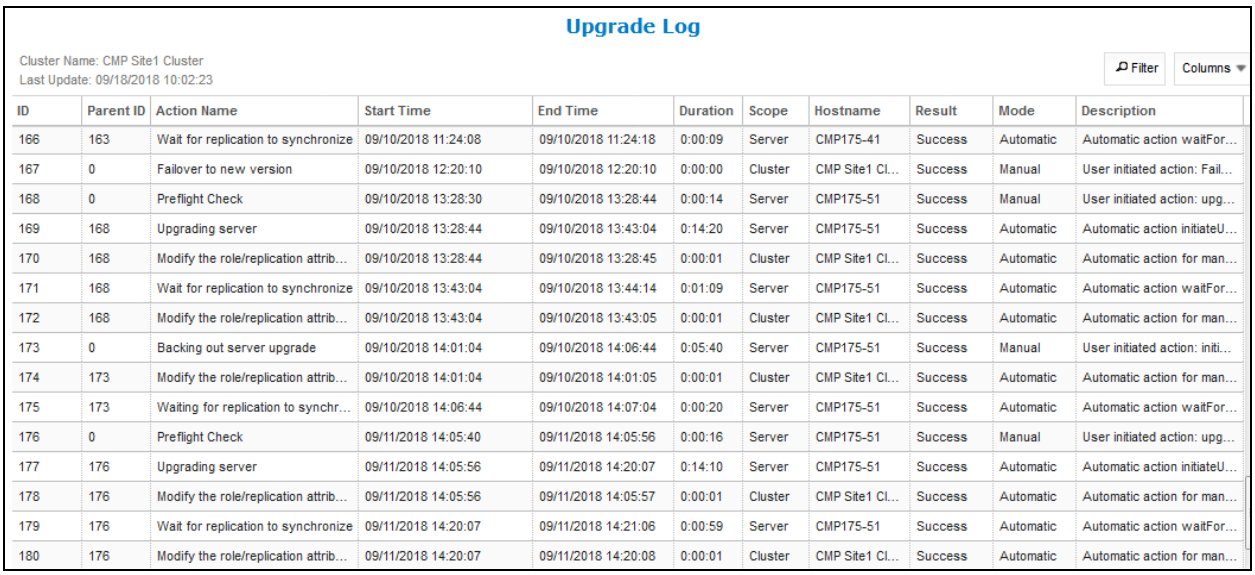
The server is running new code.

- 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.



Upgrade Log

Cluster Name: CMP Site1 Cluster
Last Update: 09/18/2018 10:02:23

Filter | Columns

| ID | Parent ID | Action Name | Start Time | End Time | Duration | Scope | Hostname | Result | Mode | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| 166 | 163 | Wait for replication to synchronize | 09/10/2018 11:24:08 | 09/10/2018 11:24:18 | 0:00:09 | Server | CMP175-41 | Success | Automatic | Automatic action waitFor... |
| 167 | 0 | Failover to new version | 09/10/2018 12:20:10 | 09/10/2018 12:20:10 | 0:00:00 | Cluster | CMP Site1 Cl... | Success | Manual | User initiated action: Fail... |
| 168 | 0 | Preflight Check | 09/10/2018 13:28:30 | 09/10/2018 13:28:44 | 0:00:14 | Server | CMP175-51 | Success | Manual | User initiated action: upg... |
| 169 | 168 | Upgrading server | 09/10/2018 13:28:44 | 09/10/2018 13:43:04 | 0:14:20 | Server | CMP175-51 | Success | Automatic | Automatic action initiateU... |
| 170 | 168 | Modify the role/replication attrib... | 09/10/2018 13:28:44 | 09/10/2018 13:28:45 | 0:00:01 | Cluster | CMP Site1 Cl... | Success | Automatic | Automatic action for man... |
| 171 | 168 | Wait for replication to synchronize | 09/10/2018 13:43:04 | 09/10/2018 13:44:14 | 0:01:09 | Server | CMP175-51 | Success | Automatic | Automatic action waitFor... |
| 172 | 168 | Modify the role/replication attrib... | 09/10/2018 13:43:04 | 09/10/2018 13:43:05 | 0:00:01 | Cluster | CMP Site1 Cl... | Success | Automatic | Automatic action for man... |
| 173 | 0 | Backing out server upgrade | 09/10/2018 14:01:04 | 09/10/2018 14:06:44 | 0:05:40 | Server | CMP175-51 | Success | Manual | User initiated action: initi... |
| 174 | 173 | Modify the role/replication attrib... | 09/10/2018 14:01:04 | 09/10/2018 14:01:05 | 0:00:01 | Cluster | CMP Site1 Cl... | Success | Automatic | Automatic action for man... |
| 175 | 173 | Waiting for replication to synchr... | 09/10/2018 14:06:44 | 09/10/2018 14:07:04 | 0:00:20 | Server | CMP175-51 | Success | Automatic | Automatic action waitFor... |
| 176 | 0 | Preflight Check | 09/11/2018 14:05:40 | 09/11/2018 14:05:56 | 0:00:16 | Server | CMP175-51 | Success | Manual | User initiated action: upg... |
| 177 | 176 | Upgrading server | 09/11/2018 14:05:56 | 09/11/2018 14:20:07 | 0:14:10 | Server | CMP175-51 | Success | Automatic | Automatic action initiateU... |
| 178 | 176 | Modify the role/replication attrib... | 09/11/2018 14:05:56 | 09/11/2018 14:05:57 | 0:00:01 | Cluster | CMP Site1 Cl... | Success | Automatic | Automatic action for man... |
| 179 | 176 | Wait for replication to synchronize | 09/11/2018 14:20:07 | 09/11/2018 14:21:06 | 0:00:59 | Server | CMP175-51 | Success | Automatic | Automatic action waitFor... |
| 180 | 176 | Modify the role/replication attrib... | 09/11/2018 14:20:07 | 09/11/2018 14:20:08 | 0:00:01 | Cluster | CMP Site1 Cl... | Success | Automatic | Automatic action for man... |

**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.

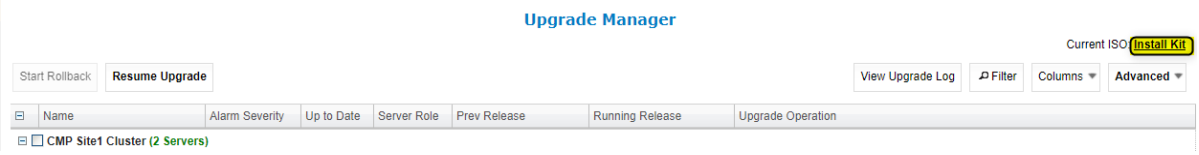
If the operator selects an optional action, they can go back to using the default/preferred at any time.

#### *2.2.2.2 The ISO Select*

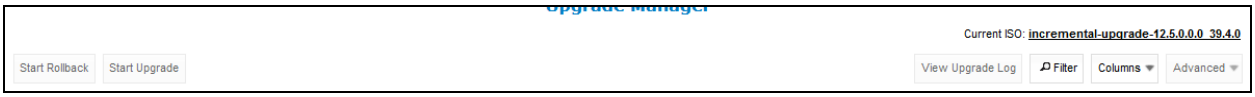
In the upper right hand corner, there is an item called the current ISO. In some respects the term ISO is misleading. A better description might be upgrade procedure. This item shows the upgrade procedure that is being used. In common cases, this is going to work out to either:

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

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




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




### *2.2.2.3 Upgrade Director Behavior*

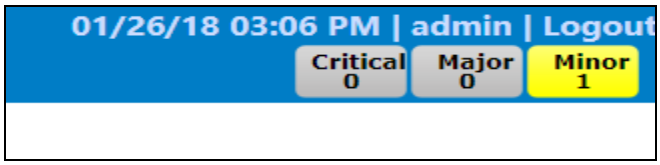
The Upgrade Director (UD) is a component that tracks the state of the servers, cluster, and system during an upgrade. The UD is hidden. However, there are conventions and operating principles that are visible.

#### 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 12.6 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 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. |

| Alarm ID | Severity | Name | Description |
|---|---|---|---|
| 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 TVOE & PMAC Server at Site 1 (if applicable)
2. Upgrade TVOE & PMAC Server at Site 2 (if applicable)
3. Firmware (if applicable)
4. Upgrade Primary (Site1) CMP
5. Upgrade Secondary (Site2) CMP (if applicable)
6. Segment 1 Site 1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
7. Segment 1 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
8. Segment 2 Site 1:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters
9. Segment 2 Site 2:
    a. Upgrade MPE clusters
    b. Upgrade MRA clusters

### 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 16 TVOE, PMAC and Firmware might need to be upgraded prior to Upgrade to Policy Management Release 12.6.**

| Step | Procedure | Details |
|---|---|---|
| 1. | Verify all required materials are present | As listed in 2.1.14 Required Materials and Remote Access |
| 2. | Review Release | Review Policy Management Release 12.6 for the following information: |

| Step | Procedure | Details |
|---|---|---|
| | Notes | • Individual Software components and versions included in target release<br>• New features included in target release<br>• Issues (Oracle BUGs) resolved in target release<br>• Known Issues with target release<br>• Any further instructions that may be required to complete the Software Upgrade for the target release. In particular, the supported browsers: **In release 12.6, only Mozilla Firefox and Google Chrome are fully supported.** |
| **—End of Procedure—** | | |

### 2.3.2 TVOE and PMAC Server Upgrade

Policy Management Release 12.6 requires PMAC version 6.6.1 to support the IPM of TPD 7.8 on c-Class blades.

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

Appendix A describes in detail the upgrade of TVOE and PMAC.

### 2.3.3 Firmware Upgrade

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

### 2.3.4 Plan and Track Upgrades

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

1. Upgrade TVOE and PMAC Server and deploy firmware upgrade if necessary
2. Upgrade CMP cluster(s)
3. Upgrade non-CMP clusters

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

**NOTES:**

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

| Step | Procedure | Result | Engineer | Time |
|---|---|---|---|---|
| 1. ☐ | Use the following checklist to plan the cluster upgrades for the entire system. | Maintenance windows are planned | | |
| 2. ☐ | Upgrade Site A and Site B TVOE/PMAC | Site Names _____ & _____ | | 3 hrs |

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

| Step | Procedure | Result | Engineer | Time |
|---|---|---|---|---|
| **7.** ☐ | Upgrade Site2 clusters for Segment-2 | Site Names _____<br>Cluster List: | | 2 hrs |

### 2.3.5 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 17 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.<br>***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<br>**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.<br>2. Confirm that time is synchronized on each server with CLI shell command of:<br>`[admusr@CMP1194 ~]$ ntpq -np`<br>3. Confirm the date is correct on each server.<br>4. Check that the BIOS clock is synced with the clock using the shell **`hwclock`** command:<br>`[admusr@CMP1194 ~]$ sudo hwclock` |
| **—End of Procedure—** | | |

### 2.3.6 Deploy Policy Management Upgrade Software

Software should be deployed to each policy server `/var/TKLC/upgrade` directory, before the actual upgrade activities. This is typically done with utilities such as SCP, WGET, SFTP, or the Upgrade Manager. Because of the large size of the software ISO files, sufficient time should be planned to accomplish this step. For Policy Management Release 12.6, each ISO image size is about 1.3 Gigabytes.

#### *2.3.6.1 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.***

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

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

#### *2.3.6.2 Copy ISO image files to the Management Server (PMAC)*

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

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

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

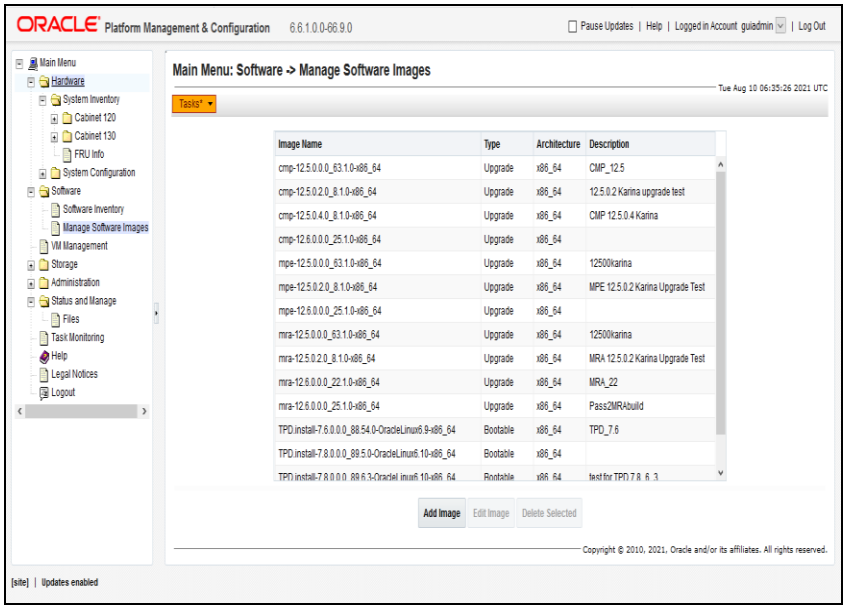
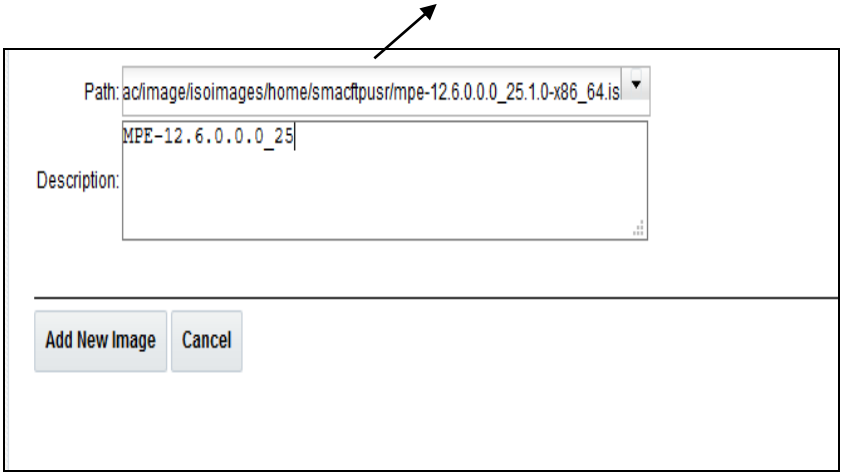
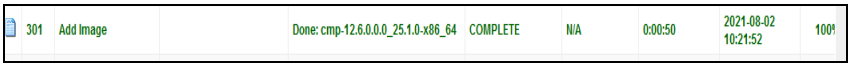
**NOTE:** ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance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

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

**Procedure 18 Copy ISO image files to the Management Server(PMAC) and Distribute Application ISO Image Files to Servers**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **PMAC GUI:** Verify that ther are not any Release 12.6 ISO files. | 1. Log on to the PMAC Server GUI<br>2. Navigate to **Software → Manage Software Images.**<br>3. If release 12.6 ISO files are in the list, remove them. |

| Step | Procedure | Result |
|---|---|---|
| 2. ☐ | SSH to PMAC server as admusr | 1. Log on as admusr to the PMAC server.<br>2. Change the target directory to `/var/TKLC/upgrade` and verify that there is at least of 3.0 GB free disk space available.<br>`$cd /var/TKLC/upgrade`<br>`$df -h /var/TKLC`<br>**NOTE:** There may be ISO files in the `/var/TKLC/upgrade` directory, they can be removed to free up disk space or added to the PMAC repository. |
| 3. ☐ | Copy Release 12.6 ISO files to the target directory in the PMAC server | Transfer all required Release 12.6 ISO files (CMP, MPE/MPE-Li, MRA) into the `/var/TKLC/upgrade` directory using one of the following methods:<br>• SCP/WGET command in the following steps outline in this procedure<br>• USB drive |

| Step | Procedure | Result |
|---|---|---|
| 4. ☐ | **PMAC GUI:** Adding the Release 12.6 ISO files | 1. Navigate to **Software → Manage Software Images**.<br>2. Click **Add Image** to select the ISO files that are just transferred into PMAC server.<br>  <br>  <br>3. Click **OK**. |
| 5. ☐ | **PMAC GUI:** Verify the ISO files are added successfully | Navigate to **Software → Manage Software Images**.<br>The status of the image being added can be monitored using the Task Monitoring menu with the display as the following:<br>  <br>**NOTE:** The added ISO files are now stored in the `/var/TKLC/smac/image/repository` directory |
| **—End of Procedure—** | | |

### *2.3.6.3 Distribute Application ISO Image Files to Servers*

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

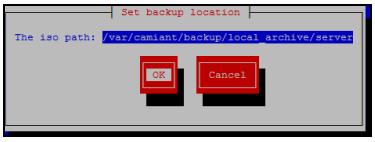
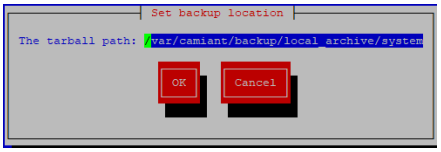
**NOTE:** ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. The ISO transfers to the target systems should be performed prior to, outside of, the scheduled maintenance window. Schedule the required maintenance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

**Procedure 19 Distribute Application ISO Image Files to Servers**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | Transfer ISO files to Policy Management Servers. | Transfer release 12.6 ISO files (CMP and non-CMP) into the `/var/TKLC/upgrade` directory on the respective server using one of the following methods<br>• SCP/WGET command<br>• USB drive<br>OR, if the images are on a server on the same network, scp via CLI.<br>Copy CMP software ISO to ONE of the other CMP servers:<br>`$sudo scp 872-* <cmp-12.6>:/var/TKLC/upgrade/`<br>Copy MPE software ISO to ONE of the other MPE servers:<br>`$sudo scp 872-* <mpe-12.6>:/var/TKLC/upgrade/`<br>Copy MPE-Li software ISO to ONE of the other MPE-Li servers:<br>`$sudo scp 872-* <mpe-li-12.6>:/var/TKLC/upgrade/`<br>Copy MRA software ISO to ONE of the other MRA servers:<br>`$sudo scp 872-* <mra-12.6>:/var/TKLC/upgrade/`<br>**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—** | | |

### *2.3.6.4 Backups and Backup Locations*

**Procedure 20 Backup servers before upgrading servers**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **SSH CLI/ iLO**: Access the server to be backed up<br><br>**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.***<br><br>1. Login into the ACTIVE Primary CMP server.<br>2. Open the platcfg utility.<br>`$sudo su - platcfg`<br>3. Navigate to **Policy Configuration→Backup and Restore→Server Backup**<br>4. Enter an ISO backup filename (or use the suggested one) in the default backup location path:<br>`var/camiant/backup/local_archive/serverbackup/<serverbackup>.iso`<br>  <br>5. Click **OK**.<br>6. Go back to the previous menu (**Policy Configuration→Backup and Restore**) and select **System Backup.**<br>7. Enter a tarball backup filename (or use the suggested one) in the default backup location path:<br>`/var/camiant/backup/local_archive/systembackup/<systembackup>.tar.gz`<br>  |
| 2. ☐ | **SSH CLI/iLO:** Verify the backup file | If the default location is accepted in the previous step, change directory to the following and verify the file exists:<br>`$ cd /var/camiant/backup/local_archive/serverbackup`<br>`$ ls <hostname>-<servertype>_x…x-serverbackup-<yyyy><mm><dd><hhmm>.iso`<br>And:<br>`$ cd /var/camiant/backup/local_archive/systembackup`<br>`$ ls <hostname>-cmp_x…x-systembackup-<yyyy><mm><dd><hhmm>.tar.gz` |

| Step | Procedure | Result |
|---|---|---|
| 3. ☐ | Copy backup files. | Copy the ISO and tarball files to a safe location, for example, for a server backup file:<br>`$sudo scp -p /var/camiant/backup/local_archive/serverbackup/<serverbackup>.iso <remoteserverIP>:<destinationpath>`<br>Another option is to scp the server and system backup files to your local workstation.<br>After copying to remote server/workstation, remove the backup files from the server.<br>`$sudo rm <serverbackup>.iso` |
| 4. ☐ | Identify backup location | Backup location is:<br>_____<br>Instructions to access to backups are as follows:<br>_____<br>_____<br>_____ |
| **—End of Procedure—** | | |

## 2.4 Upgrade CMP Clusters (12.5.0/12.5.0.4 to 12.6) 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*

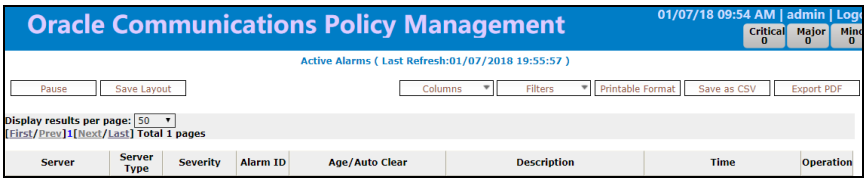
Use this procedure to upgrade a Primary CMP Cluster.

