Oracle® Communications Policy and Charging Rules Function

PCRF Software Upgrade Procedure

Release 11.5

E61656-01

February 2015

ORACLE®

Oracle® Communications Policy and Charging Rules Function, Software Upgrade Procedure, Release 11.5

Copyright © 2015 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

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

Contact MOS and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*.

TABLE OF CONTENTS

1. INTRODUCTION 5
1.1 Purpose and Scope 5
1.2 References 5
1.3 Acronyms 6
1.4 Terminologies 7
1.5 Software Release Numbering 7

2. UPGRADE OVERVIEW 8
2.1 Policy Upgrade Paths 8
2.2 Upgrade Sequence 8
2.3 Policy Release Mixed-Version Operation & Limitation 10
2.4 Customer Impacts 11
2.5 PM&C Server Version and TVOE version 11
2.6 TPD Version 11
2.7 Acquiring firmware 11
2.8 Server Hardware Platforms 12
2.9 Loading Application software 12
2.10 Required Materials and Remote Access 12
2.10.1 Upgrade Media 14

3. UPGRADE PREPARATION 15
3.1 Overview & Sequence of full upgrade with planning and tracking 15
3.2 Procedure-1: Pre-requisites 16
3.3 Procedure-2: Plan and Track Cluster Upgrades 17
3.4 Procedure-3: Perform System Health Check 20
3.5 Deploy Policy Upgrade Software 22
3.5.1 Procedure-4: Copy ISO image files to Management Server (PM&C) 22
3.5.2 Procedure-5: Distribute Application ISO image files to servers 25
3.5.3 Procedure-6: Backups and Backup Locations 28

4. SOFTWARE UPGRADE CAUTIONS 31

5. PM&C UPGRADE 32

6. UPGRADE CMP CLUSTERS 33
6.1 About ‘ACCEPT UPGRADE’: 33
6.2 Overview Upgrade CMP Clusters 34

7. UPGRADE MPE CLUSTERS AND MRA CLUSTERS 54
7.1 Procedure-8: Initial Checks on CMP cluster at Site-1 and Site-2 54
7.2 Procedure-9: Upgrade MPE clusters@Segment____@Site _____ 56
7.3 Procedure-10: Upgrade MRA clusters@Segment____@Site _____ 72
7.4 Post-upgrade 88
7.4.1 Procedure-11: Accepting Upgrade for CMP clusters 88
7.4.2 Procedure-12: Accepting Upgrade for MPE clusters 92
7.4.3 Procedure-12: Accepting Upgrade for MRA clusters 96

8. BACKOUT (ROLLBACK) 100
8.1 Procedure-11: Backout of Partially Upgraded MRA or MPE Cluster 101
8.2 Backout of Full Upgrade 105

8.2.1 Overview: Backout Sequence 105
8.3 Procedure-12: Pre-requisite: Preparation 108
8.4 Procedure-13: Backout Fully Upgraded MRA/MPE Clusters 109
8.5 Procedure-14: Backout Fully Upgraded CMP Clusters 115
8.6 Procedure-15: Finalize Backout 122

9. APPENDIX 123

APPENDIX B. COPY UPGRADE ISOS FROM USB DRIVE 143

APPENDIX C. USING ILO TO REMOTELY ACCESS A SERVER 147

APPENDIX D. RESETTING COUNTERS 150

APPENDIX E. EXPORT KPIS FROM CMP GUI USING OSSI XML INTERFACE 152

APPENDIX F. CMP GUI FILTERS 153

APPENDIX G. ACCESSING ORACLE'S CUSTOMER SUPPORT SITE & HOTLINES 154

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform Policy Release 11.5 Software upgrade and fallback, encompassing:

- In-service Policy Release (9.1.x or 10.5.x), non-geo-Redundant, multi-site CMP, MRA and MPE (or MPE-LI) servers

The audience for this document includes these Oracle groups: Software Development, Product Verification, Technical Communications, and Customer Service including Software Operations and First Office Application (FOA).

1.2 References

[1] FD008005 - Release 11.0.1 Upgrade and updated for Release 11.5 Upgrade

[2] FE007388 - Release 11.5 Upgrade

[3] HP Fimware Upgrade Procedures Release notes (for PM&C), 910-6929-001 Revision A

[4] HP Solutions Firmware Upgrade Pack Upgrade Procedures 2.2.x, 909-2234-001

[5] HP Firmware 2.2.6/2.2.7 Release Notes - E56664

[6] HP Solutions Firmware Upgrade Pack, Upgrade Guide - E56663, Revision 01

1.3 Acronyms

ACRONYM	DESCRIPTION
CMP	Oracle PCRF Management Product NOTE: This is also known as the Primary CMP
CMP-DR	Oracle PCRF Management Product at Secondary Site (DR=Disaster Recovery) NOTE: This is also known as the Secondary CMP
ISO	Refers to optical media
GUI	Web-based Graphical User Interface
MPE	Oracle PCRF Product
MRA	Oracle Diameter Routing Agent for Policy Applications Product
PCRF	Policy and Charging Rules Function – Oracle MPE
Segment	A segment is a collection of HSGWs, P-GWs, DSRs, MPEs and MRAs that provide the PCRF service. A single MPE/MRA cluster may be part of only one PCRF Segment. A CMP manages all the MPE/MRAs at multiple sites. A CMP manages one or more PCRF Segments.
LI	Lawful Interface (CALEA)
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment
PM&C	Platform Management & Configuration

1.4 Terminologies

Primary Site (Site-1) – A site where the MPE/MRA primary cluster exists with both co-located Active and Standby state servers

Secondary Site (Site-2) – A site where the MPE/MRA secondary cluster exists with both co-located Active and Standby state servers for disaster recovery

1.5 Software Release Numbering

- PM&C 5.7
- TVOE 2.7, minimum
- Policy Release 11.5, separate for each software components, such as CMP, MPE and MRA
- 2.2.6/2.2.7 firmware for Policy Applications, minimum
- 2.2.5 firmware for PM&C, minimum

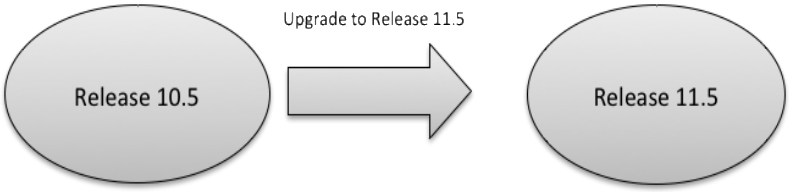
2. UPGRADE OVERVIEW

This section lists the required materials and information needed to execute Policy Release 11.5 software upgrade.

2.1 Policy Upgrade Paths

Following are the supported upgrade paths to R11.5:

1. PM&C Release 5.x to 5.7
2. Policy Release 10.5.x to 11.5



3. Policy Release 9.1.x to 11.5

2.2 Upgrade Sequence

This procedure applies to Active/Standby pair of servers. This pair of servers is referred to as the "*cluster*" or the "*HA cluster*". The customer deployment may consist of multiple clusters at Primary site and Secondary site or only at Primary site.

Required Cluster Upgrade Sequence:

Sequence laid-down below is site-specific. Other approach could be segment specific.

Site-specific:

1. PM&C Server Site-1 *(See Appendix A)*
2. PM&C Server Site-2 *(See Appendix A)*
3. Upgrade CMPs (first upgrade Primary CMP cluster, then Seconday CMP cluster)
4. Upgrade all MPEs at Site1
5. Upgrade MRA at Site1
6. Upgrade all MPEs at Site2
7. Upgrade MRA at Site2
8. Accept the Upgrade

Segment-specific:

1. PM&C Server Site-1 *(See Appendix A)*
2. PM&C Server Site-2 *(See Appendix A)*
3. Upgrade CMPs (first upgrade Primary-site CMP cluster, then Secondary-site CMP cluster)
4. Upgrade all the MPEs that belong to a particular MRA(together forming a segment) at Site1
5. Upgrade the MRA cluster that belong all the MPEs, upgraded in step 4, at Site1
6. Upgrade all the MPEs that belong to a particular MRA(together forming a segment) at Site2
7. Upgrade the MRA cluster that belong all the MPEs, upgraded in step 4, at Site2
8. Repeat step 4, 5, 6 & 7 for remaining MPEs and MRAs at site 1 and site 2.
9. Accept the Upgrade

2.3 Policy Release Mixed-Version Operation & Limitation

Mixed Version PCRF system expectations

The general expectation is that a system that is running in a mixed version configuration should support features, and perform at a level of the previous version. Thus, the system that is running Release 10.5 (or 9.1.x as the case may be) and Release 11.5 mixed configuration would support the performance and capacity of Release 10.5. The mixed version PCRF configuration would support Release 10.5 features only.

Since the CMP is the first PCRF system component that is upgraded to the new version, the Release 11.5 CMP will be managing Release 9.1.X (where 9.1.X is the latest 9.1 maintenance release) or Release 10.5 and Release 11.5 MRA and MPE servers. In this mixed version configuration Release 11.5 CMP will not prevent operator from configuring anything that you could configure in a Release 9.1.X or in Release 10.5 CMP and all configuration items from the previous release (Release 9.1.X/Release 10.5) are still available. However, the configuration changes during the upgrade of PCRF system are discouraged and have limited support. This is due to the number of permutations involved in testing different mixed version configuration scenarios.

In the mixed version PCRF configuration Release 11.5 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 reviewed by the customer before deployment to verify that these policies indeed do not use new conditions or actions.
- The support for configuration of MPE and MRA servers is limited to parameters that are available in the previous version. Specifically:
    - Network Elements can be added (see requirement [R- 232963-110])
    - Advanced Configuration settings that were valid for 10.5 may be changed (see requirement [R- 232967-105])

PCRF system Components	CMP R11.5	MRA R11.5	MPE R11.5
CMP R9.1.X	No	No	No
MRA R9.1.X	Yes	Yes	Yes
MPE R9.1.X	Yes	Yes	N/A
CMP R10.5	No	No	No
MRA R10.5	Yes	Yes	Yes
MPE R10.5	Yes	Yes	N/A

Table 1: Mixed-version configurations supported between Policy Release 9.1.X or Release 10.5 and Release 11.5.

Note: If Oracle/Tekelec SDM/SPR is deployed as part of the total Policy solution, the Oracle/Tekelec SPR must be upgraded to Release 9.3, beforehand.

2.4 Customer Impacts

The cluster upgrade proceeds by upgrading the Standby server, then switching over the Active to the Standby and upgrading the second server. The switchover of each MPE/MRA cluster will have a small impact on traffic being processed at that cluster, as in past release upgrades.

2.5 PM&C Server Version and TVOE version

Policy Release 11.5 requires **PM&C server upgrade** from version 5.x to version 5.7. PM&C server involves the upgrade of **TVOE** to Rel 2.7, minimum**.**

2.6 TPD Version

For upgrade to Policy Release 11.5, the supported (TPD) version is **6.7**

<u>The following cases require an IPM/Fresh Install</u>

- Blade/Server Replacement
- Disaster Recovery
- IPM of a server for any reason

2.7 Acquiring firmware

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices. The required firmware media and binaries are managed and distributed as part of the *HP Solutions Firmware Upgrade Pack 2.2.5/2.2.6/2.2.7*. The current ***minimum*** firmware release required for this product is *HP Solutions Firmware Upgrade Pack 2.2.6/2.2.7* and 2.2.5 for PM&C 5.7.

The *HP Solutions Firmware Upgrade Pack* contains multiple BOM items including media and documentation. This document only requires access to the media (CD/DVD or ISOs) as well as the *Release Notes* document.

The two pieces of required firmware media provided in the *HP Solutions Firmware Upgrade Kit 2.2.5* release are:

- HP Smart Update Firmware DVD/ISO - 872-2488-106-2.2.5_10.37.0-FW_SPP.iso
  - USB Part Number = 875-1124-306
- HP Misc Firmware CD/ISO - 872-2161-118-2.2.5_10.36.0-FW_MISC.iso
  - USB Part Number = 875-0903-315

The two pieces of required firmware media provided in the *HP Solutions Firmware Upgrade Kit 2.2.6/2.2.7* release are:

- HP Service Pack for ProLiant ISO 2.2.7 - FW2_SPP-2.2.7.0.0_10.41.0.iso
- HP Misc Firmware ISO 2.2.6 - FW2_MISC-2.2.7.0.0_10.41.0.iso

Refer to the Release Notes of the target release of the *HP Solutions Firmware Upgrade Pack* used to determine specific media part numbers to use and the specific firmware versions provided.

Policy 11.5 Servers and devices that may require firmware updates are:

- HP c7000 Blade System Enclosure Components:
  - Onboard Administrator (Rev 3.71 is REQUIRED to support GEN 8)
  - HP 6120XG Network Switches
  - BL460c Gen8 Blade Servers
- HP DL380 Gen8 Rack Mount Servers

2.8 Server Hardware Platforms

Release 11.5 introduces support for the Sun Netra servers on Rack Mount Servers (RMS). The existing support for the HP G6 and Gen8 servers will be continued. The PP-5160 servers will not be supported in Release 11.5.

The Policy applications in Release 11.5 shall support a mix of Sun Netra RMS systems with Policy application in Cable Mode running either on RMS HP DL360 G6, DL360 G7, and DL360 G8 or on DL380 G8.

NOTE: It is expected that the set of blades or servers within an application instance will always be of a homogenous type and configuration.

2.9 Loading Application software

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

If the system is C-class, the Application software must also be loaded into the PM&C software management library to support new installs and FRU (firmware upgrade) activities.

NOTE: PM&C is not used during the upgrade and backout procedures. PM&C GUI provides a platform for management and growth of blade applications, multiple c-class enclosures as well as networking equipment in the c-class environment.

2.10 Required Materials and Remote Access

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

1. Target-release Policy 11.5 software ISOs
2. Target-release Policy 11.5 software Upgrade Release Notes
3. The capability to remote login, using either CONSOLE or SSH, to the target server as *root*

   NOTE: The remote login can be done through SSH (as *admusr* only), local console, or iLO maintenance port. Ensure the customer network Firewall policy allows the required application and corresponding ports
4. The capability to secure copy (SCP) from the local workstation used to perform this upgrade to the target server or otherwise be able to transfer binary files to the target server
5. User logins, passwords, IP addresses and other administration information
6. VPN access to the customer's network is required if that is the only method to remote logging into the target servers. It must be also possible to access the Policy Manager/CMP GUI, iLO/OA, and the PM&C GUI.

Logins, Passwords and Server IP Addresses -

The IP Address assignments for each site from the appropriate Oracle Network IP Site Survey (example: SS005938) 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 this information in the table below.
[It is assumed that the Logins may be common among the customer sites. If not, record for each site.]

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

Table-2: Logins, Passwords and Server IP Addresses

Item	Value
CMP servers (each CMP server)	GUI Administrator Login User/Password:
	root password: **NOTE**: This is the password for the **root** login on the servers. This is not the same login as the GUI or Application Administrator.
MRE/MPA servers (each server)	**root** password:
Target iLO (each server)	iLO Administrator Login: User/Password:
Target Onboard Administrator (each C-class enclosure)	OA Administrator Login: User/Password:
PM&C server (each C-class site)	GUI Administrator Login User/Password:
	root password: **NOTE**: This is the password for the **root** login on the servers. This is not the same login as the GUI or Application Administrator.
Software Upgrade Target Release (The ISO image filenames should match those referenced in the Release Notes for the target release)	Target Release Number:
	Policy 11.5 software ISO Image (.iso) filenames :

2.10.1 Upgrade Media

The required Policy Release 11.5 software ISO image files are as below for this Upgrade procedure:

TVOE host:	**TVOE-2.7.0.0.0_84.20.0-x86_64.iso**
PMAC:	**PMAC-5.7.0.0.1_57.17.1-x86_64.iso**
TPD:	**TPD.install-6.7.0.0.1_84.18.0-OracleLinux6.5-x86_64.iso**
CMP:	**cmp-11.5.0.0.0_39.1.0-x86_64.iso**
MPE:	**mpe-11.5.0.0.0_39.1.0-x86_64.iso**
MRA :	**mra-11.5.0.0.0_39.1.0-x86_64.iso**

3. UPGRADE PREPARATION

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

3.1 Overview & Sequence of full upgrade with planning and tracking

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

1. Upgrade PM&C Server ***(to be done first)***
2. Upgrade CMP clusters
3. Upgrade MPE clusters
4. Upgrade MRA clusters

Overview:

1. Upgrade PM&C Server at Site-1 *(See Appendix A)*
2. Upgrade PM&C Server at Site-2 *(See Appendix A)*
3. Upgrade Site-1, and then Site-2 CMP clusters.

4. <u>Segment 1 Site-1:</u>
   Upgrade MPE clusters
   Upgrade MRA clusters

5. <u>Segment 1 Site-2:</u>
   Upgrade MPE clusters
   Upgrade MRA clusters

6. <u>Segment 2 Site-1:</u>
   Upgrade MPE clusters
   Upgrade MRA clusters

7. <u>Segment 2 Site-2:</u>
   Upgrade MPE clusters
   Upgrade MRA clusters

3.2 Procedure-1: Pre-requisites

The following Procedure-1 table verifies the prerequisite steps to be performed before the upgrade procedure begins.

Procedure-1: Pre-requisites		
Step	**Procedure**	
1. ☐	Verify required materials and administration data needed during upgrade	As listed in section 2.10 "Required Materials & Remote Access" Double-check all information in Table-2: Logins, Passwords and Server IP Addresses
2. ☐	Review Release Notes	Review Policy Release 11.5 for the following information: - Individual Software components and versions included in target release - New features included in target release - Issues (Oracle PRs) resolved in target release - Known Issues with target release - Any further instructions that may be required to complete the software upgrade for the target release Also review platform and firmware release notes and make preparations for the upgrade accordingly.
3. ☐	Contact Oracle Customer Care Center	Inform Oracle Customer Care Center of the upgrade plans on the target system. See section "SOFTWARE UPGRADE CAUTIONS" for contact information.

3.3 Procedure-2: Plan and Track Cluster Upgrades

The following Procedure-2 table must be completed, before performing the upgrade, to identify the clusters to be upgraded and plan the work. It can also be used to track completion of the upgrade and assign work to different engineers.

NOTE:

- It's recommended not to make policy or configuration while the system is in mixed-version mode, during upgrade or backout.
- Time estimates are for upgrade without backout. Backout procedure time is typically same or less than the upgrade procedure time.

<table>
<tr><th colspan="4">Procedure-3: Plan and Track Cluster Upgrades</th><th></th><th></th></tr>
<tr><th>Step</th><th>Procedure</th><th colspan="2">Result</th><th>Engineer</th><th>Time</th></tr>
<tr><td>1. ☐</td><td>Use the following Checklist to plan the Cluster upgrades for the entire system</td><td colspan="2">Maintenance Windows are accordingly planned per the upgrade schedule</td><td></td><td></td></tr>
<tr><td>2. ☐</td><td>Upgrade Site-1(Primary) and then Site-2(Secondary) CMP clusters</td><td colspan="2">Site Names _____ & _____</td><td></td><td>3 hrs</td></tr>
<tr><td>3. ☐</td><td>Upgrade Site-1 MPE clusters for Segment-1

NOTE: Maximum of 3 MPE clusters can be performed in parallel</td><td colspan="2">Site Name _____

Cluster List:
<table><tr><th>Cluster Name</th><th>hostname1</th><th>hostname2</th><th>Completed</th></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
<tr><td>4. ☐</td><td>Upgrade Site-1 MRA clusters for Segment-1

NOTE: Maximum of 3 MRA clusters can be performed in parallel</td><td colspan="2">Site Name _____

Cluster List:
<table><tr><th>Cluster Name</th><th>hostname1</th><th>hostname2</th><th>Completed</th></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
</table>

<table>
<tr><th colspan="4">Procedure-3: Plan and Track Cluster Upgrades</th><th></th><th></th></tr>
<tr><th>Step</th><th>Procedure</th><th colspan="2">Result</th><th>Engineer</th><th>Time</th></tr>
<tr><td>5. ☐</td><td>Upgrade Site-2 MPE clusters for Segment-1

NOTE: Maximum of 3 MPE clusters can be performed in parallel.</td><td colspan="2">Site Name _____

Cluster List:
<table><tr><th>Cluster Name</th><th>hostname1</th><th>hostname2</th><th>Completed</th></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
<tr><td>6. ☐</td><td>Upgrade Site-2 MRA clusters for Segment-1

NOTE: Maximum of 3 MRA clusters can be performed in parallel</td><td colspan="2">Site Name _____

Cluster List:
<table><tr><th>Cluster Name</th><th>hostname1</th><th>hostname2</th><th>Completed</th></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
<tr><td>7. ☐</td><td>Upgrade Site-1 MPE clusters for Segment-2

NOTE: Maximum of 3 MPE clusters can be upgraded in parallel</td><td colspan="2">Site Name _____

Cluster List:
<table><tr><th>Cluster Name</th><th>hostname1</th><th>hostname2</th><th>Completed</th></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
</table>

<table>
<tr><th colspan="4">Procedure-3: Plan and Track Cluster Upgrades</th><th></th><th></th></tr>
<tr><th>Step</th><th>Procedure</th><th colspan="2">Result</th><th>Engineer</th><th>Time</th></tr>
<tr><td>8. ☐</td><td>Upgrade Site-1 MRA clusters for Segment-2

NOTE: Maximum of 3 MRA clusters can be performed in parallel</td><td colspan="2">Site Name _____

Cluster List:
<table><tr><td>Cluster Name</td><td>hostname1</td><td>hostname2</td><td>Completed</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
<tr><td>9. ☐</td><td>Upgrade Site-2 MPE clusters for Segment-2

NOTE: Maximum of 3 MPE clusters can be performed in parallel</td><td colspan="2">Site Name _____

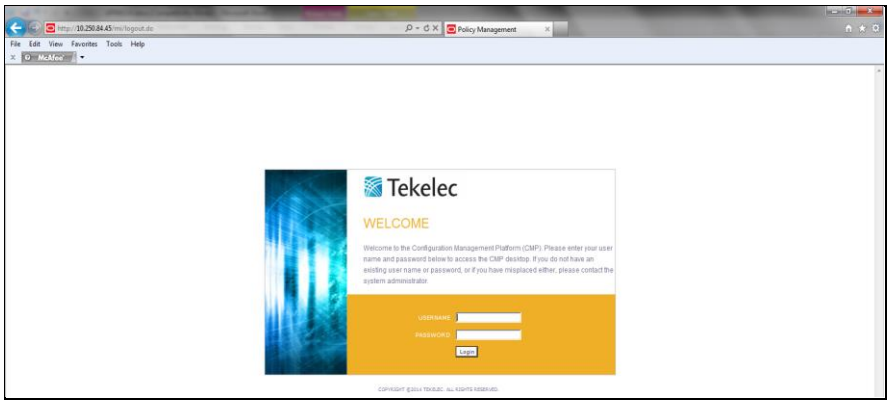
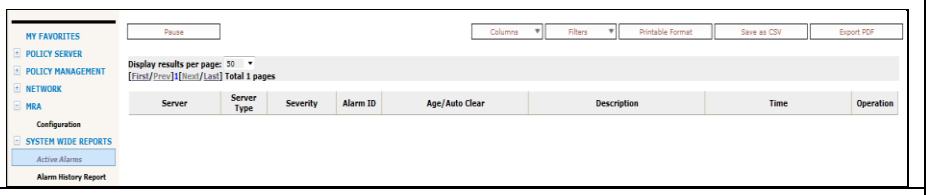
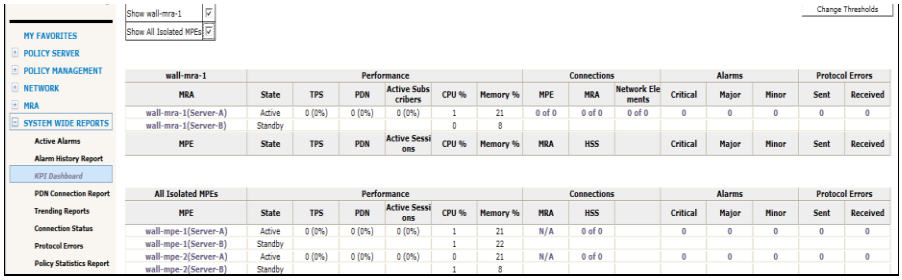
Cluster List:
<table><tr><td>Cluster Name</td><td>hostname1</td><td>hostname2</td><td>Completed</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
<tr><td>10. ☐</td><td>Upgrade Site-2 MRA clusters for Segment-2

NOTE: Maximum of 3 MRA clusters can be performed in parallel</td><td colspan="2">Site Name _____

Cluster List:
<table><tr><td>Cluster Name</td><td>hostname1</td><td>hostname2</td><td>Completed</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td><td></td><td>2 hrs</td></tr>
</table>

3.4 Procedure-3: Perform System Health Check

This procedure is to determine the health and status of the servers to be upgraded and must be executed at least once before upgrade kick-off.

Procedure-4: Perform System Health Check (Upgrade Preparation)		
Step	**Procedure**	**Result**
1. ☐	CMP GUI Access	Browse to CMP GUI VIP address: 
2. ☐	View Active Alarms	**System Wide Reports → Active Alarms** Identify the cause of any active alarms and determine if these may have impact on the upgrade. Export current Alarms to save into a file using 'Save as CSV' or 'Export PDF'. **IMPORTANT:** Before starting any upgrade activity, please ensure that all Active Alarms are well understood and resolved. 
3. ☐	View KPI reports	Verify that the system is running within expected performance parameters. Export current KPIs to save into a file, see Appendix. **System Wide Reports → KPI Dashboard** 

Procedure-4: Perform System Health Check (Upgrade Preparation)		
Step	**Procedure**	**Result**
4. ☐	Confirm NTP servers are reachable from all the servers (CMP, MPEs & MRAs) to be upgraded **NOTE:** If the time across the servers is out of sync, fix it first and re-validate this step before starting the upgrade procedures.	**Validate the IP connectivity between the servers and NTP servers:** **#** ping 10.250.32.10 PING 10.250.32.10 (10.250.32.10) 56(84) bytes of data. 64 bytes from 10.250.32.10: icmp_seq=1 ttl=60 time=0.442 ms (note: if icmp is blocked in the network ping to the NTP destination address may not respond) **Confirm that time is synchronized on each server, using the *shell:*** # ntpq -np remote refid st t when poll reach delay offset jitter ========== *10.250.32.10 192.5.41.40 2 u 38 64 377 0.265 0.449 0.069 ========== **Confirm that date and time is correct on each server**: # date Tue Jun 3 16:04:48 EDT 2014 **Check that BIOS clock is synced with kernel clock using *shell*:** # hwclock Tue 03 Jun 2014 04:02:35 PM EDT -0.087409 seconds

3.5 Deploy Policy Upgrade Software

This procedure is intended for remote execution of the upgrade.

3.5.1 Procedure-4: Copy ISO image files to Management Server (PM&C)

This procedure transfers software Upgrade ISOs to **/var/TKLC/upgrade** directory on PM&C server connected to each site being upgraded.

Because the ISO images are large, the procedure includes instructions to check space available in the **/var/TKLC/upgrade** directory before copying the ISOs to this directory.

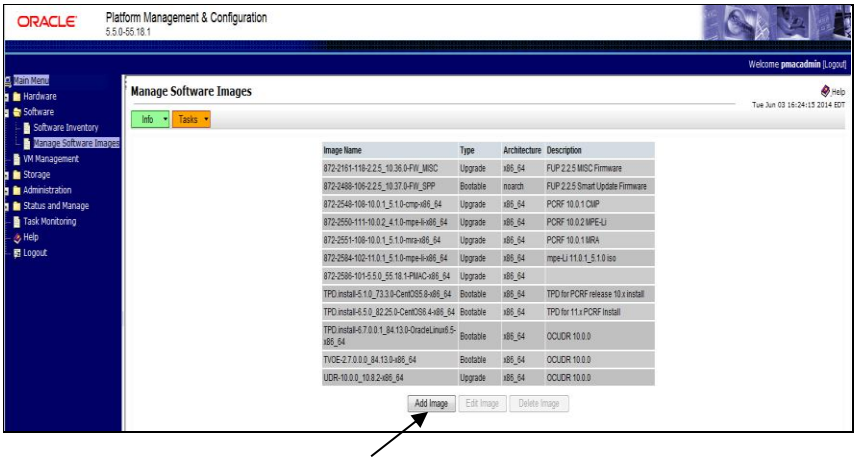
After the "Add Image" action on the PM&C, the ISO images are registered in PM&C and stored in the **/var/TKLC/smac/image/repository** directory which is very large.

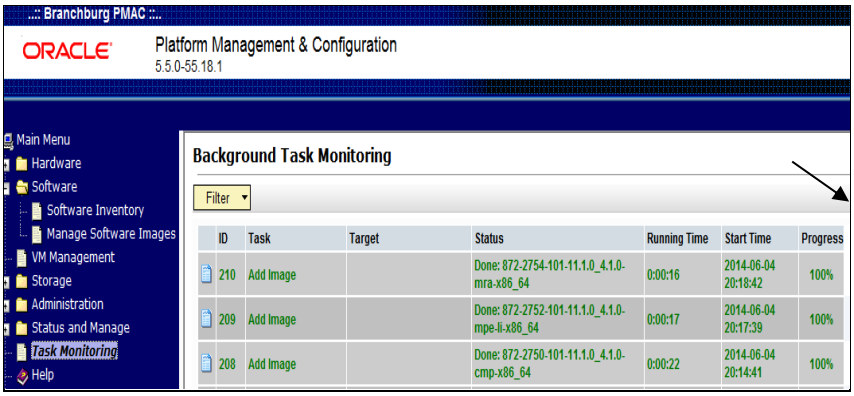
Software should be deployed to each Policy server "upgrade" directory before the actual upgrade activities. This is typically done with utilities such as SCP, WGET or SFTP.

Because of the large size of the software ISOs, sufficient time should be planned to accomplish this step.

For Policy Release 11.5, each ISO image size is about 1.0 GB in size.

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 the scheduled maintenance window and schedule the required maintenance windows accordingly before proceeding.

Procedure-5: Copy ISO images to Policy Management & Configuration Server (PM&C)		
Step	**Procedure**	**Result**
1. ☐	**PM&C GUI:** Verify no Release 11.5 ISO files exist	**Software → Manage Software Images** • Confirm there are no Release 11.5 ISO files already present
2. ☐	Access PM&C server and check disk space	• Login into the PM&C server as root with the provided password • Change Target directory to **/var/TKLC/upgrade** and ensure there is at least 3.0 GB free disk space available **# df -h /var/TKLC/upgrade** Filesystem Size Used Avail Use% Mounted on /dev/mapper/vgroot-plat_var_tklc 4.0G 451M 3.3G 12% /var/TKLC
3. ☐	Copy Release 11.5 ISO files to the target directory in the PM&C server	• Transfer all Release 11.5 ISO files (CMP, MPE, MRA) into directory **/var/TKLC/upgrade,** using either of the following methods: - SCP/WGET command OR - USB drive, follow the direction as outlined in Appendix(& *skip the following steps in this Procedure*)
4. ☐	**PM&C GUI:** Adding new Release 11.5 ISO files	**Software → Manage Software Images** • Select "**Add Image**" to select the ISO files that were transferred into PM&C server 

Procedure-5: Copy ISO images to Policy Management & Configuration Server (PM&C)		
Step	**Procedure**	**Result**
5. ☐	**PM&C GUI:** Verify new ISO files are successfully added	**Software → Manage Software Images** • The status of the image being added can be monitored via the "**Task Monitoring**" menu as below  **NOTE:** The newly added ISO files are now stored in directory **/var/TKLC/smac/image/repository.**

3.5.2 Procedure-5: Distribute Application ISO image files to servers

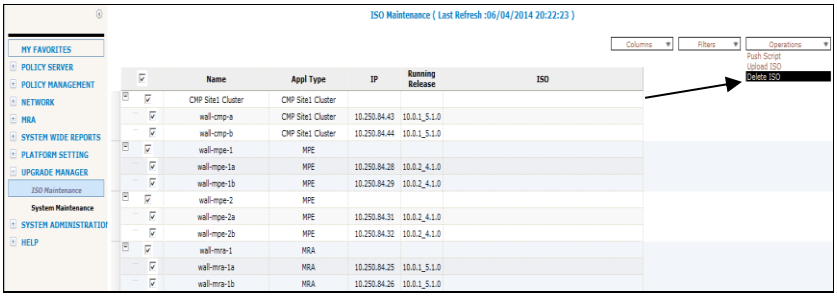
This procedure applies to all server types (CMP, MPE, and MRA). It assumes that the ISO Image files will be electronically copied to the sites to be upgraded.

There are three software images in this upgrade (CMP, MPE, and MRA).

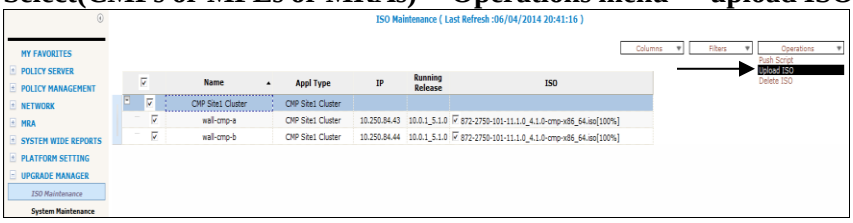
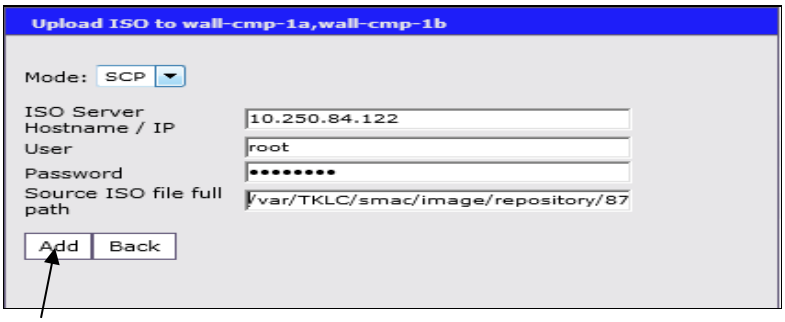
A single image must be deployed to the *upgrade* directory of each server to be upgraded, where the image is the correct type for that server, i.e. the new CMP software image must be deployed to the CMP servers, the new MPE image deployed to the MPE servers and the MRA image deployed to the MRA servers.

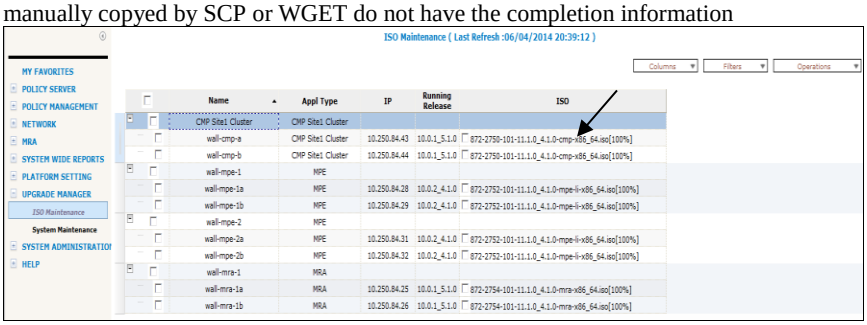
IMPORTANT: If the deployed image type (CMP, MPE, and MRA) does not match the existing installed software type, the upgrade will fail. Example: an attempt to upgrade a CMP with a MPE software image will fail during the Upgrade action. To change a server from one application type to another, the server must first be cleaned of all application software by an "Install OS" action via the PM&C GUI and then the new Application type installed, if required.

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 the scheduled maintenance window and schedule the required maintenance windows accordingly before proceeding.

Procedure-6: Distribute ISO images to target system		
Step	**Procedure**	**Result**
1. ☐	**CMP GUI: Access Primary CMP Server** – Remove old ISO files from servers, if any.	**Upgrade Manager → ISO Maintenance** • Select the server cluster(s) and choose **'delete ISO'** operation to perform the previous ISOs deletion:  • Select 'OK' to continue and wait till the successful deletion message • Wait till the 'ISO Maintenance' page is refreshed and shows the ISO files removal completion.

Procedure-6: Distribute ISO images to target system

Step	Procedure	Result
2. ☐	**CMP GUI:** Distribute ISOs to CMP/MPE/MRA servers **NOTE:** This step depends on the ISO type. Distribute ISOs accordingly. ISO image files should be copied to the each server node of the cluster.	**Upgrade Manager → ISO Maintenance** • (Optional but Preferred) Filter CMP/MPE/MRA • At one time, check one server type(MPE/MRA/CMP) to be upgraded and perform the 'upload ISOs' operation: **Select(CMPs or MPEs or MRAs)-> Operations menu -> upload ISO**  ***Upload ISO dialog -*** MODE = SCP ISO Server IP = < PM&C's IP address where the ISmd5sum O is located > USER = root Password = < root password of the PM&C server > Source ISO Full Path = /var/TKLC/smac/image/repository/< server type ISO filename > Click *Add.*  **Note: If the PM&C has been upgraded to rlealease 5.7 or above, and remote root access has been disabled, the user account pmacadmin / <pmacadmin password> can be used for this procedure.** **If the ISO upload operation cannot be done from CMP GUI for some reason then copy ISOs from PM&C to the required servers** Login to PM&C as root & access the directory where ISOs are located: *#cd* /var/TKLC/smac/image/repository Copy CMP ISO from PM&C to each of the CMP servers: **# scp cmp_iso <*cmp_hostname*>:/var/TKLC/upgrade/** Copy MPE ISO from PM&C to each of the MPE servers: **# scp mpe_iso <*mpe_hostname*>:/var/TKLC/upgrade/** Copy MRA ISO from PM&C to each of the MRA servers: **# scp mra_iso <*mra_hostname*>:/var/TKLC/upgrade/**

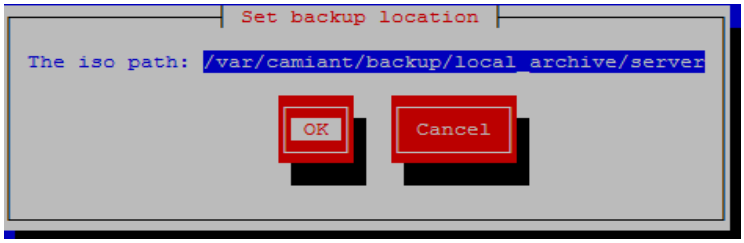
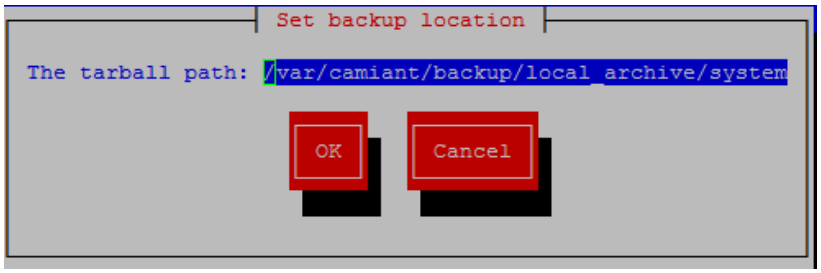
Procedure-6: Distribute ISO images to target system		
Step	**Procedure**	**Result**
3. ☐	**CMP GUI:** Verify ISO distribution to all the servers	**Upgrade Manager → ISO Maintenance** • Verify that the release 11.5 ISO file of the correct type is copied to each server node of the cluster. • When completed, the ISO column is populated with the ISO and a notification of 100% completion. ***NOTE***: Only when the ISO uploaded from CMP GUI will have the 100% flag. ISO manually copyed by SCP or WGET do not have the completion information 
THIS PROCEDURE HAS BEEN COMPLETED		

3.5.3 Procedure-6: Backups and Backup Locations

The purpose of this step is to be prepared for server recovery activities in case a server needs to be re-installed with software.

IMPORTANT:

- Server backups (for each MPE/MRA server) and the System backup (for Active CMP) must be collected and readily accessible for recovery operations.
- Perform the Backups outside the Maintenance Window period.

Procedure-7: Location of Backups for Active CMP System and MRA/MPE Servers		
Step	**Procedure**	**Result**
1. ☐	**SSH CLI/ iLO**: Access into the server to be backed up	Note: For access backups created in this section the backups should be stored at an off server location. Take Server Backup of all MPEs and MRAs: • Login to the active MPE/MRA server with root privileges • Navigate to the *platcfg* utility: #su – platcfg • Navigate to **Camiant Configuration->Backup and Restore->Server Backup** and provide the ISO backup filename in default backup location path: */var/camiant/backup/local_archive/serverbackup/<filename.iso>*  Similarly take System Backup of Active CMP: • Login into the Active CMP server with *root* privileges • Navigate to the *platcfg* utility: #su – platcfg • Navigate to **Camiant Configuration->Backup and Restore->System Backup** and provide the tar.gz backup filename in default backup location path: */var/camiant/backup/local_archive/systembackup/<filename.tra.gz>* 

Procedure-7: Location of Backups for Active CMP System and MRA/MPE Servers		
Step	**Procedure**	**Result**
2. ☐	**CLI/iLO:** Verify the backup ISO file	• If default location is accepted in the previous step, verify the file exists at each server: # cd /var/camiant/backup/local_archive/serverbackup # ls <hostname>-mpe_11.5.x_x.x.x-serverbackup-2014<xx><xx><xxxx>.iso # cd /var/camiant/backup/local_archive/serverbackup # ls <hostname>-mra_11.5.x_x.x.x-serverbackup-2014<xx><xx><xxxx>.iso # cd /var/camiant/backup/local_archive/systembackup # ls <hostname>-cmp_11.5.x_x.x.x-systembackup-2014<xx><xx><xxxx>.tar.gz
3. ☐	Identify Backups Location	Note: For access backups created in this section the backups should be stored at an off server location. Backup location is: _____ Instructions to access to backups are as follows: _____ _____ _____
THIS PROCEDURE HAS BEEN COMPLETED		

4. SOFTWARE UPGRADE CAUTIONS

Call the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US) prior to executing this upgrade to ensure that the proper media are available for use -

Access to Oracle's Customer Support site is restricted to current Oracle customers only. Following are the links to Oracle's Customer Support site and Oracle Support Hotlines

1. **Log into Oracle's new Customer Support site https://support.oracle.com**
2. **Refer Oracle Support Hotlines http://www.oracle.com/us/support/contact/index.html**

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

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

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

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

Please read the following notes on upgrade procedures:

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

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

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

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

5. PM&C UPGRADE

Please refer to appendix A for PM&C upgrade procedure. It's mandatory to upgrade PM&C before upgrading the policy servers, per the sequence outlined in section 2.2

6. UPGRADE CMP CLUSTERS

- Number of segments and sites depend on each customer network topology and so may vary.
- This procedure first upgrades Primary Site-1 CMP cluster and if Secondary Site-2 CMP cluster is available ***then*** upgrades that as well in a single maintenance window. When deployed as such, one site is designated as the Primary Site (the one managing the policy system) and the other as Secondary site (this site is ready to become Primary if needed).
- Although this procedure is not service affecting per se, yet it's recommended to perform it in a Maintenance Window.
- Policy or configuration changes should NOT be made while the system is in mixed-version operation.

IMPORTANT:

- CMP servers MUST be upgraded before the MPE or MRA clusters
- Site-1 CMP cluster ***must*** be upgraded to the new release before the Site-2 CMP is upgraded

6.1 About 'ACCEPT UPGRADE':

Once an upgrade has been completed, the upgrade must be accepted or rejected before any subsequent upgrades may occur. As part of upgrade, the Server Upgrade Pending Accept/Reject (TKSPLATMI33) alarm is set and the MOTD is updated to reflect that the upgrade has not yet been accepted.
'Accept Upgrade' will be the last thing you do in an upgrade, once the customer decides that the upgrade is successful, the upgrade may be accepted by running 'Accept Upgrade' from the UM.
After you 'Accept Upgrade':

1. Rollback will no longer be supported.
2. The server Upgrade Pending Accept/Reject alarm will be cleared.
3. If the Accept Upgrade step results in the conversion of the file system, a reboot will be triggered automatically.

'Accept Upgrade' will be only supported with these limitations:

1. All the servers in the topology have been upgrade to the new version 11.5.
2. The server's status is 'Pending'.
3. The server is 'Forced Standby'.

6.2 Overview Upgrade CMP Clusters

0) Use the UM GUI to place standby CMPs at both Primary Site and Secondary into Forced Standby
1) Use the UM GUI to upgrade Frc-Stb CMP server at the Primary Site
2) Use the UM GUI to perform Switch Forced Standby on Primary Site CMP Cluster
3) Log back into the UM GUI and upgrade remaining Primary Site CMP Frc-Stb server
4) Use the UM GUI to remove the Primary Site CMP server from Frc-Stb
5) Use the UM GUI to upgrade Frc-Stb CMP server at the Secondary Site
6) Use the UM GUI to perform Switch Forced Standby on Secondary Site CMP Cluster
7) Use the UM GUI to upgrade remaining Secondary Site CMP Frc-Stb server
8) Use the UM GUI to remove the Secondary Site CMP server from Frc-Stb
9) Use the UM GUI to select the upgraded CMP clusters and execute "Upgrade Completion"

Identify CMP sites to be upgraded and verify which sites are primary and secondary:

CMP Sites	Operator Site Name	Site Designation from Topology Form (Site-1 or Site-2)
Primary Site		
Secondary Site		

Note the Information on this CMP cluster:

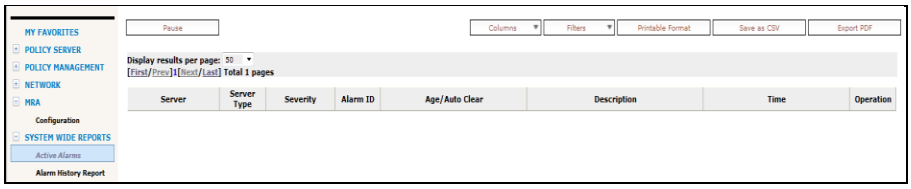
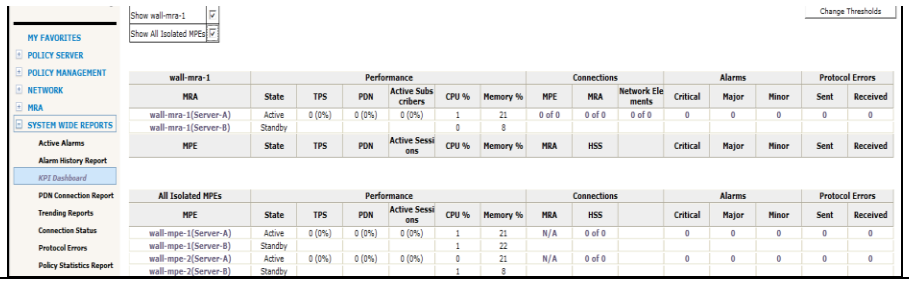
Cluster Name_____
Server-A Hostname _____
Server-A IP _____
Server-A Status _____

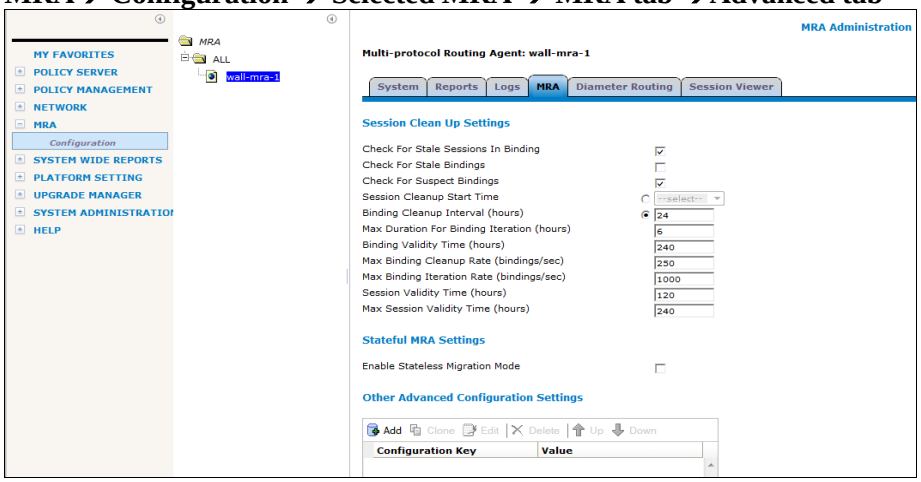
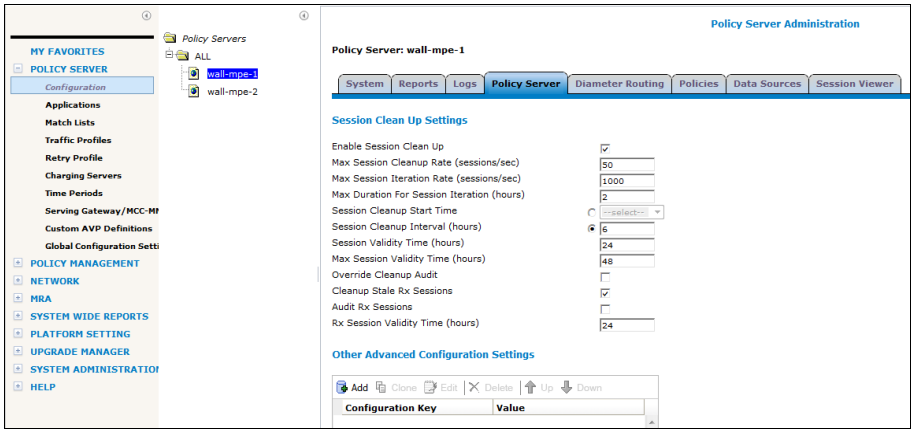
Server-B Hostname _____
Server-B IP _____
Server-B Status _____

Procedure-8: Upgrade CMP cluster@Site_____

Pre-requisites:

Previous Procedures completed!

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Alarms Status	**System Wide Reports → Active Alarms** • Confirm that any existing Alarm is well understood and no impact to the Upgrade procedure • Save a screenshot to a file for reference 
2. ☐	**CMP GUI:** Verify Traffic Status - KPI Dashboard Report	**System Wide Reports → KPI Dashboard** • Confirm all Connections and Traffic status are as expected. Observe it for few screen refreshes • Save a screenshot to a file for reference 

3. ☐	**CMP GUI:** Verify Advanced Settings on the MRA and MPE(Policy Server)	• Capture screenshots of the Advanced Settings on the MRA and MPE and save them into files for future reference: **MRA→ Configuration → Selected MRA → MRA tab →Advanced tab**  Note: It may also be advisable to capture the "MRA" tab configuration (as well as the Advanced Settings) **POLICY SERVER → Configuration → Selected MPE →Policy Server tab →Advanced tab**  Note: It may also be advisable to capture the "Policy Server" tab configuration (as well as the Advanced Settings)

<table>
<tr>
<td>4. ☐</td>
<td>CMP GUI: Identify and Record the CMP Cluster</td>
<td>

Platform Setting → Topology Settings → All Clusters

Cluster Settings

Name	Appl Type	OAM VIP	Server-A	Server-B	Operation
CMP Site1 Cluster (P)	CMP Site1 Cluster	10.240.239.39	10.240.239.37	10.240.239.38	View Demote
CMP Site2 Cluster (S)	CMP Site2 Cluster	10.250.84.46	10.250.84.25	10.250.84.26	View Delete
MPE Site1 Cluster1	MPE	<None>	10.240.239.24	10.240.239.25	View Delete
MRA Site1 Cluster1	MRA	<None>	10.240.239.22	10.240.239.23	View Delete

- The Primary CMP cluster has the annotation of "(P)" as shown on the table above with the arrow. If the topology has a Secondary CMP cluster it has the annotation of "(S)"
- Capture a screenshot and save into a file for future reference check

</td>
</tr>
<tr>
<td>5. ☐</td>
<td>CMP GUI: Verify Status of CMP Clusters</td>
<td>

Upgrade Manager → System Maintenance

Name	Appl Type	IP	Server State	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster	CMP Site1 Cluster						
slak-g6-cmp-1a	CMP Site1 Cluster	10.240.239.37	Active	Unknown	10.5.3_6.1.0	On	Completed:upgrade was completed at 10/23/2014 02:13:51 UTC
slak-g6-cmp-1b	CMP Site1 Cluster	10.240.239.38	Standby	Unknown	10.5.3_6.1.0	On	Completed:upgrade was completed at 10/23/2014 02:14:15 UTC
CMP Site2 Cluster	CMP Site2 Cluster						
site2-cmp-1a	CMP Site2 Cluster	10.250.84.25	Active	Unknown	10.5.3_6.1.0	On	Completed:upgrade was completed at 10/28/2014 16:56:46 UTC
site2-cmp-1b	CMP Site2 Cluster	10.250.84.26	Standby	Unknown	10.5.3_6.1.0	On	Completed:upgrade was completed at 10/28/2014 16:55:36 UTC
MPE Site1 Cluster1	MPE						

- Confirm the CMP clusters have the following:
  - **Active/Standby** status
  - **Running Release of 10.5.x or 9.1.x version**
  - **Replication ON**
  - **Corresponding Release 11.5 ISO files uploaded**

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

6. ☐	**To be done only on Site-1 CMP:**
	SSH CLI Primary Active CMP and verify the Primary Active CMP role
		• SSH into the Primary Active CMP with its **VIP** address.
		Login: **root**
		Password: **<provided root_password>**
		
		• Execute CLI command of "ha.mystate -i" to confirm that the CMP server's role is "**Active**":
		Primary Site CMP cluster :
		`[root@slak-g6-cmp-1a ~]#`
		`[root@slak-g6-cmp-1a ~]# ha.mystate -i`
		`resourceId role node subResources lastUpdate`
		`DbReplication Active slak-g6-cmp-1a 0 1023:224615.428`
		`VIP Active slak-g6-cmp-1a 0 1023:224615.451`
		`QP Active slak-g6-cmp-1a 0 1023:224615.429`
		`DbReplication_old OOS slak-g6-cmp-1a 0 1023:224545.127`
		`[root@slak-g6-cmp-1a ~]#`
		Secondary Site CMP cluster:
		`[root@site2-cmp-1a ~]# ha.mystate -i`
		`resourceId role node subResources lastUpdate`
		`DbReplication Active site2-cmp-1a 0 1028:161839.078`
		`VIP Active site2-cmp-1a 0 1028:161839.102`
		`QP Active site2-cmp-1a 0 1028:161839.081`
		`DbReplication_old OOS site2-cmp-1a 0 1028:161808.776`
		`[root@site2-cmp-1a ~]#`
		
		Note: DbReplication_old OOS is a non-issue status event.

7. ☐	**To be done only on Site-1 CMP:** SSH CLI Primary Active CMP then extract and update the upgrade scripts from the CMP ISO file**.**	• SSH into Primary Active CMP with its **VIP** address Login: root Password: <*provided root_password*> • Ensure the Release 11.5 CMP ISO file is present in **/var/TKLC/upgrade** directory**:** # cd /var/TKLC/upgrade # ls cmp-11.5.0.0_20.1.0-x86_64.iso Please note that the ISO images were copied to the server from PMAC in Procedure-5 of this document. • Backup, if any, the current **"policyUpgrade.pl"** and **"policyUpgradeHelper.pl"** scripts in **/opt/camiant/bin** directory # cp /opt/camiant/bin/policyUpgrade.pl /opt/camiant/bin/policyUpgrade.ofc # cp /opt/camiant/bin/policyUpgradeHelper.pl /opt/camiant/bin/policyUpgradeHelper.ofc # ls /opt/camiant/bin/*.ofc /opt/camiant/bin/policyUpgrade.ofc /opt/camiant/bin/policyUpgradeHelper.ofc • Mount the ISO file and copy the new **"policyUpgrade.pl", "qpSSHKeyProv.pl",** and **"policyUpgradeHelper.pl"** scripts into **/opt/camiant/bin** directory, overwrite the existing ones: # mount -o loop /var/TKLC/upgrade/cmp-11.5.0.0_20.1.0-x86_64.iso /mnt/upgrade # cp /mnt/upgrade/upgrade/policyScripts/policyUpgrade.pl /opt/camiant/bin cp: overwrite `/opt/camiant/bin/policyUpgrade.pl'? **yes**  # cp /mnt/upgrade/upgrade/policyScripts/qpSSHKeyProv.pl /opt/camiant/bin  # cp /mnt/upgrade/upgrade/policyScripts/policyUpgradeHelper.pl /opt/camiant/bin cp: overwrite `/opt/camiant/bin/policyUpgradeHelper.pl'? **yes** • Unmount the **/mnt/upgrade** directory # cd / # umount /mnt/upgrade

8. ☐

To be done only on Site-1CMP:
SSH CLI Primary Active CMP and append new Table Exclusions replication for data tables- ***PcmmSession,PcmmSessionPhysT***

This step allows the new *Table Exclusions* to be automatically replicated to all servers including the Secondary Active CMP server, from the Primary Active CMP existing Topology configuration, and notifies those servers NOT to process further updates to these excluded tables

This Minor Alarm may be expected from servers but clears itself very quickly.
31101 - DB replication to a slave DB has failed

- From the **Primary Site Active CMP** blade**,** execute:

#qpSSHKeyProv.pl --prov --user=root

This operation will exchange SSH keys for the topology; ***root password*** will be needed.

```
[root@slak-g6-cmp-1a /]# qpSSHKeyProv.pl --prov --user=root

The password of root in topology:
Connecting to root@site2-cmp-1b (10.250.84.26) ...
Connecting to root@slak-g6-mpe-1b (10.240.239.25) ...
Connecting to root@slak-g6-mra-1b (10.240.239.23) ...
Connecting to root@slak-g6-cmp-1b (10.240.239.38) ...
Connecting to root@slak-g6-mra-1a (10.240.239.22) ...
Connecting to root@slak-g6-cmp-1a (10.240.239.37) ...
Connecting to root@site2-cmp-1a (10.250.84.25) ...
Connecting to root@slak-g6-mpe-1a (10.240.239.24) ...

[1/8] Provisioning SSH keys on site2-cmp-1b (10.250.84.26) ...
[2/8] Provisioning SSH keys on slak-g6-mra-1b (10.240.239.23) ...
[3/8] Provisioning SSH keys on slak-g6-mpe-1b (10.240.239.25) ...
[4/8] Provisioning SSH keys on slak-g6-cmp-1b (10.240.239.38) ...
[5/8] Provisioning SSH keys on slak-g6-mra-1a (10.240.239.22) ...
[6/8] Provisioning SSH keys on slak-g6-cmp-1a (10.240.239.37) ...
[7/8] Provisioning SSH keys on site2-cmp-1a (10.250.84.25) ...
[8/8] Provisioning SSH keys on slak-g6-mpe-1a (10.240.239.24) ...

SSH keys are OK.
```

- List out the current **Table Exclusions a**nd no tables should be listed under column **excludeTables:**

iqt -p NodeInfo

```
[root@slak-g6-cmp-1a /]# iqt -p NodeInfo
nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables
A0188.078 site2-cmp-1b site2-cmp-1b,10.250.84.26 Active  Unspecified
A0188.129 site2-cmp-1a site2-cmp-1a,10.250.84.25 Active  Unspecified
A1041.147 slak-g6-cmp-1a slak-g6-cmp-1a,10.240.239.37 Active  Unspecified
A1041.203 slak-g6-cmp-1b slak-g6-cmp-1b,10.240.239.38 Active  Unspecified
C1213.145 slak-g6-mpe-1a slak-g6-mpe-1a,10.240.239.24 Active  Unspecified
C1213.230 slak-g6-mpe-1b slak-g6-mpe-1b,10.240.239.25 Active  Unspecified
C2563.007 slak-g6-mra-1a slak-g6-mra-1a,10.240.239.22 Active  Unspecified
C2563.151 slak-g6-mra-1b slak-g6-mra-1b,10.240.239.23 Active  Unspecified
[root@slak-g6-cmp-1a /]#
```