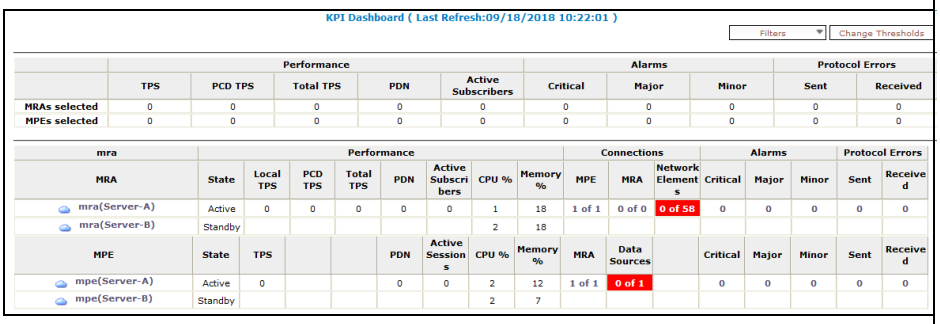
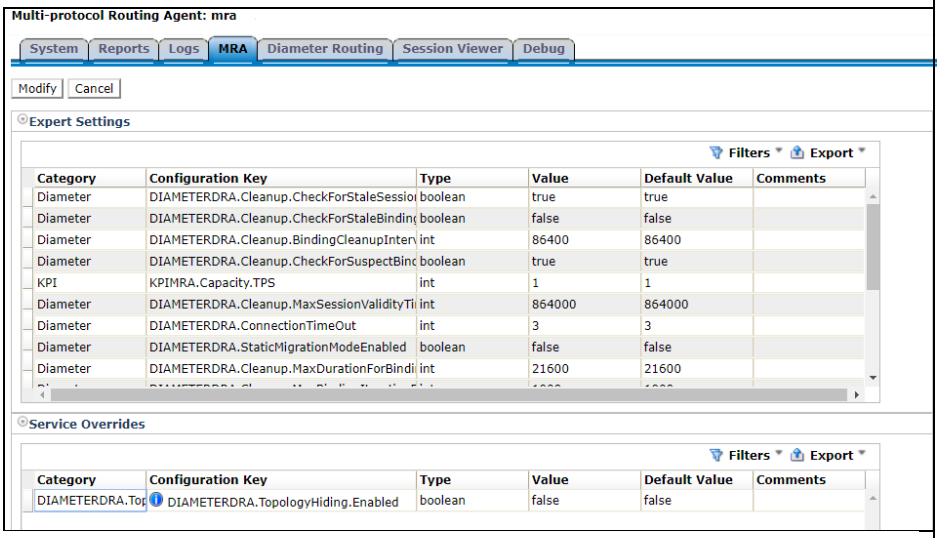
**NOTES:**

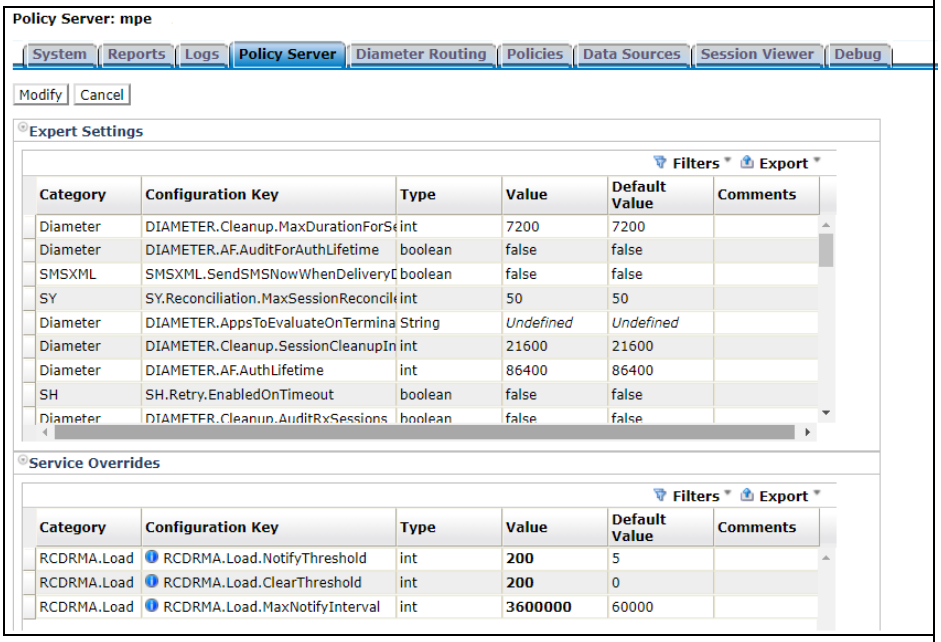
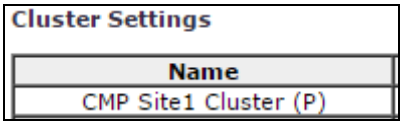
- This procedure must be performed in a maintenance window.
- This procedure takes approximately 60-120 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

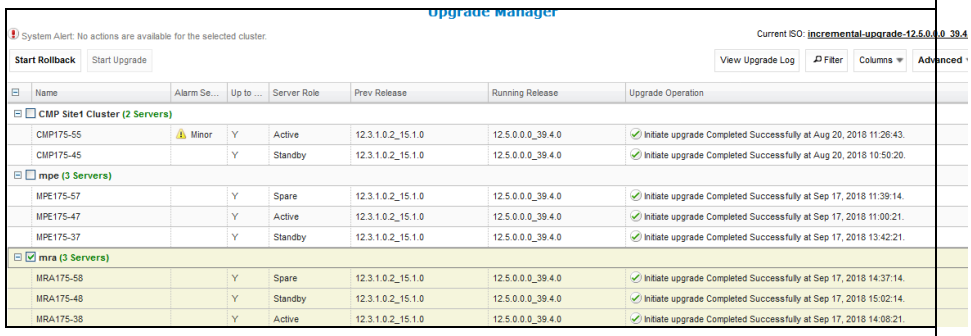
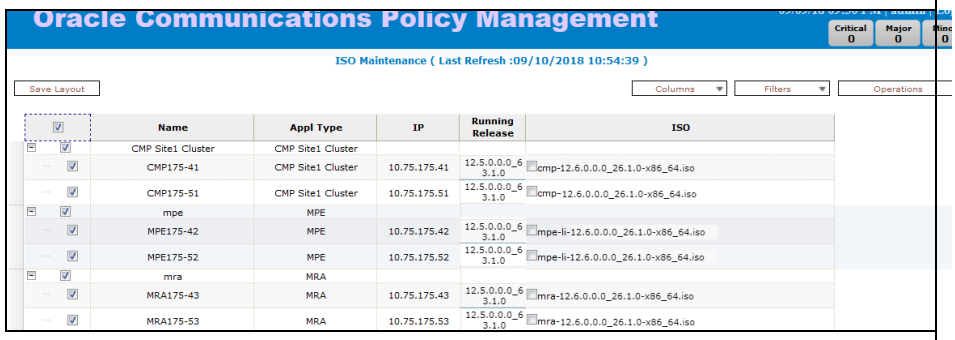
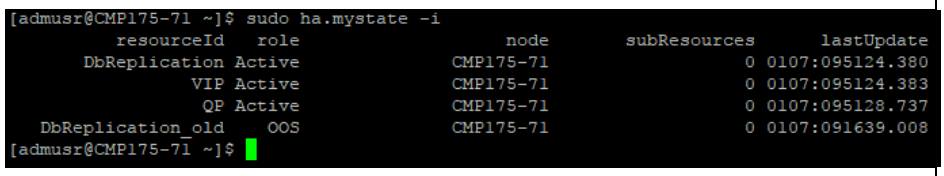
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

**Procedure 21 Upgrade CMP Cluster**

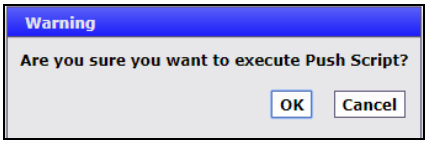
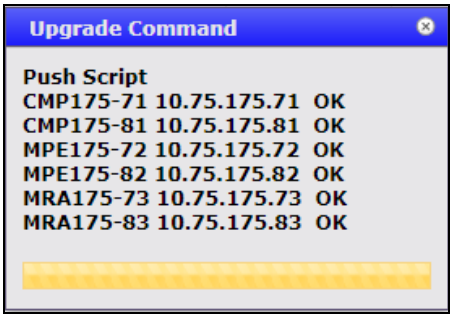
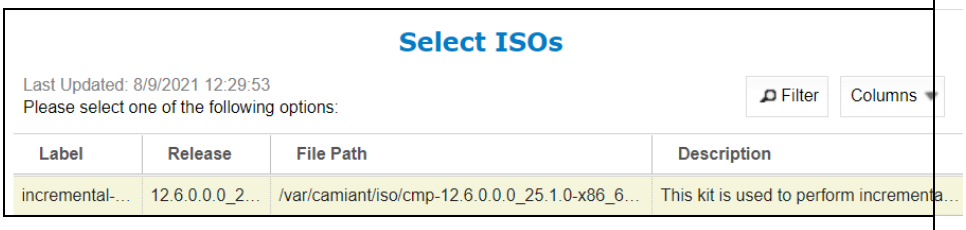
| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **CMP GUI:** Verify Alarm Status. | 1. Navigate to **System Wide Reports → Alarms → Active Alarms**<br>2. Confirm that any existing alarm is understood and there is not any impact to the Upgrade procedure.<br>3. Capture a screenshot and save it into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

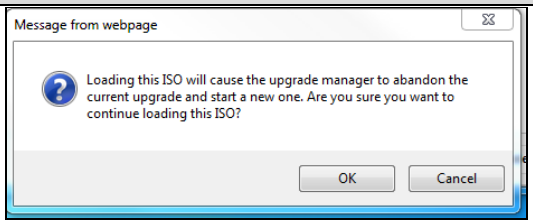
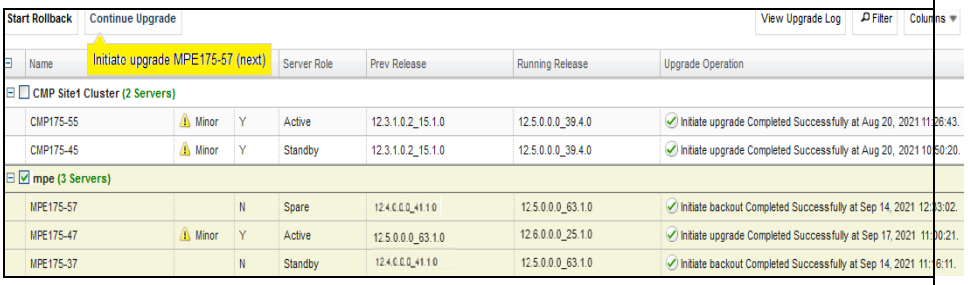
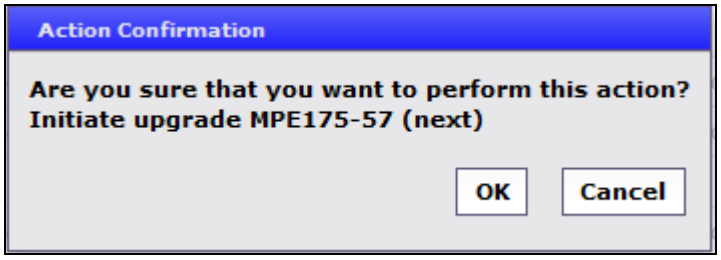
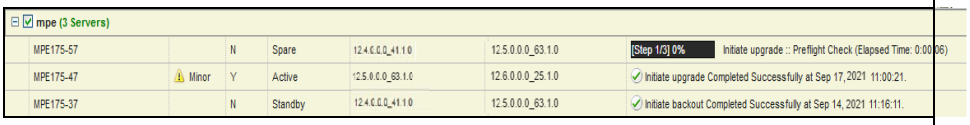
| Step | Procedure | Result |
|---|---|---|
| 2. ☐ | **CMP GUI:** Verify Traffic Status - KPI Dashboard Report | 1. Navigate to **System Wide Reports → KPI Dashboard**<br>2. Confirm that all Connections and Traffic status are as expected. Observe it for a few refresh updates.<br>3. Capture a screenshot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

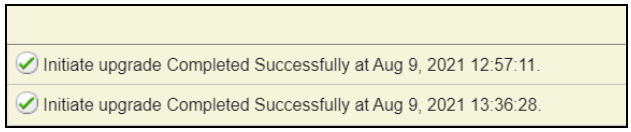
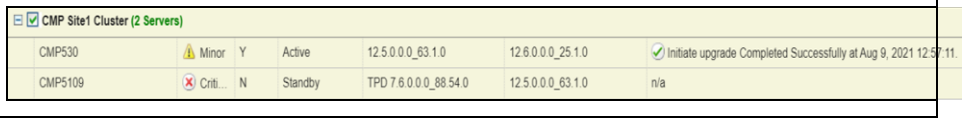
| Step | Procedure | Result |
|---|---|---|
| 4. ☐ | **CMP GUI:** Capture MPE Advanced Settings | 1. Capture screenshots of the advanced settings on the MPE prior to upgrading the CMP and save them for future reference.<br>2. Navigate to **Policy Server → Configuration →** <*MPE*> **→ Policy Server**<br>3. Click **Advanced Settings**.<br>  <br>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**.<br>2. Note which cluster is the primary and which cluster is the secondary.<br>3. Save a screenshot for future reference.<br>The primary CMP is noted with a P<br>  |

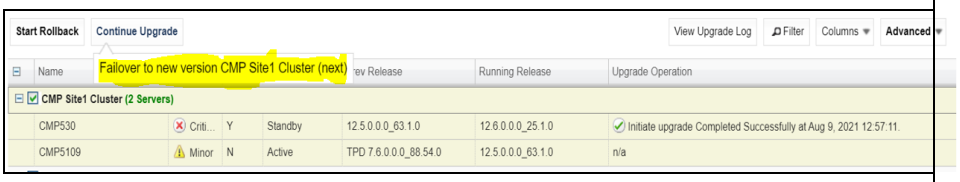
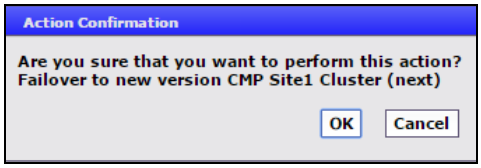
| Step | Procedure | Result |
|---|---|---|
| 6. ☐ | **CMP GUI**: Verify Status of CMP clusters and ISO files are copied to each server | 1. Navigate to **Upgrade → Upgrade Manage**r.<br>2. Verify that the CMP clusters have the following:<br>- Server Role: Active/Standby status.<br>- Running Release: 12.5.0 or 12.5.0.4 version.<br>  <br>3. Navigate to **Upgrade → ISO Maintenance**.<br>4. Corresponding Release 12.6 ISO files copied to each of the servers (CMP/MRA/MPE)<br>  |
| 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.<br>Login: admusr<br>Password: <*provided password*><br>2. Run the **`sudo ha.mystate -i`** command to confirm the role is Active.<br>`$ sudo ha.mystate -i`<br>  <br>**NOTE:** DbReplication_old_OOS is a non-issue status event. |

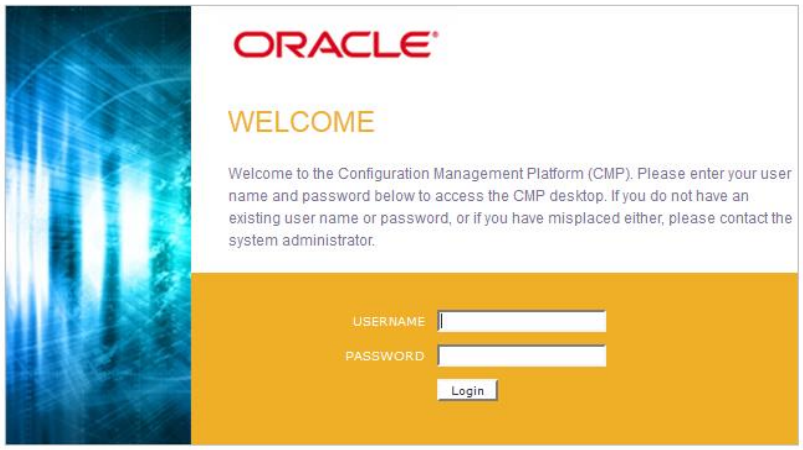
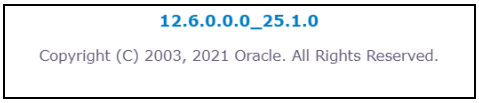
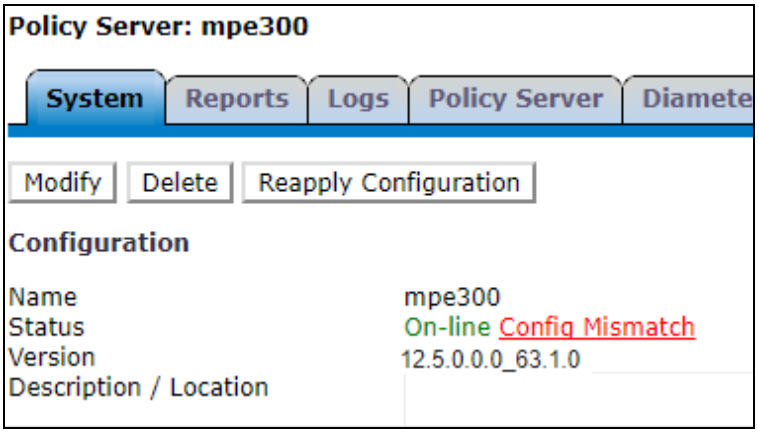
| Step | Procedure | Result |
|---|---|---|
| 8. ☐ | **SSH Primary Active CMP:** exchange keys | 1. Exchange keys to all servers from the SITE 1 Active Primary CMP.<br>2. Login as admusr user.<br>3. Notes: This step could be skipped if your system was fresh installed in R12.3 or R12.4.<br>`$ sudo mount -o loop /var/TKLC/upgrade/cmp-12.5.0.0_x.x.0-x86_64.iso /mnt/upgrade/`<br>`$ sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`<br>**NOTE:** If prompted, answer Yes to all.<br>`$ sudo umount /mnt/upgrade`<br>`$ sudo qpSSHKeyProv.pl --prov`<br>• Required to enter the PASSWORD for admusr user.<br>• Ensure that the Keys are exchanged successfully with all the server clusters<br>For example:<br>`$ sudo qpSSHKeyProv.pl --prov`<br>`The password of admusr in topology:<admusr password>`<br>`Connecting to admusr@njbbs07cmp01b ...`<br>`Connecting to admusr@njbbs07cmp01a ...`<br>`Connecting to admusr@txsls07mra01b ...`<br>`Connecting to admusr@njbbs07mpe02a ...`<br>`Connecting to admusr@txsls07mpe01b ...`<br>`Connecting to admusr@njbbs07mra01a`<br>`[16/17] Provisioning SSH keys on txsls07mpe02b ...`<br>`[17/17] Provisioning SSH keys on njbbs07mra01b ...`<br>`SSH keys are OK.` |

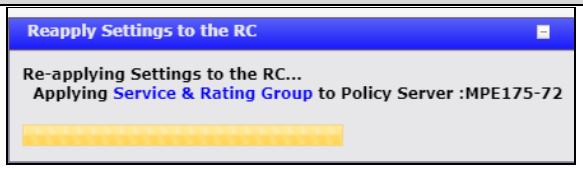
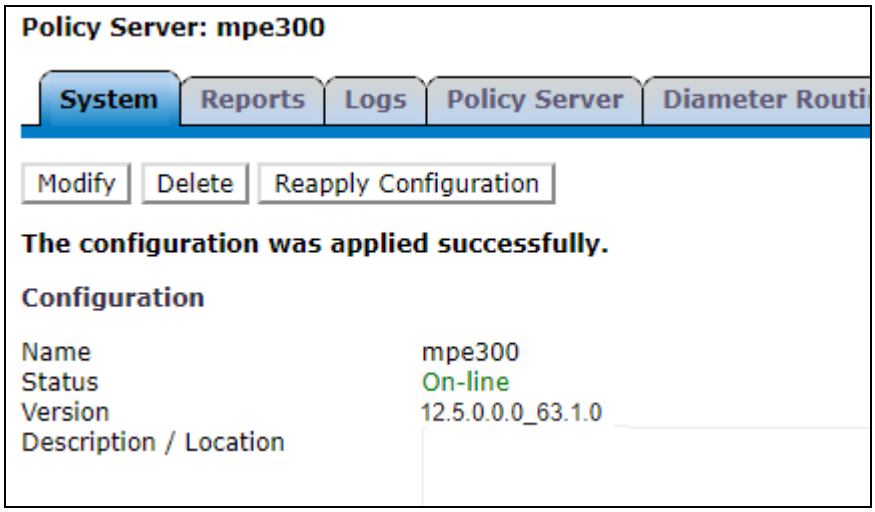
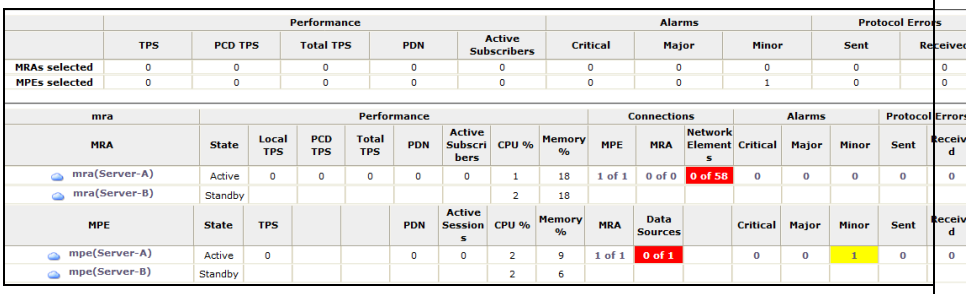
| Step | Procedure | Result |
|---|---|---|
| 9. ☐ | **CMP GUI**: Push the Release 12.6 upgrade Scripts to all servers in the segment topology | 1. Navigate to **Upgrade → ISO Maintenanc**e.<br>2. Select all the servers in the Topology.<br>3. Select **Operations → Push Script**s. (It is safe to run the push script multiple times as needed).<br>4. Click **OK** to continue the operation.<br>  <br>5. Verify that operation was successful with OK for every server.<br>  <br>**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.<br>2. Copy the 12.6 ISO to the `/var/camiant/iso` directory:<br>`$ sudo cp /var/TKLC/upgrade/cmp-12.6.0.0_x.x.0-x86_64.iso /var/camiant/iso/`<br>3. Verify:<br>`$ ls /var/camiant/iso` |
| 11. ☐ | **CMP GUI:** Select the 12.6 Upgrade release | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Current ISO.<br>3. This opens a dialog box with a description of the ISO that was copied into the `/var/camiant/iso` directory.<br>4. Highlight the available 12.6 ISO.<br>5. Click **Select incremental-upgrade-12.6 ISO** on the bottom right hand corner of the window.<br>  <br>6. Click **OK**. |

| Step | Procedure | Result |
|---|---|---|
| | |  <br>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<br><br>**NOTE:** This takes approximately 30 minutes at most to complete.<br><br>**NOTE:** Up to 8 clusters can be upgraded at the same time, selecting one at a time. | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Click **Filter** and enter `CMP` in the **Name** field.<br>3. Select the Primary CMP Server Cluster.<br>4. Click **Continue Upgrade**.<br>  <br>5. Click **OK** to confirm and continue with the operation.<br>  <br>The specific action taken is determined by the Upgrade Manager and based on the specific version change being performed.<br><br>This continues to upgrade the standby server only in the CMP Cluster<br><br>In the Upgrade Operation column, the In Progress status along with the upgrade activities cdisplays.<br>  <br>Upgrade Status changes to Completed Successfully when done.<br><br>During the Upgrade activities, the following alarms may be generated and are considered normal reporting events:<br><br>**<u>Expected Critical Alarms</u>**<br><br>**70001** The qp_procmgr process has failed<br><br>**31227** The high availability status is failed due to raised alarms |

| Step | Procedure | Result |
|---|---|---|
| | | **70025** The MySQL slave has a different schema version than the master<br>**31283** High availability server is offline<br><br>**Expected Major Alarms**<br><br>**70004** The QP processes have been brought down for maintenance<br>**31233** High availability path loss of connectivity<br>**70021** The MySQL slave is not connected to the master<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**70500** The system is running difference versions of software<br>**31101** DB replication to a slave DB has failed<br>**31106** DB merging to the parent Merge Node has failed<br>**31107** DB merging from a child Source Node has failed<br>**31102** DB replication from a master DB has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31105** The DB merge process (inetmerge) is impaired by a s/w fault<br>Upgrade is complete on the first CMP server in the cluster when the following message (completed successfully) displays in the Upgrade Operation column.<br>  |
| 13. ☐ | **CMP GUI:** Verify the upgrade is successful | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. View the cluster. At this point, one server is on 12.6 and the other server in the cluster is on 12.5.0/12.5.0.4. The Up To Date column shows Y for the 12.6 server and N for the 12.5.0/12.5.0.4 server.<br>  |

| Step | Procedure | Result |
|---|---|---|
| 14. ☐ | **CMP CLI:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the upgrade is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. Login as admusr and run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth01. If it is set to eth11, follow these instructions, otherwise skip to the nextr step.<br>3. If this blade is the active blade, change it to standby.<br>4. Enter the following command:<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>5. Find eth11.<br>6. Change from `primary=eth11` to `primary=eth01`<br>7. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 15. ☐ | **CMP GUI:** Verify System Wide Reports—KPI Dashboard Report | 1. Navigate to **System Wide Reports → KPI Dashboard**.<br>2. Verify that report shows all normal traffic processing for the MPEs/MRAs. Observe it for a few refresh updates. |
| 16. ☐ | **CMP GUI:** Continue Upgrade CMP cluster | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Primary CMP Server cluster.<br>3. Click **Continue Upgrade**. Notice the failover to new version message.<br>4. **NOTE:** This causes a failover of the Primary CMP cluster<br>  <br>5. Click **OK** to confirm and continue with the operation.<br>  <br>The action takes less than a minute to complete. |