- Execute **"policyUpgrade.pl"** script to append the new table exclusions:

policyUpgrade.pl —prepareUpgrade

- List out, again, the current Table Exclusions showing the newly appended **excludeTables:**

iqt -p NodeInfo

```
[root@slak-g6-cmp-1a /]# iqt -p NodeInfo
nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables
A0188.078 site2-cmp-1b site2-cmp-1b,10.250.84.26 Active  Unspecified PcmmSession,PcmmSessionPhysT
A0188.129 site2-cmp-1a site2-cmp-1a,10.250.84.25 Active  Unspecified PcmmSession,PcmmSessionPhysT
A1041.147 slak-g6-cmp-1a slak-g6-cmp-1a,10.240.239.37 Active  Unspecified PcmmSession,PcmmSessionPhysT
A1041.203 slak-g6-cmp-1b slak-g6-cmp-1b,10.240.239.38 Active  Unspecified PcmmSession,PcmmSessionPhysT
C1213.145 slak-g6-mpe-1a slak-g6-mpe-1a,10.240.239.24 Active  Unspecified PcmmSession,PcmmSessionPhysT
C1213.230 slak-g6-mpe-1b slak-g6-mpe-1b,10.240.239.25 Active  Unspecified PcmmSession,PcmmSessionPhysT
C2563.007 slak-g6-mra-1a slak-g6-mra-1a,10.240.239.22 Active  Unspecified PcmmSession,PcmmSessionPhysT
C2563.151 slak-g6-mra-1b slak-g6-mra-1b,10.240.239.23 Active  Unspecified PcmmSession,PcmmSessionPhysT
[root@slak-g6-cmp-1a /]#
```

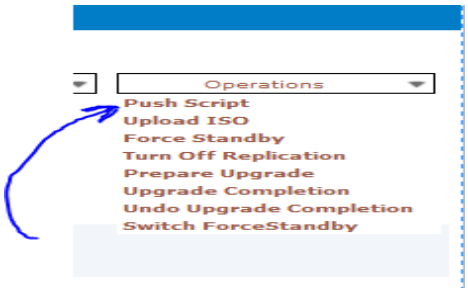
9. ☐ **CMP GUI**: Push the Release 11.5 upgrade Scripts to all servers in the segment topology

Upgrade Manager → System Maintenance

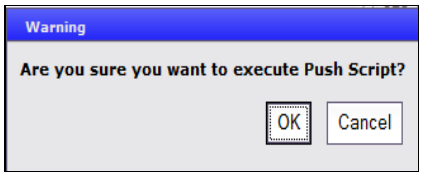
- **Select** all servers in the topology:

Name	Appl Type	IP	Server State
CMP Site1 Cluster	CMP Site1 Cluster		
slak-g6-cmp-1a	CMP Site1 Cluster	10.240.239.37	Active
slak-g6-cmp-1b	CMP Site1 Cluster	10.240.239.38	Standby
CMP Site2 Cluster	CMP Site2 Cluster		
site2-cmp-1a	CMP Site2 Cluster	10.250.84.25	Active
site2-cmp-1b	CMP Site2 Cluster	10.250.84.26	Standby
MPE Site1 Cluster1	MPE		
slak-g6-mpe-1a	MPE	10.240.239.24	Active
slak-g6-mpe-1b	MPE	10.240.239.25	Standby
MRA Site1 Cluster1	MRA		
slak-g6-mra-1a	MRA	10.240.239.22	Active
slak-g6-mra-1b	MRA	10.240.239.23	Standby

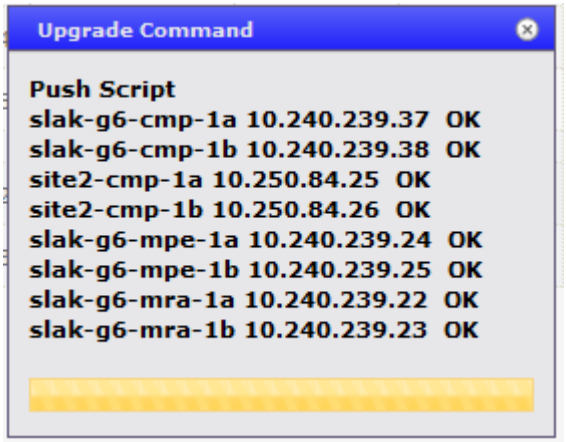
- Under **Operations menu**, select "**Push Script**" (It is safe to run Push Script repeatedly, if needed):

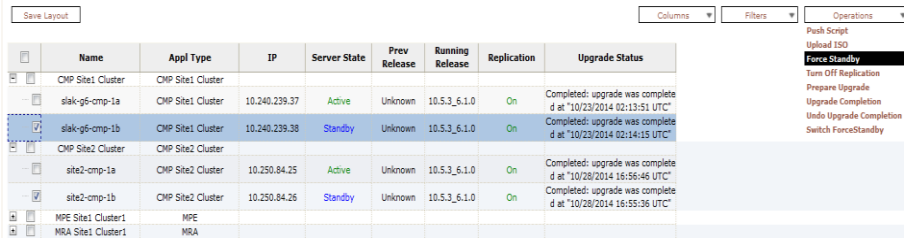
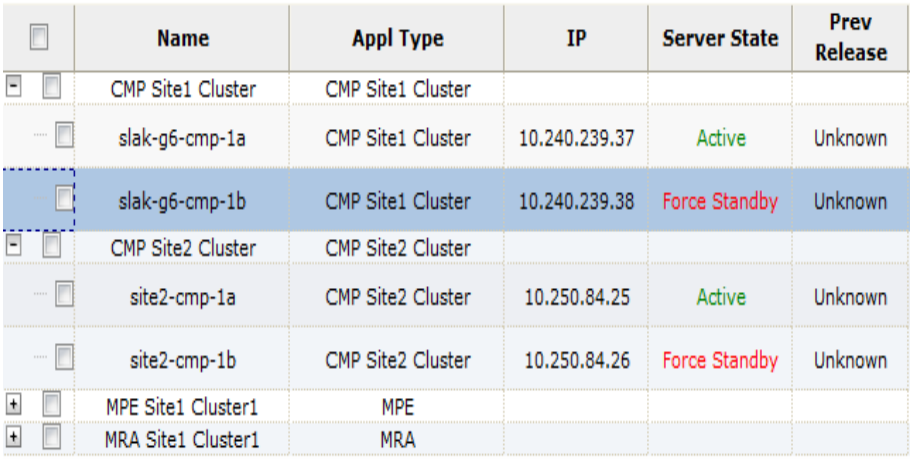


- Select "**OK**" to continue the operation:



- Operation successful:



10. ☐	**To be done only if topology has Site-2CMP:** SSH CLI Secondary Active CMP to validate its Role and the Table Exclusions for these data tables newly replicated from the Primary Active CMP -- ***PcmmSession,PcmmSessionPhysT***	On Secondary Active CMP, perform the same checks done on the Primary Active CMP: To check role: # ha.mystate –i To Check replicated excludeTables: # iqt -p NodeInfo
11. ☐	**CMP GUI:** Place standby CMPs at **both** Primary Site and Secondary into Forced Standby	**Upgrade Manager → System Maintenance** • **Select** checkbox for **Standby** CMP Server at **Site-1** • If the topology has a Secondary CMP cluster *then* **select** checkbox for **Standby CMP** Server at **Site-2** • Under **Operations menu**, select "***Force Standby***"  • Click "**OK**" to acknowledge the operation. • The Standby CMP server state changes to "***Force Standby***" 

Name	Appl Type	IP	Server State	Prev Release
CMP Site1 Cluster	CMP Site1 Cluster			
slak-g6-cmp-1a	CMP Site1 Cluster	10.240.239.37	Active	Unknown
slak-g6-cmp-1b	CMP Site1 Cluster	10.240.239.38	Force Standby	Unknown
CMP Site2 Cluster	CMP Site2 Cluster			
site2-cmp-1a	CMP Site2 Cluster	10.250.84.25	Active	Unknown
site2-cmp-1b	CMP Site2 Cluster	10.250.84.26	Force Standby	Unknown
MPE Site1 Cluster1	MPE			
MRA Site1 Cluster1	MRA			

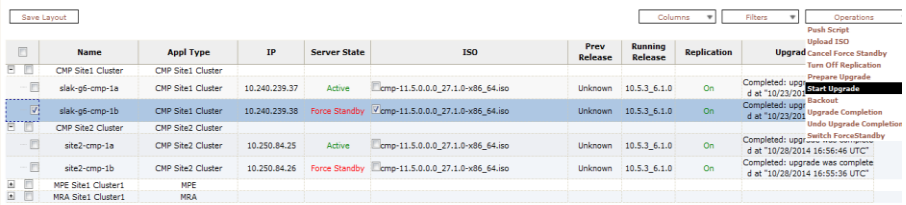
12. ☐

CMP GUI:
Upgrade the **Force Standby** CMP server at Primary Site

NOTE: This takes ~35 minutes to complete

Upgrade Manager → System Maintenance

- Select the checkbox of "Force Standby" CMP Server at Site-1
- Under **Operations menu**, select '**Start Upgrade'**

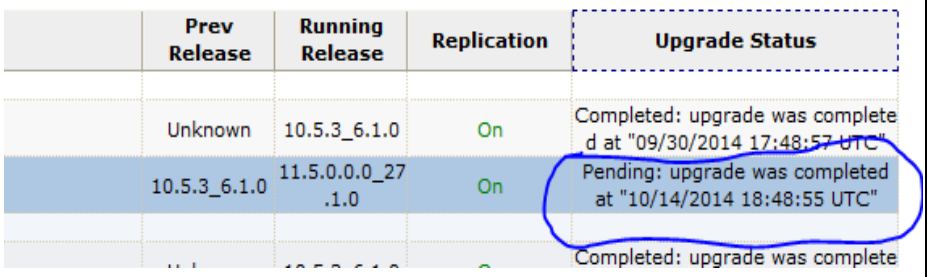


- Select "**OK**" to acknowledge the operation
- "*Upgrade Status*" column shows the ***InProgress*** status alongside different messages referring to different upgrade stages.
- In the meantime, following alarms may be generated and are considered normal reporting events:
  Expected Critical alarm:
  31283 High availability server is offline
  70025 The MySQL slave has a different schema version than the master

  Expected Major Alarm:
  70004 The QP processes have been brought down for maintenance.

  Expected Minor Database replication Alarms:
  31101, 31102, 31106, 31107, 31114.

- Wait till "*Pending: upgrade was completed….*" Status message appears and "Sync broken" indicator disappears:



Note: If the status message "*Pending: upgrade was completed….*" does not appear after estimated time, stop here and contact Oracle Technical Services to troubleshoot.

13. ☐

(OPTIONAL) iLO Remote Console:
Monitoring *Upgrade* progress on the CMP server being upgraded!

NOTE: In release 11.5, the ***root*** user's direct login can only be done using for Serial Console connectivity.

- iLO Remote Console (see Appendix) can be used to monitor the activities of the upgrade without losing IP connecitivity if using SSH CLI access:

  # tail –f /var/TKLC/log/upgrade/upgrade.log

- Once the upgrade script completes, the server automatically reboots and upon login, MOTD message displays as shown below:

Note: After the upgrade remote root access by the user root will be disabled. If you using ssh you will need to access the server with user "admusr/<default password>" and then su to root. You can login directly as root if you are using the remote console of the iLO.

```
slak-g6-cmp-1b login: root
Password:
Last login: Tue Oct 14 14:21:32 on tty1

|==============================================================|
| This system has been upgraded but the upgrade has not yet    |
| been accepted or rejected.  Please accept or reject the      |
| upgrade soon.                                                |
|==============================================================|
[root@slak-g6-cmp-1b ~]#
```

iLO Console on "Force Standby" CMP servers:
Verify the status of upgraded server

- **Confirm the upgraded version with the following commands:**

  # getPlatRev && getPolicyRev && ha.mystate -i

```
[root@slak-g6-cmp-1b ~]# getPlatRev && getPolicyRev && ha.mystate -i
6.7.0.0.1-84.20.0
11.5.0.0.0_27.1.0
          resourceId   role                    node      subResources      lastUpdate
       DbReplication   Stby          slak-g6-cmp-1b                 0 1014:144911.192
                 VIP   Stby          slak-g6-cmp-1b                 0 1014:144911.194
                  QP   Stby          slak-g6-cmp-1b                 0 1014:144911.490
   DbReplication_old    OOS          slak-g6-cmp-1b                 0 1014:144859.957
[root@slak-g6-cmp-1b ~]#
```

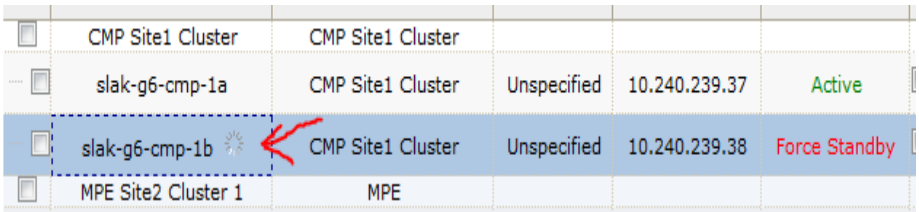
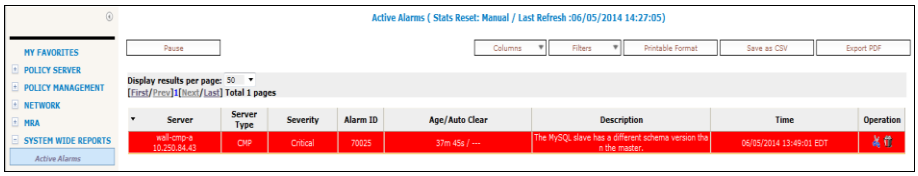
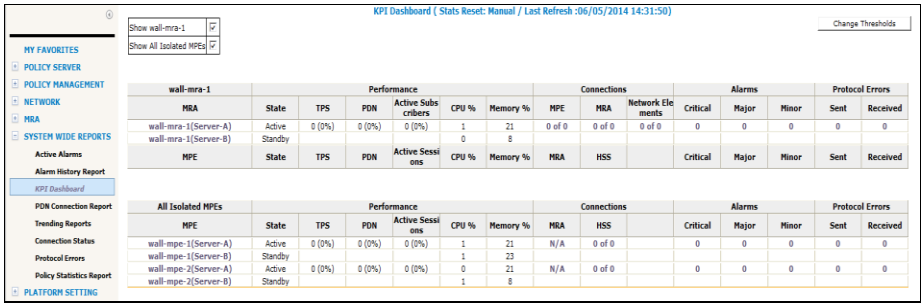
NOTE: Expect this server role is still shown as "stby" i.e. Standby state - same as prior to the upgrade

- Confirm the Database Replication operational status with the current Active server -

irepstat

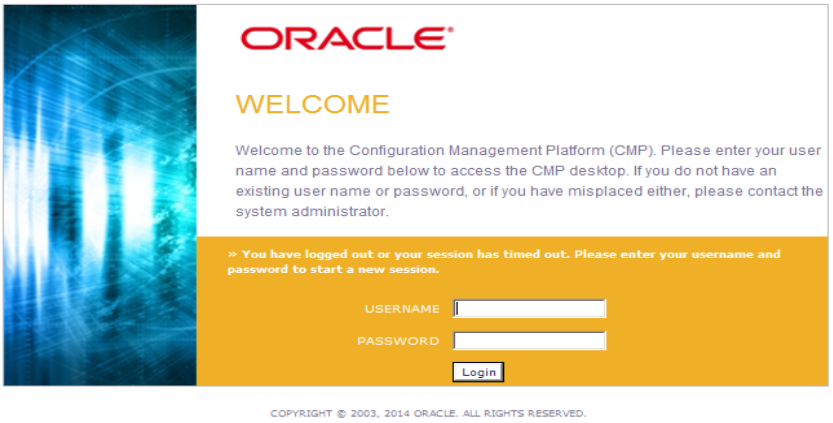
```
-- Policy 0 ActStb [DbReplication] ------------------------------
AA From slak-g6-cmp-1a Active      0   0.00 ^0.05%cpu 57B/s
```

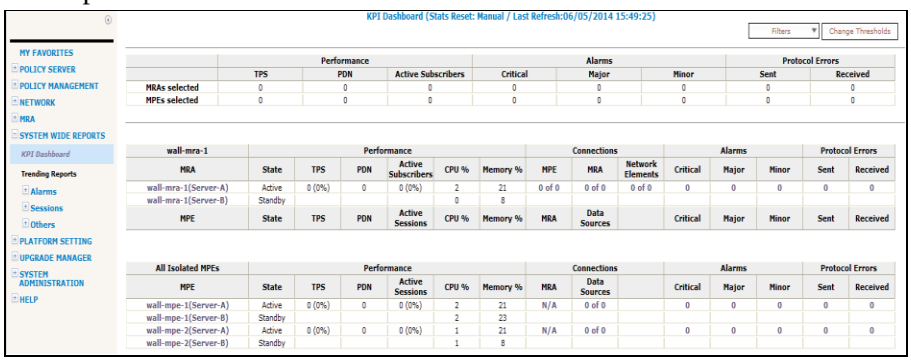
NOTE: This server's DbReplication status role is "Active" now with the current active server.

14. ☐	**CMP GUI:** Verify Upgrade Completion is successful	**Upgrade Manager → System Maintenance**  **Expect the server state is still shown as "Force Standby" - same as prior to the upgrade.** Any "***Sync Broken***" or '***Spinner***' indicator indicates that the data replication between the two servers of the cluster is not synced yet or the '***Pending'*** status. Wait for the replication if it's a replication broken indicator.
15. ☐	**CMP GUI:** Verify Alarms	**System Wide Reports → Active Alarms:** Expected alarms 70025- The MySQL slave has a different schema version than the master 32532-Server Upgrade Pending Accept/Reject  • Capture a screenshot and save into a file. The alarm 70025 is cleared after the cluster is fully upgraded to the same release. The alarm 32532 is cleared after the upgrade has been accepted.
16. ☐	**CMP GUI:** Verify System Wide Reports – KPI Dashboard Report	**System Wide Reports → KPI Dashboard**  • Verify that report shows normal traffic processing for the MPEs/MRAs. Observe it for a few screen refreshes

17. ☐	In next steps, proceed to switch the upgraded Release 11.5 CMP server to Active state	• At this point, the upgraded Standby server at Primary Site-1 running Release 11.5 should still be in "Force Standby" state **<u>DO NOT MODIFY ANYTHING FOR THE SERVER UNDER FORCE STANDBY CONDITION !!!</u>**
18. ☐	**CMP GUI:** Switch the upgraded Release 11.5 CMP server to Active	**Upgrade Manager → System Maintenance** • **Select** the checkbox for CMP cluster to be switched • Select "***Switch ForceStandby***" under **Operations menu** • Click "***OK***" to continue the operation and a success message appears. **NOTE:** At this point the current CMP GUI browser connection is lost – if it is the primary CMP cluster, need to re-login as illustrated in the next step
19. ☐	**CMP GUI:** Re-login to CMP server VIP and verify access to Policy Release 11.5 CMP GUI login form	• Close the current CMP GUI browser tab and re-open another browser tab with the same CMP VIP address. • The Policy Release 11.5 CMP GUI Login form appears as shown – Login and password credentials are the same as the pre-upgrade ones.

	Name	Appl Type	Site	IP	Server State
☑	CMP Site1 Cluster	CMP Site1 Cluster			
☑	slak-g6-cmp-1a	CMP Site1 Cluster	Unspecified	10.240.239.37	Active
☑	slak-g6-cmp-1b	CMP Site1 Cluster	Unspecified	10.240.239.38	Force Standby
☐	MPE Site2 Cluster 1	MPE			
☐	slak-g6-mpe-1a	MPE	Unspecified	10.240.239.24	Standby



20. ☐	**CMP GUI:** Verify System Wide Reports – KPI Dashboard Report	**System Wide Reports → KPI Dashboard** • Verify that report shows normal traffic processing for the MPEs/MRAs • Capture a screenshot and save into a file  KPI Dashboard (Stats Reset: Manual / Last Refresh:06/05/2014 15:49:25) Filters Change Thresholds MY FAVORITES POLICY SERVER POLICY MANAGEMENT NETWORK MRA SYSTEM WIDE REPORTS KPI Dashboard Trending Reports Alarms Sessions Others PLATFORM SETTING UPGRADE MANAGER SYSTEM ADMINISTRATION HELP Performance: TPS, PDN, Active Subscribers; Alarms: Critical, Major, Minor; Protocol Errors: Sent, Received MRAs selected 0 0 0 0 0 0 0 0 MPEs selected 0 0 0 0 0 0 0 0 wall-mra-1 — Performance: State, TPS, PDN, Active Subscribers, CPU %, Memory %; Connections: MPE, MRA, Network Elements; Alarms: Critical, Major, Minor; Protocol Errors: Sent, Received wall-mra-1(Server-A) Active 0 (0%) 0 0 (0%) 2 21 0 of 0 0 of 0 0 of 0 0 0 0 0 0 wall-mra-1(Server-B) Standby 0 8 MPE — State, TPS, PDN, Active Sessions, CPU %, Memory %; MRA, Data Sources; Critical, Major, Minor, Sent, Received All Isolated MPEs — Performance: State, TPS, PDN, Active Sessions, CPU %, Memory %; Connections: MRA, Data Sources; Alarms: Critical, Major, Minor; Protocol Errors: Sent, Received wall-mpe-1(Server-A) Active 0 (0%) 0 0 (0%) 2 21 N/A 0 of 0 0 0 0 0 0 wall-mpe-1(Server-B) Standby 2 23 wall-mpe-2(Server-A) Active 0 (0%) 0 0 (0%) 1 21 N/A 0 of 0 0 0 0 0 0 wall-mpe-2(Server-B) Standby 1 8
21. ☐	**CMP GUI:** Verify Alarms	**System Wide Reports → Alarms → Active Alarms:** Following are the expected **Alarm(s) ID:** **70022** – MySQL Slave failed Sync with the master **70025** -- The MySQL slave has a different schema version than the master **Capture a screenshot and save into a file. The alarms is cleared after the cluster is fully upgraded to the same release.**
22. ☐	**CMP GUI:**	**DO NOT MODIFY THE FORCE STANDBY CONDITION ON CMP.**

23. ☐	**CMP GUI:** Confirm current status of CMP Cluster	**Upgrade Manager → System Maintenance**
		
		• Verify the following -
		  ○ Active server is on Running Release 11.5
		  ○ Force Standby server is on the previous Release 10.5.x or 9.1.x
		  ○ "Sync Broken" indicator is NOT shown next to each server in the cluster i.e. all servers are in sync.

24. ☐

CMP GUI:
Upgrade "Force Standby" CMP server

NOTE: This takes ~35 minutes to complete.

Upgrade Manager → System Maintenance

- Select the checkbox of the "***Force Standby***" CMP server:

Save Layout

	Name	Appl Type	IP	Server State	ISO	Prev Release	Running Release
	CMP Site1 Cluster	CMP Site1 Cluster					
☑	slak-g6-cmp-1a	CMP Site1 Cluster	10.240.239.37	Force Standby	☑ cmp-11.5.0.0.0_27.1.0-x86_64.iso	10.5.3_6.1.0	10.5.3_6.1.0
	slak-g6-cmp-1b	CMP Site1 Cluster	10.240.239.38	Active	cmp-11.5.0.0.0_27.1.0-x86_64.iso	10.5.3_6.1.0	11.5.0.0.0_27.1.0
	CMP Site2 Cluster	CMP Site2 Cluster					

- Under ***Operations menu***, select "***Start Upgrade***"
- Select "**OK**" to acknowledge the operation.
- "*Upgrade Status*" column shows the *InProgress* status along with the upgrade activities. Progress is also indicated by a "*spinner*" displayed next to the CMP server name
- During the Upgrade activities, the following Alarms may be generated and are considered normal reporting events - These is cleared after the whole Cluster is completely upgraded

  Expected Critical Alarm:
  31283 High availability server is offline
  70025 The MySQL slave has a different schema version than the master

  Expected Major Alarm:
  70004 The QP processes have been brought down for maintenance

  Expected Minor Database Replication Alarms:
  31101, 31102, 31106, 31107, 31114

- Wait till "*Pending: upgrade was completed….*" Status message appears and "Sync broken" indicator disappears as shown –

	Name	Server State	Prev Release	Running Release	Replication	Upgrade Status
	CMP Site1 Cluster					
	slak-g6-cmp-1a	Force Standby	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/14/2014 19:55:17 UTC"
	slak-g6-cmp-1b	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/14/2014 18:48:55 UTC"
	MPE Site2 Cluster 1					

Note: If the status message "*Pending: upgrade was completed….*" does not appear after estimated time, stop here and contact Oracle Technical Services to troubleshoot.

25. ☐

<OPTIONAL> SSH CLI / iLO Remote Console: Monitoring Upgrade progress

- The iLO Remote Console (see Appendix) can be used to monitor activities of the upgrade without losing IP connectivity if using SSH CLI access

tail –f /var/TKLC/log/upgrade/upgrade.log

- Once the upgrade script completes, the server automatically reboots

NOTE: If a step in the upgrade fails, the upgrade script attempts to backout the upgrade automatically

26. ☐

iLO Console: Verify status of upgraded server

NOTE: SSHing to the servers using *root* credentials in release 11.5 is prohibited. Use *admusr* to SSH and then either use *sudo* with utilities or switch up the user as root using *su* commond.

- **Confirm the upgraded version with the following commands and outputs as example -**

getPlatRev && getPolicyRev && ha.mystate -i

```
|==========================================================|
[admusr@slak-g6-cmp-1a ~]$ getPlatRev && getPolicyRev && ha.mystate -i
6.7.0.0.1-84.20.0
11.5.0.0.0_27.1.0
ha.mystate: Cannot open NodeInfo at /opt/TKLCcomcol/cm6.3/prod/bin/ha.mystate li
ne 75.
[admusr@slak-g6-cmp-1a ~]$
```

NOTE: Expect this server role still shown as "Stby" i.e."Force Standby" - same as prior to the upgrade

- **Confirm the Database Replication operational status -**

irepstat

```
-- Policy 0 ActStb [DbReplication] ----------------------------------------
AA From slak-g6-cmp-1b Active      0   0.25 ^0.04%cpu 55B/s
```

NOTE: This server's DbReplication status role is now "Active"with the current active server, wall-cmp-1a in this example

27. ☐

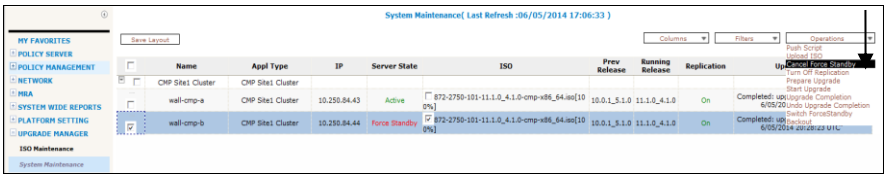
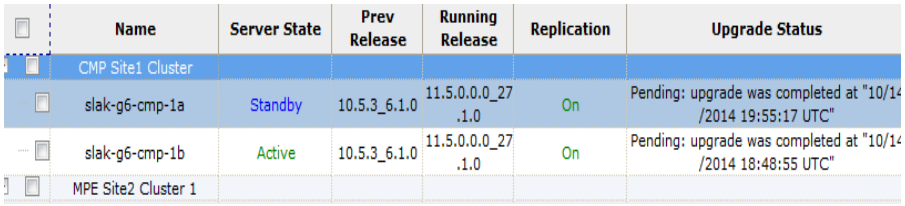
CMP GUI: Verify CMP Upgrade Completion is successful

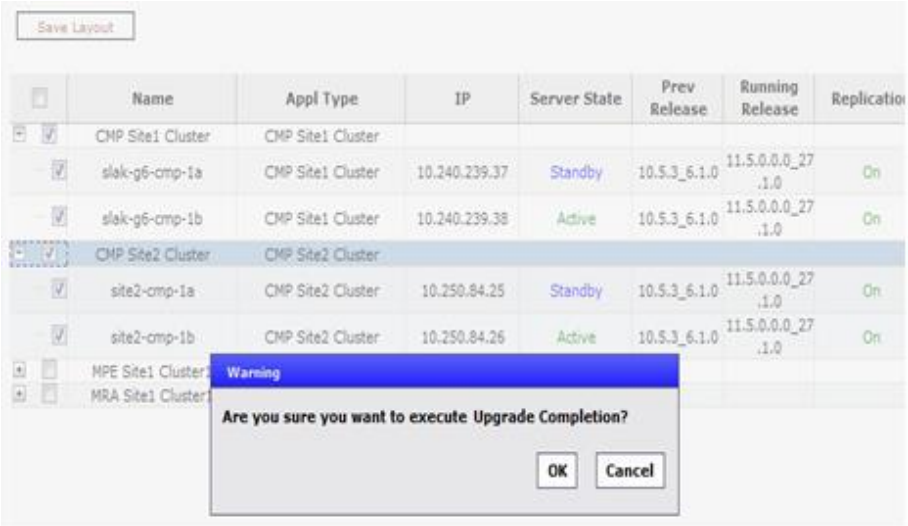
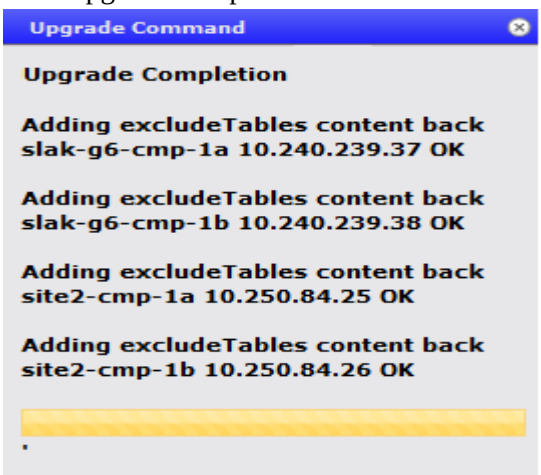
Upgrade Manager → System Maintenance

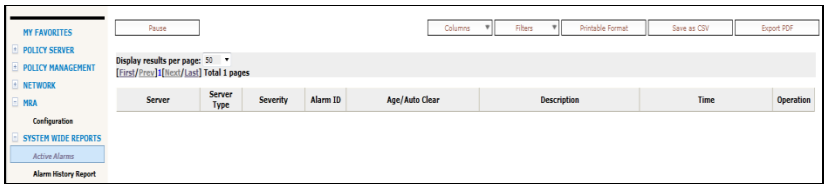
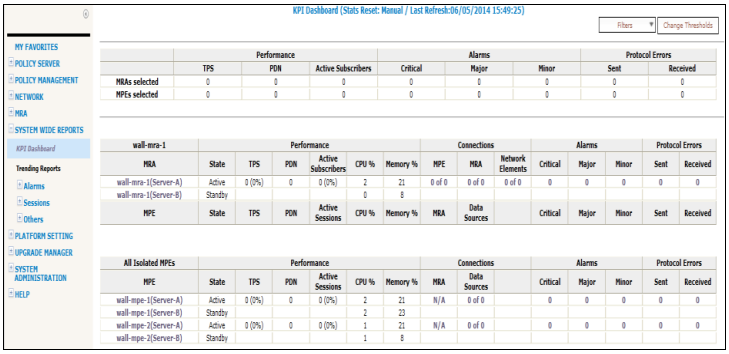
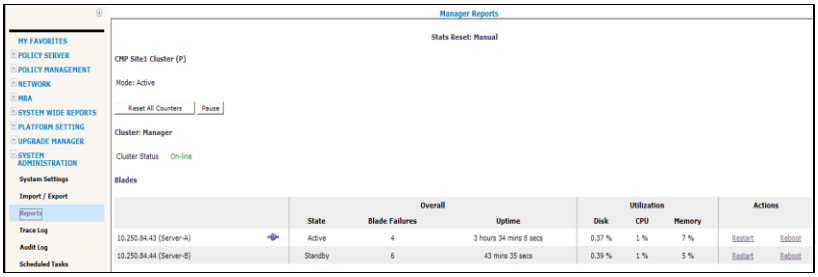
- Successful upgrade status shows both servers running the Release 11.5 under the "Running Release" column as an example shown below:

	Name	Server State	Prev Release	Running Release	Replication	Upgrade Status
	CMP Site1 Cluster					
	slak-g6-cmp-1a	Force Standby	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/14/2014 19:55:17 UTC"
	slak-g6-cmp-1b	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/14/2014 18:48:55 UTC"
	MPE Site2 Cluster 1					

NOTE: Expect the server state still shown as "Force Standby" - same as prior to the upgrade

28. ☐	**CMP GUI:** Cancel "Force Standby" back to "Standby" state	**Upgrade Manager → System Maintenance** • **Select** the checkbox of the "Force Standby" CMP Server • Under **Operations menu**, select "Cancel Force Standby"  • Select "OK" to continue the operation
29. ☐	**CMP GUI:** Verify Active and Standby CMP Cluster	**Upgrade Manager → System Maintenance** • Confirm CMP cluster has both "Active" and "Standby" status 
30. ☐	**Repeat for the Secondary site CMP cluster.**	If the topology has a Secondary CMP cluster at Site-2, **REPEAT Step-12 thru 29 of this procedure this procedure for Secondary CMP cluster at Site-2**. Move onto the following validation steps once both the CMP clusters are successfully upgraded.