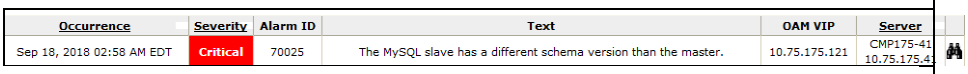
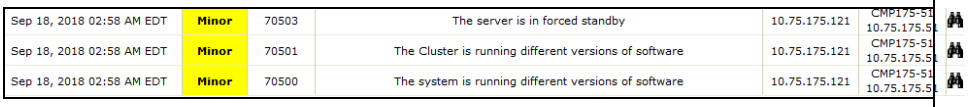
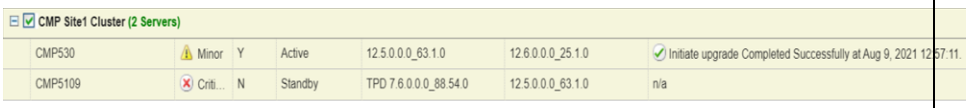
| Step | Procedure | Result |
|---|---|---|
| 17. ☐ | **CMP GUI:** Re-login to the CMP server VIP | Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address.<br><br>The Policy Management Release 12.6 CMP GUI Login displays as shown. Login and password credentials are the same as the pre-upgrade.<br><br>  |
| 18. ☐ | **CMP GUI:** Verify Policy Management Release | 1. Navigate to **Help→About**.<br><br>2. Verify the release displayed is 12.6<br><br>**NOTE:** Any '12.6.0.0.0_x.y.z' is correct<br><br>  |
| 19. ☐ | **CMP GUI:** Reapply Configuration to MPE/MRA | • For MPE: **Policy Server → Configuration →** <*MPE cluster*> **→ System**<br>• For MRA: **MRA→Configuration→**<*MRA cluster*>**→System**<br><br>The selected cluster has the status shown as Degraded and still shows the old release version. Config mismatch may be displayed as well.<br><br>1. Click the **Reapply Configuration** operation.<br><br>  <br><br>**NOTE:** A progress banner displays for the MPE reapply configuration. A progress banner DOES NOT display for the MRA reapply configuration. |

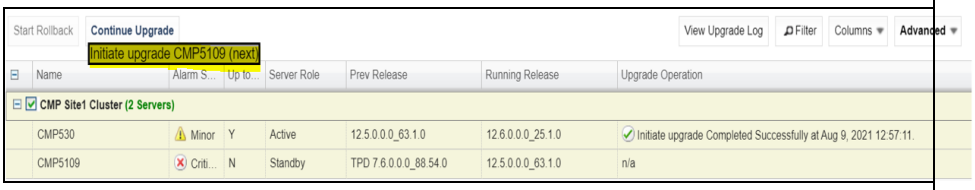
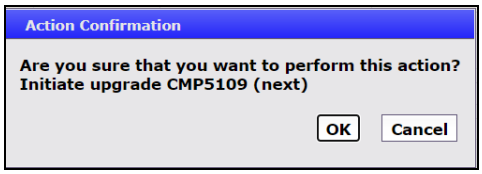
| Step | Procedure | Result |
|---|---|---|
| | |  <br>2. Verify that the Reapply Configuration is successfully:<br>  |
| 20. ☐ | **CMP GUI:**<br>Verify traffic | 1. Navigate to **System Wide Reports → KPI Dashboard**.<br>2. Verify that report shows all normal traffic processing for the MPEs/MRAs. Observe it for few updates refresh.<br>  |

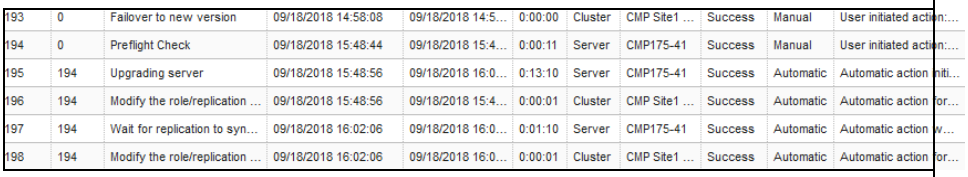
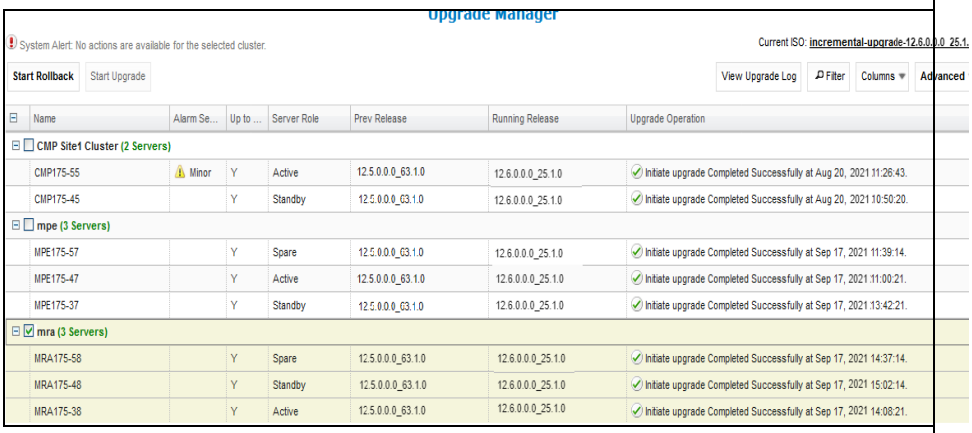
| | Performance | | | | | Alarms | | | Protocol Errors | |
|---|---|---|---|---|---|---|---|---|---|---|
| | TPS | PCD TPS | Total TPS | PDN | Active Subscribers | Critical | Major | Minor | Sent | Received |
| MRAs selected | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| MPEs selected | 0 | 0 | 0 | 0 | 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 |
|---|---|---|
| 21. ☐ | **CMP GUI:**<br>Critical Alarms | Multiple critical alarms (70025) are seen until the SQL Database matches the master (12.6). Thise alarms are expected and remain until all CMPs have been upgraded to the same version.<br>  <br>**Current Minor Alarms**<br>**70503** Server Forced Standby<br>**70501** Cluster Mixed Version<br>**70500** System Mixed Version<br>  <br>**NOTE:** The Upgrade Manager also displays alarms. |
| 22. ☐ | **CMP GUI:**<br>Verify the Policy Management Release 12.6 CMP is Active | 1. Navigate to **Upgrade→ Upgrade Manager**<br>2. Verify the following -<br>- Active server is on Running Release 12.6<br>- Standby server is on the previous Release<br>  <br>As noted, the Active CMP server is now on the Running Release of 12.6 |

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

| Step | Procedure | Result |
|---|---|---|
| 24. ☐ | **CMP GUI:** Tracking the upgrade complete | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. The last step in the upgrade for the first CMP cluster is to wait for replication to complete.<br>3. Select the upgraded CMP cluster.<br>4. Click **View Upgrade** Log.<br>  <br>193 \| 0 \| Failover to new version \| 09/18/2018 14:58:08 \| 09/18/2018 14:5... \| 0:00:00 \| Cluster \| CMP Site1 ... \| Success \| Manual \| User initiated action:...<br>194 \| 0 \| Preflight Check \| 09/18/2018 15:48:44 \| 09/18/2018 15:4... \| 0:00:11 \| Server \| CMP175-41 \| Success \| Manual \| User initiated action:...<br>195 \| 194 \| Upgrading server \| 09/18/2018 15:48:56 \| 09/18/2018 16:0... \| 0:13:10 \| Server \| CMP175-41 \| Success \| Automatic \| Automatic action initi...<br>196 \| 194 \| Modify the role/replication ... \| 09/18/2018 15:48:56 \| 09/18/2018 15:4... \| 0:00:01 \| Cluster \| CMP Site1 ... \| Success \| Automatic \| Automatic action for...<br>197 \| 194 \| Wait for replication to syn... \| 09/18/2018 16:02:06 \| 09/18/2018 16:0... \| 0:01:10 \| Server \| CMP175-41 \| Success \| Automatic \| Automatic action w...<br>198 \| 194 \| Modify the role/replication ... \| 09/18/2018 16:02:06 \| 09/18/2018 16:0... \| 0:00:01 \| Cluster \| CMP Site1 ... \| Success \| Automatic \| Automatic action for... |
| 25. ☐ | **CMP GUI:** Verify the status of the upgraded CMP server. | Navigate to **Upgrade Manager → Upgrade Manager**.<br>  <br>Upgrade Manager<br>System Alert: No actions are available for the selected cluster.<br>Current ISO: incremental-upgrade-12.6.0.0.0_25.1.<br>Start Rollback \| Start Upgrade \| View Upgrade Log \| Filter \| Columns \| Advanced<br>Name \| Alarm Se... \| Up to ... \| Server Role \| Prev Release \| Running Release \| Upgrade Operation<br>CMP Site1 Cluster (2 Servers)<br>CMP175-55 \| Minor \| Y \| Active \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Aug 20, 2021 11:26:43.<br>CMP175-45 \| Y \| Standby \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Aug 20, 2021 10:50:20.<br>mpe (3 Servers)<br>MPE175-57 \| Y \| Spare \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Sep 17, 2021 11:39:14.<br>MPE175-47 \| Y \| Active \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Sep 17, 2021 11:00:21.<br>MPE175-37 \| Y \| Standby \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Sep 17, 2021 13:42:21.<br>mra (3 Servers)<br>MRA175-58 \| Y \| Spare \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Sep 17, 2021 14:37:14.<br>MRA175-48 \| Y \| Standby \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Sep 17, 2021 15:02:14.<br>MRA175-38 \| Y \| Active \| 12.5.0.0.0_63.1.0 \| 12.6.0.0.0_25.1.0 \| Initiate upgrade Completed Successfully at Sep 17, 2021 14:08:21.<br>• Successful upgrade status shows both servers running the Release 12.6 in the Running Release column and Y for both servers in the Up To Date column<br>• Active/standby state for both servers in the Primary CMP Cluster. |
| 26. ☐ | Proceed to next upgrade procedure | At this point, the Primary Site-1 is running Release 12.6<br>• Secondary SITE is on 12.5.0 or 12.5.0.4.<br>• Proceed to the next procedure to upgrade the non-CMP servers. |
| **—End of Procedure—** | | |

## 2.5 Upgrade non-cmp clusters 12.5.0/12.5.0.4 to 12.6

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 22 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 12.6 ISO files | **Upgrade → Upgrade Manager**<br>• Verify that all CMP clusters have both Active and Standby status.<br>• Verify that all MPE & MRA clusters have both Active and Standby status.<br>• Verify that the CMP cluster is upgraded successfully and running Policy Management Release 12.6<br>**Upgrade → ISO Maintenance**<br>• Verify that Policy Management release 12.6 ISO files are available for all clusters. One 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 12.5.0 or 12.5.0.4 upgrade to 12.6

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

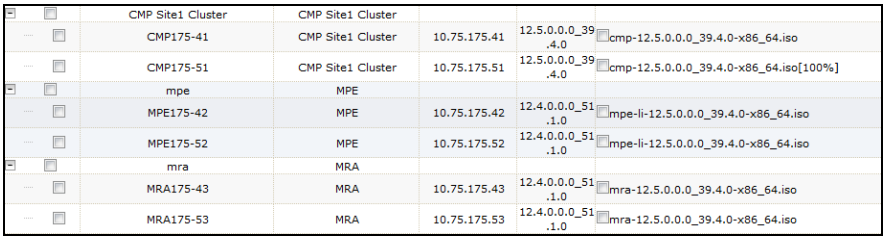
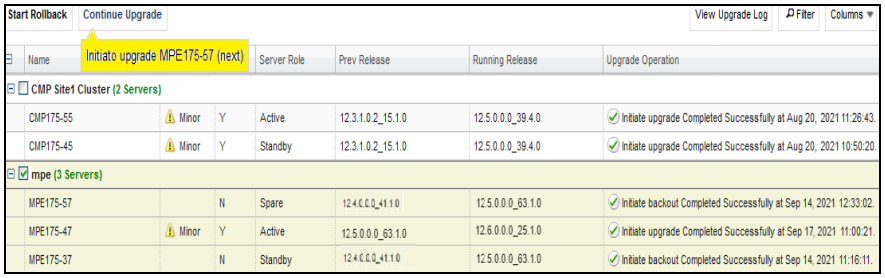
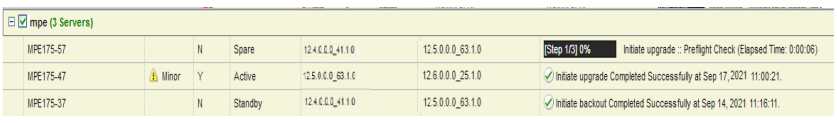
The upgrade procedure is essentially the same for any non-CMP cluster.

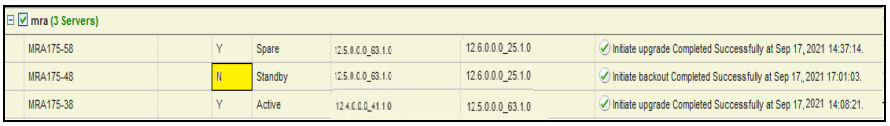
1. Select and start upgrade on the Standby server
2. Failover
3. Continue upgrade on remaining server
4. Re-apply configuration

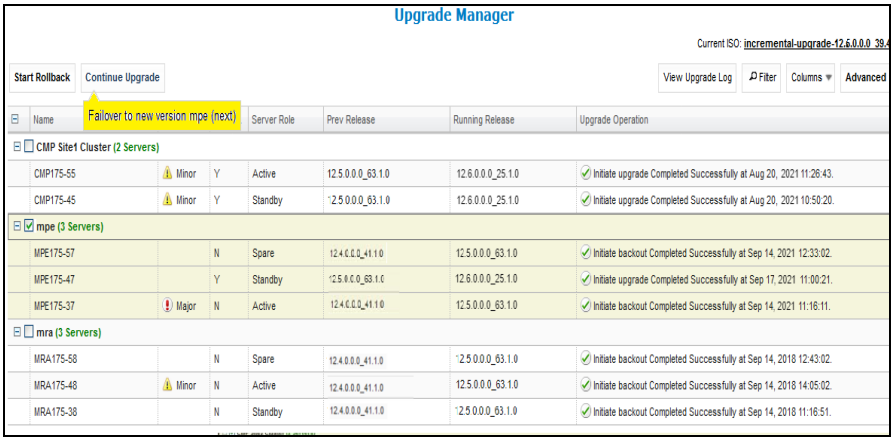
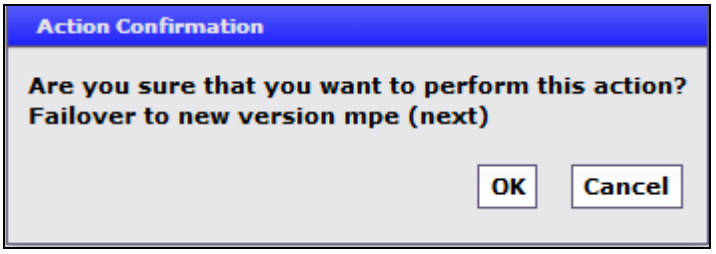
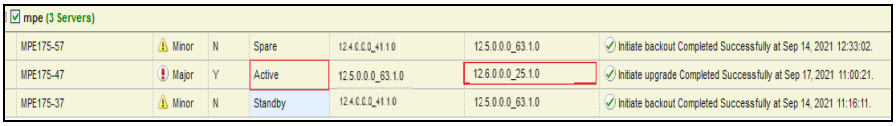
**NOTES:**

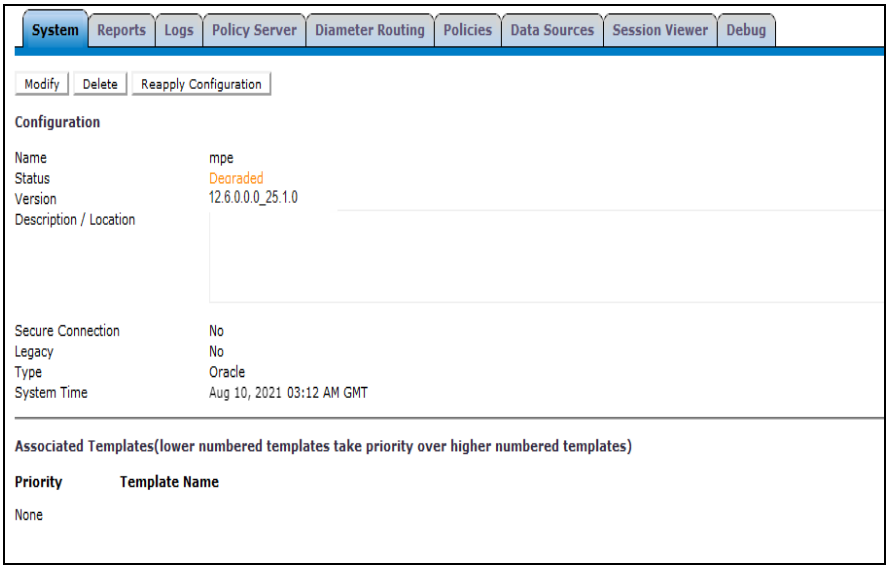
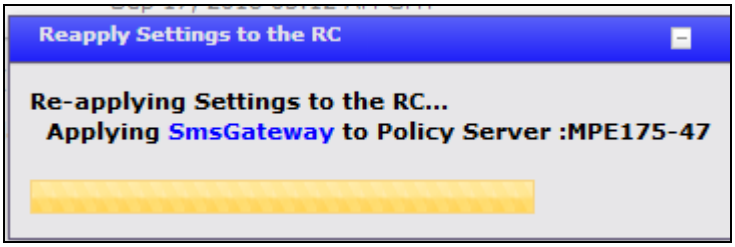
- All CMP clusters must have been upgraded to Policy Management release 12.6 before performing the following procedures.
- The maximum clusters to be running the upgrade at one time is 16.

**Procedure 23 Upgrade NON-CMP Servers**

| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **CMP GUI:** Health checks on the servers to be upgraded | 1. Check for current active alarms<br>- For the MPE: **Policy Server→Configuration→Reports → Reset Counters**<br>- For the MRA: **MRA→Configuration→Reports → Reset Counters**<br>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**.<br>2. Verify information for the MRAs/MPEs:<br>- Current Release 12.5.0 or 12.5.0.4 installed<br>- Running with Active/Standby status<br>3. Navigate to **Upgrade → ISO Maintenance**<br>4. Verify the ISO version to be deployed is 12.6<br>  |
| 3. ☐ | **CMP GUI:** Upgrade clusters<br>**NOTE:** The upgrade of one server takes approximately 35 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.<br>1. Navigate to **Upgrade → Upgrade Manager**<br>2. Click the checkbox for the desired cluster (one cluster at a time.) It can be an MRA or an MPE.<br>3. Click **Continue Upgrade** or **Resume Upgrade**<br>  <br>4. Click **OK** to confirm and continue with the operation. It begins the upgrade of the standby server for that cluster.<br>  <br>5. Wait until the standby server reports OOS before selecting the next cluster |

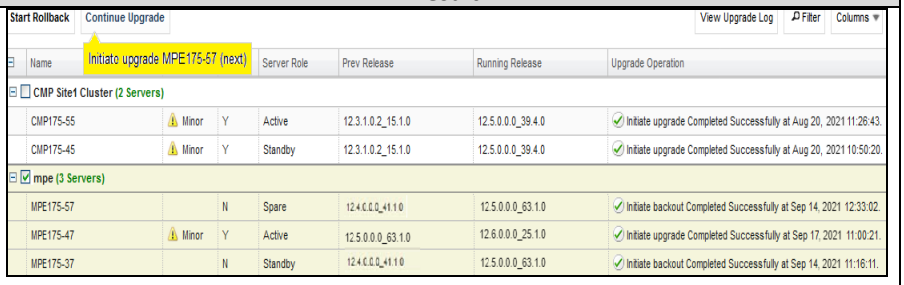
| Step | Procedure | Result |
|---|---|---|
| | | 6. Follow the progress status in the Upgrade Operation column.<br>7. During the upgrade activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the clusters are completely upgraded.<br><br>**Expected Critical Alarms**<br><br>**31283** High availability server is offline<br>**70001** QP_procmgr failed<br>**31227** High availability status failed<br><br>**Expected Major Alarm:**<br><br>**70004** QP Processes down for maintenance<br>**31233** High availability path loss of connectivity<br><br>**Expected Minor Alarms**<br><br>**70503** Upgrade Director Server Forced Standby<br>**70507** Upgrade Director In Progress<br>**70500** Upgrade Director System Mixed Version<br>**70501** Upgrade Director Cluster Mixed Version<br>**31114** DB Replication over SOAP has failed<br>**31102** DB replication from a master DB has failed<br>**31106** DB Merge To Parent Failure<br>**31107** DB Merge From Child Failure<br>**31101** DB Replication To Slave Failure<br>**31282** HA management fault<br>**78001** RSYNC Failed<br>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.<br>  <br><br>A number of different alarms may be raised at this point:<br><br>**Expected Minor Alarms**<br><br>**78001** RSYNC Failed<br>**70500** The system is running different versions of software<br>**70501** The Cluster is running different versions of software<br>**70503** The server is in forced standby |

| Step | Procedure | Result |
|---|---|---|
| 4. ☐ | **CMP GUI**: Continue Upgrade MRA/MPE clusters. Next operation is a failover.<br><br>**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.<br><br>1. Navigate to **Upgrade → Upgrade Manager**<br><br>2. Select the cluster (one cluster at a time). It can be an MRA or MPE.<br><br>3. Click **Continue Upgrade**. When hovering over the **Continue Upgrade** button, it displays the Failover to new version message.<br><br>  <br><br>4. Click **OK** to confirm and continue with the operation. It begins to failover the cluster.<br><br>  <br><br>5. Wait until failover completes, that is, the server running 12.5 becomes the active server before failing over the next cluster.<br><br>  |

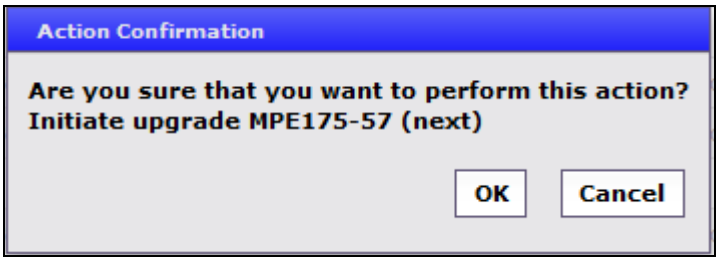
| Step | Procedure | Result |
|---|---|---|
| 5. ☐ | **CMP GUI:** Reapply configuration on the MPE/MRA cluster that failed over successfully. | • For MPE: **Policy Server → Configuration → <***MPE cluster***> → System**<br>• For MRA: **MRA→Configuration→<***MRA cluster***>→System**<br>The selected cluster has the status shown as Degraded and still shows the old release version. Config mismatch may be displayed as well.<br>1. Click the **Reapply Configuration** operation.<br>  <br>**NOTE:** A progress banner displays for the MPE reapply configuration. A progress banner DOES NOT display for the MRA reapply configuration.<br>  <br>2. Verify that the Version is changed to the upgraded Release 12.5<br>3. The cluster still shows the Degraded status:<br>  |

| Step | Procedure | Result |
|---|---|---|
| 6. ☐ | **CMP GUI:** Current alarms | Some of the alarms below may appear:<br><br>**Expected Critical alarm**<br><br>None<br><br>**Expected Major Alarm**<br><br>**78001** Rsync Failed<br><br>**Expected Minor Alarms**<br><br>**70500** The system is running different versions of software<br>**70501** The Cluster is running different versions of software<br>**70503** The server is in forced standby<br>**71402** Diameter Connectivity Lost<br>**31101** DB Replication To Slave Failure<br>**31113** DB Replication Manually Disabled |
| 7. ☐ | **CMP GUI:** Verify traffic becomes active within 90 seconds | 1. Navigate to **Upgrade Manager → System Maintenance**<br>- If traffic is active, go to step 9.<br>- If traffic does not become active within 90 seconds:<br>2. Select the checkbox for the partially upgraded cluster, and select **Operations → Rollback**.<br>3. The pre-12.6 MPE server should become active and resume handling traffic. |
| 8. ☐ | **CMP GUI:** Reapply configuration | 1. Navigate to **Policy Server → Configuration →** *<mpe_cluster name>* **→ System**<br>or<br>**MRA → Configuration →** *<mra_cluster name>* **→ System**<br>2. Click **Reapply Configuration**<br>• Verify that the version is changed back to 12.5.0 or 12.5.0.4, and the action report success.<br>• 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.<br>1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select a cluster (one cluster at a time), it can be an MRA or an MPE.<br>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

**Expected Major Alarm**

**70004** QP Processes down for maintenance

**Expected Minor Alarms**

**70503** Upgrade Director Server Forced Standby

**70507** Upgrade Director In Progress

**70500** Upgrade Director System Mixed Version

**70501** Upgrade Director Cluster Mixed Version

**70502** Upgrade Director Cluster Replication Inhibited

**31114** DB Replication over SOAP has failed

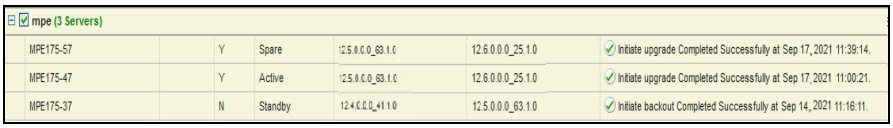
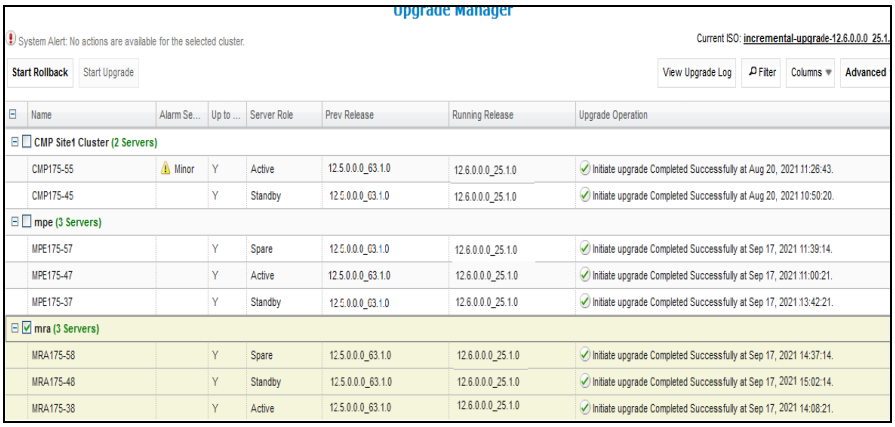
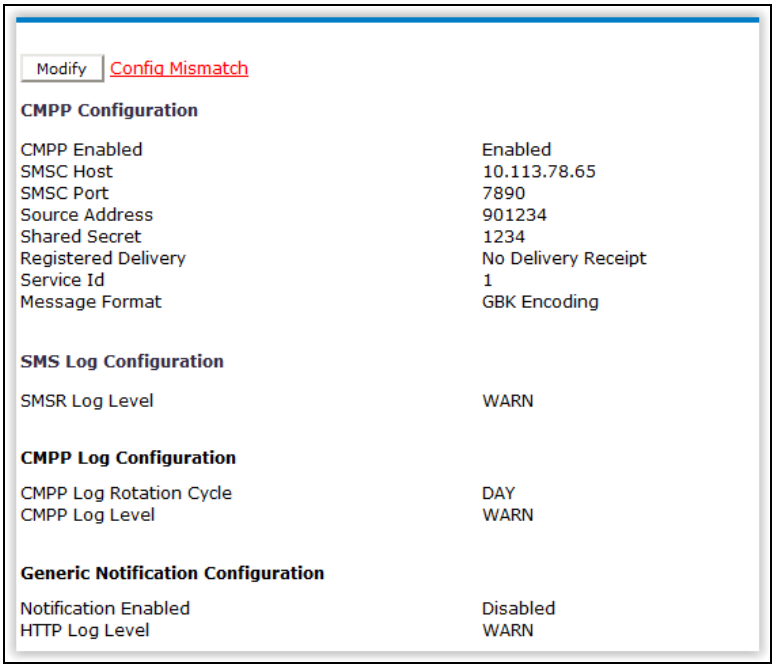
**31106** DB Merge To Parent Failure

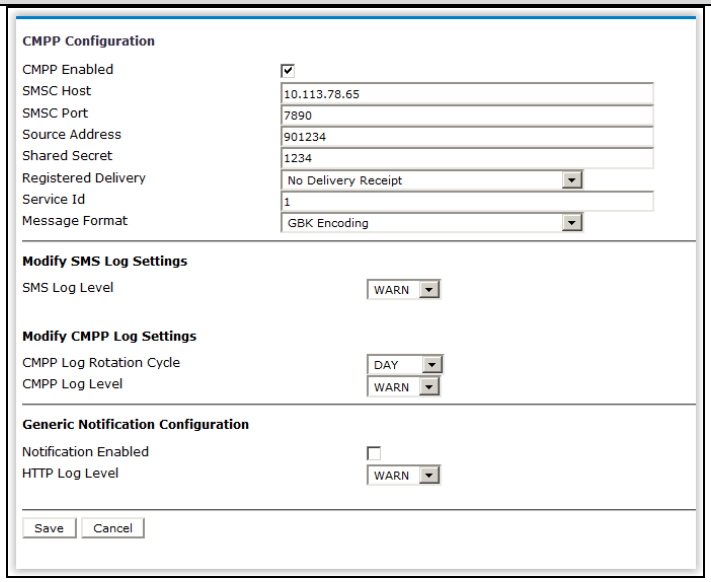
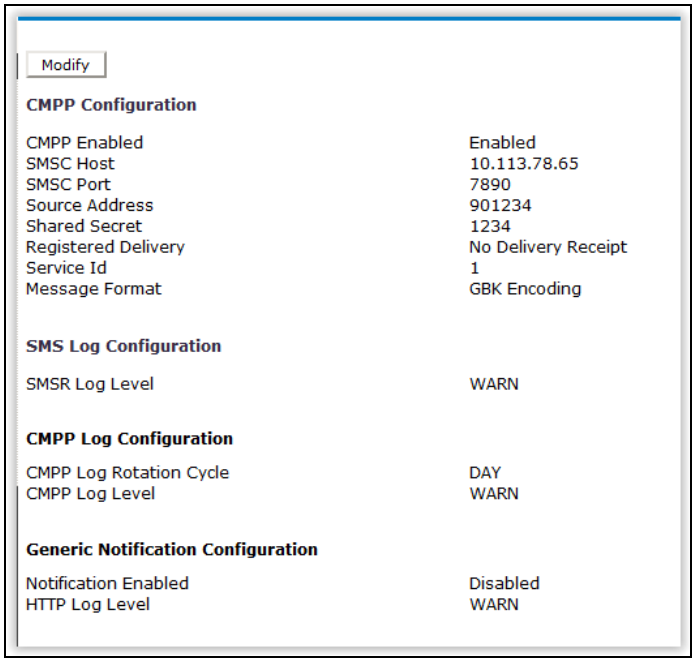
**31107** DB Merge From Child Failure

**31101** DB Replication To Slave Failure

**31102** DB Replication from Master Failure

**31113** DB Replication manually Disabled

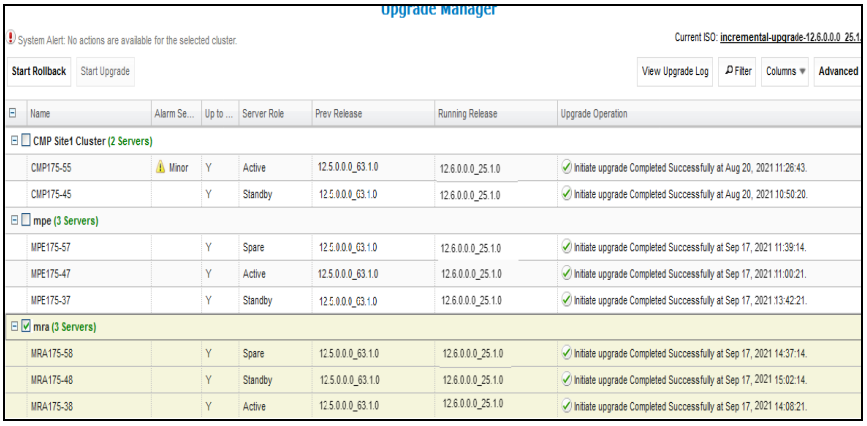
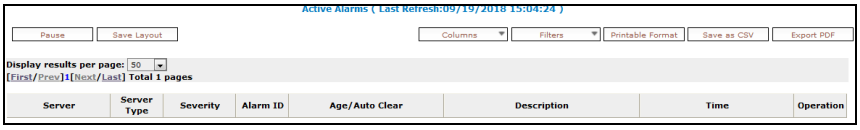
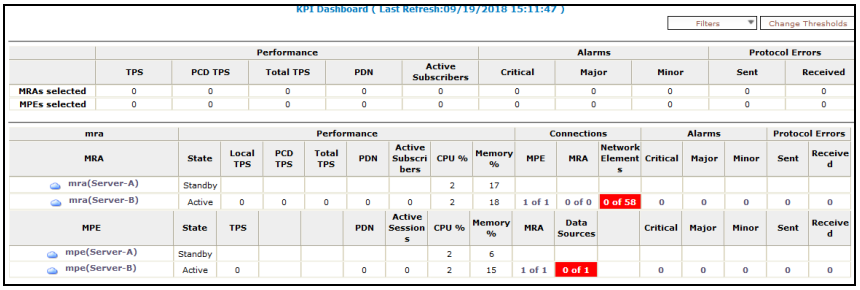
| Step | Procedure | Result |
|---|---|---|
| | | Upgrade is complete when the `Initiate upgrade completed successfully at…` message displays in the Upgrade Operation column. The server goes back to Standby state and the Up to Date column shows a Y (YES).<br>  |
| 10. ☐ | REPEAT steps 1 through 10 for next MPE/MRA cluster(s) | Proceed with the next clusters until all clusters have been upgraded<br>  |
| 11. ☐ | **CMP GUI:**<br>Modify/save SMSR configuration | **System Administration → SMS Relay → Modify**<br>**NOTE: This step is only for Wireless-C system. If you do not see SMS Relay under System Administration, skip this step.**<br>Initial access into this configuration upon upgrade to release 12.6, the configuration shows as such with Config Mismatch.<br>  <br>1. Click **Modify.** The following is an example of the SMSR configuration. DO NOT change any of the configuration if it has been working in the past. |

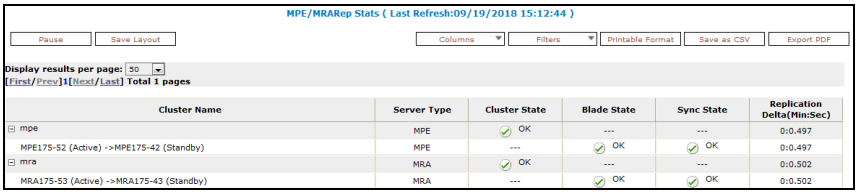
| Step | Procedure | Result |
|---|---|---|
| | |  <br>2. Click **Save** to save the configuration and continue as shown.<br>  <br>**NOTE:** The Config Mismatch message is not there with the saved configuration. |
| **—End of Procedure—** | | |

## 2.6 Post Upgrade health Check for wireless systems

**NOTE:** This section is used when the entire topology is running release 12.6

**Procedure 24 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**.<br>2. View the Up to Date, Running Release, and Upgrade Operation columns and verify they read Y, 12.6…., and Initiate upgrade completed successfully at… respectively, for all servers in all clusters.<br>  |
| 2. ☐ | **CMP GUI:** View current alarms | 1. Navigate to **System Wide Reports→Alarms→Active Alarms**.<br>2. Verify that all alarms due to the upgrade have been cleared.<br>  |
| 3. ☐ | **CMP GUI**: View current KPIs | 1. Navigate to **System Wide Reports→KPI Dashbord.**<br>2. Make sure the counter stats are incrementing properly.<br>  |

| Step | Procedure | Result |
|---|---|---|
| 3. ☐ | **CMP GUI:** Replication stats | 1. Navigate to **System Wide Reports→Others→MPE/MRA Rep Stats** (for a wireless system)<br>2. Verify all clusters and servers are in OK state.<br>  |
| 3. ☐ | Verify System Health | 1. Use the **`sudo syscheck`** command on every server.<br>2. Verify that each class test returns OK. For example:<br>`$ sudo syscheck`<br>`Running modules in class disk... OK`<br>`Running modules in class hardware... OK`<br>`Running modules in class net... OK`<br>`Running modules in class proc... OK`<br>`Running modules in class system...OK`<br>LOG LOCATION: `/var/TKLC/log/syscheck/fail_log` |
| **—End of Procedure—** | | |

## 2.7 Backout (ROLLBACK) 12.5.0/12.5.0.4 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-12.6 release with Active, Standby status.

Expected pre-conditions:

- The primary active CMP is on release 12.6
- The cluster servers to be backed out are on release 12.5.0/12.5.0.4

### *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)**

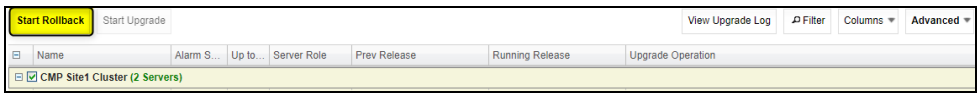
**NOTE:** At this time, all MPEs and MRAs must be backed out to the previous release.

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

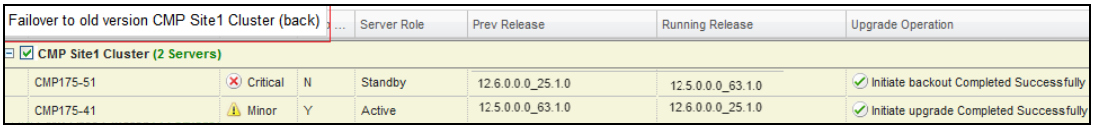
**Backout Primary CMP (From 12.6 to 12.5.0/12.5.0.4)**

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

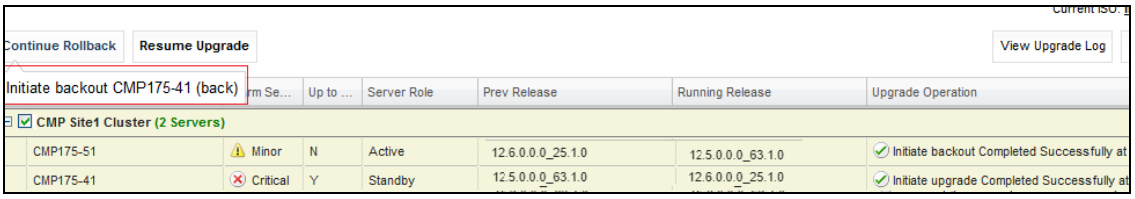
1. Use the CMP GUI (Upgrade Manager) to backout the Primary standby CMP cluster
2. Select the CMP cluster and click **Start Rollback** on the top left to initiate backout on Standby CMP




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



4. Log in to the Primary CMP VIP
5. Use the 12.5.0/12.5.0.4 Ugrade Manager to complete backout of the Primary CMP cluster




6. 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 12.6
2. Cluster is any of MPE or MRA
3. One server of target cluster is on Release 12.6
4. Other servers of target cluster are on Release 12.5.0 or 12.5.0.4

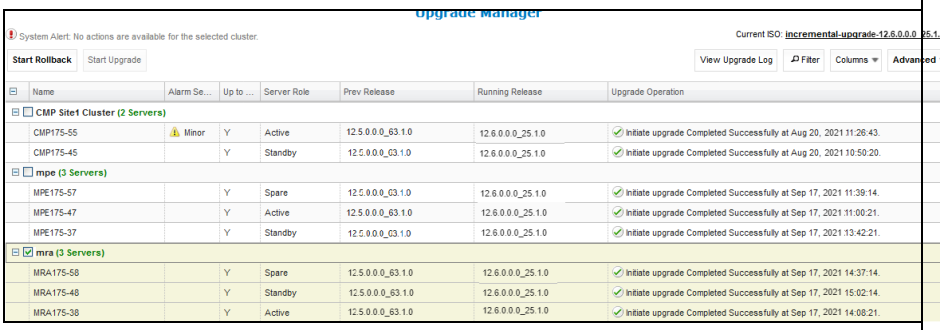
**NOTES:**

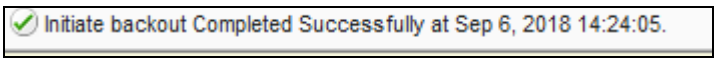
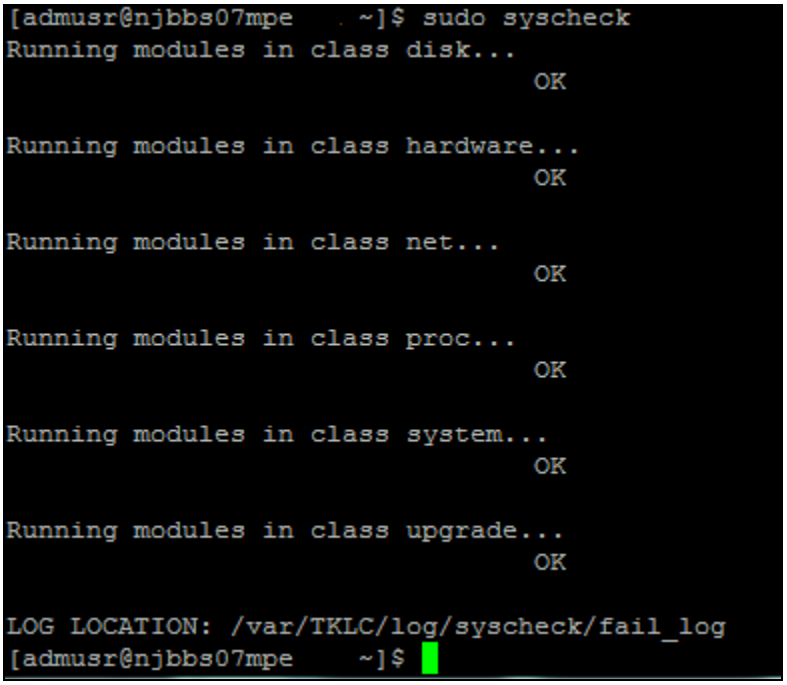
- This procedure must be performed within a maintenance window.
- This procedure takes approximately 45 minutes at most per server.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

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

**Procedure 25 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**<br>2. Confirm status of the cluster to be backed out:<br>- Primary Active CMP is on Release 12.6<br>- Target Cluster has 1 server on Release 12.5.0/12.5.0.4, and 1 server on Release 12.6<br>- Active server is on 12.5.0/12.5.0.4 |
| 2. ☐ | **MPE/MRA SSH:** Verify `/var/log/messages` file size | 1. Using SSH, login to the Standby server to be backed out as admusr.<br>`$ ls -lh /var/log/messages`<br>2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |

| Step | Procedure | Result |
|---|---|---|
| 3. ☐ | **CMP GUI:** Verify the status of affected Clusters<br><br>**NOTE:** This takes approximately30 minutes to complete. | 1. Select **Start Rollback** or **Continue Rollback**. When hovering over the button, it indicates the server to get backed out.<br>  <br>2. Click **OK** to confirm and continue with the operation. It begins to back-out.<br>3. Follow the progress status in the Upgrade Operation column.<br>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.<br><br>**Expected Critical Alarms**<br><br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br>**70028** Signaling bonded interface is down<br>**31283** High availability server is offline<br><br>**Expected Major Alarms**<br><br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31282** The HA manager (cmha) is impaired by a s/w fault<br>**31232** High availability server has not received a message<br>**31284** High availability remote subscriber has not received a heartbeat<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31104** DB Replication latency has exceeded thresholds<br>**78001** Transfer of Policy jar files failed<br>**70500** The system is running difference versions of software<br>**31100** The DB replication process is impaired by a s/w fault<br>Back-out of the server is complete when the successful completion message |

| Step | Procedure | Result |
|---|---|---|
| | | (Initiate Back-out Completed Successfully)<br>  |
| 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:<br>`$ sudo syscheck`<br>  <br>2. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>3. **NOTE:** Permissions should be the following,<br>`drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp`<br>4. If the permissions are not as listed above then perform the following; otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>5. Verify:<br>`$ ls -l /`<br>6. Perform syscheck again:<br>`$ sudo syscheck` |

| Step | Procedure | Result |
|---|---|---|
| 7. ☐ | **MPE/MRA CLI:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the upgrade is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable when primary is set to eth02.<br>3. If this blade is the active blade, change it to standby.<br>4. Open the ifcfg-bond0 file.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>5. Find the eth02.<br>6. Change primary=eth02 to primary=eth01.<br>7. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| **—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 12.5.x (MRA, MPE, CMP) with Active, Standby status.