31. ☐	**CMP GUI:** Execute 'Upgrade Completion' to finalize the upgrade procedure	**Upgrade Manager → System Maintenance** • **Select** the checkbox for both CMP clusters • Under **Operations menu**, select "Upgrade Completion"  • A **Warning** will pop-up, click 'OK' to continue the operation. • The following message appears for Exclusion Tables clearance; these tables were appended in Step8 of this procedure and are now cleared after Upgrade Completion. 

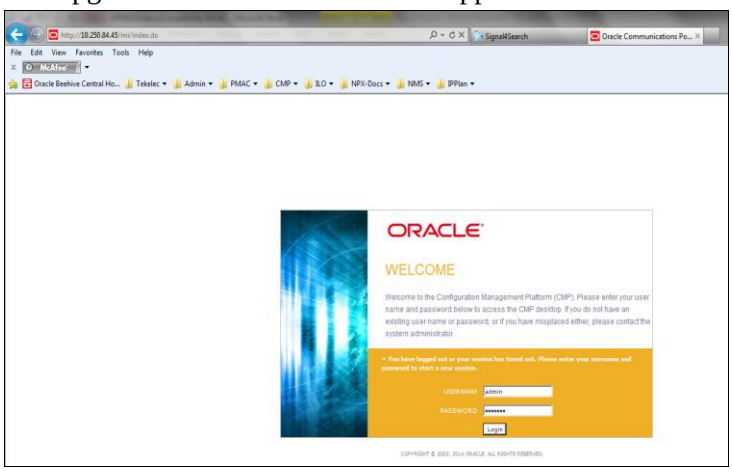
32. ☐	**CMP GUI:** Verify Alarms	**System Wide Reports → Active Alarms:** • Now all Critical & Major alarms which appeared during the Upgrade should be cleared after Site-1 cluster is fully upgraded to the new release as shown. If the topology has a Secondary CMP cluster then all Critical & Major alarms which appeared during the Upgrade should be cleared for Site-2 cluster as well - 
33. ☐	**CMP GUI:** Verify System Wide Reports – KPI Dashboard Report	**System Wide Reports → KPI Dashboard** • Verify that report shows all normal traffic processing for the MPEs/MRAs 
34. ☐	**CMP GUI:** Verify System Administration Reports	**System Administration → Reports** • Verify CMP cluster stats in the report and CMP Cluster Status as Online 
35. ☐	**CMP GUI:** Verify Active Alarm Status	• Certain Alarm(s) raised during the upgrade activities may take up to 15 minutes to clear. Verify the alarm has cleared in sometime. **(In Release 11.5, the Active Alarm display shows the auto-clear time for each alarm. This provides the user an idea of what time the alarm is expected to clear)** • NO Critical Alarm is expected

36. ☐	**CMP GUI:** Verify Advanced settings on the MPE and MRA	• Compare the current MRA and MPE advanced settings with those captured prior to upgrading the CMP clusters in Step3 of this procedure
37.	Procedure is complete	• Upgrade of CMP Clusters is complete • No unexpected Active Alarm is raised • At this point the PCRF system is running in mixed-version mode
THIS PROCEDURE HAS BEEN COMPLETED		

7. UPGRADE MPE CLUSTERS AND MRA CLUSTERS

The following procedures upgrade MPE cluster(s) and MRA cluster(s) under a segment at a site as per the overview and sequence explained in section 2.2.

7.1 Procedure-8: Initial Checks on CMP cluster at Site-1 and Site-2

Procedure-8: Initial Verification on CMP cluster at Site-1 and Site-2 (if topology has Site-2)		
Step	**Procedure**	**Result**
1. ☐	**CMP GUI at Site-1 & Site-2(if Site-2 exists) :** Using the supported browser, login to CMP server VIP as "admin" or another account defined Navigate to Help->About	The upgraded CMP GUI 11.5 should appear:  **Help** -> **About** shows the upgraded version 11.5

Procedure-8: Initial Verification on CMP cluster at Site-1 and Site-2 (if topology has Site-2)		
Step	**Procedure**	**Result**
2. ☐	**CMP GUI at Site-1 and Site-2(if Site-2 exists) :** Verify Current Upgrade Manager status and Software Release 11.5 ISO files	**Upgrade Manager → System Maintenance** • Verify all CMP, MPE & MRA Clusters have both Active & Standby status • Verify Policy Release 11.5 ISO files are available on all CMP, MPE & MRA clusters • Verify CMP cluster was successfully upgraded and running Policy Release 11.5.
THIS PROCEDURE HAS BEEN COMPLETED		

7.2 Procedure-9: Upgrade MPE clusters@Segment____@Site _____

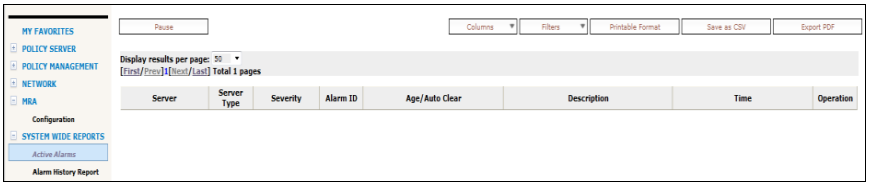
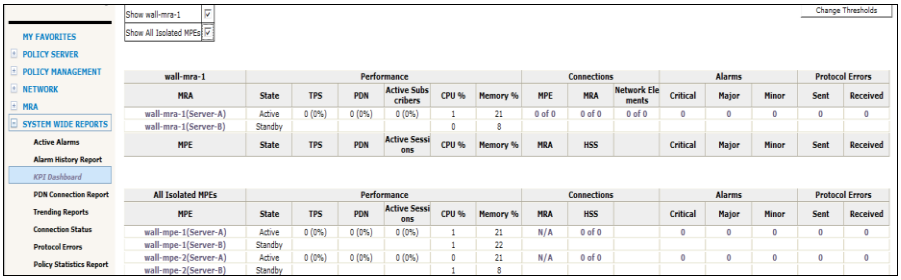
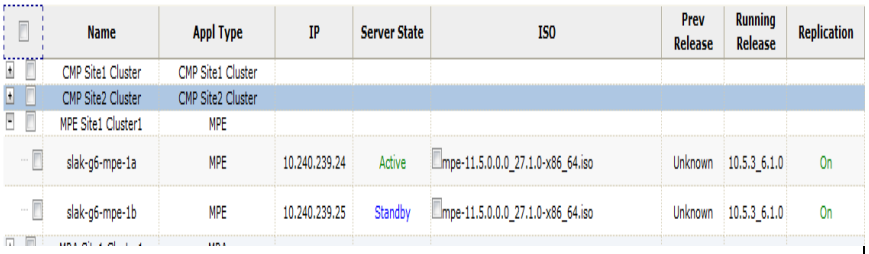
Pre-requisites and important notes:

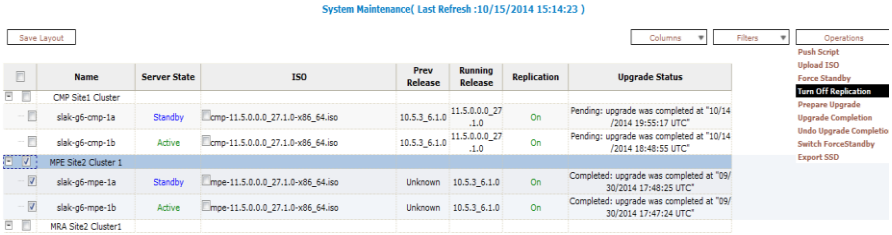
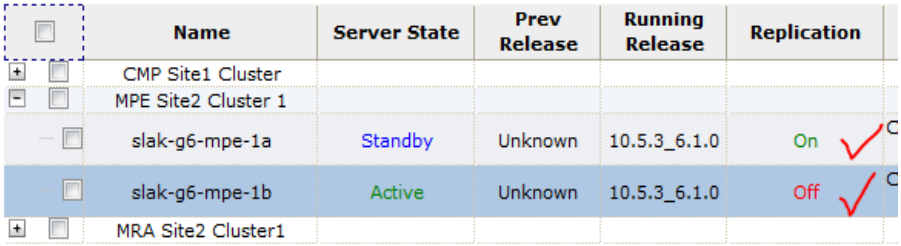
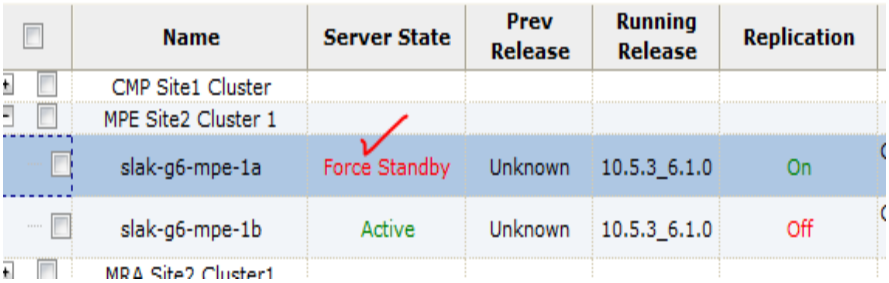
- Review of section 2.2
- This procedure upgrades one or more MPE clusters under a segment at a site.
- Number of segments and sites depend on customer network topology.
- MPE upgrade should precede the MRA upgrade at a site/segment.
- CMP upgrade has been completed
- In a segment at a given site, the recommended number of clusters to be upgraded at a time is 3 during a 2hour Maintenance window.
- It should also be noted that Policy or Configuration changes ought NOT to be carried out while the system is in mixed-version operation.

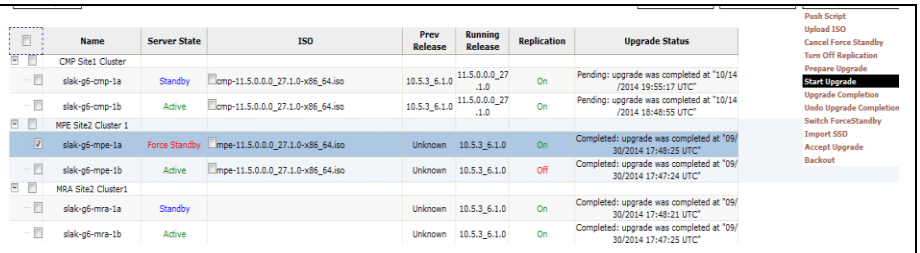
Overview:

1. Use the UM GUI to Turn Off Replication on the Active blade in the MPE cluster
2. Use the UM GUI to place standby MPE into Forced Standby
3. Use the UM GUI to Upgrade Frc-Stb MPE server
4. Use the UM GUI to Perform Switch Forced Standby on the MPE Cluster
5. Reapply Configuration for the cluster
6. Use the UM GUI to Upgrade remaining MPE Frc-Stb server
7. Use the UM GUI to turn On Replication for the Frc-Stb server
8. Use the UM GUI to Remove the MPE server from Frc-Stb
9. Use the UM GUI to select the upgraded MPE cluster and execute "Upgrade Completion"

Executional Guidance:

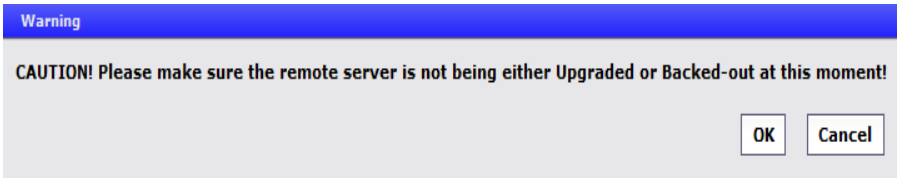
Step	Procedure	Result
1. ☐	**CMP GUI:** Perform health checks	• Perform the following health checks: - Check for current Active Alarms using CMP GUI **System Wide Reports → Active Alarms**  - Check KPI Dashboard (save screenshot to a file) **System Wide Reports → KPI Dashboard**  - *(Optional)* Reset MPE counters to make a baseline, see Appendix.
2. ☐	**CMP GUI:** Verify Upgrade Status of the MPE cluster(s)	**Upgrade Manager →System Maintenance** • (Optional but Preferred) Filter MPEs as described in Appendix • Verify information for the MPEs: - **Current Release 10.5.x or 9.1.x installed** - **Active/Standby status** - **ISO version to be deployed** 
3. ☐	**CMP GUI**: Apply Policy Release 11.5 upgrade scripts to all MPE cluster(s) to be upgraded	**Upgrade Manager →System Maintenance** • "**Push Script"** operation: **It's not needed to repeat this operation, since it's already completed in "Procedure 7 Step 9!"**

4. ☐	**CMP GUI:** Turn-OFF Replication on Active server(s)	**Upgrade Manager → System Maintenance** • ***Select*** checkbox for the ***Active*** MPE server • Under Operations menu, select "***Turn Off Replication***" operation.  • Select "**OK**" to continue the operation • Ensure Replication status under the column is **OFF** as shown  Expected **Minor** Alarm: **31113** Replication Manually Disabled
5. ☐	**CMP GUI:** Apply "Force Standby" state on Standby MPE server	**Upgrade Manager → System Maintenance** • ***Select*** checkbox for the ***Standby*** MPE server • Under ***Operations menu***, select "***Force Standby***" operation • Select "***OK***" to continue the operation  • Confirm that Server State is updated as "Force Standby".
6. ☐	**CMP GUI:** Start Upgrade on "Force Standby" MPE server(s)	**Upgrade Manager →System Maintenance** • ***Select*** checkbox for the "***Force Standby***" MPE server(s) and the ISO file is selected as well (ISO selection, however, happens automatically once Start Upgrade operation is triggered) • Under **Operations menu**, select "***Start Upgrade***" operation



Name	Server State	ISO	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster						
slak-g6-cmp-1a	Standby	cmp-11.5.0.0.0_27.1.0-x86_64.iso	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/14/2014 19:55:17 UTC"
slak-g6-cmp-1b	Active	cmp-11.5.0.0.0_27.1.0-x86_64.iso	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/14/2014 18:48:55 UTC"
MPE Site2 Cluster 1						
slak-g6-mpe-1a	Force Standby	mpe-11.5.0.0.0_27.1.0-x86_64.iso	Unknown	10.5.3_6.1.0	On	Completed: upgrade was completed at "09/30/2014 17:48:25 UTC"
slak-g6-mpe-1b	Active	mpe-11.5.0.0.0_27.1.0-x86_64.iso	Unknown	10.5.3_6.1.0	Off	Completed: upgrade was completed at "09/30/2014 17:47:24 UTC"
MRA Site2 Cluster1						
slak-g6-mra-1a	Standby		Unknown	10.5.3_6.1.0	On	Completed: upgrade was completed at "09/30/2014 17:48:21 UTC"
slak-g6-mra-1b	Active		Unknown	10.5.3_6.1.0	On	Completed: upgrade was completed at "09/30/2014 17:47:25 UTC"

Click OK if following ***Warning*** message pops-up:



7. ☐

CMP GUI: Monitor upgrade process on MPE server

NOTE: This step takes about 45 minutes and the selected server(s) are rebooted during this time

Upgrade Manager → System Maintenance

- Follow the progress status under the "***Upgrade Status***" column and the "***Name***" column

- The Upgrade status runs through several status messages displaying "***spinner***" and also the '***Sync Broken'*** indicators which are normal reporting events. "Sync Broken" indicator indicates that the data replication between the two servers of the cluster is not synced yet. Wait for the replication to completely sync – waiting time depends on the Replication size at the time.

- During the Upgrade activities, the following Alarms may be generated and are normal reporting events – these are cleared after the MPE cluster is completely upgraded
  Expected Critical Alarm:
  31283 High availability server is offline

  Expected Major Alarm:
  70004 The QP processes have been brought down for maintenance

  Expected Minor Database Replication Alarms:
  31101, 31102, 31106, 31107, 31114, 31113

- < ***Optional*** > Login to iLO remote Console of the server(s) and execute the following command to monitor the upgrade operation:

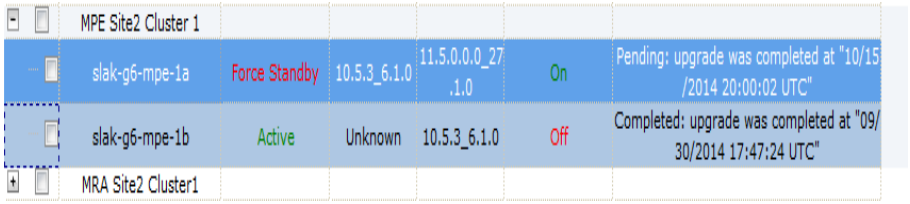
tail –f /var/TKLC/log/upgrade/upgrade.log

```
==> /var/TKLC/log/upgrade/upgrade.log <==
1402100971::  Waiting for reboot
1402100972::  Updating platform revision file...
1402100973::  Upgrade returned success!
1402100973::
1402100973::
1402100973::  A reboot of the server is required.
1402100973::  The server will be rebooted in 10 seconds
1402100973::  Using forced reboot...
1402101444::  Chroot execing /var/TKLC/backout/upgrade_dispatcher --continueUpgrade
1402101446::  Now dispatching /var/TKLC/backout/ugwrap  --session
```

<table>
<tr>
<td>8. ☐</td>
<td>CMP GUI: Verify successful upgrade on MPE server(s)</td>
<td>

Upgrade Manager →System Maintenance

- Expect the server state is still under "Force Standby" status - same as prior to the upgrade.
- "*Sync Broken*" and "*Spinner*" indicators should disappear after the data replication syncs between the two servers of the cluster
- The expected alarms should clear after the replication is successfully done
- Successful upgrade status shows the upgraded MPE server running the Release 11.5 under the "Running Release" column:



MPE Site2 Cluster 1					
slak-g6-mpe-1a	Force Standby	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/15/2014 20:00:02 UTC"
slak-g6-mpe-1b	Active	Unknown	10.5.3_6.1.0	Off	Completed: upgrade was completed at "09/30/2014 17:47:24 UTC"
MRA Site2 Cluster1					

Note: If the status message *"Pending: Upgrade was complete…"* does not appear, stop here and please contact Oracle Technical Services to troubleshoot.

</td>
</tr>
<tr>
<td>9. ☐</td>
<td>iLO Remote Console: Verify Upgrade is successful on "Force Standby" MPE server</td>
<td>

- **Confirm the upgraded version with the following commands showing the latest Platform version and Policy version and server role -**

getPlatRev && getPolicyRev && ha.mystate -i

```
[root@slak-g6-mpe-1a ~]# getPlatRev && getPolicyRev && ha.mystate -i
6.7.0.0.1-84.20.0
11.5.0.0.0_27.1.0
         resourceId   role                    node      subResources      lastUpdate
      DbReplication   Stby          slak-g6-mpe-1a                 0 1015:160013.213
                VIP   Stby          slak-g6-mpe-1a                 0 1015:160013.215
                 QP   Stby          slak-g6-mpe-1a                 0 1015:160019.219
  DbReplication_old    OOS          slak-g6-mpe-1a                 0 1015:160007.212
```

At this stage, the server set to Force standby will be shown as "Stby", when HA status is queried using CLI.

- **Confirm the Database Replication operational status -**

irepstat

```
-- Policy 0 ActStb [DbReplication] ----------------------------------------
AC From slak-g6-cmp-1b Active      0   0.25 ^0.04%cpu 41B/s  A=C2890.000
CC From slak-g6-mpe-1b Active      0   0.25 ^0.05 1.14%cpu 90B/s  A=C2890.000
```

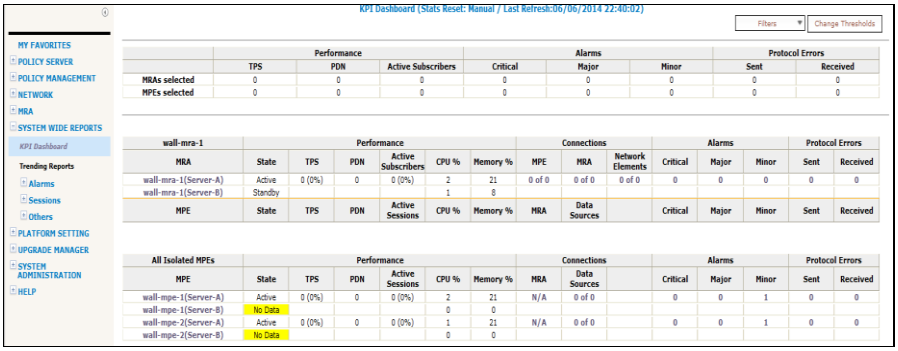
NOTE: This server's DbReplication status role is now "Active" with the currently Active servers (Active CMP & Active MPE) , that this Standby MPE is mated to. Similarly check for all Force Standby MPE servers, if any!

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

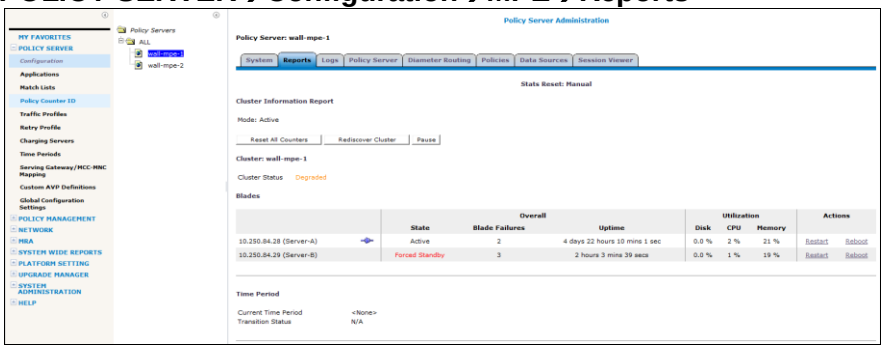
10. ☐

CMP GUI: Capture the Baseline prior to switchover

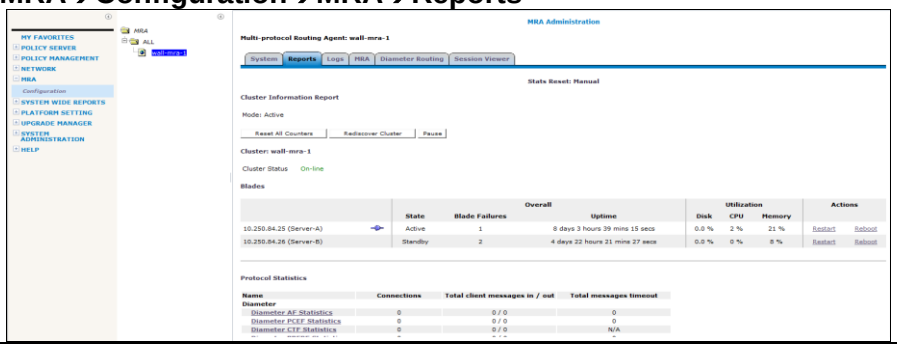
System Wide Reports → KPI Dashboard



POLICY SERVER→Configuration→MPE→Reports



MRA→Configuration→MRA→Reports



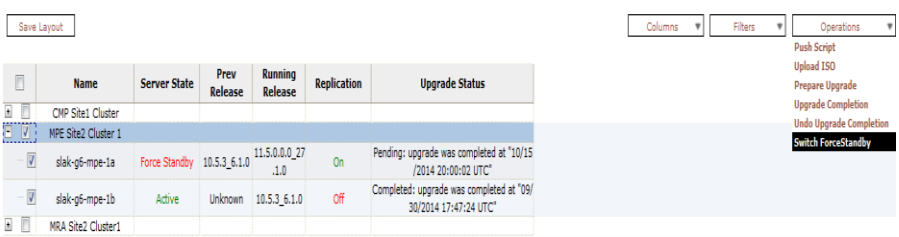
11. ☐

CMP GUI: Switchover "Force Standby" upgraded MPE server with the Active MPE server in the cluster

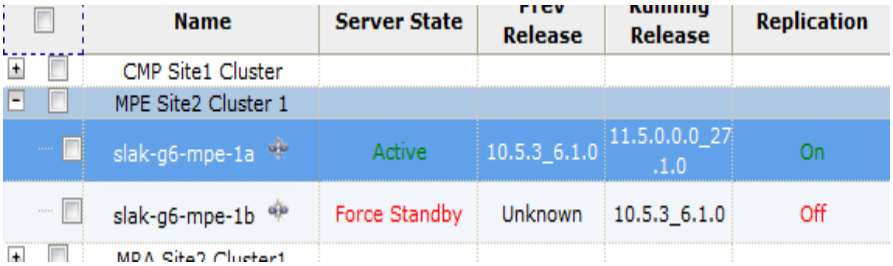
CAUTION: This step can impact user traffic – the duration can be up to 5 seconds.

Upgrade Manager → System Maintenance

- **Select** checkbox for the MPE cluster to be switched
- Under **Operations menu**, select "**Switch ForceStandby**" operation:



- Select "**OK**" to continue the operation

	Note: following operation should be applied to one cluster at a time.	• Wait for at least 5 seconds for the successful switchover between the "Active" and "Force Standby" servers as shown under the "**Server State**" column • During the switch-over, the following Alarm may be generated and is normal reporting event – this is cleared after about 5 minutes. Expected Major Alarm: **31224 High availability configuration error** • The Active server is now running new Release 11.5 with Replication ON. • The Replication status remains the same as prior to the switchover • The 'Sync Broken' indicators on the server appear as expected. • Repeat this whole step for the other MPE node of the cluster being upgraded.
12. ☐	**CMP GUI:** Verify the Server State switched for MPE cluster(s)	**Upgrade Manager → System Maintenance**  Name | Server State | Prev Release | Running Release | Replication CMP Site1 Cluster MPE Site2 Cluster 1 slak-g6-mpe-1a | Active | 10.5.3_6.1.0 | 11.5.0.0.0_27.1.0 | On slak-g6-mpe-1b | Force Standby | Unknown | 10.5.3_6.1.0 | Off MPA Site2 Cluster1

13. ☐	**CMP GUI:** Re-apply Configuration on MPE cluster	**PolicyServer → Configuration →** *<MPE cluster name>* **→ System Tab** • The selected MPE Cluster has the status ***"Degraded..."*** as expected • Older Policy version being shown. • Click "***Reapply Configuration***" **Policy Server: MPE Site1 Cluster1** System | Reports | Logs | Policy Server | Diameter Rou Modify | Delete | Reapply Configuration **Configuration** Name: MPE Site1 Cluster1 Status: Degraded Version: 11.5.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Oct 29, 2014 07:47 PM EDT • Note the "Version" is now successfully changed to the upgraded Release 11.5 and the message in green reports success. Modify | Delete | Reapply Configuration **The configuration was applied successfully.** **Configuration** Name: MPE Site1 Cluster1 Status: Degraded Version: 11.5.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Oct 29, 2014 07:48 PM EDT **NOTE:** The cluster status still shown as "Degraded" is a normal reporting event as the server states are "Active" and "Force Standby".

14. ☐

CMP GUI: Additional verification of traffic on MPE cluster(s)

PolicyServer → Configuration → *<MPE cluster name >* **→ Reports Tab**

- Verify that the upgraded MPE server is "Active" and the other server of this cluster is "Forced Standby"
- If network traffic is on then verify that the servers are processing traffic.