Expected pre-conditions:

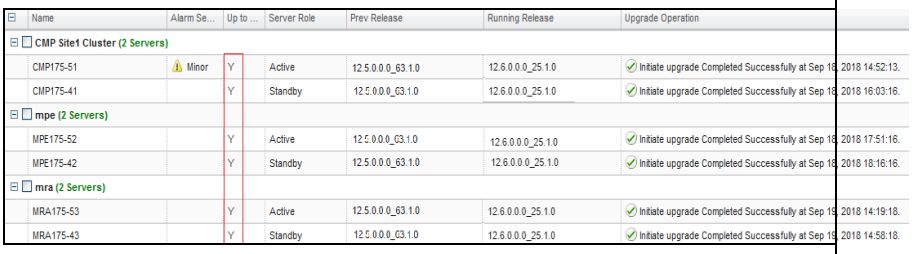
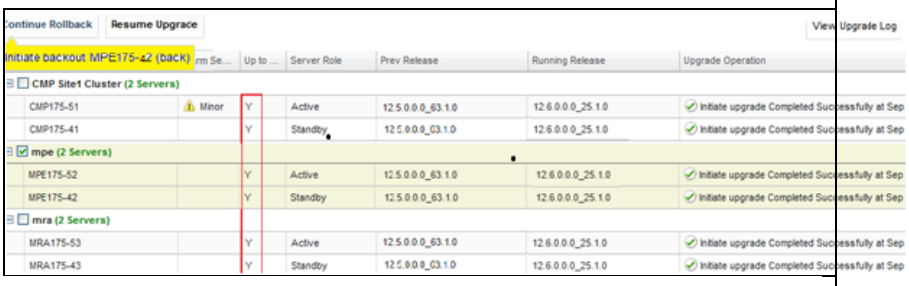
1. Primary Active CMP is on Release 12.6.
2. Cluster is of MPE or MRA.
3. Servers of target cluster are on Release 12.6 in either in Active, Standby or Force Standby role.

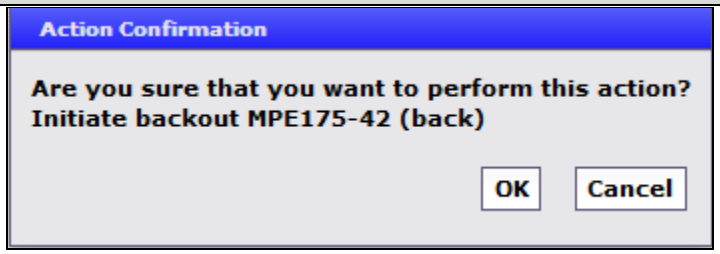
**NOTES:**

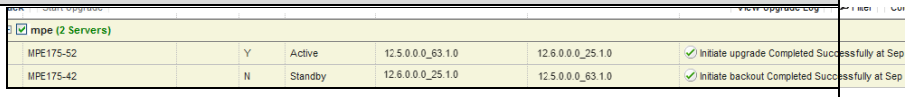
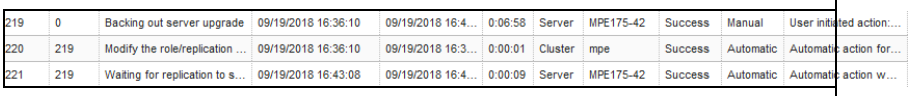
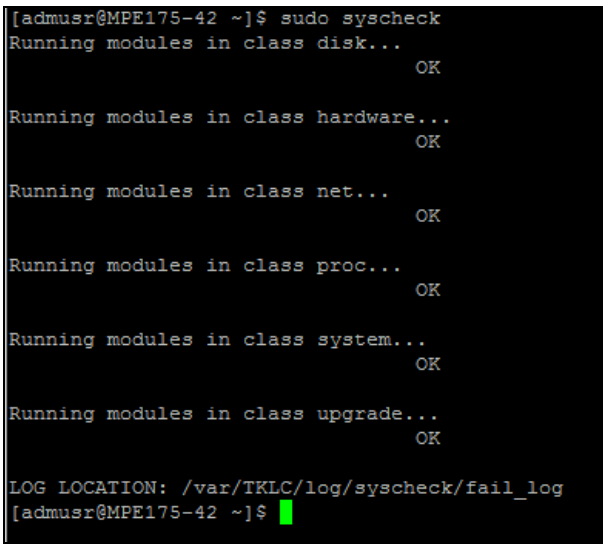
- This procedure must be performed within a maintenance window.
- This takes approximately 105 minutes per MPE or MRA cluster.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

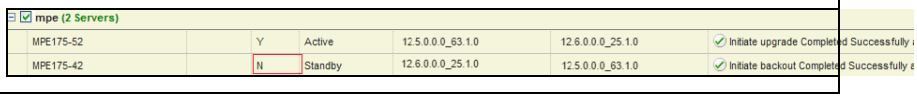
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

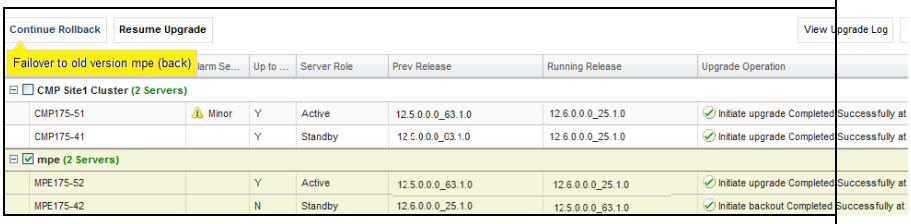
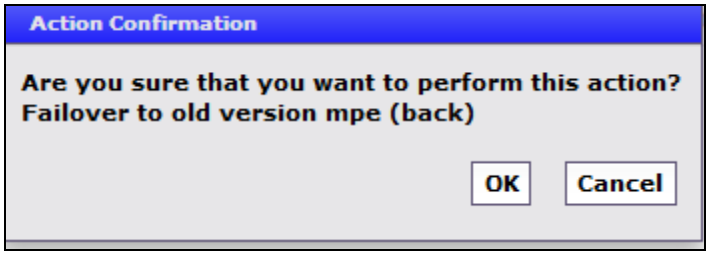
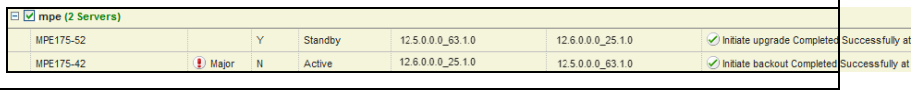
**Procedure 26 Back-out Fully Upgraded MPE/MRA Cluster**

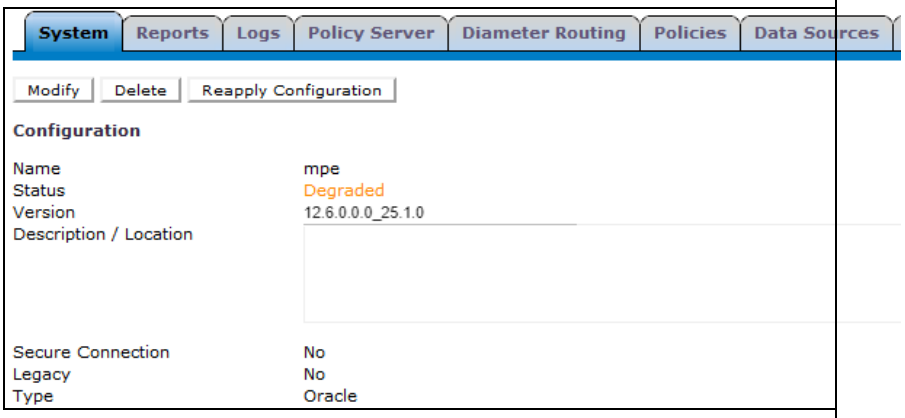
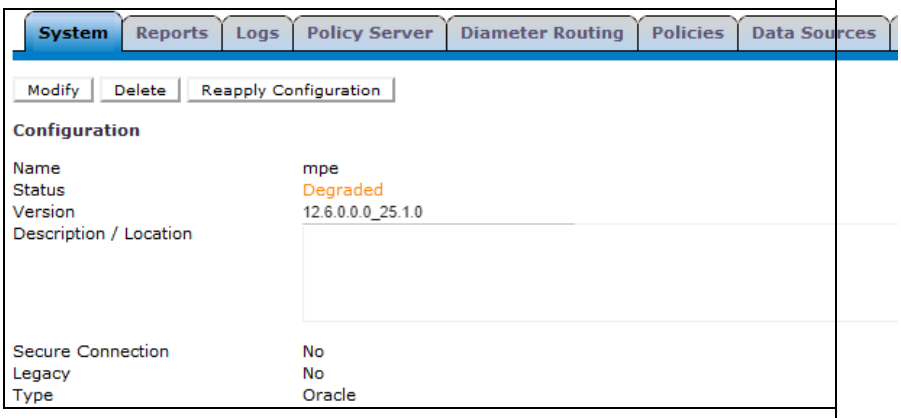
| Step | Procedure | Result |
|---|---|---|
| 1. ☐ | **CMP GUI:** Verify the status of affected Clusters | 1. Navigate to **Upgrade → Upgrade Manager**<br>2. Confirm status of the cluster is backed out:<br>- Primary Active CMP is on Release 12.6<br>- MPE/MRA is on Release 12.6 Up to Date Column shows Y for all servers in this cluster<br>**EXAMPLE**<br>  |
| 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<br>**NOTE:** The Active server is checked after the failover later on in this procedure.<br>`$ ls -lh /var/log/messages`<br>2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following commands, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |
| 3. ☐ | **CMP GUI:** Initiate Back-out<br>**NOTES:**<br>Each back-out of one blade server completes in approximately 30 minutes.<br>Up to 8 clusters can be backed out at the same time, selecting one at a time. | 1. Navigate to **Upgrade → Upgrade Manager**<br>2. Select the cluster (one cluster at a time) (can be an MRA or MPE)<br>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.<br>  <br>4. Click **OK** to confirm and continue with the operation. It begins to back-out. |

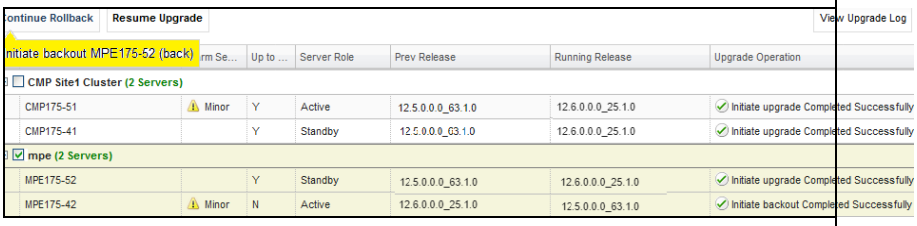
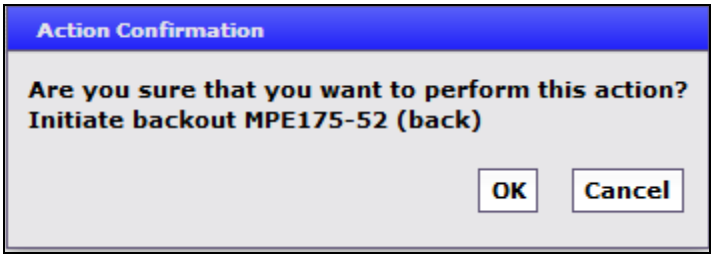
| Step | Procedure | Result |
|---|---|---|
| | |  <br>5. Follow the progress status in the Upgrade Operation column.<br>6. At this point, the server backing out goes into OOS state<br>7. Wait until the server goes to an OOS state before selecting the next cluster to back-out.<br>During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out.<br>**Expected Critical Alarms**<br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br>**70028** Signaling bonded interface is down<br>**31283** High availability server is offline<br>**Expected Major Alarms**<br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br>**Expected Minor Alarms**<br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31282** The HA manager (cmha) is impaired by a s/w fault<br>**31232** High availability server has not received a message ….<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31104** DB Replication latency has exceeded thresholds<br>**78001** Transfer of Policy jar files failed<br>**70500** The system is running difference versions of software<br>**31100** The DB replication process is impaired by a s/w fault<br>Back-out of the server is complete when the successful completion displays in the Upgrade Operation column. The server shows running release of 12.5.0 and 12.5.0.4 and return to standby with an N in the Up To Date Column. |

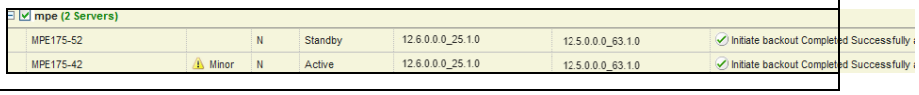
<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td></td><td></td><td> 
</td></tr>
<tr><td>4. ☐</td><td>CMP GUI<br><br>Verify the back-out is successful</td><td>1. Select the partially Backed out cluster<br>2. Select the View Upgrade LOG<br> 
<br>3. Check upgrade logs for the remainder of partially Backed out clusters.</td></tr>
<tr><td>5. ☐</td><td>MPE/MRA SSH<br><br>Verify <code>syscheck</code> and <code>/tmp</code> directory permission</td><td>1. Log into the backed-out standby server and verify that there are no failures in syscheck:<br><code>$ sudo syscheck</code><br> 
<br>2. Verify the <code>/tmp</code> directory permissions:<br><code>$ ls -l /</code><br>3. NOTE: Permissions should be:<br><code>drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp</code><br>4. If the permissions are not as listed above then perform the following otherwise skip to next step:<br><code>$ sudo chmod 777 /tmp</code><br><code>$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp</code><br><code>$ sudo chmod +t /tmp</code><br>5. Verify:<br><code>$ ls -l /</code><br>6. Perform syscheck again:<br><code>$ sudo syscheck</code></td></tr>
</table>

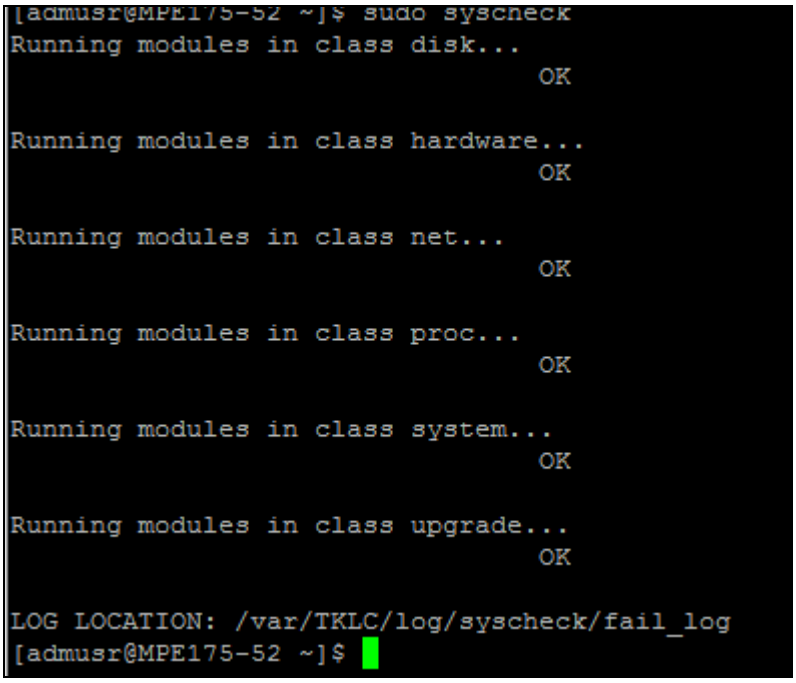
| Step | Procedure | Result |
|---|---|---|
| 6. ☐ | **MPE/MRA CLI:** Verify eth01 is primary device interface | This step only applies if the backed-out Standby server has a condition in which after the upgrade is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable when primary is set to eth02.<br>If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>1. Find the following keyword:<br>2. Change primary=eth02 to primary=eth01<br>3. Save and exit (for example, in vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 7. ☐ | Confirm MPE/MRA server status | Ensure that the Active are on 12.6 and the standby server shows running release of 12.5.0 or 12.5.0.4<br>  |

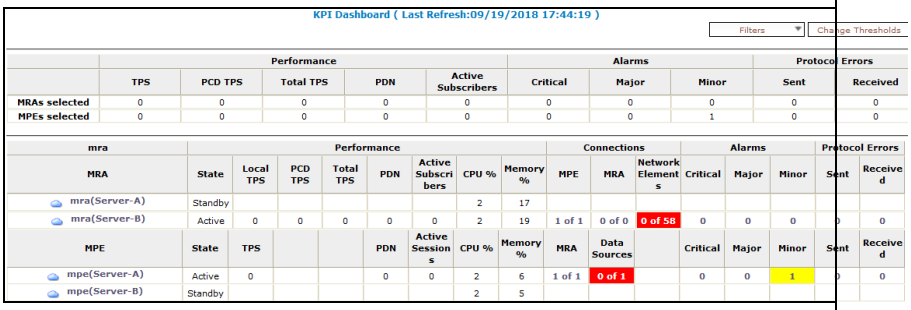
| Step | Procedure | Result |
|---|---|---|
| 8. ☐ | **CMP GUI**: Continue the back-out of the MRA/MPE clusters. Next operation is failover to the 12.5.0/12.5.0.4 server.<br><br>**NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time. | Current state of the cluster must be as follows.<br>• Active Server is on Release 12.6<br>• Standby Server is on Previous release<br>1. Select the cluster (one cluster at a time) (can be an MRA or MPE)<br>2. Click Continue Rollback. When hovering over the button, it informs you to failover to old version, which is 12.5.0/12.5.0.4.<br>  <br><br>3. Click **OK** to confirm and continue with the operation. It begins to failover.<br>  <br><br>Wait until the server fails over before selecting the next cluster. This takes approximately 2 minutes<br><br>**Expected Critical Alarms**<br><br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br><br>**Expected Major Alarms**<br><br>**74603** The number of failed MPE primary cluster reaches the threshold<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**31102** DB replication from a master DB has failed<br>**71402** Diameter Connectivity Lost<br>**31101** DB replication to a slave DB has failed<br>**78001** Transfer of Policy jar files failed<br>State of the cluster looks like the following when the failover completes.<br>  <br> |

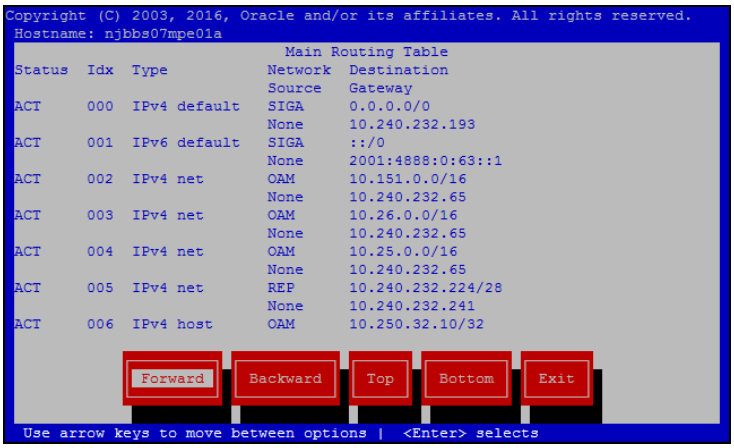
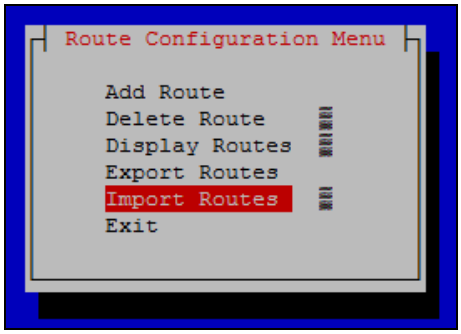
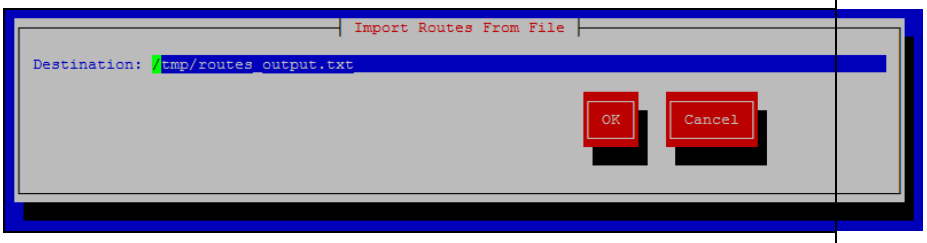
| Step | Procedure | Result |
|---|---|---|
| 9. ☐ | **CMP GUI:** Reapply Configuration on MPE/MRA cluster that competed the failover successfully | • For MPE: Navigate to **Policy Server → Configuration →** <*MPE*> **→ System**<br>• For MRA: Navigate to **MRA → Configuration →** <*MRA*> **→ System**<br>The selected cluster status is Degraded as expected as shown:<br>  <br>Click **Reapply Configuration** operation.<br>• The Version is successfully changed to the upgraded Release 12.6.0<br>• The status is Degraded which is a normal reporting event as the servers are in different status.<br>**MPE**<br>  |
| 10. ☐ | **MPE/MRA SSH:** Verify `/var/log/messages` file size | Use SSH to login to the Standby server to be backed out as admusr.<br>`$ ls -lh /var/log/messages`<br>ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>Verify:<br>`$ ls -lh /var/log/messages` |

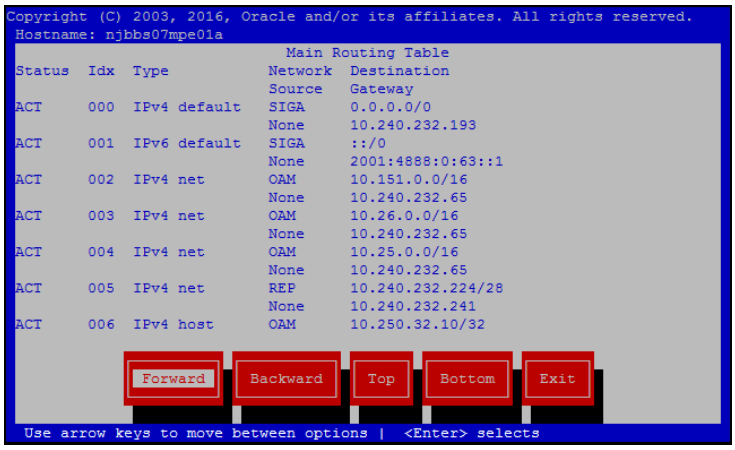
| Step | Procedure | Result |
|---|---|---|
| 11. ☐ | **CMP GUI:** Complete Back-out of cluster(s)<br><br>**NOTE:** Up to 8 clusters can be backed out at the same time, selecting one at a time.<br><br>**NOTE:** Each back-out of one blade server completes in approximately 30 minutes | 1. Select the cluster (one cluster at a time) (can be an MRA or MPE)<br>2. Click **Continue Rollbac**k. When hovering over the button, it indicates the back-out server.<br>  <br><br>3. Click **OK** to confirm and continue with the operation. It begins to back-out.<br>  <br><br>4. Follow the progress status in the Upgrade Operation column.<br>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.<br><br>**Expected Critical Alarms**<br><br>**70001** The qp_procmgr process has failed<br>**31227** The high availability status is failed due to raised alarms<br>**70028** Signaling bonded interface is down<br>**31283** High availability server is offline<br><br>**Expected Major Alarms**<br><br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br><br>**Expected Minor Alarms**<br><br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31282** The HA manager (cmha) is impaired by a s/w fault<br>**31232** High availability server has not received a message<br>**31284** High availability remote subscriber has not received a heartbeat<br>**31107** DB merging from a child Source Node has failed |

| Step | Procedure | Result |
|---|---|---|
| | | **31114** DB Replication of configuration data via SOAP has failed<br>**31104** DB Replication latency has exceeded thresholds<br>**78001** Transfer of Policy jar files failed<br>**70500** The system is running difference versions of software<br>**31100** The DB replication process is impaired by a s/w fault<br>6. Back-out of the server is complete when the successful completion message (initiate Back-out completed successfully) displays in the Upgrade Operation column.<br>7. Verify in Upgrade Log that that back-out was successful:<br>8. All of the servers are on Release 12.5.x at this point and show active/standby<br>  |

| Step | Procedure | Result |
|---|---|---|
| 12. ☐ | **MPE/MRA SSH:** Verify syscheck and `/tmp` directory permission | 1. Login to the backed-out standby server as admusr.<br>2. Verify that there are no failures in syscheck:<br>`$ sudo syscheck`<br>  <br>3. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>4. **NOTE:** Permissions should be the following,<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>5. If the permissions are not as listed above then perform the following otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>6. Verify:<br>`$ ls -l /`<br>7. Perform syscheck again:<br>`$ sudo syscheck` |

| Step | Procedure | Result |
|---|---|---|
| 13. ☐ | **MPE/MRA CLI:** Verify eth01 is primary device interface | This step only applies if the backed-out standby server has a condition in which after the back-out is successful ETH02 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br>2. Check that the output shows that the primary is set to eth02, it should be eth01. This step is only applicable when primary is set to eth02.<br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>4. Find eth02.<br>5. Change primary=eth02 to primary=eth01<br>6. Save and exit (for example, in vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 14. ☐ | **CMP GUI:** Verify that backed out cluster is processing traffic normally. | Verify Cluster is processing traffic normally.<br>Navigate to **System Wide Reports → KPI Dashboard**.<br>  |
| 15. ☐ | **CMP GUI:** Verify alarms | 1. Navigate to System Wide Reports → Alarms → Active Alarms<br>2. Verify that there are no unexpected active alarms present.<br>**NOTE:** Some alarms may take 30 minutes to 1 hour for auto clearing time. |
| 16. ☐ | **MPE/MRA SSH:** Verify routes | 1. Login into MPE/MRA server as admusr.<br>2. Copy routes_output.txt from the `/home/admusr` directoy to the `/tmp` directory.<br>`$ sudo cp routes_output.txt /tmp`<br>`$ cd /tmp`<br>`$ ls`<br>`routes_output.txt`<br>**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** |

| Step | Procedure | Result |
|---|---|---|
| | | **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.**<br><br>3. Start the platcfg utility.<br>`$ sudo su - platcfg`<br>4. Navigate to **Policy Configuration → Routing Config → Display Routes**<br>5. Click **Forward** to view all the routes.<br>6. Verify that all routes are present.<br>**Example**<br>  <br>7. If any of the routes are missing then perform the following otherwise skip to step 18<br>8. Navigate back to Route Configuration Menu and select **Import Routes**.<br>  <br>9. Click **OK**.<br>  <br>10. Routes are imported from `/tmp/routes_output.txt` file and Route |

| Step | Procedure | Result |
|---|---|---|
| | | Configuration menu displays.<br>11. Select Display Routes<br>12. Verify that all routes are present.<br>13. Click **Forward** to view all the routes.<br>**Example**<br>  <br><br>14. Exit platcfg utility<br>**WARNING: It is critical that proper exit of the platcfg menu is strictly adhered to. Not exiting the platcfg menu and or in the event of a blade service interruption occur while still within the platcfg menu can cause an adverse impact to application functionality on the blade. If this occurs contact Oracle personnel immediately and alert Maintenance Engineering.** |
| 17. ☐ | Repeat for other clusters as needed | Repeat this procedure for the remaining MPE/MRA servers. |
| 18. ☐ | Perform syscheck and verify that alarms are clear. | Another syscheck on all the back-out servers can be performed to ensure all modules are still operationally OK before progressing to the next Procedure.<br>1. Navigate to **System Wide Reports → Alarms → Active Alarms**<br>2. Verify that there are no unexpected active alarms present.<br>**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 12.6
2. Secondary CMP, MPE and MRA Clusters are on Release 12.5.0 or 12.5.0.4

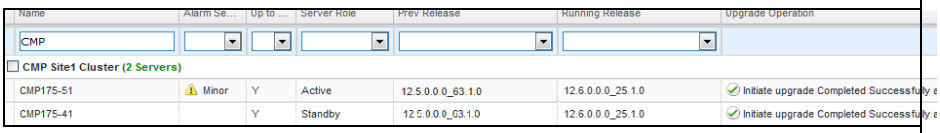
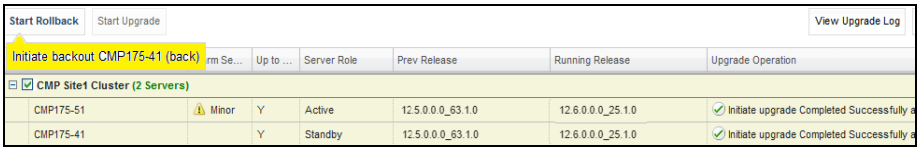
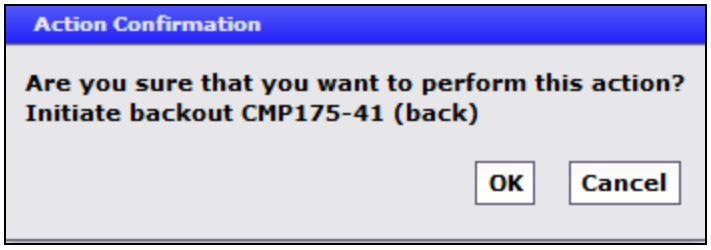
**NOTES:**

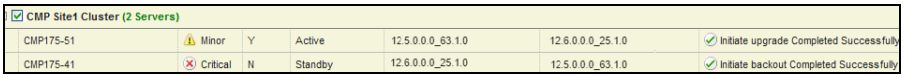
- This procedure must be performed within a maintenance window.

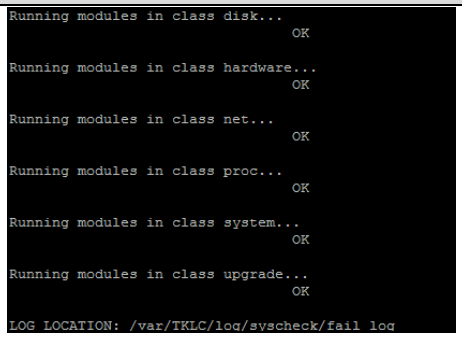
- This procedure takes approximately 105 minutes.
- If this procedure fails, contact Oracle Technical Services and ask for ASSISTANCE.

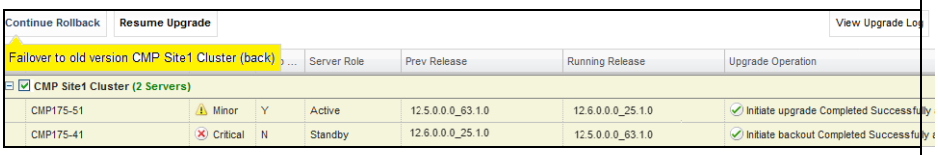
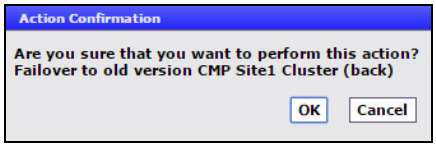
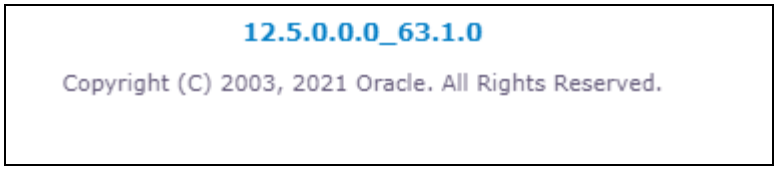
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

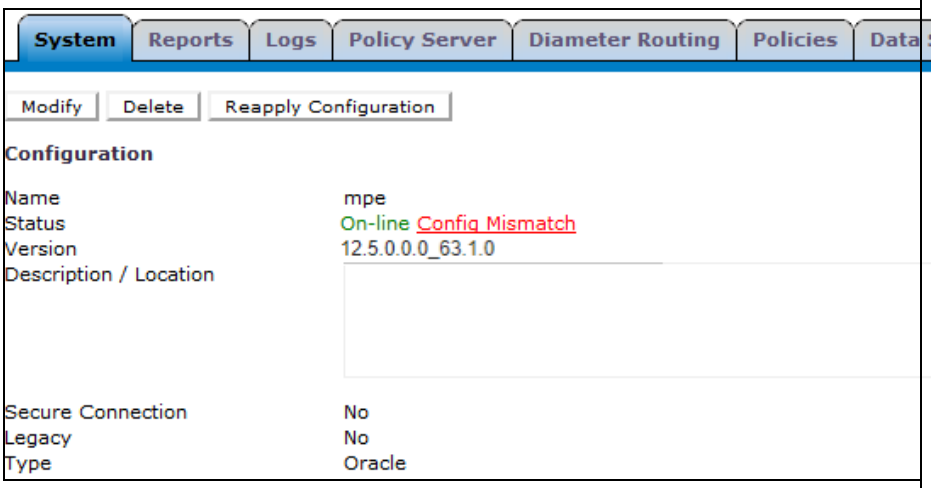
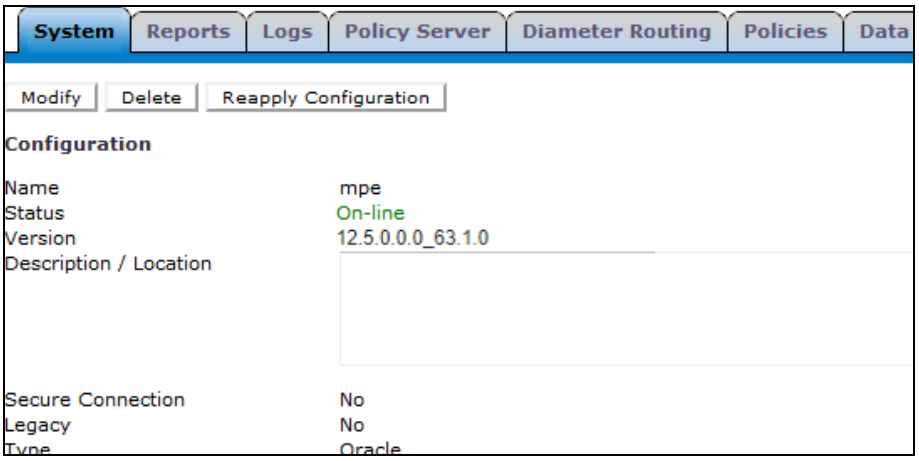
**Procedure 27 Back-out Fully Upgraded Primary CMP Cluster**

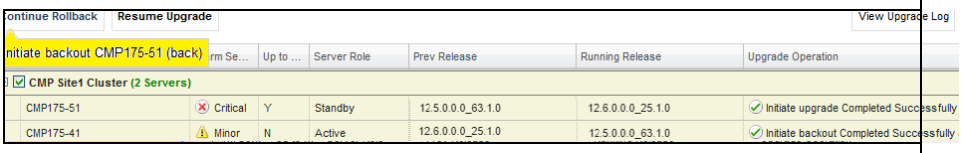
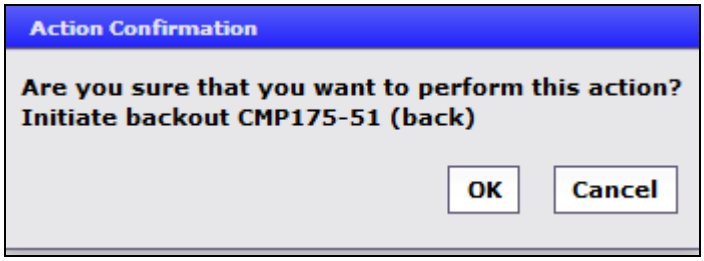
| Step | Procedure | Details |
|---|---|---|
| 1. ☐ | **CMP GUI:**<br><br>Verify the status of CMP Clusters | 1. Navigate to **Upgrade → Upgrade Manager**<br>2. Confirm status of the cluster to be backed out:<br>- Primary Active CMP is on Release 12.6<br>- Secondary CMP, MPE and MRA Clusters are on Release 12.5.0 or 12.5.0.4<br>- Up to Date Column shows Y for all servers in Primary CMP Cluster<br>3. Click **Filter** and enter `CMP` in the **Name** field.<br>**Example**<br>  |
| 2. ☐ | **CMP SSH:**<br>Verify `/var/log/messages` file size | 1. SSH into the standby server to be backed out as admusr.<br>`$ ls -lh /var/log/messages`<br>2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |
| 3. ☐ | **CMP GUI:** Back-out standby server of Primary CMP cluster<br><br>**NOTE:** Back-out of one server takes approximately 30 minutes to complete. | 1. Select the Primary CMP Cluster<br>2. Click **Start Rollback**. When hovering over the button, it indicates the server to back out.<br>  <br>3. Click **OK** to confirm and continue with the operation. It begins to back-out.<br>  |

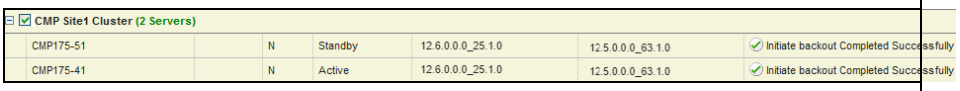
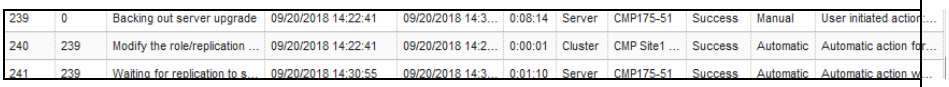
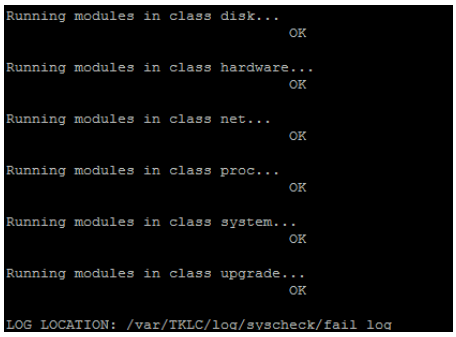
| Step | Procedure | Details |
|---|---|---|
| | | 4. Server goes into an OOS server role<br>5. Follow the progress status in the Upgrade Operation column.<br>During the back-out activities, the following alarms may be generated and are considered normal reporting events. These alarms are cleared after the cluster is completely backed out.<br><br>**Expected Critical Alarms**<br>**70001** The qp_procmgr process has failed.<br>**31227** The high availability status is failed due to raised alarms<br>**31283** High availability server is offline<br>**70025** The MySQL slave has a different schema version than the master<br>**Expected Major Alarms**<br>**70004** The QP processes have been brought down for maintenance<br>**31236** High availability TCP link is down<br>**31233** High availability path loss of connectivity<br>**70021** The MySQL slave is not connected to the master<br>**Expected Minor Alarms**<br>**70503** The server is in forced standby<br>**70507** An upgrade/backout action on a server is in progress<br>**70501** The Cluster is running different versions of software<br>**31232** High availability server has not received a message<br>**31101** DB replication to a slave DB has failed<br>**31102** DB replication from a master DB has failed<br>**31107** DB merging from a child Source Node has failed<br>**31114** DB Replication of configuration data via SOAP has failed<br>**31106** DB merging to the parent Merge Node has failed<br>**70500** The system is running different versions of software<br>Back-out of the server is complete when the successful completion message displays in the Upgrade Operation column. The server goes back to standby state and shows a running release of 12.6.0<br>  |
| 4. ☐ | **CMP SSH:** Verify syscheck and `/tmp` directory permission | 1. Login to the backed-out server as admusr<br>2. Verify that there are no failures in syscheck:<br>`$ sudo syscheck` |

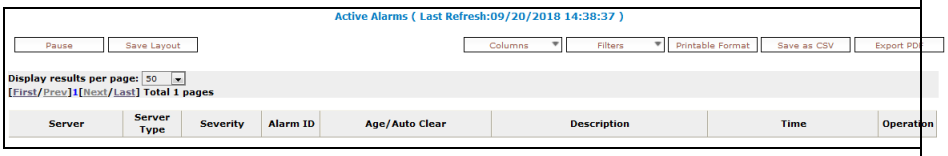
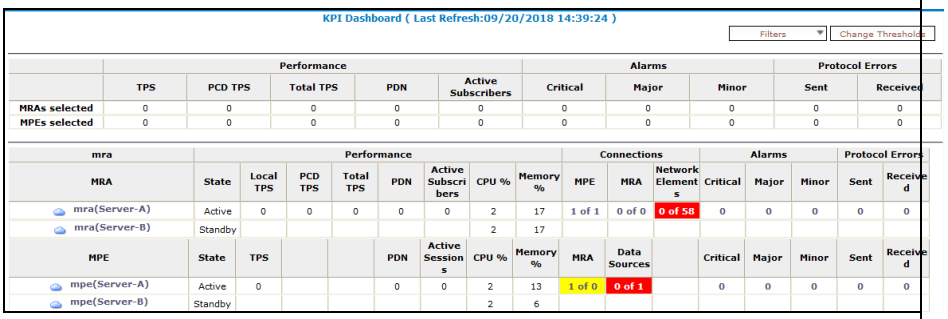
| Step | Procedure | Details |
|---|---|---|
| | |  <br>3. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>4. **NOTE:** Permissions should be the following,<br>`drwxrwxrwt. 5 root root 4096 Apr 27 10:54 tmp`<br>5. If the permissions are not as listed above then perform the following otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>6. Verify:<br>`$ ls -l /`<br>7. Perform syscheck again:<br>`$ sudo syscheck` |
| 5. ☐ | **CMP SSH:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br>To resolve this situation permanently, perform the following:<br>1. Login as admusr<br>2. Run thecat command.:<br>`$ sudo cat /proc/net/bonding/bond0`<br>3. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable when primary is set to eth11.<br>4. If this blade is the active blade, change it to standby before performing the rcstool command.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br>5. Find eth11.<br>6. Change from `primary=eth11` to `primary=eth01`<br>7. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |

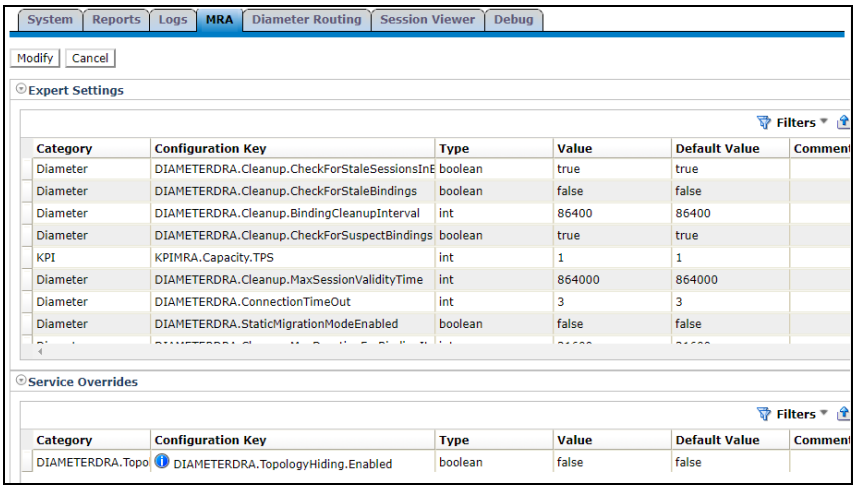
| Step | Procedure | Details |
|---|---|---|
| 6. ☐ | **CMP GUI**: Continue the back-out. Next operation is failover | 1. Navigate to **Upgrade → Upgrade Manager**.<br>2. Select the Primary CMP cluster<br>3. Click **Continue Rollback**. When hovering over the button, it informs you of the failover.<br>  <br>4. Click **OK** to confirm and continue with the operation. It begins to failover and takes couple of minutes to complete.<br>  <br>After a minute, you are required to log back in. |
| 7. ☐ | **CMP GUI:** Log back into the Primary CMP VIP | After failover, you are required to log back in to the CMP GUI using the Primary CMP VIP.<br>  |
| 8. ☐ | **CMP GUI:** Verify previous Policy Management release | 1. Navigate to **Help → About**.<br>2. Verify the release displayed is 12.5.x.x<br>  |

| Step | Procedure | Details |
|---|---|---|
| 9. ☐ | **CMP GUI:** If a Config Mismatch is observed on MPE or MRA | **MPE:**<br>Navigate to **Policy → Configuration →** <*MPE Cluster*> **→ System**<br>**MRA:**<br>Navigate to **MRA → Configuration →** *MRA Cluster*> **→ System**<br>  <br>Click **Reapply Configuration**.<br>Config Mismatch is resolved:<br>  |
| 10. ☐ | **CMP SSH:** Verify `/var/log/messages` file size | 1. Use SSH to login to the Standby server to be backed out as admusr<br>`$ ls -lh /var/log/messages`<br>2. ONLY if the resulting size of `/var/log/messages` is above 20M, run the following, otherwise proceed to the next step.<br>`$ sudo cp /var/log/messages /var/camiant/log/messages.preBack-out`<br>`$ sudo cat /dev/null > /var/log/messages`<br>`$ logger -s "Truncated this file prior to back-out. Copy is in /var/camiant/log/messages.preBack-out"`<br>3. Verify:<br>`$ ls -lh /var/log/messages` |