Reset All Counters | Rediscover Cluster | Pause

Cluster: MPE Site2 Cluster 1

Cluster Status Degraded
Site Preference Normal

Blades

	Overall			Utilization		
	State	Blade Failures	Uptime	Disk	CPU	Memory
10.240.239.24 (Server-A)	Active	3	1 hour 46 mins 59 secs	0.0 %	1 %	20 %
10.240.239.25 (Server-B)	Forced Standby	3	14 mins 13 secs	0.0 %	0 %	22 %

15. ☐

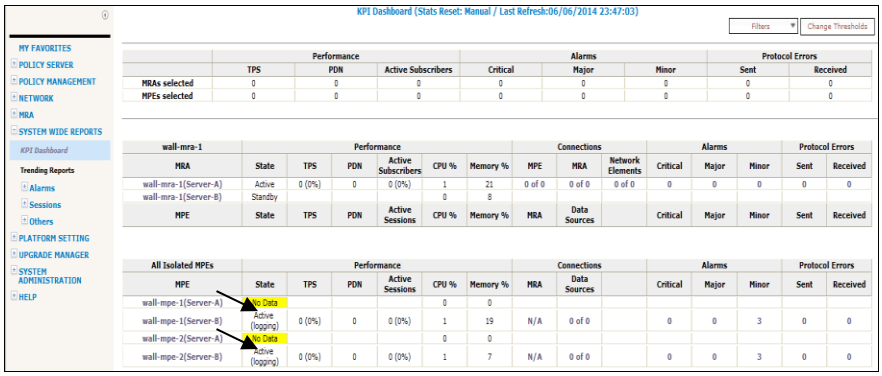
CMP GUI: Verify the connections become active on the upgraded Active MPE server(s) and traffic comes up if network traffic is on

During the Switchover activity in Step11, the MRA sees the associated MPEs as down and re-directs traffic to other MPEs. As the 11.5 MPE becomes Active, the MPE listens and accepts new connections from the MRA and requests new connections to the HSS.

CMP GUI**: System Wide Reports → KPI Report**

From the KPI Reports, there are several indicators seen over the next 30-60 seconds:

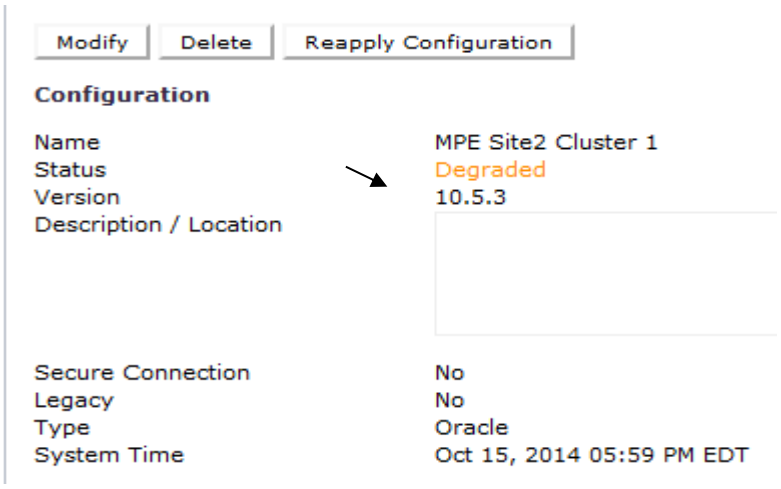
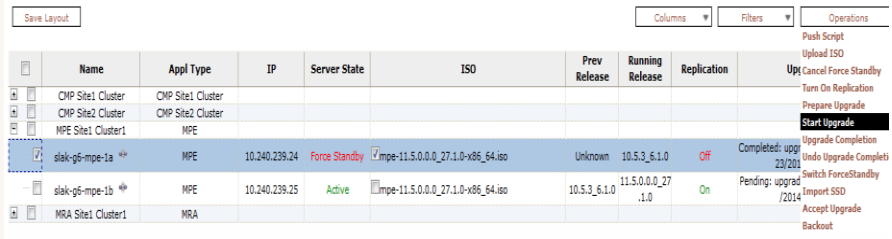
- The upgraded MPE server shows as Active
- the MRA and Date Source/HSS connections on this server go down and re-establish
- Traffic goes to zero for a few seconds and then starts to increase again to the expected level



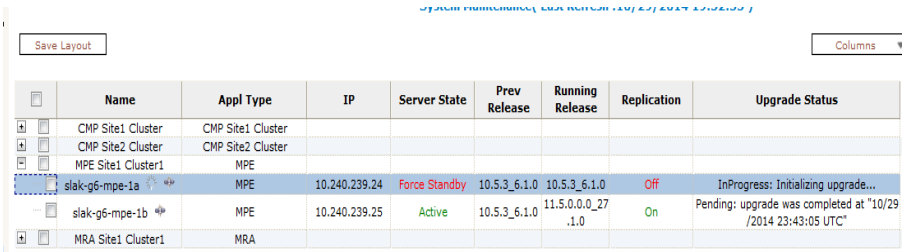
- Allow any Major Alarm to clear under **System Wide Reports →Alarms**

NOTE:

- IF the MPE server is performing as expected, proceed to Step 17 to upgrade the second MPE server of this same cluster
  IF NOT, proceed to Step 16 and also see the procedure "Backout of Partial Upgraded Cluster"

16. ☐	**CMP GUI: IF** Traffic does not become active within 60 seconds	**Upgrade Manager → System Maintenance** • **Select** the checkbox for the partially upgraded cluster, and execute "**Switch ForceStandby**" operation. • Release 10.5.x (OR 9.1.X, as the case may be) MPE server should become Active and resume handling traffic.
	CMP GUI: Re-apply Configuration back to Release 10.5.x (OR 9.1.X, as the case may be)	**MPE → Configuration →** *<cluster name>* **→ System Tab** • Select "Reapply Configuration" operation • Verify that the "Version" is changed from 11.5 to 10.5.x (OR 9.1.X, as the case may be) and the action reports ***success.***  • If NOT, contact Oracle support to consider backout of "Partially Upgraded Cluster" procedure.
17. ☐	**CMP GUI:** Upgrade "Force Standby" MPE server(s)	**Upgrade Manager →System Maintenance** • ***Select*** the checkbox for the "Force Standby" MPE server(s) and the ISO file is selected as well (ISO selection, however, may take place automatically once ***Start Upgrade*** operation is triggered) • Under ***Operations menu***, select "***Start Upgrade***" operation.  • Click **OK** if any Warning pops-up.
18. ☐	**CMP GUI:** Monitor upgrade process on MPE server(s)	**Upgrade Manager → System Maintenance** • Follow the progress status under the "***Upgrade Status*"** column and the "***Name*"** column • The Upgrade status proceeds through several status messages displaying "***spinner***" and also the "***Sync Broken'*** indicators which are

<table>
<tr>
<td></td>
<td>NOTE: This step takes about 45 minutes and the selected server(s) are rebooted during this time</td>
<td>
normal reporting events. “Sync Broken” indicator indicates that the data replication between the two servers of the cluster is not synced yet. Wait for the replication to completely sync – waiting time depends on the Replication size at the time.



Name	Appl Type	IP	Server State	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster	CMP Site1 Cluster						
CMP Site2 Cluster	CMP Site2 Cluster						
MPE Site1 Cluster1	MPE						
slak-g6-mpe-1a	MPE	10.240.239.24	Force Standby	10.5.3_6.1.0	10.5.3_6.1.0	Off	InProgress: Initializing upgrade...
slak-g6-mpe-1b	MPE	10.240.239.25	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/29/2014 23:43:05 UTC"
MRA Site1 Cluster1	MRA						

- During the Upgrade activities, the following Alarms may be generated and are normal reporting events – these are cleared after the MPE cluster is completely upgraded

  Expected Critical Alarm:
  31283 High availability server is offline

  Expected Major Alarm:
  70004 The QP processes have been brought down for maintenance

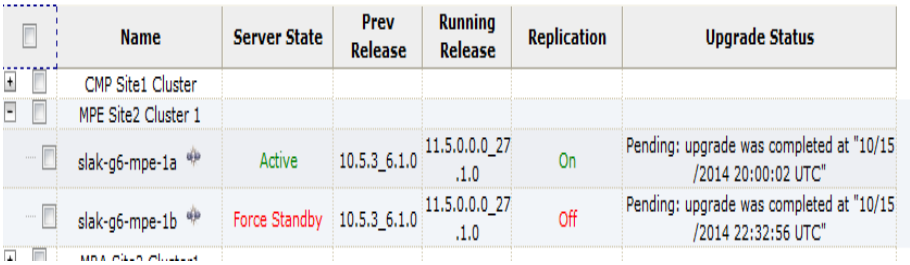
  Expected Minor Database Replication Alarms:
  31101, 31102, 31106, 31107, 31114, 31113

- < ***Optional*** > Login iLO remote Console to the server(s) and execute the following command to monitor the upgrade operation:

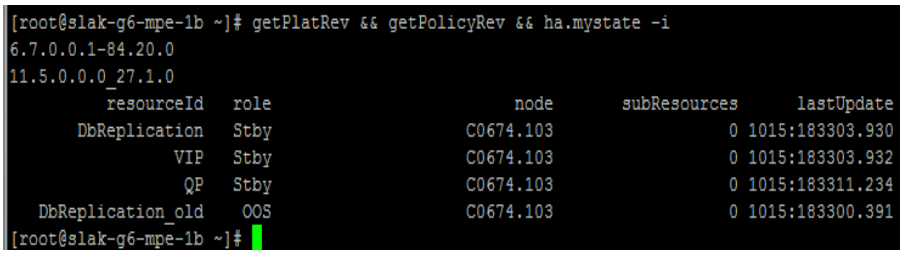
tail –f /var/TKLC/log/upgrade/upgrade.log

```
1418565813::  Updating platform revision file...
1418565813::  Marking task 1418565202.0 as Success
1418565813::  Upgrade returned success!
```
</td>
</tr>
<tr>
<td>19. ☐</td>
<td>CMP GUI: Verify successful upgrade on MPE server(s)</td>
<td>
Upgrade Manager →System Maintenance

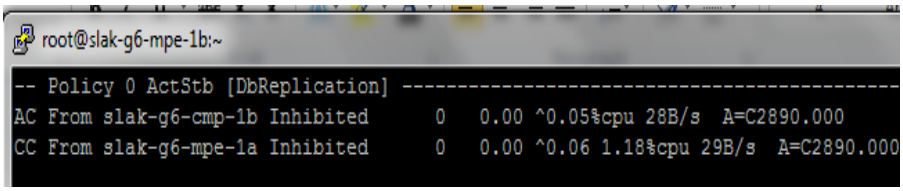
- Expect the server state(s) are still “*Force Standby*” - same as prior to the upgrade
- “*Sync Broken*” and “*Spinner*” indicators should disappear after the data replication syncs between the two servers of the cluster
- The expected alarms should clear after the Replication is successfully done
- Successful upgrade status shows the upgraded MPE server(s) running the Release 11.5 under the “Running Release” column –
</td>
</tr>
</table>

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


Name	Server State	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster					
MPE Site2 Cluster 1					
slak-g6-mpe-1a	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/15/2014 20:00:02 UTC"
slak-g6-mpe-1b	Force Standby	10.5.3_6.1.0	11.5.0.0.0_27.1.0	Off	Pending: upgrade was completed at "10/15/2014 22:32:56 UTC"

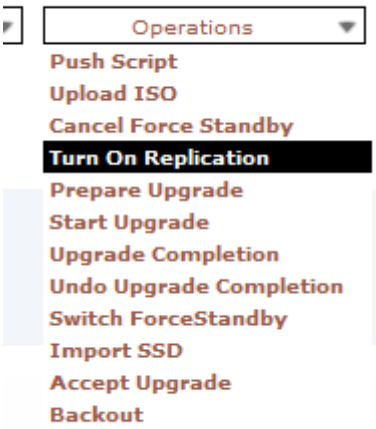
Note: If the status message “Pending: Upgrade complete…” does not appear, stop here and please contact Oracle Technical Services to troubleshoot.
</td>
</tr>
<tr>
<td>20. ☐</td>
<td>SSH CLI / iLO Remote Console:
Verify the upgrade is successful on “Force Standby” MPE server(s)</td>
<td>
• Confirm the upgraded version with the following commands showing the latest Platform version and Policy version and server role:
getPlatRev && getPolicyRev && ha.mystate –i


```
[root@slak-g6-mpe-1b ~]# getPlatRev && getPolicyRev && ha.mystate -i
6.7.0.0.1-84.20.0
11.5.0.0.0_27.1.0
          resourceId   role                      node       subResources      lastUpdate
       DbReplication   Stby                 C0674.103                  0 1015:183303.930
                 VIP   Stby                 C0674.103                  0 1015:183303.932
                  QP   Stby                 C0674.103                  0 1015:183311.234
   DbReplication_old    OOS                 C0674.103                  0 1015:183300.391
[root@slak-g6-mpe-1b ~]#
```

• Confirm the Database Replication operational status:
irepstat


```
root@slak-g6-mpe-1b:~
-- Policy 0 ActStb [DbReplication] ----------------------------------------
AC From slak-g6-cmp-1b Inhibited      0   0.00 ^0.05%cpu 28B/s  A=C2890.000
CC From slak-g6-mpe-1a Inhibited      0   0.00 ^0.06 1.18%cpu 29B/s  A=C2890.000
```

NOTE: As Replication is Off, server’s DbReplication status role is now “Inhibited” with the currently Active servers (Active CMP & Active MPE) that this Standby MPE is mated to.
Status becomes “Active” when Replication is turned ON in the next step.
Similarly check for all other Force Standby MPE servers, if any.
</td>
</tr>
<tr>
<td>21. ☐</td>
<td>CMP GUI:
Turn-ON Replication for all “Force Standby” MPE servers</td>
<td>
Upgrade Manager → System Maintenance
• Select checkbox for “Force Standby” MPE servers
• Under Operations menu, select “Turn ON Replication” operation
</td>
</tr>
</table>



- Select "***OK***" to continue the operation
- Ensure that Replication status under the column is ON and 'Sync Broken' indicators are cleared after some wait time

	Name	Server State	Prev Release	Running Release	Replication	Upgrade Status
+	CMP Site1 Cluster					
-	MPE Site2 Cluster 1					
	slak-g6-mpe-1a	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "1 /2014 20:00:02 UTC"
	slak-g6-mpe-1b	Force Standby	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "1 /2014 22:32:56 UTC"
+	MRA Site2 Cluster1					

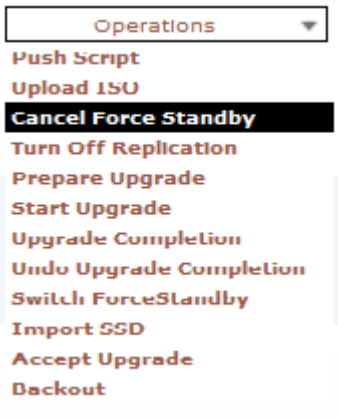
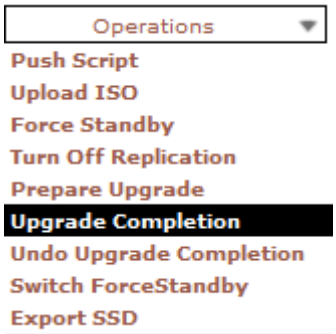
NOTE: "Sync Broken" indications on the cluster get cleared as soon as the replication is completed. The time taken to clear depends on the Db Replication size.

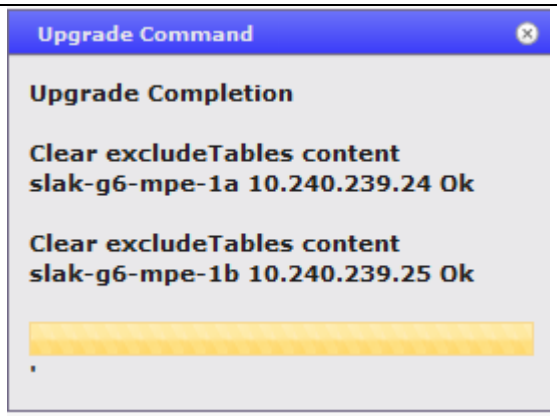
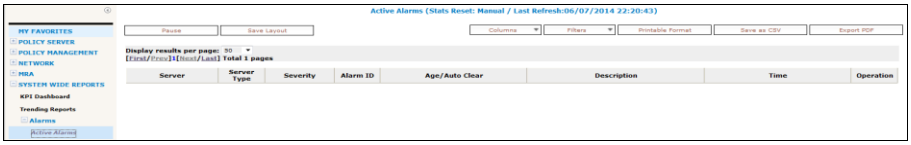
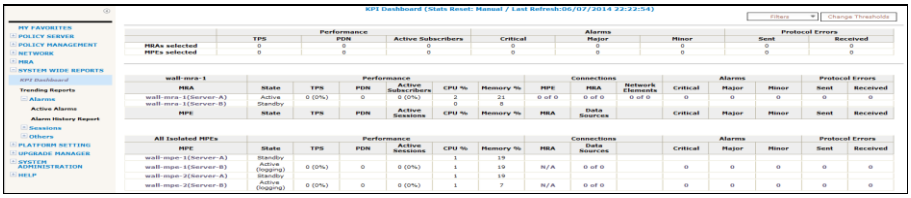
irepstat

```
root@slak-g6-mpe-1b:~
-- Policy 0 ActStb [DbReplication] ----------------------------------------
AC From slak-g6-cmp-1b Active      0   0.00 ^0.04%cpu 60B/s  A=C2890.000
CC From slak-g6-mpe-1a Active      0   0.26 ^0.06 1.23%cpu 65B/s  A=C2890.000
```

NOTE: Now that Replication is ON, this server's DbReplication status role is now "Active" with the currently Active servers (Active CMP & Active MPE) that this Standby MPE is mated to.
Similarly check for all Force Standby MPE servers.

22. ☐	**CMP GUI:** Cancel	**Upgrade Manager → System Maintenance**

	all "Force Standby" servers back to "Standby" state	• *Select* checkbox for the current "***Force Standby***" MPE Servers • Under *Operations menu*, select "***Cancel ForceStandby***" operation  • Select "***OK***" to continue the operation • "*Force Standby*" MPE server(s) are in "*Standby*" state with the Replication ON: Name / Server State / Prev Release / Running Release / Replication / Upgrade Status CMP Site1 Cluster MPE Site2 Cluster 1 slak-g6-mpe-1a — Active — 10.5.3_6.1.0 — 11.5.0.0.0_27.1.0 — On — Pending: upgrade was completed at "10/15/2014 20:00:02 UTC" slak-g6-mpe-1b — Standby — 10.5.3_6.1.0 — 11.5.0.0.0_27.1.0 — On — Pending: upgrade was completed at "10/15/2014 22:32:56 UTC" MRA Site2 Cluster1
23. ☐	**CMP GUI:** Execute 'Upgrade Completion' to finalize the upgrade procedure	**Upgrade Manager → System Maintenance** • *Select* checkbox for the upgraded MPE cluster(s) • Under *Operations menu*, select "*Upgrade Completion*" operation:  • Select '***OK'*** to continue • There is no difference in the above system display – only the checkmarks disappear. • This completes the MPE upgrade and the following message appears for Exclusion Tables clearance, these tables were appended in Procedure-7 and are cleared after Upgrade Completion:

		
24. ☐	**CMP GUI:** Verify Alarms and Reports for upgraded MPE servers	**SystemWideReports → Active Alarms** • Check for any unexpected alarms **NOTE**: Some Alarms have 30 minutes auto clearing time  **SystemWideReports → KPI DashBoard** • Compare current status report to pre-upgrade collected report  **Policy Server → Configuration →** < *MPE Cluster Name* > **→ Reports Tab** • Compare current status report to the pre-upgrade collected report **Policy Server → Configuration →** < *MPE Cluster Name* > **→System Tab** If the cluster is under *Config-mismatch* status, as shown in the snapshot below, re-applying configuration will be necessary:

		Modify Delete Reapply Configuration **Configuration** Name: MPE Site2 Cluster 1 Status: On-line Config Mismatch Version: 11.5.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Oct 15, 2014 08:27 PM EDT Confirm the status as "On-line" once the re-application of configuration is completed. Modify Delete Reapply Configuration **The configuration was applied successfully.** **Configuration** Name: MPE Site2 Cluster 1 Status: On-line Version: 11.5.0 Description / Location: Secure Connection: No Legacy: No Type: Oracle System Time: Oct 15, 2014 08:31 PM EDT
25. ☐	As required, **REPEAT** the above steps for the remaining MPE clusters.	• Proceed with next cluster to be upgraded – MPE cluster _____
26. ☐	**Soak Period**	• Recommend to soak the new Release 11.5 for a pre-determined period of time according to Customer Operation Policy to confirm system post-upgrade stability and traffic/policy operations as expected.
THIS PROCEDURE HAS BEEN COMPLETED		

7.3 Procedure-10: Upgrade MRA clusters@Segment____@Site _____

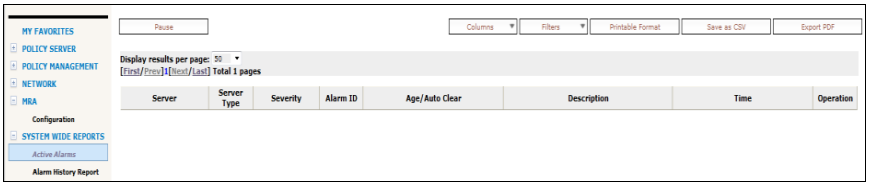
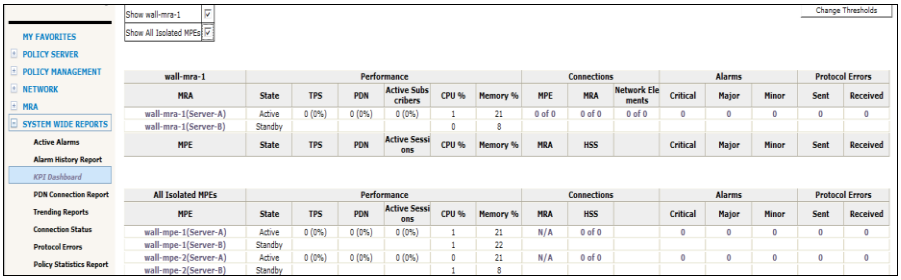
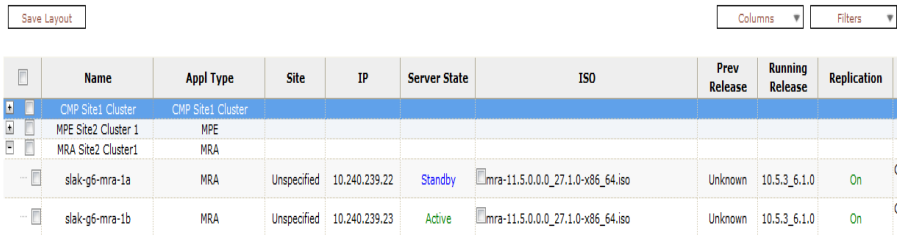
Pre-requisites and important notes:

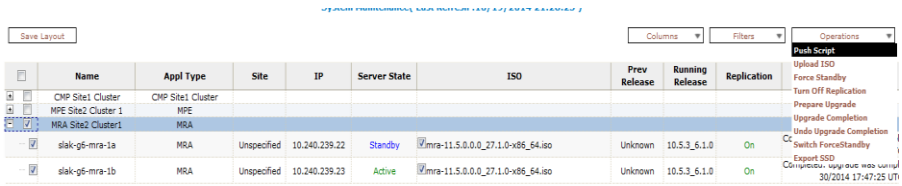
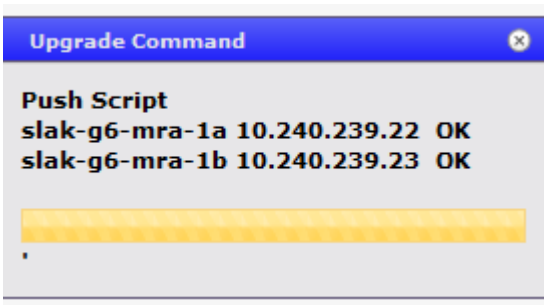
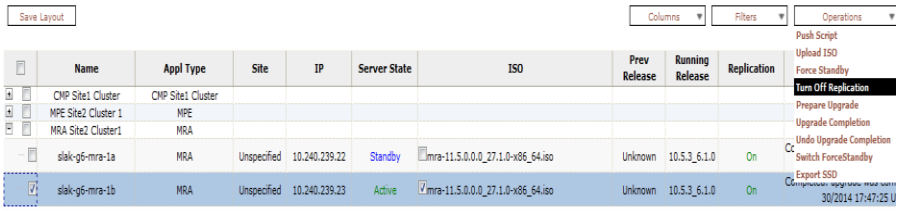
- Review of section 3.1.
- This procedure upgrades one or more MRA clusters under a segment at a site.
- Number of segments and sites depend on customer network topology.
- This should be performed after the MPE upgrade under a segment at that site.
- In a segment at a given site, the recommended maximum number of clusters to be upgraded at a time is 3 during a 2-hour maintenance window.
- Policy Changes or Configuration change should NOT be made while the system is in Mixed-Version operation.

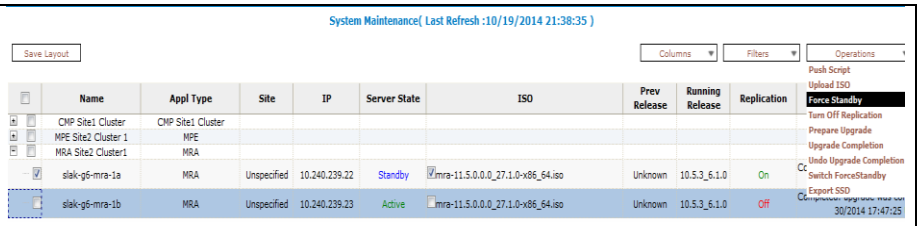
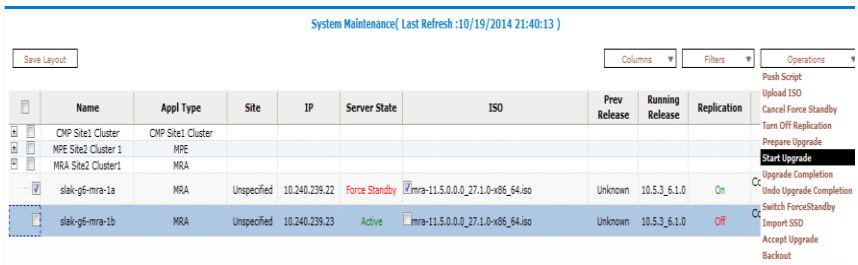
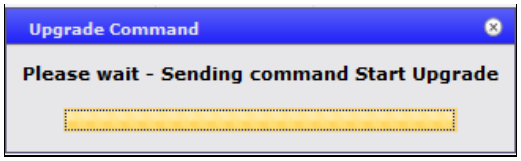
Overview:

1) Use the UM GUI to Turn-Off Replication on the active blade in the MRA cluster
2) Use the UM GUI to place standby MRA into Forced Standby
3) Use the UM GUI to upgrade Frc-Stb MRA server
4) Use the UM GUI to perform Switch Forced Standby on the MRA Cluster
5) ‘Reapply Configfuration’ for the cluster
6) Use the UM GUI to Upgrade remaining MRA Frc-Stb server
7) Use the UM GUI to turn On Replication for the Frc-Stb server
8) Use the UM GUI to Remove the MRA server from Frc-Stb
9) Use the UM GUI to select the upgraded MRA cluster and execute "Upgrade Completion"

Executional Guidance:

Step	Procedure	Result
1. ☐	**CMP GUI:** Health Checks on MRA cluster(s) to be upgraded	• Perform the following health checks : - Check for current active alarms on CMP GUI: **System Wide Reports → Active Alarms**  - Check KPI dashboard (save screenshot to a file) **System Wide Reports → KPI Dashboard**  *(Optional)* Reset MRA counters to make a baseline, see Appendix-C
2. ☐	**CMP GUI:** Verify Upgrade Status of the MRA cluster(s)	**Upgrade Manager →System Maintenance** • (Optional but Preferred) Filter MRAs as described in Appendix • Verify information for the MRAs - Current Release 10.5.x or 9.1.x installed - Active/Standby status - ISO version to be deployed  ***NOTE***: The display form can be sorted by Name or Application Type by selecting the column header. In this case, ONLY MRAs are selected to be displayed i.e. filtered out both CMP and MRA at this time.