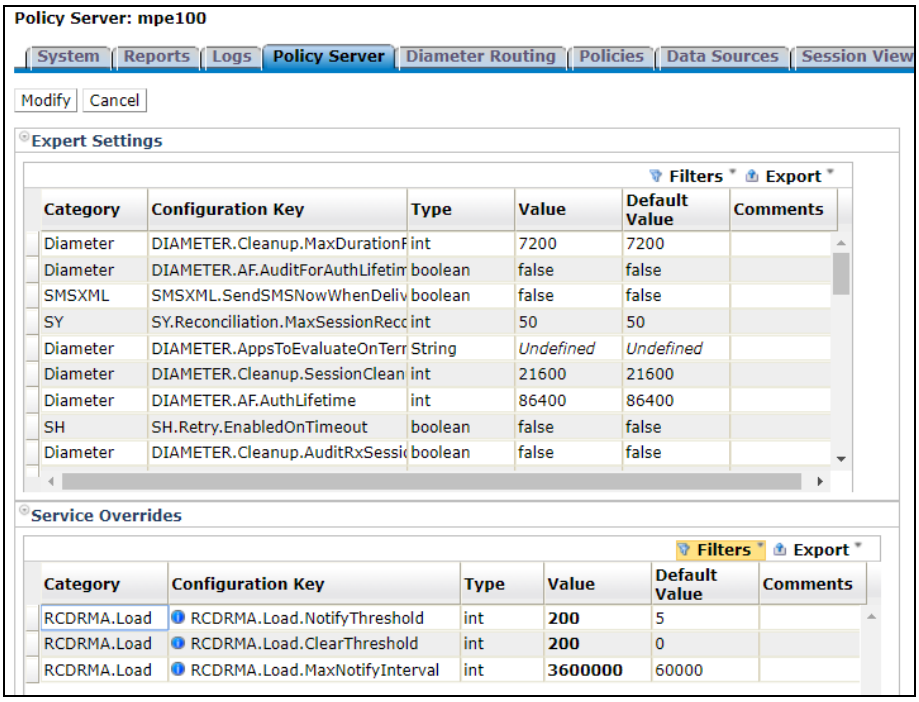
| Step | Procedure | Details |
|---|---|---|
| 11. ☐ | **CMP GUI:** Continue the back-out of the Primary CMP Cluster<br><br>**NOTE:** Back-out of one server takes approximately 30 minutes to complete. | 1. Navigate to **Upgrade → Upgrade Manager**<br>2. Select the Primary CMP Cluster.<br>3. Click **Continue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

| Step | Procedure | Details |
|---|---|---|
| | | **70500** The system is running different versions of software<br>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.<br>  <br>5. Verify in Upgrade Log that that back-out was successful:<br>  <br>All Primary CMP servers are on Release 12.5.0 at this point and show active/standby |
| 12. ☐ | **CMP SSH:** Verify syscheck and `/tmp` directory permission | 1. Login to the backed-out server as admusr.<br>2. Verify that there are no failures in syscheck:<br>`$ sudo syscheck`<br>  <br>3. Verify `/tmp` directory permissions:<br>`$ ls -l /`<br>**NOTE:** Permissions should be the following,<br>`drwxrwxrwt.  5 root root  4096 Apr 27 10:54 tmp`<br>4. If the permissions are not as listed above then perform the following otherwise skip to next step:<br>`$ sudo chmod 777 /tmp`<br>`$ sudo chcon -h system_u:object_r:tmp_t:s0 /tmp`<br>`$ sudo chmod +t /tmp`<br>5. Verify:<br>`$ ls -l /`<br>6. Perform syscheck again:<br>`$ sudo syscheck` |

| Step | Procedure | Details |
|---|---|---|
| 13. ☐ | **CMP SSH:** Verify eth01 is primary device interface | This step only applies if the server has a condition in which after the back-out is successful ETH11 becomes the primary Ethernet interface versus ETH01 becoming the primary interface.<br><br>To resolve this situation permanently, perform the following:<br><br>1. As admusr, run the following:<br>`$ sudo cat /proc/net/bonding/bond0`<br><br>2. Check that the output shows that the primary is set to eth11, it should be eth01. This step is only applicable when primary is set to eth11.<br><br>3. If this blade is the active blade, change it to standby before performing the following operations.<br>`$ sudo rcstool co /etc/sysconfig/network-scripts/ifcfg-bond0`<br><br>5. Find eth11.<br><br>6. Change from `primary=eth11` to `primary=eth01`<br><br>7. Save and exit (for example, vi uses ESC :wq!)<br>`$ sudo rcstool ci /etc/sysconfig/network-scripts/ifcfg-bond0`<br>`$ sudo reboot` |
| 14. ☐ | **CMP GUI:** Verify Alarm Status. | Navigate to **System Wide Reports → Alarms → Active Alarms**<br><br>Confirm that any existing alarm is understood.<br><br>  |
| 15. ☐ | **CMP GUI:** Verify Traffic Status—KPI Dashboard Report | **System Wide Reports → KPI Dashboard**<br><br>Confirm that all Connections and Traffic status are as expected. Observe it for a few refresh updates.<br><br>  |

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

| Step | Procedure | Details |
|---|---|---|
| 17. ☐ | **CMP GUI:** Verify Advanced Settings on the MPE | 1. Capture screenshots of the advanced settings on the MPE and compare it with prior to upgrade screen captures.<br>2. Verify that there are no differences.<br>3. Navigate to **Policy Server → Configuration →** <*MPE Cluster*> **→ Policy Server**<br>4. Click **Advanced**. |




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

**—End of Procedure—**

## 2.8 Workaround for Netbackup Client Installation after Upgrading to 12.6

If you were on R12.5.x CMP with netbackup client R7.1 installed, then upgrade the CMP to R12.6 and install R7.7 netbackup client, perform the following steps if the installation fails:

1. Force standby the CMP server to install or upgrade netbackup client:
   `Vim /etc/fstab` to make the **/tmp** mount options back to defaults
   Find the below line:
   `/dev/mapper/vgroot-plat_tmp /tmp ext4 noexec,nosuid,nodev 1 2`

   update to:
   `/dev/mapper/vgroot-plat_tmp /tmp ext4 defaults 1 2`
2. Reboot the server for re-mount the **/tmp** with defaults.
3. Perform the netbackup client following installation steps. The netbackup client must be installed successfully on the CMP server.
4. Back the **/etc/fstab** for **/tmp** to the original value.

5. Reboot the server.
6. The netbackup server could retrieve the backup content from the CMP server.

# Appendix A. TVOE and PMAC SERVER UPGRADE

## A.1 Adding TVOE software image to TVOE host

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

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

**Procedure 28 Adding TVOE software image to TVOE host**

| Step | Task | Description |
|---|---|---|
| 1. ☐ | **TVOE Host:** Verify there is enough space on the server for TVOE software image | Log in to the TVOE host and run the following to verify there is sufficient space:<br>`$ df -h /var/TKLC/upgrade/`<br>The system returns output similar to the following to indicate the disk usage of where the TVOE software image should reside.<br>`Filesystem Size Used Avail Use% Mounted on`<br>`/dev/mapper/vgroot-plat_var_tklc`<br>`4.0G 848M 3.0G 23% /var/TKLC`<br>If the Avail column is smaller than the size of the TVOE software image, contact Oracle Support for information about how to proceed. |
| 2. ☐ | Add TVOE software image to TVOE host | Place a copy of the TVOE software image to the `/var/TKLC/upgrade/` directory on the TVOE host by utilizing scp or USB media.<br>• SCP from PC using Linux<br>From the command line of a Linux machine, use the following command to copy the backup ISO image to the TVOE host:<br>`$ sudo scp <path_to_image> <user>@<TVOE_ip>:/var/TKLC/upgrade/`<br>Where *<path_to_image>* is the path to the TVOE ISO image local to the Customer PC and *<TVOE_ip>* is the TVOE IP address. *<user>* should be admusr for TVOE releases 2.5 or newer.<br>• SCP from PC using Windows<br>Use WinSCP to copy the TVOE ISO image to the TVOE host.<br>• USB Media<br>Attach the USB media to the TVOE host.<br>Login on the TVOE host and run the following to list ISO files on the USB media:<br>`$ sudo ls /media/*/*.iso`<br>`/media/usb/TVOE-3.8.0.0.0_89.5.0-x86_64.iso`<br>Replacing *<PATH_TO_TVOE_ISO>* with the output of the command above, copy the ISO to the `/var/TKLC/upgrade` directory:<br>`$ sudo cp <PATH_TO_TVOE_ISO> /var/TKLC/upgrade/`<br>Unmount the USB media:<br>`$ sudo umount /media/usb` |

| —End of Procedure— |
|---|

## A.2 TVOE Upgrade

Use this procedure to upgrade the PMAC Server to 6.6.1 and the TVOE host to 3.8.0

**NOTES:**

- The TVOE upgrade procedure can be performed either during the same maintenance window as PMAC upgrade or in a separate maintenance window.
- If PMAC TVOE host cannot be upgraded at this time then PMAC upgrade must not be attempted.

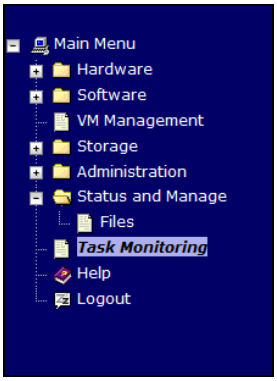
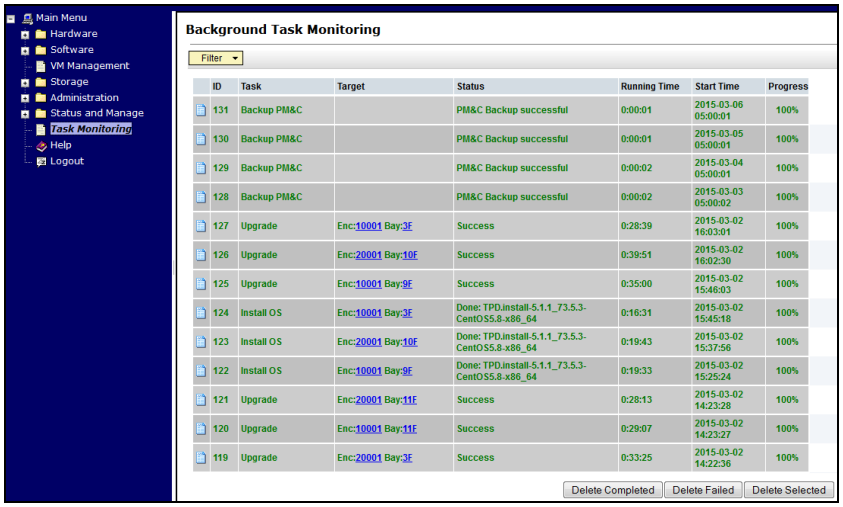
1. TVOE Pre-Upgrade Validation
2. Pre-Upgrade Backup
3. Add TVOE Software Image to TVOE HOST
4. Add PMAC Upgrade Software to PMAC Server
5. Stand Alone TVOE Host Upgrade
6. TVOE Post-Upgrade Validation
7. PMAC upgrade
8. Stand Alone TVOE Upgrade Accept
9. PMAC Upgrade Accept

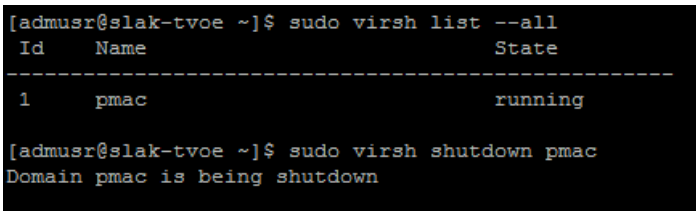
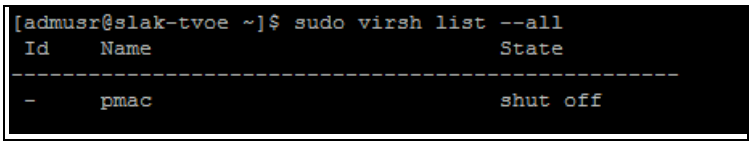
**NOTE:** It is recommended NOT to accept TVOE upgrade until after PMAC upgrade has been accepted for the following reasons:

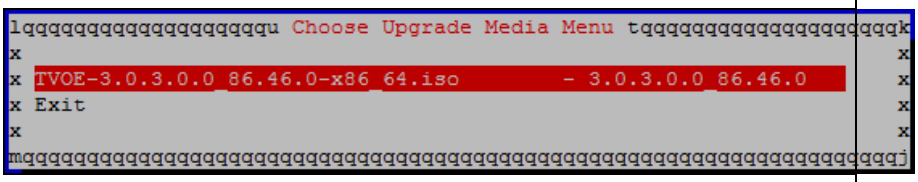
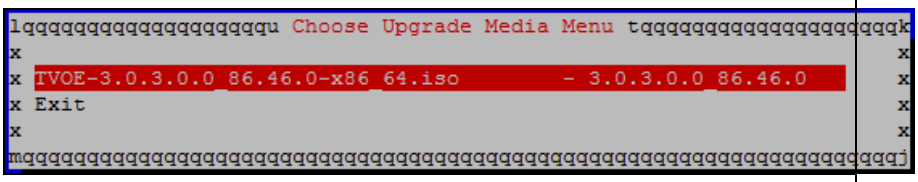
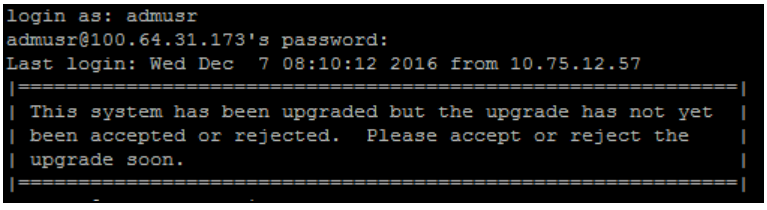
- If you are upgrading from PMAC 5.5, this release cannot be deployed on an upgraded TVOE 3.8.0 system.
- If an issue occurs during PMAC upgrade, it may require disaster recovery for which TVOE upgrade has to be rejected to allow PMAC 5.5 to be re-deployed.
- A reject cannot be performed after an upgrade has been accepted.

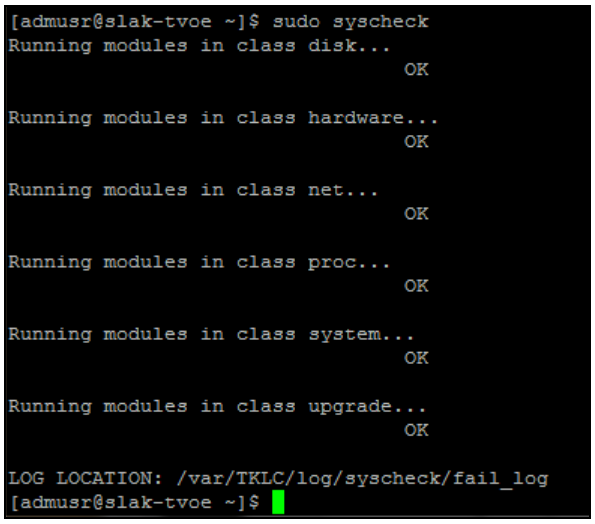
**Procedure 29 TVOE Upgrade**

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

| Step | Task | Description |
|---|---|---|
| 2. ☐ | Check any in-progress task(s) on PMAC | 1. On a supported web browser, log in to PMAC GUI as pmacadmin<br>2. Navigate to PMAC GUI background tasks page:<br>**Main Menu → Task Monitoring**<br>  <br><br>3. Verify all tasks are complete indicated by green 100% progress<br>**NOTE:** If any task shows in-progress (blue or red) then wait for the task to complete prior to continuing the next step.<br>  <br> |

| Step | Task | Description |
|---|---|---|
| 3. ☐ | Shutdown PMAC | **NOTE:** Assuming all tasks are completed (previous step) it is safe to shut down PMAC<br>1. Log on to the TVOE host as admusr<br>2. Obtain the name of the PMAC guest by running the following command:<br>`$ sudo virsh list --all`<br>`Id Name State`<br>`----------`<br>`1 <pmac_name> running`<br>3. Stop the PMAC process by using the following command:<br>`$ sudo virsh shutdown <pmac_name>`<br>  <br>`[admusr@slak-tvoe ~]$ sudo virsh list --all`<br>` Id Name State`<br>`----------`<br>` 1 pmac running`<br>`[admusr@slak-tvoe ~]$ sudo virsh shutdown pmac`<br>`Domain pmac is being shutdown`<br>**NOTE:** It is imperative to log in to the TVOE host instead of using SSH to the PMAC guest. The upgrade might fail otherwise. |
| 4. ☐ | Verify PMAC guest is shut down | 1. Login to the TVOE host as admusr.<br>2. Verify that the PMAC is shut down with the following command:<br>`[admusr@tvoe approximately]# sudo virsh list --all`<br>  <br>`[admusr@slak-tvoe ~]$ sudo virsh list --all`<br>` Id Name State`<br>`----------`<br>` - pmac shut off`<br>**NOTE:** This should show the PMAC guest state as shut off. |

| Step | Task | Description |
|---|---|---|
| 5. ☐ | Validate media | 1. Login to the TVOE host as admusr.<br>2. Start the platcfg utility<br>`$ sudo su - platcfg`<br>3. Navigate to **Maintenance → Upgrade → Validate Media**.<br>4. Select the TVOE ISO file.<br>  <br>5. Press **Enter** to validate the ISO file.<br>The TVOE ISO image is validated with an expected result of:<br>`The media validation is complete, the result is: PASS`<br>If the image validation fails, this procedure should be stopped. The ISO image should be copied again to the TVOE host and this procedure should be re-started from the beginning. |
| 6. ☐ | Start TVOE upgrade<br>**NOTE:** The upgrade process takes 15 minutes | 1. Press Enter to return to platcfg and then press Exit to go back to the Upgrade menu. Do not quit platcfg.<br>Navigate to **Maintenance → Upgrade → Initiate Upgrade**.<br>2. Select the TVOE ISO filename.<br>  <br>3. Press **Enter** to initiate the upgrade.<br>**NOTE:** The TVOE host is rebooted at the end of the upgrade process (about 15 minutes) and returns to the login prompt. At this point the TVOE upgrade is complete. |
| 7. ☐ | Verify the Upgrade status | 1. Log in to TVOE as admusr<br>  <br>2. Verify the upgraded TVOE revision by running the following command:<br>`$appRev`<br>3. You receive an output similar to this: |

| Step | Task | Description |
|---|---|---|
| | | `[admusr@slak-tvoe ~]$ appRev`<br>`Install Time: Wed Dec 7 09:44:48 2016`<br>`Product Name: TVOE`<br>`Product Release: 3.0.3.0.0_86.46.0`<br>`Base Distro Product: TPD`<br>`Base Distro Release: 7.0.3.0.0_86.46.0`<br>`Base Distro ISO: TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64.iso`<br>`ISO name: TVOE-3.0.3.0.0_86.46.0-x86_64.iso`<br>`OS: OracleLinux 6.7`<br><br>4. Run the following command:<br>`$sudo verifyUpgrade`<br>5. The command does not produce output. Any output that displays are potential issues.<br>6. Run the syscheck command:<br>`$sudo syscheck`<br>  <br>`[admusr@slak-tvoe ~]$ sudo syscheck`<br>`Running modules in class disk...`<br>`OK`<br>`Running modules in class hardware...`<br>`OK`<br>`Running modules in class net...`<br>`OK`<br>`Running modules in class proc...`<br>`OK`<br>`Running modules in class system...`<br>`OK`<br>`Running modules in class upgrade...`<br>`OK`<br>`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`<br>`[admusr@slak-tvoe ~]$`<br><br>**NOTE:** It is recommended not to accept TVOE upgrade until after PMAC upgrade has been accepted for the following reasons:<br>• Some older PMAC releases cannot be deployed on upgraded TVOE 3.8.0 system.<br>• If issues occurs during PMAC upgrade, disaster recovery may be required for which the TVOE upgrade has to be rejected to allow older PMAC to be re-deployed.<br>***A reject cannot be performed after an upgrade has been accepted.*** |
| 8. ☐ | Remove the TVOE ISO version file to free up disk space | Logged in from previous step, issue the following<br>`$sudo rm /var/TKLC/upgrade/TVOE-3.8.0.0.0_89.5.0-x86_64.iso` |
| **—End of Procedure—** | | |

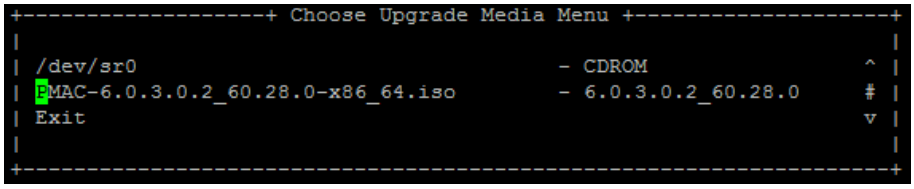
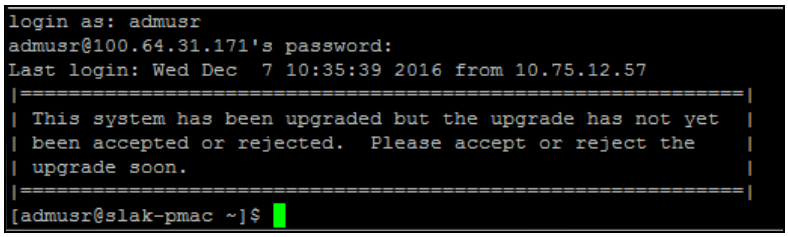
## A.3 PMAC Upgrade

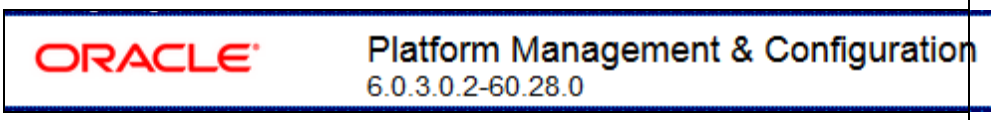
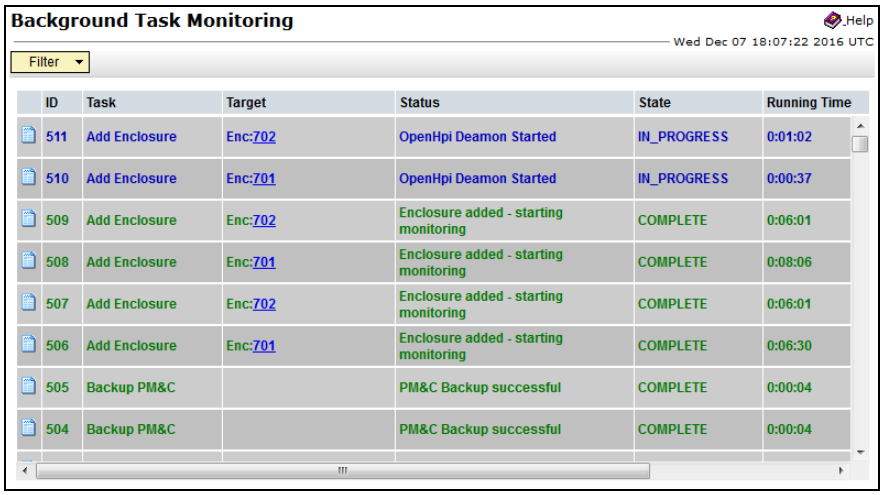
Use this procedure to perform software upgrade of the PMAC.