3. ☐	**CMP GUI:** Apply Policy Release 11.5 upgrade scripts to all MRA cluster(s) to be upgraded	**Upgrade Manager →System Maintenance** • Select checkbox for all MRA cluster(s) to be upgraded • Under **Operations menu**, select "**Push Script"** operation (It is safe to run Push Script operation repeatedly if needed)  • Select **OK** to continue the operation • Operation successful: 
4. ☐	**CMP GUI:** Turn-OFF Replication on Active server(s)	**Upgrade Manager → System Maintenance** • **Select** checkbox for the **Active MRA** server(s) • Under **Operations menu**, select "**Turn Off Replication**" operation  • Select "**OK**" to continue the operation • Ensure Replication status under the column is **OFF** as shown **Expected Minor Alarm: 31113 Replication Manually Disabled**
5. ☐	**CMP GUI:** Apply "Force Standby" status on Standby MRA server(s)	**Upgrade Manager → System Maintenance** • **Select** checkbox for the **Standby** MRA server(s) • Under **Operations menu**, select "**Force Standby**" operation • Select "**OK**" to continue the operation

		 ***NOTE:*** • This step prevents the server from becoming Active after it is upgraded. • No Alarm is expected!
6. ☐	**CMP GUI:** Start Upgrade on "Force Standby" MRA server(s)	**Upgrade Manager →System Maintenance** • **Select** checkbox for the "**Force Standby**" MRA server(s) • Under **Operations menu**, select "**Start Upgrade**" operation. Click **OK** of if any **WARNING** pops-up.  • Message confirmation for "**Start Upgrade**" operation: 
7. ☐	**CMP GUI:** Monitor the upgrade process on MRA server(s) ***NOTE***: This step takes about 45 minutes and the selected server(s) are rebooted during this time	**Upgrade Manager → System Maintenance** • Follow the progress status under the "**Upgrade Status"** column and the "**Name"** column • The Upgrade status proceeds through several status messages displaying "*spinner*" and also the "*Sync Broken'* indicators which are normal reporting events. "Sync Broken" indicator indicates that the data replication between the two servers of the cluster is not synced yet. Wait for the replication to complete; waiting time depends on the database replication size. • During the upgrade activities, the following alarms may be generated and are normal reporting events – these are cleared after the MRA cluster is completely upgraded Expected Critical Alarm: **31283 High availability server is offline**

Expected Major Alarm:
70004 The QP processes have been brought down for maintenance

Expected Minor Database Replication Alarms:
31101, 31102, 31106, 31107, 31114, 31113

- < ***Optional*** > Login using iLO remote Console to the server(s) and execute the following command to monitor the upgrade operation:

tail –f /var/TKLC/log/upgrade/upgrade.log

```
1402272227::  Waiting for reboot
1402272227::  Updating platform revision file...
1402272228::  Upgrade returned success!
1402272228::
1402272228::
1402272228::  A reboot of the server is required.
1402272228::  The server will be rebooted in 10 seconds
1402272228::  Using forced reboot...
1402273002::  Chroot execing /var/TKLC/backout/upgrade_dispatcher --continueUpgrade
1402273004::  Now dispatching /var/TKLC/backout/ugwrap  --session
```

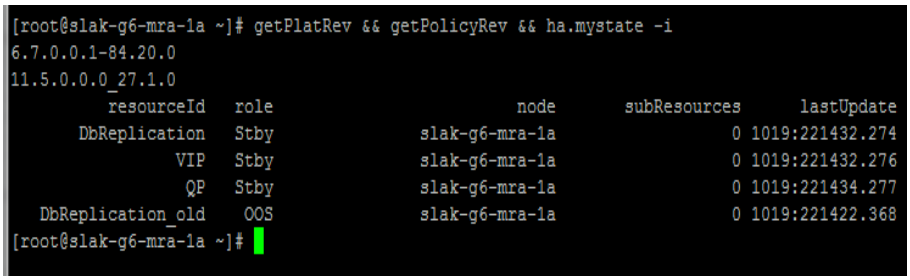
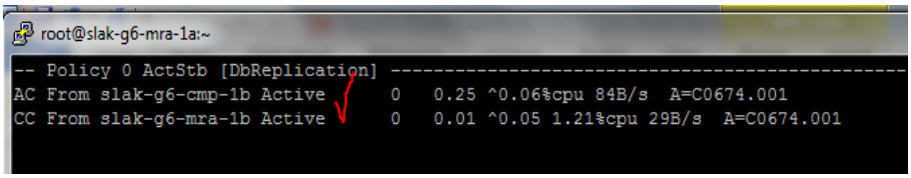
8. ☐ **CMP GUI:** Verify successful upgrade on MRA server(s)

Upgrade Manager →System Maintenance

- Expect the server state is still "**Force Standby**" - same as prior to the upgrade
- "*Sync Broken*" and "*Spinner*" indicators should disappear after the data replication syncs between the two servers of the cluster
- The expected alarms should clear after the replication is successfully done.
- Successful upgrade status shows the upgraded MRA server(s) running the release 11.5 under the "Running Release" column:

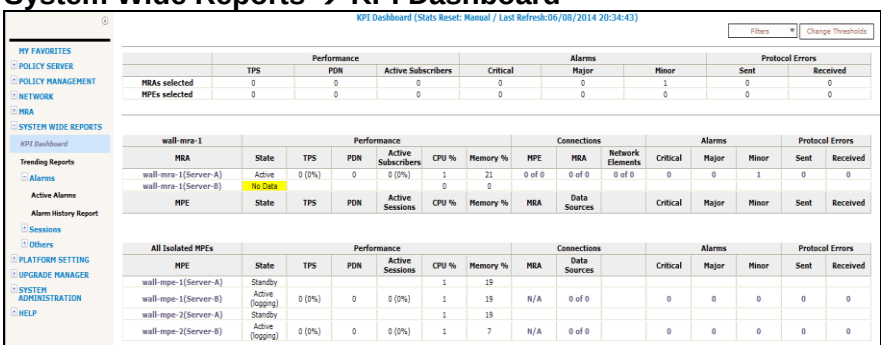
	Name	Server State	Prev Release	Running Release	Replication	Upgrade Status
+	CMP Site1 Cluster					
+	MPE Site2 Cluster 1					
−	MRA Site2 Cluster1					
	slak-g6-mra-1a	Force Standby	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/20/2014 02:14:17 UTC"
	slak-g6-mra-1b	Active	Unknown	10.5.3_6.1.0	Off	Completed: upgrade was completed at "09/30/2014 17:47:25 UTC"

Note: If the status message "Pending: Upgrade complete…" does not appear, stop here and please contact Oracle Technical Services to troubleshoot.

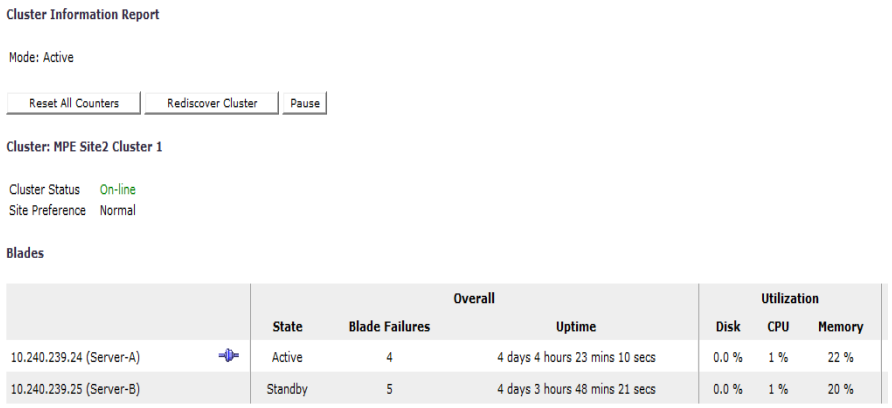
9. ☐	**SSH CLI / iLO Remote Console:** Verify the Upgrade is successful on the "Force Standby" MRA server(s)	• Confirm the upgraded version with the following commands showing the latest Platform version and Policy version and server role: # getPlatRev && getPolicyRev && ha.mystate -i  [root@slak-g6-mra-1a ~]# getPlatRev && getPolicyRev && ha.mystate -i 6.7.0.0.1-84.20.0 11.5.0.0.0_27.1.0 resourceId role node subResources lastUpdate DbReplication Stby slak-g6-mra-1a 0 1019:221432.274 VIP Stby slak-g6-mra-1a 0 1019:221432.276 QP Stby slak-g6-mra-1a 0 1019:221434.277 DbReplication_old OOS slak-g6-mra-1a 0 1019:221422.368 [root@slak-g6-mra-1a ~]# ***NOTE:*** Expect this server role still shown as "Stby" when querying using CLI i.e. "Force Standby". • Confirm that the replication status is *active*: # irepstat  root@slak-g6-mra-1a:~ -- Policy 0 ActStb [DbReplication] ---------- AC From slak-g6-cmp-1b Active 0 0.25 ^0.06%cpu 84B/s A=C0674.001 CC From slak-g6-mra-1b Active 0 0.01 ^0.05 1.21%cpu 29B/s A=C0674.001 ***NOTE:*** This server's DbReplication status role is now "Active" with the currently active servers (Active CMP & Active MRA) that this Standby MRA is mated to. Similarly check for all force standby MRA servers.

<table>
<tr>
<td>10. ☐</td>
<td>CMP GUI: Capture the Baseline prior to switchover</td>
<td>

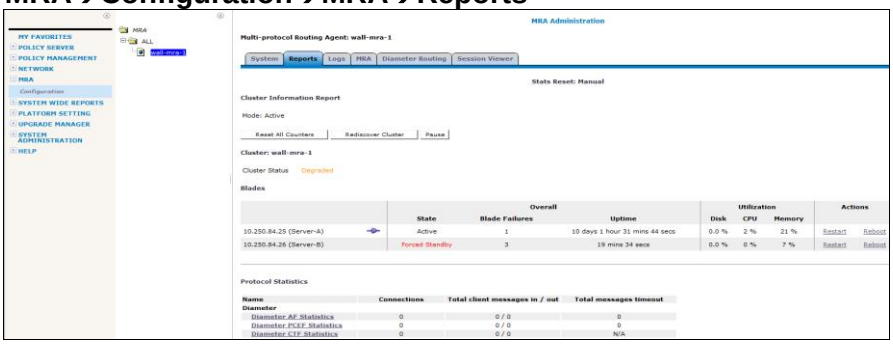
System Wide Reports → KPI Dashboard



POLICY SERVER→Configuration→MPE→Reports



MRA→Configuration→MRA→Reports



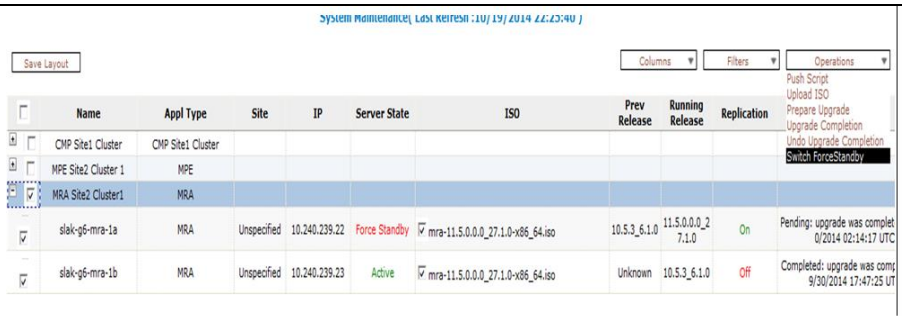
</td>
</tr>
<tr>
<td>11. ☐</td>
<td>CMP GUI: Switchover “Force Standby” upgraded MRA server with the Active MRA server in the cluster</td>
<td>

Upgrade Manager → System Maintenance

Note: This step should be carried out one cluster at a time

- **Select** checkbox for the MRA cluster to be switched
- Under **Operations menu**, select “**Switch ForceStandby**” operation

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

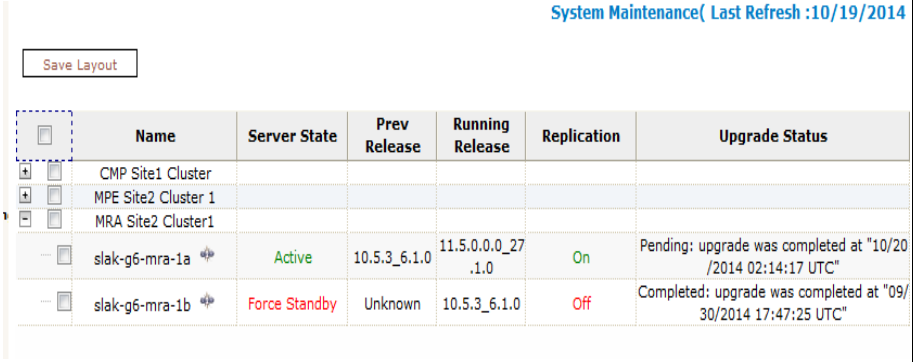
<table>
<tr>
<td></td>
<td>IMPORTANT: Service affecting could possibly last for 5 seconds when carrying out this step.</td>
<td>


- Select “**OK**” to continue the operation
- Wait for at least 5 seconds for the successful switchover between the “*Active*” and “*Force Standby*” servers as shown under the “*Server State*” column
- During the switch-over, following alarms may be generated and is normal reporting event; this is cleared after about 5 minutes.
  Possible temporary *Major* Alarm:
  31224 High availability configuration error
  Expected *Minor* Alarms:
  71402, 71403

NOTE:

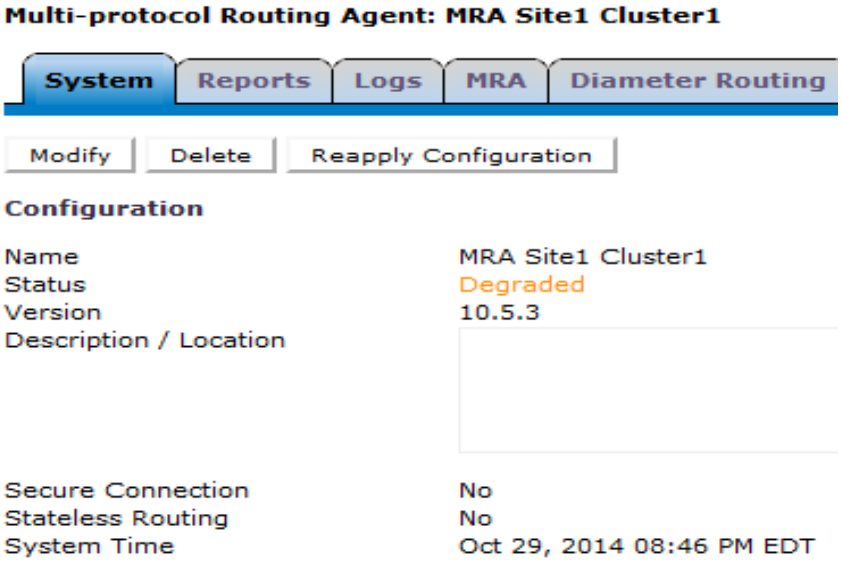
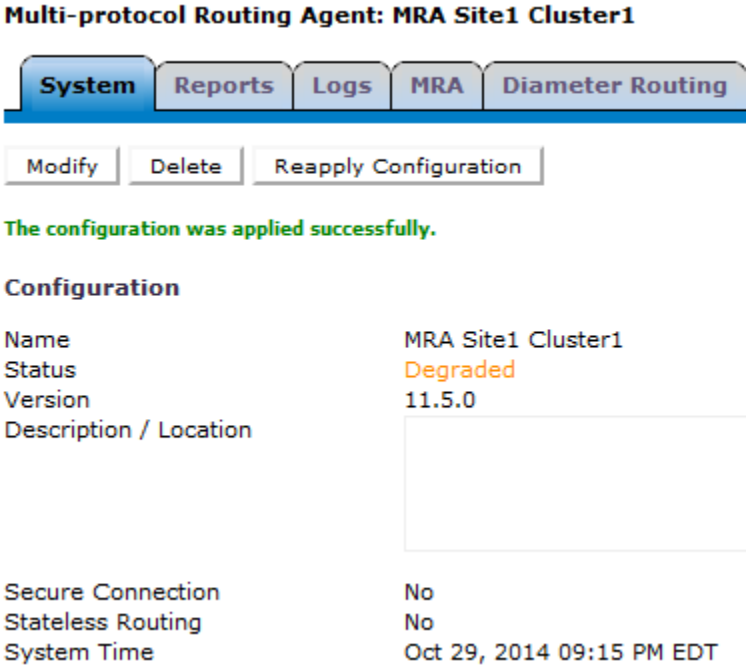
- The Active server is now running new Release 11.5 with Replication ON
- The Replication status remains the same as prior to the switchover
- The ‘Sync Broken’ indicators on the server appear as expected

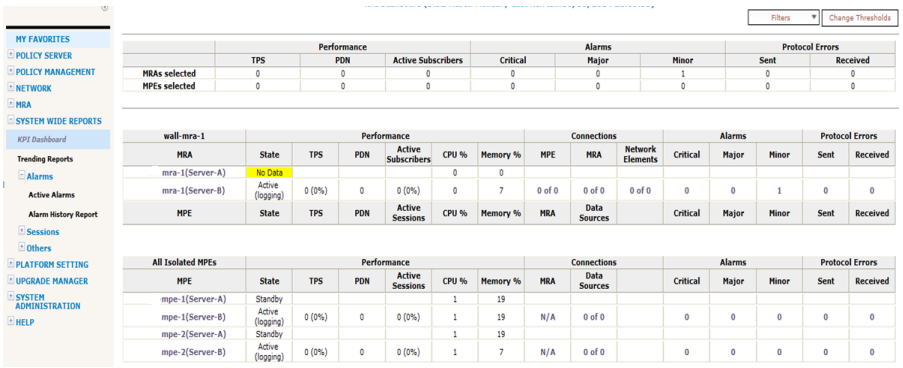
Repeat this whole step for the next MRA cluster, if any, being upgrade.
</td>
</tr>
<tr>
<td>12. ☐</td>
<td>CMP GUI: Verify the Server State switched for MRA cluster(s)</td>
<td>
Upgrade Manager → System Maintenance

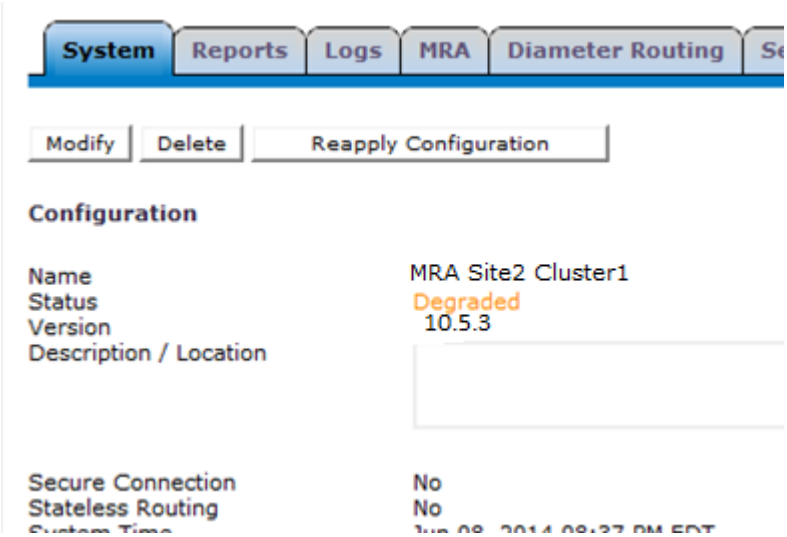
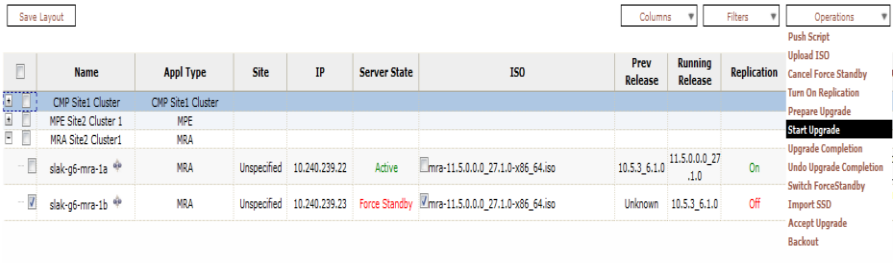


</td>
</tr>
<tr>
<td>13. ☐</td>
<td>CMP GUI: Re-apply Configuration on MRA cluster(s) where switch forced</td>
<td>
MRA → Configuration → <MRA cluster name> → System Tab

- The selected MRA Cluster may have the status “*Degraded Config mismatch*”
</td>
</tr>
</table>

	standby was performed	• The version is still 10.5.x or 9.1.x • Click "Reapply Configuration"  • "*Reapply Configuration*" operation executes. Note the "version" is now successfully changed to the upgraded release 11.5 and the message in green reports success.  ***NOTE***: The cluster status still shown as "Degraded" is a normal reporting event as the server states are "Active" and "Force Standby". This is changed to "On-Line" status in the steps below.

14. ☐	**CMP GUI:** Additional verification of traffic on MRA cluster(s)	**MRA → Configuration →** *<MRA cluster name >* **→ Reports Tab** • Verify that the upgraded MRA server is "Active" and the other server of this cluster is "Forced Standby" • If network traffic is ON then verify that the servers are processing traffic.
15. ☐	**CMP GUI:** Verify the connections become active on the upgraded Active MRA server(s) and traffic comes up if network traffic is on	During the Switchover activity in Step11, the MRA sees the associated MRAs as down and re-directs traffic to other MRAs. As the 11.5 MRA becomes Active, the MRA listens and accepts new connections from the PGW, the MPE and other MRAs. CMP GUI: **System Wide Reports → KPI Report** From the KPI Reports, there are several indicators seen over the next 30-60 seconds: • The upgraded MRA server shows as Active • the MRA and HSS connections on this server go down and re-establish • Traffic goes to zero for a few seconds and then starts to increase again to the expected level  • Allow any Major Alarm to clear under **System Wide Reports →Alarms** **NOTE:** • **If** the MRA server is performing as expected, proceed to the step-17 to upgrade the second MRA server of this same cluster. If **NOT**, proceed to the step-16 and also see the procedure "Backout of Partial Upgraded Cluster".

16. ☐	**CMP GUI: IfTraffic does not become active within 60 seconds**	**Upgrade Manager → System Maintenance** • Select the checkbox for the partially upgraded cluster, and execute "Switch ForceStandby" operation • Release 10.5.x (or 9.1.x as the case may be) MRA server should become Active and resume handling traffic
	CMP GUI: Re-apply Configuration back to Release 10.5.x	**MRA → Configuration →** *<cluster name>* **→ System Tab** • Select "Reapply Configuration" operation • Verify that the "Version" is changed from 11.5 to 10.5.x (or 9.1.x as the case may be) and the action reports success  • If NOT, contact Oracle support to consider backout of "Partially Upgraded Cluster" procedure.
17. ☐	**CMP GUI:** Upgrade "Force Standby" MRA server(s)	**Upgrade Manager →System Maintenance** • **Select** the checkbox for the "**Force Standby**" MRA server(s) • Under **Operations menu**, select "**Start Upgrade**" operation  Click **OK** if any Warning message pops-up.

<table>
<tr>
<td>18. ☐</td>
<td>CMP GUI: Monitor upgrade process on MRA server(s)

NOTE: This step takes about 45 minutes and the selected server(s) are rebooted during this time</td>
<td>
Upgrade Manager → System Maintenance

Follow the progress status under the ”Upgrade Status” column and the “Name” column
The Upgrade status proceeds through several status messages displaying “spinner” and also the “Sync Broken’ indicators which are normal reporting events. “Sync Broken” indicator indicates that the data replication between the two servers of the cluster is not synced yet. Wait for the replication to complete.
During the Upgrade activities, the following alarms may be generated and are normal reporting events; they are cleared after the MRA cluster is completely upgraded.
Expected Critical Alarm:
31283 High availability server is offline

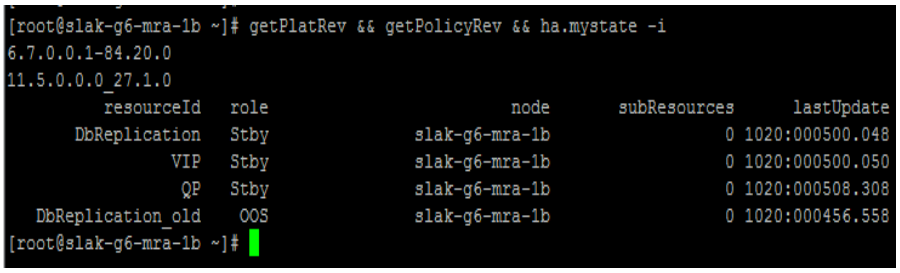
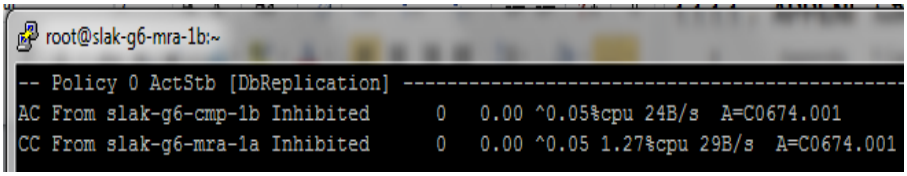
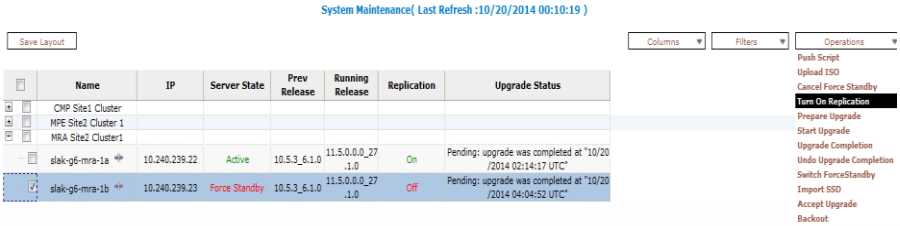
Expected Major Alarm:
70004 The QP processes have been brought down for maintenance

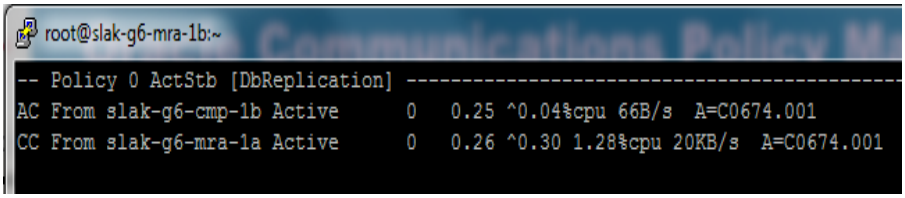
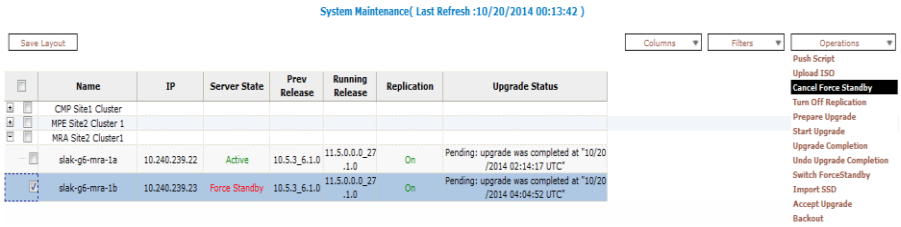
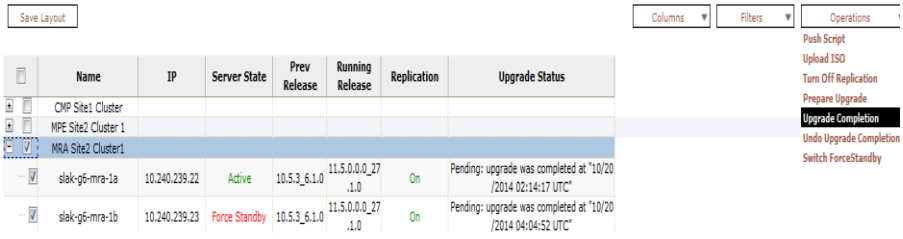
Expected Minor Database Replication Alarms:
31101,31107, 31114
< Optional > Login using iLO remote Console to the server(s) and execute the following command to monitor the upgrade operation:

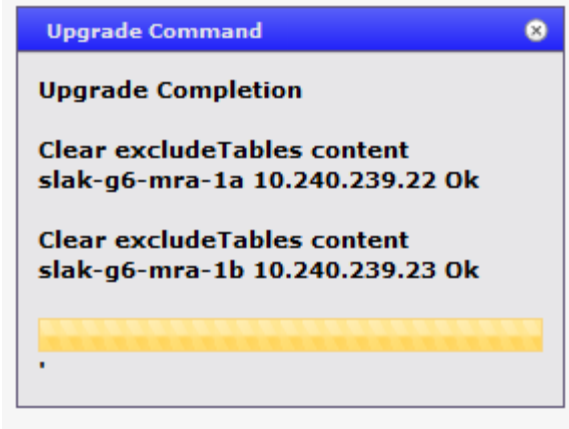
#tail –f /var/TKLC/log/upgrade/upgrade.log
<pre>1418565813:: Updating platform revision file...
1418565813:: Marking task 1418565202.0 as Success
1418565813:: Upgrade returned success!</pre>
</td>
</tr>
<tr>
<td>19. ☐</td>
<td>CMP GUI: Verify successful upgrade on MRA server(s)</td>
<td>
Upgrade Manager →System Maintenance

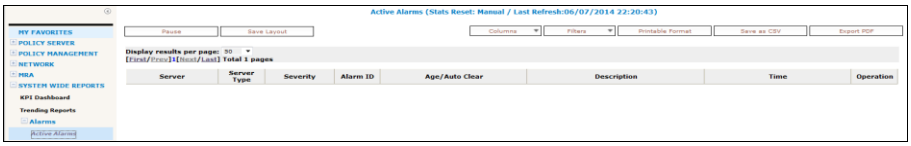
Expect the server state(s) are still “Force Standby” - same as prior to the upgrade.
“Sync Broken” and “Spinner” indicators should disappear after the data replication syncs between the two servers of the cluster.
The expected alarms should clear after the replication is successfully done.
Successful upgrade status shows the upgraded MRA server(s) running the Release 11.5 under the “Running Release” column:

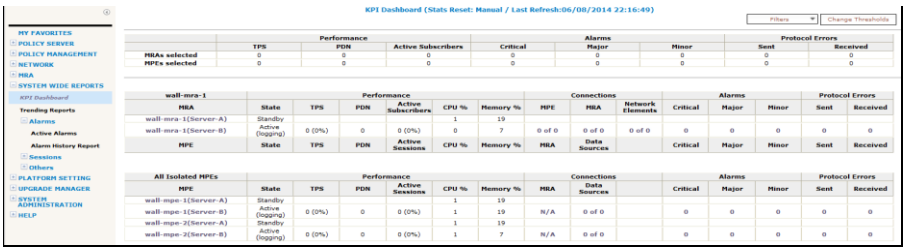
<table>
<tr><th></th><th>Name</th><th>IP</th><th>Server State</th><th>Prev Release</th><th>Running Release</th><th>Replication</th><th>Upgrade Status</th></tr>
<tr><td></td><td>CMP Site1 Cluster</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>MPE Site2 Cluster 1</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>MRA Site2 Cluster1</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>slak-g6-mra-1a</td><td>10.240.239.22</td><td>Active</td><td>10.5.3_6.1.0</td><td>11.5.0.0.0_27.1.0</td><td>On</td><td>Pending: upgrade was completed at "10/20/2014 02:14:17 UTC"</td></tr>
<tr><td></td><td>slak-g6-mra-1b</td><td>10.240.239.23</td><td>Force Standby</td><td>10.5.3_6.1.0</td><td>11.5.0.0.0_27.1.0</td><td>Off</td><td>Pending: upgrade was completed at "10/20/2014 04:04:52 UTC"</td></tr>
</table>
Note: If the status message “Pending: Upgrade complete…” does not appear, stop here and please contact Oracle Technical Services to troubleshoot.
</td>
</tr>
</table>

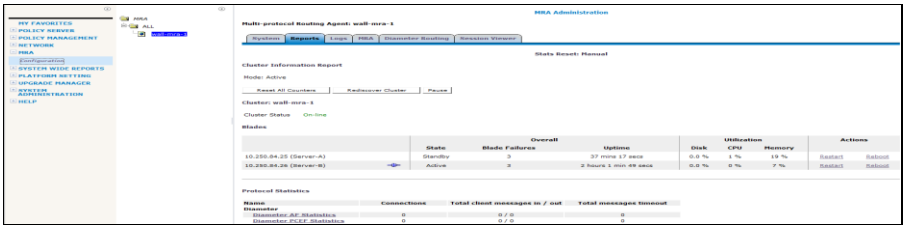
20. ☐	**CLI / iLO Remote Console:** Verify the Upgrade is successful on the "Force Standby" MRA server(s)	• Confirm the upgraded version with the following commands showing the latest platform version and policy version and server role: # getPlatRev && getPolicyRev && ha.mystate -i  [root@slak-g6-mra-1b ~]# getPlatRev && getPolicyRev && ha.mystate -i 6.7.0.0.1-84.20.0 11.5.0.0.0_27.1.0 resourceId role node subResources lastUpdate DbReplication Stby slak-g6-mra-1b 0 1020:000500.048 VIP Stby slak-g6-mra-1b 0 1020:000500.050 QP Stby slak-g6-mra-1b 0 1020:000508.308 DbReplication_old OOS slak-g6-mra-1b 0 1020:000456.558 [root@slak-g6-mra-1b ~]# ***NOTE***: Expect this server role still shown as "Stby" when querying using CLI i.e. "Force Standby" - same as prior to the upgrade • Confirm the Database Replication operational status: # irepstat  root@slak-g6-mra-1b:~ -- Policy 0 ActStb [DbReplication] ---------- AC From slak-g6-cmp-1b Inhibited 0 0.00 ^0.05%cpu 24B/s A=C0674.001 CC From slak-g6-mra-1a Inhibited 0 0.00 ^0.05 1.27%cpu 29B/s A=C0674.001 ***NOTE*:** As Replication is Off, this server's DbReplication status role is now "*Inhibited*" with the currently Active servers (Active CMP & Active MRA) that this Standby MRA is mated to. Status becomes "Active" when Replication is turned ON in the next step. Similarly, check for all Force Standby MRA servers.
21. ☐	**CMP GUI:** Turn-ON Replication for all "Force Standby" MRA servers	**Upgrade Manager → System Maintenance** • **Select** checkbox for "Force Standby" MRA servers • Under **Operations menu**, select "Turn ON Replication" operation  System Maintenance(Last Refresh :10/20/2014 00:10:19) Save Layout Columns Filters Operations Name IP Server State Prev Release Running Release Replication Upgrade Status CMP Site1 Cluster MPE Site2 Cluster 1 MRA Site2 Cluster1 slak-g6-mra-1a 10.240.239.22 Active 10.5.3_6.1.0 11.5.0.0.0_27.1.0 On Pending: upgrade was completed at "10/20/2014 02:14:17 UTC" slak-g6-mra-1b 10.240.239.23 Force Standby 10.5.3_6.1.0 11.5.0.0.0_27.1.0 Off Pending: upgrade was completed at "10/20/2014 04:04:52 UTC" Push Script Upload ISO Cancel Force Standby Turn On Replication Prepare Upgrade Start Upgrade Upgrade Completion Undo Upgrade Completion Switch ForceStandby Import SSD Accept Upgrade Backout • Select "**OK**" to continue the operation • Ensure that Replication status under the column is ON and '*Sync Broken*' indicators are cleared after some time. ***NOTE***: "Sync Broken" indicator on the cluster are cleared as the Replication is now sync-ed. The time taken to clear depends on the Db Replication size.

		# irepstat  ***NOTE*:** Now that Replication is ON, this server's DbReplication status role is now "Active" with the currently Active servers (Active CMP & Active MRA) that this Standby MRA is mated to. Similarly check for all Force Standby MRA servers.
22. ☐	**CMP GUI:** Cancel all "Force Standby" servers back to "Standby" state	**Upgrade Manager → System Maintenance** • **Select** checkbox for the current "Force Standby" MRA Servers • Under **Operations menu**, select "**Cancel ForceStandby**" operation  • Select "**OK**" to continue the operation • Verify "**Force Standby**" MRA server(s) are at '**Standby'** state with Replication ON.
23. ☐	**CMP GUI:** Execute 'Upgrade Completion' to finalize the upgrade procedure	**Upgrade Manager → System Maintenance** • **Select** checkbox for the upgraded MRA cluster(s) • Under **Operations menu**, select "**Upgrade Completion**" operation  • Select '**OK'** to continue • This completes the MRA upgrade and the following message appears to indicate Exclusion Tables' clearance:

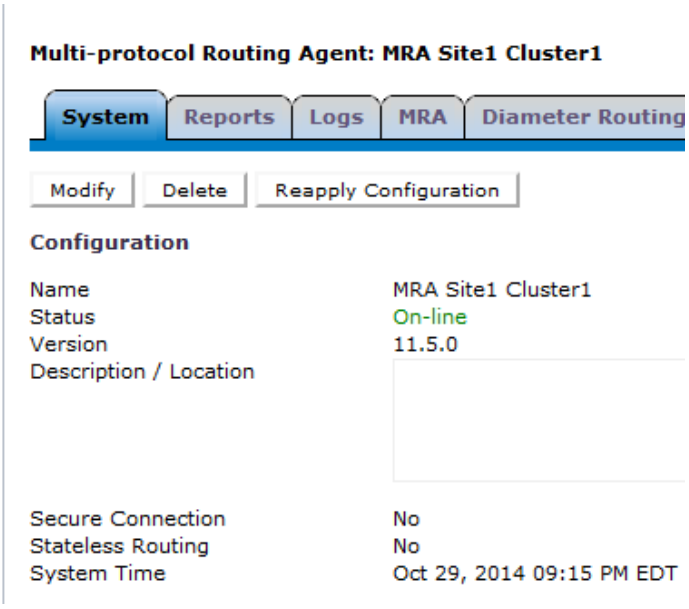
<table>
<tr>
<td></td>
<td></td>
<td>


</td>
</tr>
<tr>
<td>24. ☐</td>
<td>CMP GUI: Verify Alarms and Reports for upgraded MRA servers</td>
<td>
SystemWideReports → Active Alarms
Check for any unexpected alarms
NOTE: Some Alarms have 30 minutes auto clearing time


SystemWideReports → KPI DashBoard
Compare current status report to pre-upgrade collected report


MRA → Configuration → < MRA Cluster Name > → Reports Tab
Compare current status report to the pre-upgrade collected report


MRA → Configuration → < MRA Cluster Name > →System Tab
Confirm current status as ”On-line” as expected
</td>
</tr>
</table>

		
25. ☐	As required, ***REPEAT*** the above Sseps for the next MRA cluster to be upgraded	• Proceed with next cluster to be upgarded – MRA cluster _____
26. ☐	Soak Period	• Recommend to soak the new Release 11.5 for a pre-determined period of time according to Customer Operation Policy to confirm system post-upgrade stability and traffic/policy operations as expected.
27. ☐	Backout ,if Upgrade FAILED	• Backout to Release 10.5.x (or 9.1.x as the case may be) ***NOTE*:** See the procedure of "Backout of Fully Upgraded Cluster" section.
THIS PROCEDURE HAS BEEN COMPLETED		

7.4 Post-upgrade

7.4.1 Procedure-11: Accepting Upgrade for CMP clusters

Description:

Once an upgrade has been completed, the upgrade must be accepted or rejected before any subsequent upgrades may occur. As part of upgrade, the Server Upgrade Pending Accept/Reject (TKSPLATMI33) alarm is set and the MOTD is updated to reflect that the upgrade has not yet been accepted.

'Accept Upgrade' will be the last thing to do in an upgrade, once the customer decides that the upgrade is successful, the upgrade may be accepted by running 'Accept Upgrade' from the UM (CMP GUI).

Notes:

- Rollback will no longer be supported.
- The server Upgrade Pending Accept/Reject alarm will be cleared.
- If the Accept Upgrade step results in the conversion of the file system, a reboot will be triggered automatically.

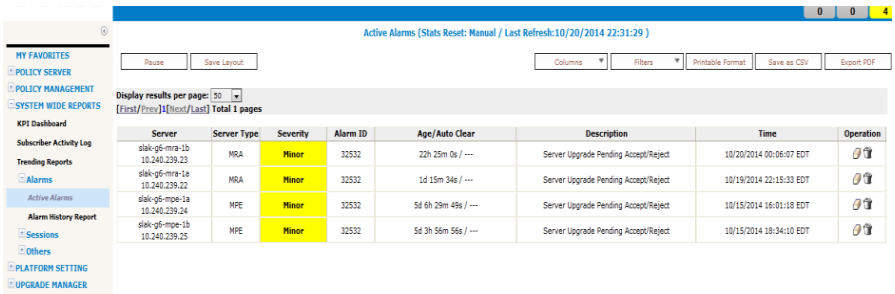
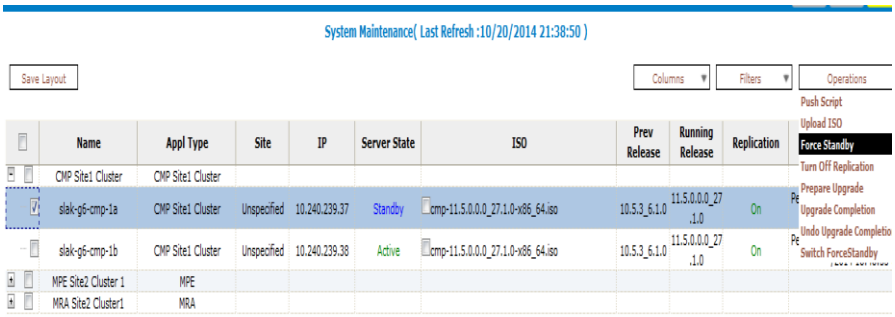
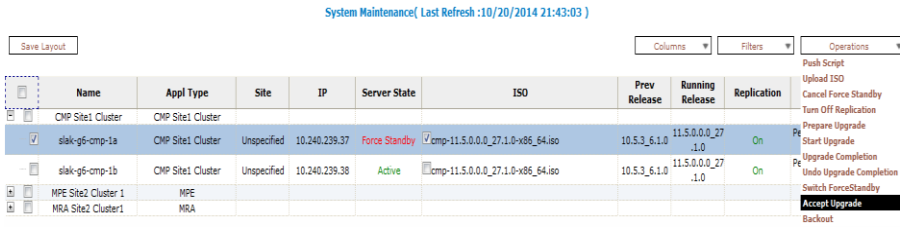
Accept-Upgrade should only be executed when:

- All the servers in the topology have been upgrade to the new version 11.5.
- The server's status is 'Pending'.
- The server is 'Forced Standby'.

CMP Accept-upgrade Overview:

1. Use the UM GUI to place Primary Site standby CMP into Forced Standby
2. Use the UM GUI to 'Accept Upgrade' for the Forced Standby CMP
3. Use the UM GUI to perform Switch Forced Standby on Primary Site CMP Cluster
4. Log back into the UM GUI and 'Accept Upgrade' for the Forced Standby CMP
5. Use the UM GUI to remove the Primary Site CMP server from Frc-Stb
6. Use the UM GUI to place Secondary Site standby CMP into Forced Standby
7. Use the UM GUI to 'Accept Upgrade' for the Forced Standby CMP
8. Use the UM GUI to perform Switch Forced Standby on Secondary Site CMP Cluster
9. Use the UM GUI to 'Accept Upgrade' for the Forced Standby CMP
10. Use the UM GUI to remove the Secondary Site CMP server from Frc-Stb

Executional Guidance:

Step	Procedure	Result
1. ☐	**CMP GUI:** Backup an screenshot of Alarms	**SYSTEM WIDE REPORTS →ALARMS→ACTIVE ALARMS** Export the active alarms either in .csv or .pdf format, by clicking Save as CSV or Export as PDF, respectively. 
2. ☐	**CMP GUI:** Place the primary-site, Standby CMP under Force Standby	**Upgrade Manager →System Maintenance** - **Select** the checkbox of Primary-site, **standby** CMP server - From **Operation menu**, click **Force Standby** - Click **OK** to acknowledge the action. 
3. ☐	**CMP GUI:** Accept Upgrade for Primary-site **Force Standby** CMP server Time Duration: This step may take somewhere from 5-7 minutes.	**Upgrade Manager →System Maintenance** - **Select** the checkbox of Primary-site, **Force standby** CMP server - From **Operation menu**, click **Accept Upgrade** - Click **OK** to acknowledge the action.  Please note that the ***Upgrade Status*** column will change to "*In-Progress: Accepting the upgrade*", followed by "I*n-Progress: Rebooting the server to convert file system to ext4*", and eventually a message depicting '*Accept-upgrade*' completion; an spinner and sync broken icons will also appear by

<table>
<tr><td></td><td></td><td>the CMP server name under Name column, as can be seen in snapshot below:

<table>
<tr><th></th><th>Name</th><th>IP</th><th>Server State</th><th>Prev Release</th><th>Running Release</th><th>Replication</th><th>Upgrade Status</th></tr>
<tr><td></td><td>CMP Site1 Cluster</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>slak-g6-cmp-1a</td><td>10.240.239.37</td><td>Force Standby</td><td>10.5.3_6.1.0</td><td>11.5.0.0.0_27.1.0</td><td>On</td><td>InProgress: Rebooting server to convert file system to ext4</td></tr>
<tr><td></td><td>slak-g6-cmp-1b</td><td>10.240.239.38</td><td>Active</td><td>10.5.3_6.1.0</td><td>11.5.0.0.0_27.1.0</td><td>On</td><td>Pending: upgrade was completed at "10/14/2014 18:48:55 UTC"</td></tr>
<tr><td></td><td>MPE Site2 Cluster 1</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>MRA Site2 Cluster1</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

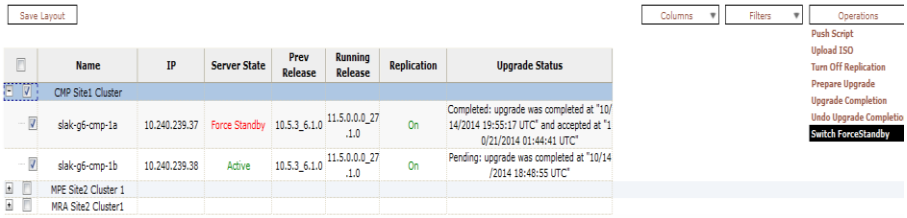
Expected Critical Alarms:

31283 High availability server is offline

Expected Major Alarms:

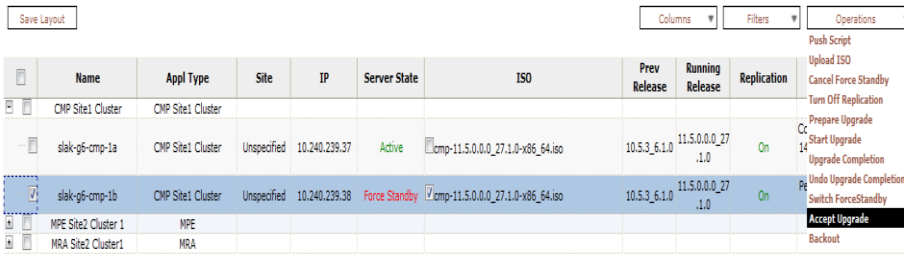
70021 The MySQL slave is not connected to the master</td></tr>
<tr><td>4. ☐</td><td>CMP GUI: Switch Force Standby status between Primary-site CMP servers</td><td>Upgrade Manager →System Maintenance

- Select the checkbox of Primary-site, CMP Cluster
- From Operation menu, click Switch Force Standby
- Click OK to acknowledge the action.

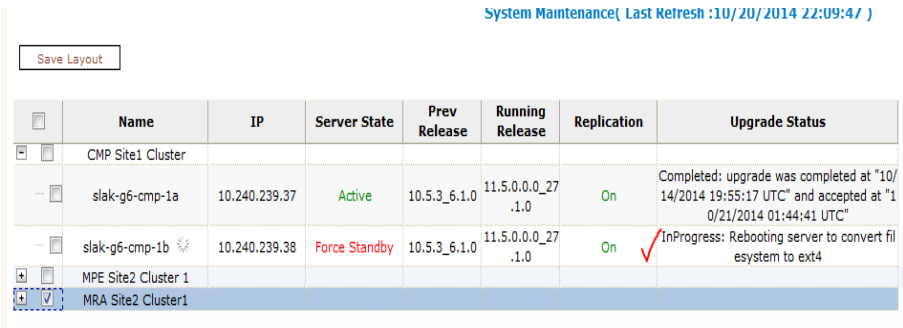
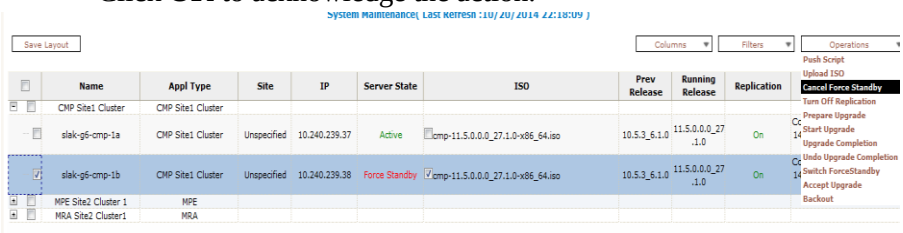
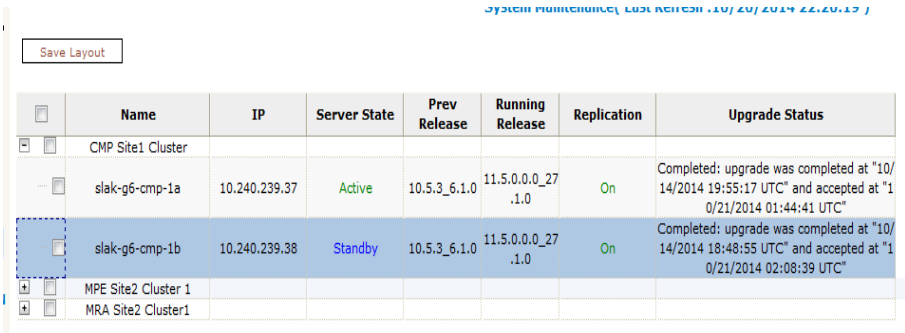

</td></tr>
<tr><td>5. ☐</td><td>CMP GUI: Accept Upgrade for Primary-site Force Standby CMP server

Time Duration: This step may take somewhere from 5-7 minutes.</td><td>Upgrade Manager → System Maintenance

- Select the checkbox of Primary-site, Force standby CMP server
- From Operation menu, click Accept Upgrade
- Click OK to acknowledge the action.



Please note that the Upgrade Status column will change to "In-Progress: Accepting the upgrade", followed by "In-Progress: Rebooting the server to convert file system to ext4", and eventually a message depicting 'Accept-upgrade' completion; an spinner will also appear by the CMP server Name,</td></tr>
</table>

		as can be seen in snapshot below: 
6. ☐	**CMP GUI:** Remove the CMP server from **Force Standby** status	**Upgrade Manager → System Maintenance** - **Select** the checkbox of Primary-site, **Force standby** CMP server - From **Operation menu**, click **Cancel Force Standby** - Click **OK** to acknowledge the action.  Make sure that both CMP server at Primary-site have returned to regular Active-Standby status and the servers are synchronized completely, as exemplified in snapshot below: 
7. ☐	**CMP GUI:** Verify the Alarms' status	**SYSTEM WIDE REPORTS →ALARMS→ACTIVE ALARMS** Check the alarms and compare with the active alarms backup taken in step-1 of the procedure.
8.	**Repeat!**	Repeat this procedure for the remaining, secondary Site CMP cluster.
THIS PROCEDURE HAS BEEN COMPLETED		

7.4.2 Procedure-12: Accepting Upgrade for MPE clusters

Description:

Once an upgrade has been completed, the upgrade must be accepted or rejected before any subsequent upgrades may occur. As part of upgrade, the Server Upgrade Pending Accept/Reject (TKSPLATMI33) alarm is set and the MOTD is updated to reflect that the upgrade has not yet been accepted.

'Accept Upgrade' will be the last thing to do in an upgrade, once the customer decides that the upgrade is successful, the upgrade may be accepted by running 'Accept Upgrade' from the UM (CMP GUI).

Notes:

- Rollback will no longer be supported.
- The server Upgrade Pending Accept/Reject alarm will be cleared.
- If the Accept Upgrade step results in the conversion of the file system, a reboot will be triggered automatically.

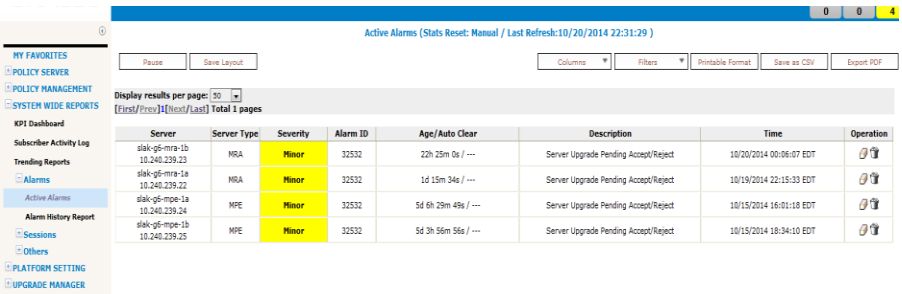
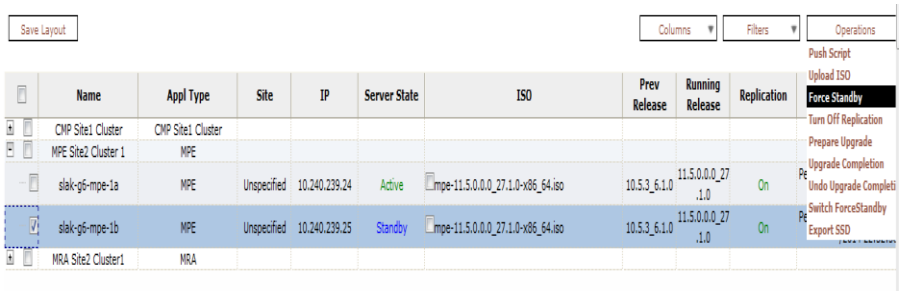
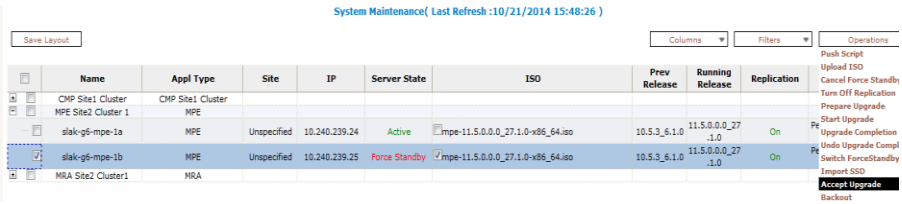
Accept-Upgrade should only be executed when:

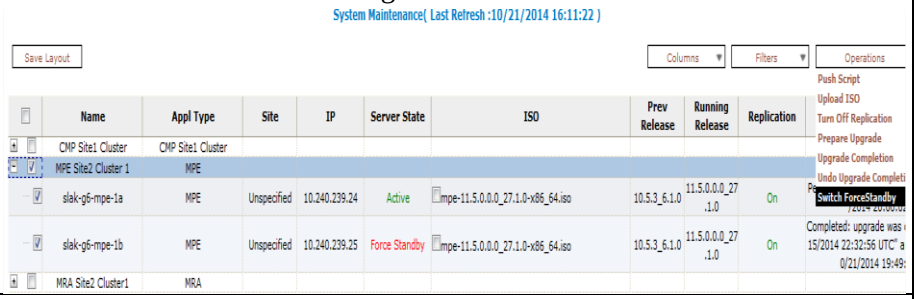
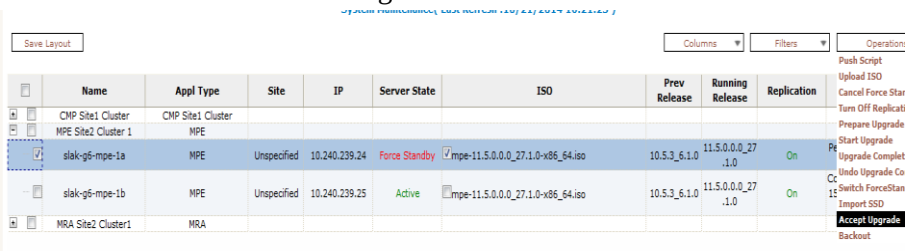
- All the servers in the topology have been upgrade to the new version 11.5.
- The server's status is 'Pending'.
- The server is 'Forced Standby'.

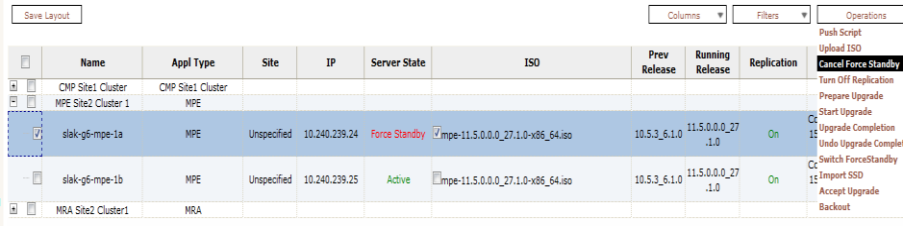
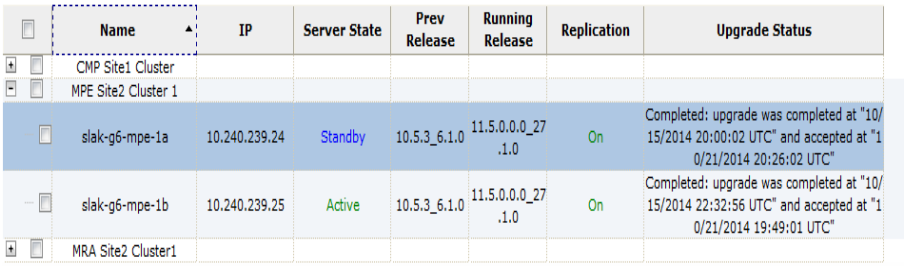
MPE Accept-upgrade Overview:

1. Use the UM GUI to place standby MPE into Forced Standby
2. Use the UM GUI to 'Accept Upgrade' for the Forced Standby MPE
3. Use the UM GUI to perform Switch Forced Standby on the MPE Cluster
4. Use the UM GUI to 'Accept Upgrade' for the Forced Standby MPE
5. Use the UM GUI to Remove the MPE server from Frc-Stb

Executional Guidance:

Step	Procedure	Result
1. ☐	**CMP GUI:** Backup an screenshot of Alarms	**SYSTEM WIDE REPORTS →ALARMS→ACTIVE ALARMS** Export the active alarms either in .csv or .pdf format, by clicking Save as CSV or Export as PDF, respectively. 
2. ☐	**CMP GUI:** Place *Standby* MPE node under *Force Standby* status. Note: It's recommended that you choose no more than 03 clusters at a time for Accept-upgrade operation.	**Upgrade Manager →System Maintenance** - **Select** the checkbox of **standby MPE** server - From **Operation menu**, click **Force Standby** - Click **OK** to acknowledge the action. 
3. ☐	**CMP GUI:** Accept Upgrade Time Duration: This step may take somewhere from 5-7 minutes.	**Upgrade Manager →System Maintenance** - **Select** the checkbox of **Force standby MPE** server - From **Operation menu**, click **Accept Upgrade** - Click **OK** to acknowledge the action.  Please note that the ***Upgrade Status*** column will change to *"In-Progress: Accepting the upgrade*", followed by "*In-Progress: Rebooting the server to convert file system to ext4"*, and eventually a message depicting 'Accept-upgrade' completion; an spinner and sync broken icons will also appear by the MPE server name under ***Name*** column. Expected temporary Critical Alarms:

		31283 High availability server is offline **70001** The qp_procmgr process has failed. Expected temporary Major Alarms: **70004** The QP processes have been brought down for maintenance. **31233** High availability path loss of connectivity
4.☐	**CMP GUI:** Switch Force Standby Note: This step may cause temporary service disruption, which may last for no more than 5 seconds.	**Upgrade Manager →System Maintenance** - **Select** the checkbox of MPE **Cluster** - From **Operation menu**, click **Switch Force Standby** - Click **OK** to acknowledge the action. 
5. ☐	**CMP GUI:** Accept Upgrade for **Force Standby** MPE server Time Duration: This step may take somewhere from 5-7 minutes.	**Upgrade Manager → System Maintenance** - **Select** the checkbox of **Force standby** MPE server - From **Operation menu**, click **Accept Upgrade** - Click **OK** to acknowledge the action.  Please note that the ***Upgrade Status*** column will change to *"In-Progress: Accepting the upgrade*", followed by "*In-Progress: Rebooting the server to convert file system to ext4"*, and eventually a message depicting 'Accept-upgrade' completion; an spinner and sync broken icons will also appear by the MPE server name under ***Name*** column. Expected temporary Critical Alarms: **31283** High availability server is offline **70001** The qp_procmgr process has failed. Expected temporary Major Alarms: **70004** The QP processes have been brought down for maintenance. **31233** High availability path loss of connectivity

6. ☐	**CMP GUI:** Remove the MPE server from **Force Standby** status	**Upgrade Manager → System Maintenance** - **Select** the checkbox of **Force standby** MPE server - From **Operation menu**, click **Cancel Force Standby** - Click **OK** to acknowledge the action.  Make sure that both MPE server have returned to regular Active-Standby status and the servers are synchronized completely, as exemplified in snapshot below: 
7. ☐	**CMP GUI:** Verify the Alarms' status	**SYSTEM WIDE REPORTS →ALARMS→ACTIVE ALARMS** Check the alarms and compare with the active alarms backup taken in step-1 of the procedure.
8.	**Repeat!**	Repeat this procedure for the remaining MPE clusters.
THIS PROCEDURE HAS BEEN COMPLETED		

7.4.3 Procedure-12: Accepting Upgrade for MRA clusters

Description:

Once an upgrade has been completed, the upgrade must be accepted or rejected before any subsequent upgrades may occur. As part of upgrade, the Server Upgrade Pending Accept/Reject (TKSPLATMI33) alarm is set and the MOTD is updated to reflect that the upgrade has not yet been accepted.

'Accept Upgrade' will be the last thing to do in an upgrade, once the customer decides that the upgrade is successful, the upgrade may be accepted by running 'Accept Upgrade' from the UM (CMP GUI).

Notes:

- Rollback will no longer be supported.
- The server Upgrade Pending Accept/Reject alarm will be cleared.
- If the Accept Upgrade step results in the conversion of the file system, a reboot will be triggered automatically.