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

**Procedure 30 PMAC Upgrade**

| Step | Task | Description |
|---|---|---|
| 1. ☐ | Start the PMAC guest | 1. If not logged in to the TVOE host as admusr, login.<br>2. Start the PMAC guest if not started:<br>3. Query the list of guests to check whether the PMAC guest is in the running state.<br>`$ sudo virsh list --all`<br>`Id Name State`<br>`----------`<br>`1 <pmac_name> running`<br>- If it is running, skip to the next step.<br>- If it is not running, issue the following command.<br>`$ sudo virsh start <pmac_name>`<br>`Domain <pmac_name> started` |
| 2. ☐ | Close any active browser sessions to PMAC | If any open browsers are connected to PMAC, close them before proceeding |
| 3. ☐ | Login to the TVOE host as root | 1. From the TVOE host CLI, issue the following command to log on to the PMAC guest as admusr:<br>`$sudo virsh console <pmac_name>`<br>**NOTE:** It might be needed to press **Enter** twice.<br>2. Verify the correct ISO file is located in the `/var/TKLC/upgrade` directory of the PMAC guest. If not, copy the PMAC ISO to the `/var/TKLC/upgrade` directory on the PMAC guest.<br>3. Verify by issuing the following command:<br>`# ls -lth /var/TKLC/upgrade` |
| 4. ☐ | Run the upgrade from PMAC Server | From PMAC guest, login as admusr (accessed via the TVOE virsh console in the previous step), run the platcfg utility:<br>`# sudo su - platcfg` |

| Step | Task | Description |
|---|---|---|
| 5. ☐ | In the platcfg utility, select **Initiate Upgrade** to start the upgrade process | 1. In platcfg, select **Maintenance → Upgrade**.<br>2. Select **Initiate Upgrade** to start the upgrade process<br>3. Wait until the Choose Upgrade Media Menu window opens before proceeding to the next step<br>  <br>4. Select the PMAC 6.6 target ISO filename and press **Enter** to start the upgrade process.<br>5. The upgrade begins and after 20 minutes the connection is lost as it reboots.<br>- Do not take any action on the PMAC until the server reboots. The reboot takes approximately 5 minutes.<br>- After you log back into PMAC, you see something similar to this:<br>  |

<table>
<tr><th>Step</th><th>Task</th><th>Description</th></tr>
<tr><td>6. ☐</td><td>PMAC GUI:<br>Verify the upgrade after 30 minutes</td><td>1. Open a browser and enter the IP address of the PMAC server<br>2. Login as pmacadmin<br>3. Verify the release at the top of the page.<br>  <br>4. Navigate to the task manager and verify that all tasks are complete. DO NOT proceed with the next step until all tasks are completed.<br>Tasks still in progress:<br>  </td></tr>
<tr><td colspan="3">—END OF PROCEDURE—</td></tr>
</table>

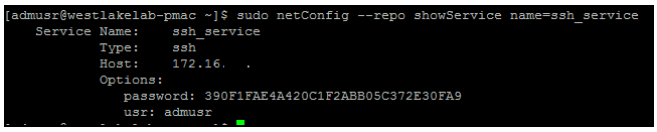
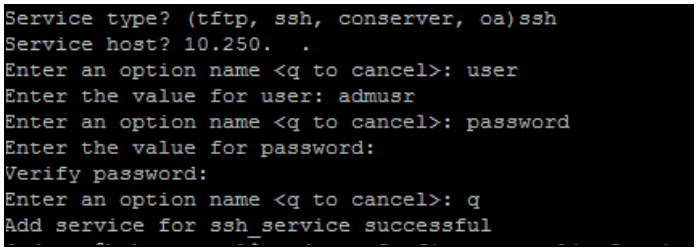
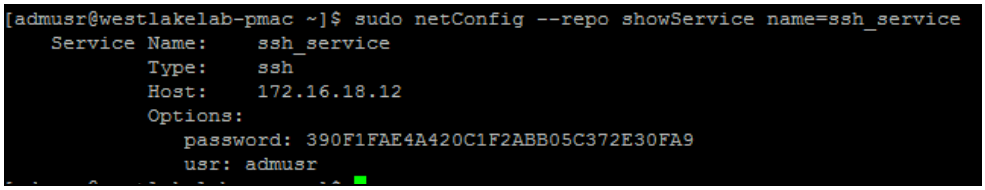
## A.4 Verify PMAC Upgrade

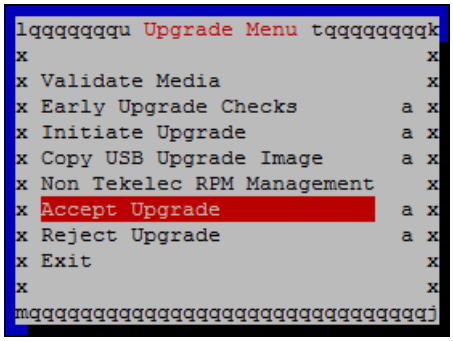
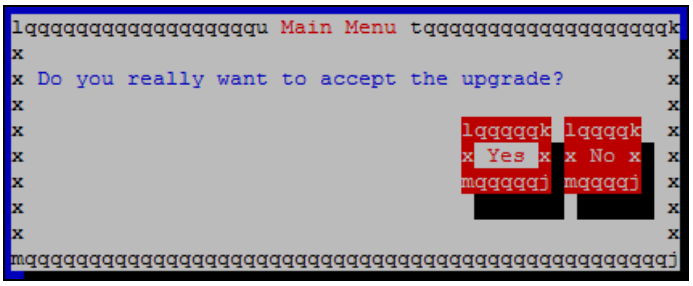
Use this procedure to verify success of the PMAC upgrade and perform other required post upgrade steps

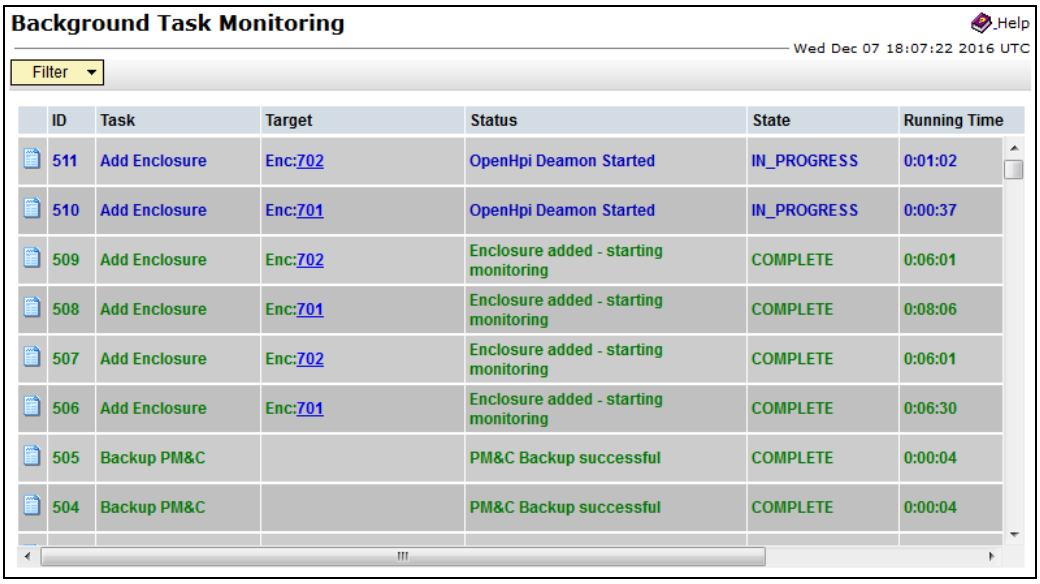
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

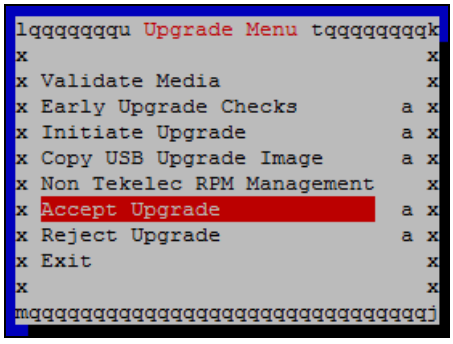
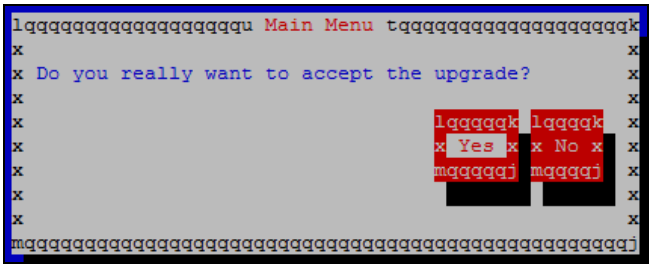
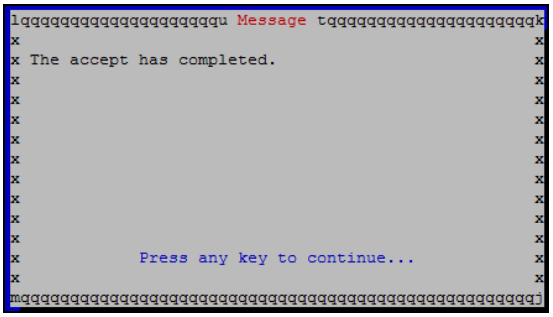
**Procedure 31 Verify PMAC Upgrade**

| Step | Task | Description |
|---|---|---|
| 1. ☐ | Access PMAC guest console | 1. Log on to TVOE host SSH as admusr<br>2. Verify that the PMAC console is running by issuing the following command<br>`$ sudo virsh list`<br>`[admusr@brbg-tvoe-host ~]$ sudo virsh list`<br>` Id  Name  State`<br>`----------`<br>` 1  brbgpmac  running`<br>3. Log on to PMAC guest console by issuing the following command from the TVOE console:<br>`$ sudo virsh console <pmac_name>`<br>4. Press **Enter** twice.<br>**NOTE:** If you connected from the TVOE console, the guest session to PMAC is broken with **CTRL+]** |
| 2. ☐ | Verify the date/timestamp | 1. Login to the PMAC console.<br>2. Run the following command:<br>`$ ls -l /var/TKLC/log/upgrade/upgrade.log`<br>`[admusr@slak-pmac ~]$ ls -l /var/TKLC/log/upgrade/upgrade.log`<br>`-rw-rw-r-- 1 platcfg root 127103 Dec  7 11:51 /var/TKLC/log/upgrade/upgrade.log`<br>`[admusr@slak-pmac ~]$`<br>3. Verify that the date and timestamps up the upgrade align with the actual time of the upgrade. |
| 3. ☐ | Verify that the release version has been updated | Run the following command and verify the release.<br>`$ appRev`<br>`[admusr@slak-pmac ~]$ appRev`<br>`Install Time: Wed Dec 7 11:50:31 2016`<br>`Product Name: PMAC`<br>`Product Release: 6.0.3.0.2_60.28.0`<br>`Base Distro Product: TPD`<br>`Base Distro Release: 7.0.3.0.0_86.45.0`<br>`Base Distro ISO: TPD.install-7.0.3.0.0_86.45.0-OracleLinux6.7-x86_64.iso`<br>`ISO name: PMAC-6.0.3.0.2_60.28.0-x86_64.iso`<br>`OS: OracleLinux 6.7` |
| 4. ☐ | Verify successful completion through the upgrade log | Run the following commands on PMAC<br>`$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log`<br>`[admusr@brbgpmac ~]$ grep COMPLETE /var/TKLC/log/upgrade/upgrade.log`<br>`1419272892::UPGRADE IS COMPLETE`<br>`$sudo verifyUpgrade`<br>**NOTE:** This command could take over a minute to complete. No output is expected, only the prompt should return. If there are messages, contact My Oracle Support. |
| 5. ☐ | Run syscheck | Run syscheck and verify everything is correct.<br>`$ sudo syscheck` |

| Step | Task | Description |
|---|---|---|
| 6. ☐ | **PMAC SSH CLI:** Recreate the ssh_service with admusr credentials on PMAC guest console if it does not exist | 1. Verify that the ssh service exists with admusr credentials by running the following command:<br>`$ sudo netConfig --repo showService name=ssh_service`<br>  <br>2. If the results are similar to the above, that is, options include usr: admusr and an encrypted password, skip to the next step.<br>3. If the results do not include the usr: admusr option or if the service does not exist, continue with this step:<br>4. Delete the ssh_service if it exists<br>`$ sudo netConfig --repo deleteService name=ssh_service`<br>5. Click **YES** to the message if prompted.<br>6. Recreate ssh_service with admusr user.<br>`$ sudo netConfig --repo addService name=ssh_service`<br>`Service type? (tftp, ssh, conserver, oa) ssh`<br>`Service host? <PMAC_ip_address>`<br>`Enter an option name (q to cancel): user`<br>`Enter a value for user: admusr`<br>`Enter an option name(q to cancel): password`<br>`Enter a value for password: Duk******`<br>`Verify Password : Duk******`<br>`Enter an option name(q to cancel): q`<br>**Example output**<br>  <br>7. Verify that the information is correct by running the following command and comparing the output with the configuration in the last step.<br>`$ sudo netConfig --repo showService name=ssh_service`<br>**Example output**<br>  |

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

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

| Step | Task | Description |
|---|---|---|
| 10. ☐ | Accept the upgrade for TVOE | **NOTE:** It is recommended not to accept the TVOE upgrade until after the PMAC upgrade has been accepted for the following reasons:<br>• Some older PMAC releases cannot be deployed on upgraded TVOE 3.8.0 system.<br>• If issues occurs during PMAC upgrade it may require disaster recovery for which TVOE upgrade has to be rejected to allow older PMAC to be re-deployed.<br>• A reject cannot be performed after an upgrade has been accepted.<br>**NOTE:** Once the upgrade is accepted, you cannot roll back to the previous release.<br>Login as admusr to TVOE host CLI<br>5. Start the platcfg utility:<br>`$ sudo su - platcfg`<br>6. Navigate to **Maintenance→Upgrade→Accept Upgrade**.<br>  <br>7. Select **Accept Upgrade** and press **Enter**.<br>  <br>8. Click **Yes** to start accept upgrade process.<br>**NOTE:** A session is launched when accepting the upgrade, press **q** to close the window and return to platcfg.<br>  <br>9. Press any key and then press Enter on Exit or press F12 until you exit platcfg.<br>The upgrade process is now complete. |

| Step | Task | Description |
|---|---|---|
| --END OF PROCEDURE-- | | |

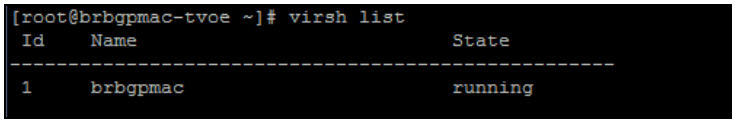
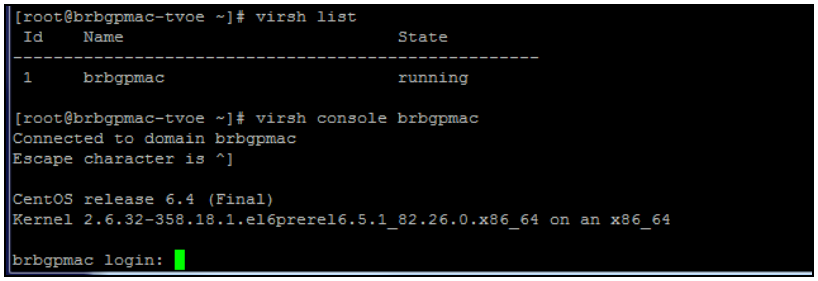
## Appendix B. TVOE and PMAC Server Backout

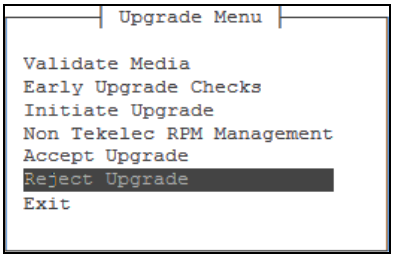
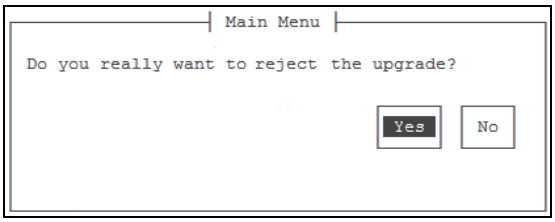
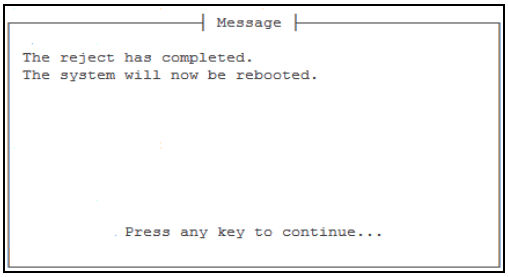
Use this procedure to backout/reject the PMAC server upgrade.

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

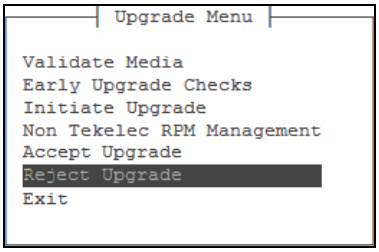
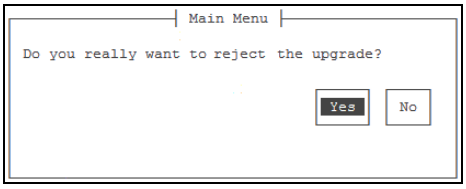
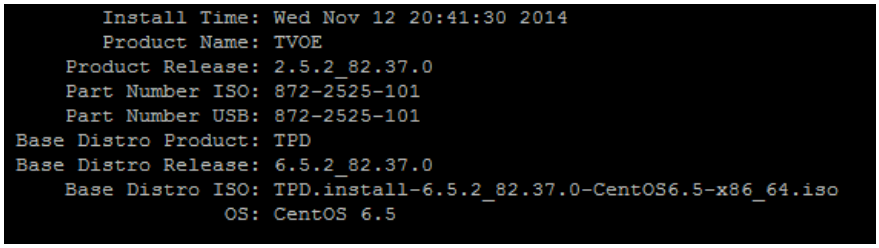
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

**Procedure 31: TVOE and PMAC Server Backout**

| Step | Task | Description |
|---|---|---|
| 1. ☐ | Close any active browser sessions of PMAC | Close any open browsers connected to PMAC before proceeding. |
| 2. ☐ | If necessary, access PMAC guest console | 1. Log on to TVOE host as admusr<br>2. Verify PMAC console is running by issuing the following command.<br>`$sudo virsh list`<br>  <br>3. Log on to PMAC guest console by issuing the following command<br>`$sudo virsh console <pmacname>`<br>  <br>4. Log on to PMAC as admusr if needed—may not require a login.<br>`Last login: Wed Jun 6 08:39:14 on ttyS0`<br>`\|============================================================\|`<br>`\| This system has been upgraded but the upgrade has not yet \|`<br>`\| been accepted or rejected. Please accept or reject the \|`<br>`\| upgrade soon. \|`<br>`\|============================================================\|`<br>`[admusr@pmac approximately]$`<br>**NOTE:** To break the guest session to go back to TVOE host, press **CTRL+]** |

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

| Step | Task | Description |
|---|---|---|
| 6. ☐ | Verify backout completed | Run the following command to verify source PMAC release:<br>`[admusr@pmac approximately]# appRev`<br>`Install Time: Thu Nov 13 10:04:56 2014`<br>`Product Name: PMAC`<br>`Product Release: 5.5.2_55.20.0`<br>`Part Number ISO: 872-2586-102`<br>`Part Number USB: 872-2586-102`<br>`Base Distro Product: TPD`<br>`Base Distro Release: 6.5.2_82.37.0`<br>`Base Distro ISO: TPD.install-6.5.2_82.37.0-CentOS6.5-x86_64.iso`<br>`OS: CentOS 6.5`<br>If the correct Product Release is not displayed, contact Oracle Customer Service and do not proceed until instructed by a Oracle Customer Care representative. |
| 7. ☐ | TVOE iLo SSH | As Administrator on the TVOE iLO, log in through the iLO and run the following command to check the logical drives that are used for the backout.<br>Login as admusr to the TVOE console<br>`$sudo /sbin/lvs -o lv_name,snap_percent @upgrade`<br>`Typical output:`<br>`LV snap %`<br>`plat_root_snap 27.52`<br>`plat_usr_snap 7.70`<br>`plat_var_snap 5.08`<br>`plat_var_tklc_snap 19.14`<br>**NOTE:** Anything below 50% is OK. |

| Step | Task | Description |
|---|---|---|
| 8. ☐ | **TVOE Server iLO:**<br>Manually backout upgrade | 1. At the prompt run:<br>`$sudo su - platcfg`<br>2. Navigate to **Maintenance → Upgrade**<br>  <br>3. Select **Reject Upgrade** and press **Enter** to start the reject process.<br>4. The following window opens, click **Yes** to begin the backout.<br>  <br>5. The system undergoes a backout. As part of the process the system reboots several times.<br>6. After completing the final reboot the login prompt opens. Some of the final startup output along with an example of the login prompt is shown below:<br>7. Login as admusr<br>`CentOS release 6.2 (Final)`<br>`Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.16.0.x86_64 on an x86_64`<br>`hostname1342210584 login:` |
| 9. ☐ | **TVOE Server iLO:** check server health. | Log in and run the **`apprev`** command.<br>`# appRev`<br>  |
| 10. ☐ | **TVOE Server iLO:** check server health | Run the following command to check the health of the server:<br>`# sudo alarmMgr --alarmStatus`<br>If any output is produced, an alarm is present on the system. Contact Oracle for information about how to proceed. |
| 11. ☐ | Clear browser cache | Clear browser cache to ensure that browser has the latest client-side code loaded. Refer to browser documentation if necessary. |
| 12. ☐ | **PMAC GUI** | Login to the PMAC GUI to verify the old PMAC version |

| Step | Task | Description |
|---|---|---|
| —END OF PROCEDURE— | | |

## Appendix C. Accessing the Oracle Customer support site and Hotlines

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

1. Log into the Oracle Customer Support site at https://support.oracle.com

13. 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