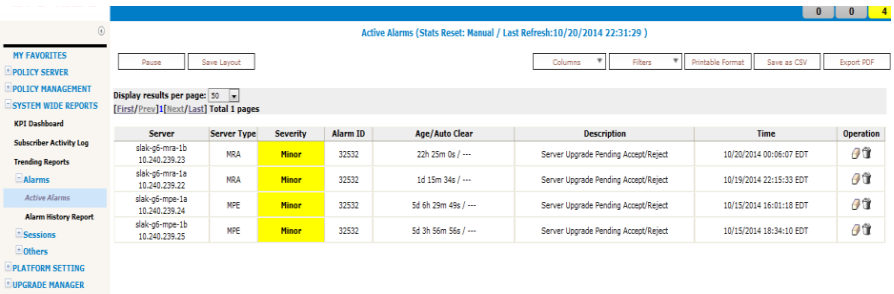
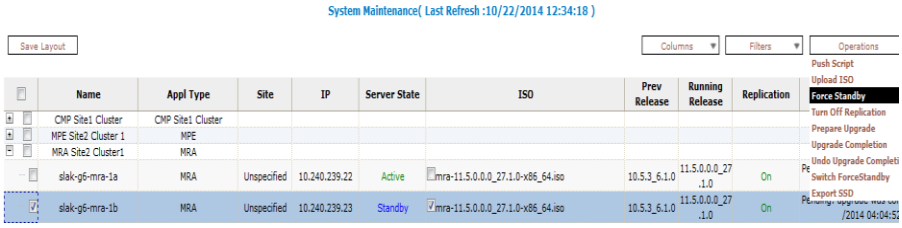
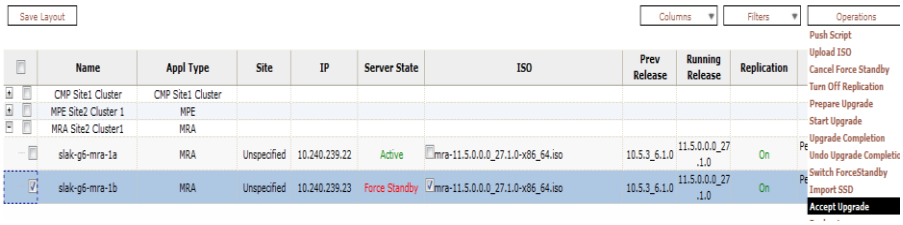
Accept-Upgrade should only be executed when:

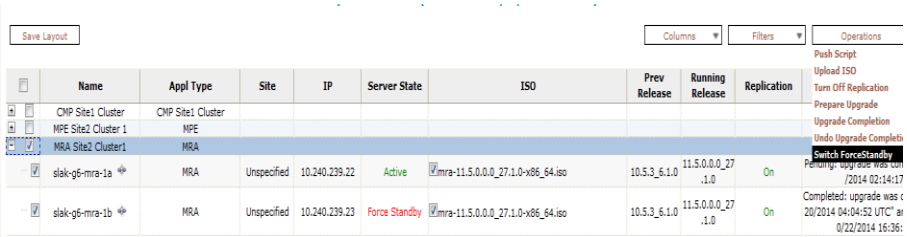
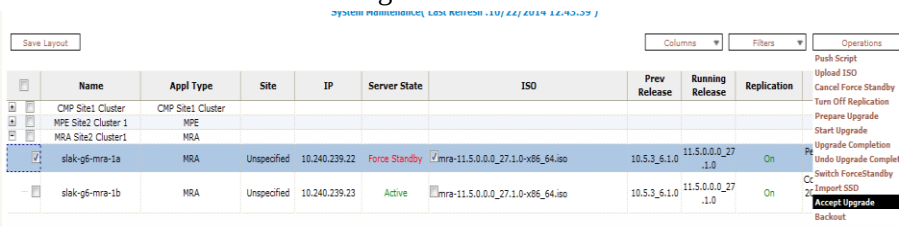
- All the servers in the topology have been upgrade to the new version 11.5.
- The server's status is 'Pending'.
- The server is 'Forced Standby'.

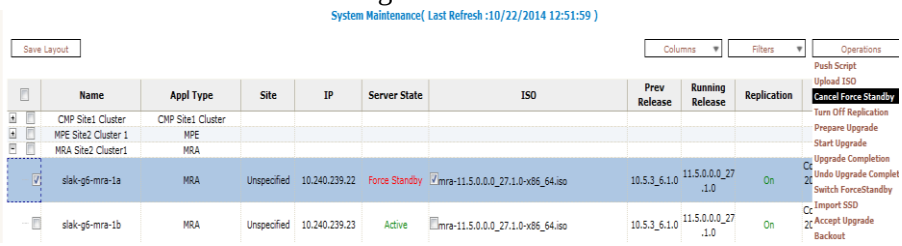
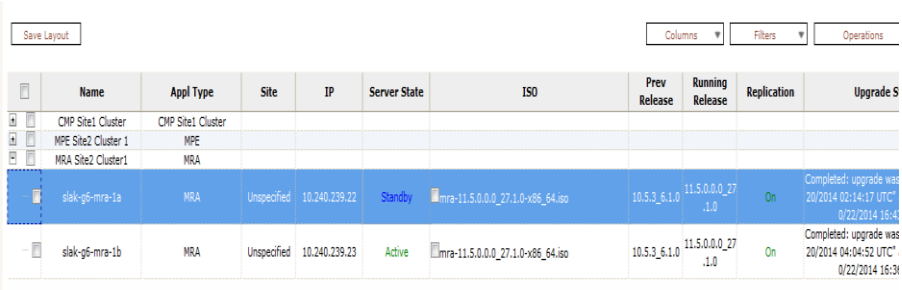
MPE Accept-upgrade Overview:

1. Use the UM GUI to place standby MRA into Forced Standby
2. Use the UM GUI to 'Accept Upgrade' for the Forced Standby MRA
3. Use the UM GUI to perform Switch Forced Standby on the MRA Cluster
4. Use the UM GUI to 'Accept Upgrade' for the Forced Standby MRA
5. Use the UM GUI to Remove the MRA server from Frc-Stb

Executional Guidance:

Step	Procedure	Result
1. ☐	**CMP GUI:** Backup an screenshot of Alarms	**SYSTEM WIDE REPORTS →ALARMS→ACTIVE ALARMS** Export the active alarms either in .csv or .pdf format, by clicking Save as CSV or Export as PDF, respectively. 
2. ☐	**CMP GUI:** Place *Standby* MRA node under *Force Standby* status.	**Upgrade Manager →System Maintenance** - **Select** the checkbox of **standby MRA** server - From **Operation menu**, click **Force Standby** - Click **OK** to acknowledge the action. 
6. ☐	**CMP GUI:** Accept Upgrade Time Duration: This step may take somewhere from 5-7 minutes.	**Upgrade Manager →System Maintenance** - **Select** the checkbox of **Force standby MRA** server - From **Operation menu**, click **Accept Upgrade** - Click **OK** to acknowledge the action.  Please note that the ***Upgrade Status*** column will change to *"In-Progress: Accepting the upgrade*", followed by "*In-Progress: Rebooting the server to convert file system to ext4"*, and eventually a message depicting 'Accept-upgrade' completion; an spinner and sync broken icons will also appear by the MRA server name under ***Name*** column. Expected temporary Critical Alarms:

		31283 **H**igh availability server is offline **70001** The qp_procmgr process has failed. Expected temporary Major Alarms: **70004** The QP processes have been brought down for maintenance. **31233** High availability path loss of connectivity
7. ☐	**CMP GUI:** Switch Force Standby Note: This step may cause temporary service disruption, which may last for no more than 5 seconds.	**Upgrade Manager →System Maintenance** - **Select** the checkbox of MRA **Cluster** - From **Operation menu**, click **Switch Force Standby** - Click **OK** to acknowledge the action. 
8. ☐	**CMP GUI:** Accept Upgrade for **Force Standby** MRA server Time Duration: This step may take somewhere from 5-7 minutes.	**Upgrade Manager → System Maintenance** - **Select** the checkbox of **Force standby** MRA server - From **Operation menu**, click **Accept Upgrade** - Click **OK** to acknowledge the action.  Please note that the ***Upgrade Status*** column will change to *"In-Progress: Accepting the upgrade*", followed by "*In-Progress: Rebooting the server to convert file system to ext4"*, and eventually a message depicting 'Accept-upgrade' completion; an spinner and sync broken icons will also appear by the MPE server name under ***Name*** column. Expected temporary Critical Alarms: **31283** High availability server is offline **70001** The qp_procmgr process has failed. Expected temporary Major Alarms: **70004** The QP processes have been brought down for maintenance. **31233** High availability path loss of connectivity

9. ☐	**CMP GUI:** Remove the MRA server from **Force Standby** status	**Upgrade Manager → System Maintenance** - **Select** the checkbox of **Force standby** MRA server - From **Operation menu**, click **Cancel Force Standby** - Click **OK** to acknowledge the action.  Make sure that both MRA server have returned to regular Active-Standby status and the servers are synchronized completely, as exemplified in snapshot below: 
10. ☐	**CMP GUI:** Verify the Alarms' status	**SYSTEM WIDE REPORTS →ALARMS→ACTIVE ALARMS** Check the alarms and compare with the active alarms backup taken in step-1 of the procedure.
11.	**Repeat!**	Repeat this procedure for the remaining MRA clusters.
THIS PROCEDURE HAS BEEN COMPLETED		

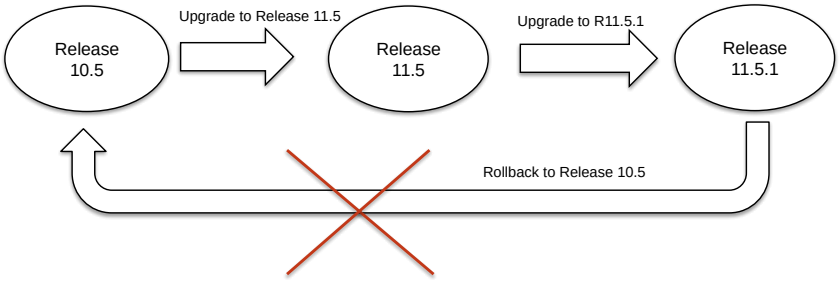
8. BACKOUT (ROLLBACK)

Once MPE, MRA, and CMP servers are upgraded to Release 11.5 but **not** 'Accept Upgrade' yet, customer(s) may decide that a backout to the previous release is required. In that case, each individual server has to be backed out. If it is necessary to backout multiple servers, it is recommended that the systems be rolled back in the reverse order in which they were upgraded. This implies that MRA or MPE servers are rolled back first before the active CMP and CMP-DR can be rolled back to the previous version.

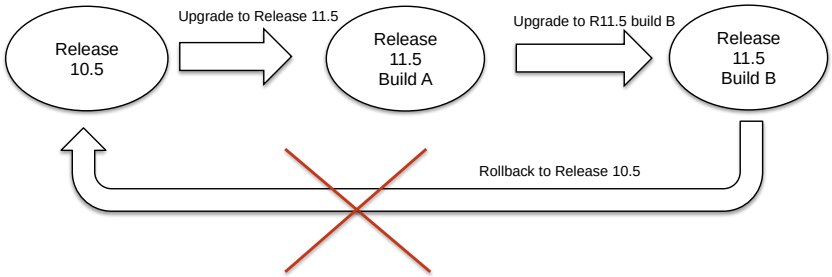
Once all the servers in the system are backed out to the previous release, the servers in this PCRF system could be upgraded to another supported minor or major release.Backout may be performed at any time after the upgrade but before 'Accept Upgrade', with the following limitations:

1. If any new features have been enabled, they must be disabled prior to any backout.
2. If there is an unexpected problem that requires backout after a feature has been enabled, it is possible that transient subscriber data that is changed by the new feature may be impacted by the unexpected problem. In this situation those sessions cannot be guaranteed to be unaffected for any subsequent actions (this includes any activity after the feature is disabled). The impact of any unexpected problem must be analyzed when it occurs to determine the best path forward (or backward) for the customer.

One additional restriction of backout is that it can only be used to go back one release. This restriction applies to all types of releases including any major, minor, maintenance or incremental release including a re-build of 11.5. To be specific, the following diagrams depict backouts that are NOT supported.



Backout after incremental upgrade to Release 11.5.x



Backout after an upgrade to the next build of the same release

8.1 Procedure-11: Backout of Partially Upgraded MRA or MPE Cluster

This procedure is used to backout a cluster that has been partially upgraded. If both server nodes in the cluster are on the same 11.5 release, then escape this procedure and refer to the section 8.2 -"Backout a fully upgraded cluster".

At the end of this procedure, both cluster nodes are expected to be at 10.5.x (or 9.1.x) with *Active/Standby* states.

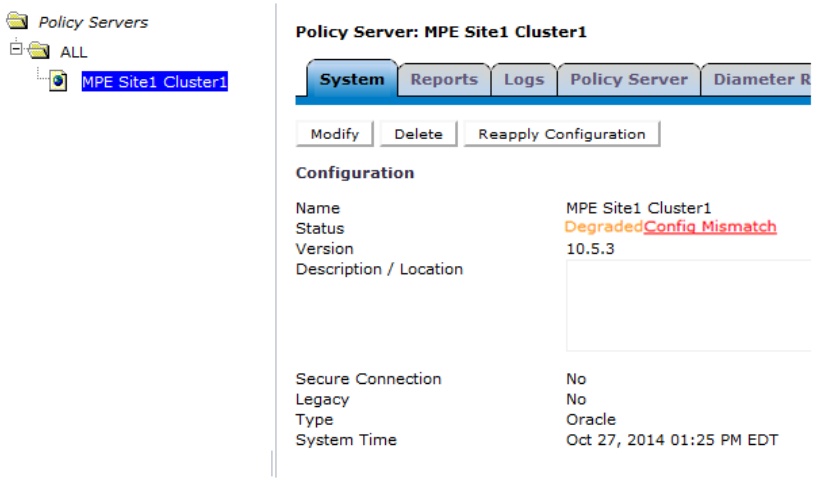
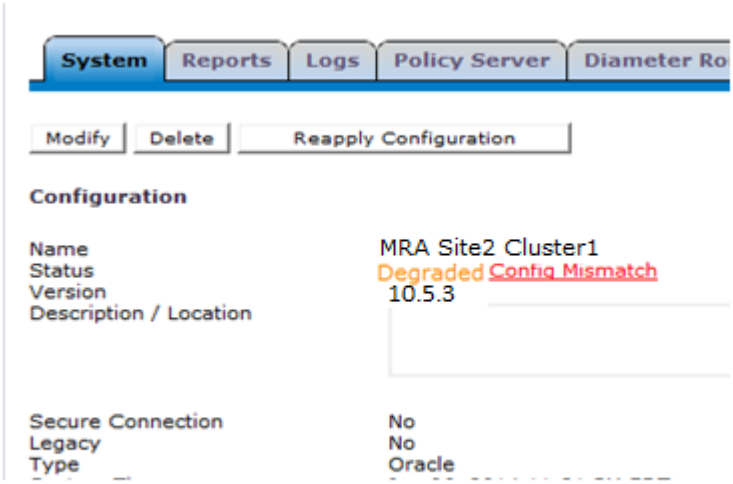
Expected Pre-conditions:

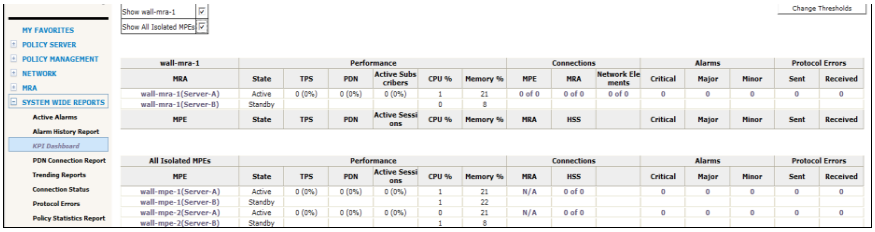
- Primary-site *active* CMP is at release 11.5
- Partially-upgraded cluster can be MPE, MRA or CMP
- One server of target cluster is at release 11.5 and under "Force Standby" state
- One server of target cluster is at release 10.5.x (or 9.1.x) and under "Active" state
- Upgrade Completion was not previously executed on this target cluster
- Release 10.5.x MPE/MRA servers (while being worked on) should have the replication turned OFF as required during the upgrade.

Procedure-11: Backout partially upgraded Cluster		
Step	**Procedure**	**Result**

1. ☐	**CMP GUI:** Verify the status of affected Clusters	**Upgrade Manager → System Maintenance**
		
		• Confirm status of the cluster to be backed out:
		  ○ Primary Active CMP is on Release 11.5
		  ○ Target cluster should have one server in release 10.5.x or 9.1.x, and the other is in Release 11.5. Take note on which server is "Active" and which is "Force Standby".

2. ☐	**CMP GUI:** Switch back the Active server to release 10.5.x or 9.1.x as the case may be **IMPORTANT:** This step may be service Affecting for MPE/MRA session/bindi5ng state and data loss is expected!!	• If release 11.5 server is currently in "Force Standby" state, skip this step and proceed to step-3 of this procedure. • If release 11.5 server is currently under "Active" state: Execute "Switch Force Standby" operation to switch the Active release 11.5 server into "Force Standby" state and the older release 10.5.x server into "Active" state. **Upgrade Manager → System Maintenance** • **Select** the checkbox for the partially upgraded (mix of older, release 10.5.x and release 11.5) cluster • Under **Operations menu**, select "**Switch ForceStandby**" operation • Click **OK** to acknowledge the action • Wait and ensure that release 10.5.x server is now in "Active" state. Expected Alarms: 31102: DB replication from master DB has failed 31224: High availability configuration error 31101: DB replication to a slave has failed 31113: Replication Manually Disabled 75000: Policy Library loading failed 78001: Transfer of Policy jar files failed

Procedure-11: Backout partially upgraded Cluster		
Step	**Procedure**	**Result**
3. ☐	**CMP GUI:** Re-Apply Configuration to MPE/MRA cluster	For MPE: **Policy Server → Configuration: System → Re-Apply Configuration** • The Version now shows release 10.5.x  For MRA: **MRA → Configuration: System → Re-Apply Configuration** • The version now shows release 10.5.x  S

Procedure-11: Backout partially upgraded Cluster		
Step	**Procedure**	**Result**
4. ☐	**CMP GUI:** Verify release 10.5.x server is handling traffic via KPI Dashboard.	**System Wide Reports → KPI Dashboard**  	
5. ☐	**CMP GUI:** Turn Replication ON for Active MPE/MRA server	**Upgrade Manager → System Maintenance** • Select Checkbox for the Active server with Replication OFF and under Operations menu, select "Turn ON Replication" operation Expected Alarms – 31113: Replication Manually Disabled (Clear in 5 min) 31101: DB replication to a slave has failed (Clear in 5 min) 31102: DB replication from a s master DB has failed (Clear in 5 min)
6. ☐	**CMP GUI**: Executing Backout on Release 11.5 Server **NOTE:** Backout takes about 30 minutes to complete	**Upgrade Manager → System Maintenance** • Select checkbox for the Release 11.5 Server in "Force Standby" state • Under Operations menu, select "Backout" operation
	CMP GUI: Verify successful Backout status	**Upgrade Manager → System Maintenance** • A backout completion message appears under "Upgrade Status" column - *"Completed: backout was completed at ……"* • Verify "Sync Broken" indicator is cleared in a few minutes
	CMP GUI: Execute "Cancel Force Standby" status on the backed out server	**Upgrade Manager → System Maintenance** • Select checkbox for "Force Standby" server and select "Cancel Force Standby" operation under Operations menu
7. ☐	**CMP GUI:** Verify the cluster is handling traffic as expected	• As done during the Upgrade sections above, verify: - MPE/MRA Reports - Active Alarms - KPI Dashboard
THIS PROCEDURE HAS BEEN COMPLETED		

8.2 Backout of Full Upgrade

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

This procedure is used to back out a cluster that has been fully upgraded. The cluster could the CMP, the MPE or the MRA. At the end of this procedure, all servers of the target cluster will be on release 10.5.x (or 9.1.x) with Active and Standby status.

Expected pre-conditions:

1. *Accept-upgrade* is not carried out yet for any of the clusters in the network
2. The upgrade has not been accepted
3. **NO** new features or functionality can have been used or configured
4. The CMP cannot be backout if any other components remain on the new version
5. Redo the prepare upgrade from the Primary-site Active CMP with command:

   ```
   policyUpgrade.pl --prepareUpgrade
   ```

   For this release on a **wireless** office, the table exclusions should also be:
   PcmmSession,PcmmSessionPhysT

6. One server of target cluster is on Release 11.5 in either “Standby” or “Force Standby”

8.2.1 Overview: Backout Sequence

1. Re-Add Table exclusions
2. MRA Site-2 clusters
3. MRA Site-1 clusters
4. MPE Site-2 clusters
5. MPE Site-1 clusters
6. CMP Site-2 cluster
7. CMP Site-1 cluster

8.2.1.1 Backout MRA server - overview

1) Use the UM GUI to place standby MRA into forced standby
2) Use the UM GUI to turn off replication for the MRA server in Frc-Stb
3) Use the UM GUI to backout Frc-Stb MRA server
4) Use the UM GUI to perform Switch Forced Standby on the MRA cluster
5) Use the CMP GUI for the MRA cluster to re-apply config
6) Use the UM GUI to backout remaining server
7) Use the UM GUI to turn on replication for the MRA blade
8) Use the UM GUI to Cancel Forced Standby for the MRA blade
9) Use the UM GUI to select the backed out MRA cluster and execute "Upgrade Completion"

8.2.1.2 Backout MPE server - Overview

1) Use the UM GUI to place standby MPE into forced standby
2) Use the UM GUI to turn off replication for the MPE server in Frc-Stb
3) Use the UM GUI to backout Frc-Stb MPE server
4) Use the UM GUI to perform Switch Forced Standby on the MPE cluster
5) Use the CMP GUI for the MPE cluster to re-apply config
6) Use the UM GUI to backout remaining server
7) Use the UM GUI to turn on replication for the MPE blade
8) Use the UM GUI to Cancel Forced Standby for the MPE blade
9) Use the UM GUI to select the backed out MPE cluster and execute "Upgrade Completion"

8.2.1.3 Backout CMP Secondary Site - Overview

NOTE: All other components (MPEs and MRAs) must already be backed out:

1) Use the UM GUI to place the Standby CMP at Secondary Site into forced standby
2) Use the UM GUI to backout Frc-Stb server on Secondary Site CMP Cluster
3) Use the UM GUI to perform Switch Forced Standby on Secondary Site CMP Cluster
4) Use the UM GUI to backout remaining server on Secondary Site CMP Cluster
5) Leave the CMP server at the Secondary site in Forced Standby

Note: If Secondary (Site-2) Standby CMP server is not left in Force Standby, then Secondary (Site-2) CMP cluster will failover during Primary (Site-1) CMP Backout. Also note that CMP failover may need manual intervention (promote/demote) unlike MPE, MRA failover which is automatic.

8.2.1.4 Backout CMP Primary Site - Overview

NOTE: Secondary CMP must have been backed out already

1) Use the UM GUI to place the Standby CMP at Primary Site into forced standby
2) Use the UM GUI to backout the Frc-Stb server on Primary Site CMP Cluster
3) Use the UM GUI to perform Switch Forced Standby on Primary Site CMP Cluster
4) Log back into the new active CMP
5) Use the UM GUI to Backout remaining server on Primary Site CMP Cluster
6) Use the UM GUI to Cancel Forced Standby for both Primary Site CMP and Secondary Site CMP

8.2.1.5 Overview: Post CMP Backout

NOTE: These steps are for when a full segment backout has been completed.

1) From the Primary Site Active CMP blade, runn the following command:

```
policyUpgrade.pl --cleanupUpgrade
```

This will clear the excludeTables for all the items list in NodeInfo.

8.3 Procedure-12: Pre-requisite: Preparation

The procedure prepares the fully upgraded Policy servers for a *Backout* course. Make sure that ***Accept Upgrade*** has not been carried out for any of the servers in the topology.

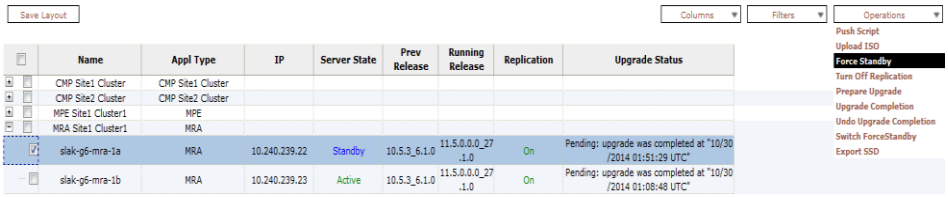
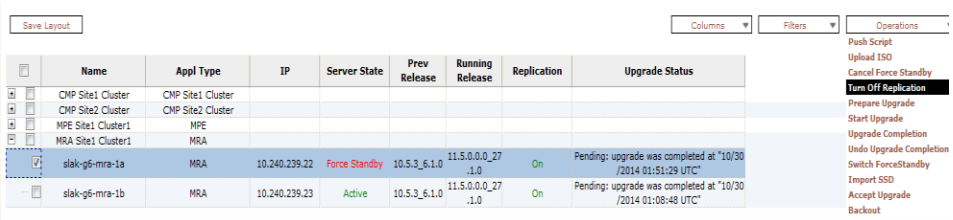
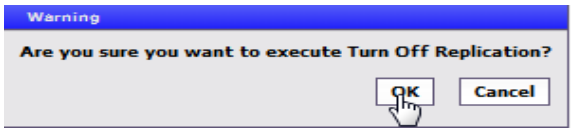
Procedure-12: Re-add Replication Exclusions		
Step	**Procedure**	**Result**
1.	**CLI:** Executing *PrepareUpgrade*	Login to the Primary CMP VIP and as user *root*, execute the following: policyUpgrade.pl –prepareUpgrade
2. ☐	**CLI:** Verify the Exclusions are re-added	• As user *root*, execute the following command: # iqt -p NodeInfo [root@slak-g6-cmp-1b ~]# iqt -p NodeInfo nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables A0188.078 site2-cmp-1b site2-cmp-1b,10.250.84.26 Active Unspecified PcmmSession,PcmmSessionPhysT A0188.129 site2-cmp-1a site2-cmp-1a,10.250.84.25 Active Unspecified PcmmSession,PcmmSessionPhysT A1041.147 slak-g6-cmp-1a slak-g6-cmp-1a,10.240.239.37 Active Unspecified PcmmSession,PcmmSessionPhysT A1041.203 slak-g6-cmp-1b slak-g6-cmp-1b,10.240.239.38 Active Unspecified PcmmSession,PcmmSessionPhysT C1213.145 slak-g6-mpe-1a slak-g6-mpe-1a,10.240.239.24 Active Unspecified PcmmSession,PcmmSessionPhysT C1213.230 slak-g6-mpe-1b slak-g6-mpe-1b,10.240.239.25 Active Unspecified PcmmSession,PcmmSessionPhysT C2563.007 slak-g6-mra-1a slak-g6-mra-1a,10.240.239.22 Active Unspecified PcmmSession,PcmmSessionPhysT C2563.151 slak-g6-mra-1b slak-g6-mra-1b,10.240.239.23 Active Unspecified PcmmSession,PcmmSessionPhysT [root@slak-g6-cmp-1b ~]# • Verify that each server should list the following exclusion parameters: ○ PcmmSession ○ PcmmSessionPhysT
THIS PROCEDURE HAS BEEN COMPLETED		

8.4 Procedure-13: Backout Fully Upgraded MRA/MPE Clusters

Procedure-13: Backout Fully Upgraded MRA/MPE clusters

NOTE:

- Backout steps are same for both MRA and MPE server types, but follow the Backout Sequence, as outlined in section 8.2.1. If the topology has Site-2 Clusters, first perform backout steps on Site-2 Clusters followed by Site-1 Clusters**.**

Step	Procedure	Result
1. ☐	**CMP GUI:** Setting "Standby" server to "Force Standby"	**Upgrade Manager → System Maintenance** • This action can be applied to more than one MRA/MPE cluster *(Must adhere to the NOTE above).* • (Optional but Preferred) Filter MRAs/MPEs as described in Appendix • **Select** checkbox for "Standby" server(s) and then select "Force Standby" from **Operations menu:**  • Select "**OK**" to continue the operation
2. ☐	**CMP GUI:** Turn OFF Replication for "Force Standby" server	**Upgrade Manager → System Maintenance** • **Select** "Force Standby" Server(s) and then **select** "Turn OFF Replication" from **Operation menu**:  • Click **OK** to acknowledge the operation.  *Expected Minor Alarm:* **31113 Replication manually disabled** *"SyncBroken"* indicator appears.

3. ☐

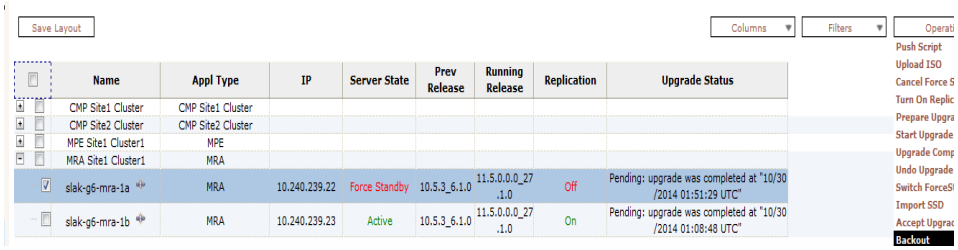
CMP GUI: Executing Backout

NOTE: Backout takes about 30 minutes to complete

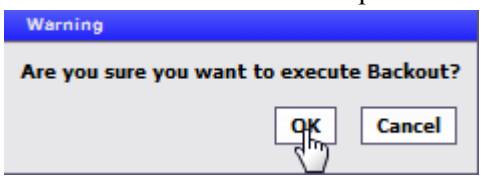
This action can be applied to more than one MRA/MPE cluster

Upgrade Manager → System Maintenance

- **Select** checkbox for Release 11.5 "Force Standby" server(s) to be backed out
- From **Operations menu**, select "Backout"



- Select "**OK**" to continue the operation



- During Backout activities, the following Alarms may be generated as normal reporting events - These will be cleared after the whole Cluster is completely backed out

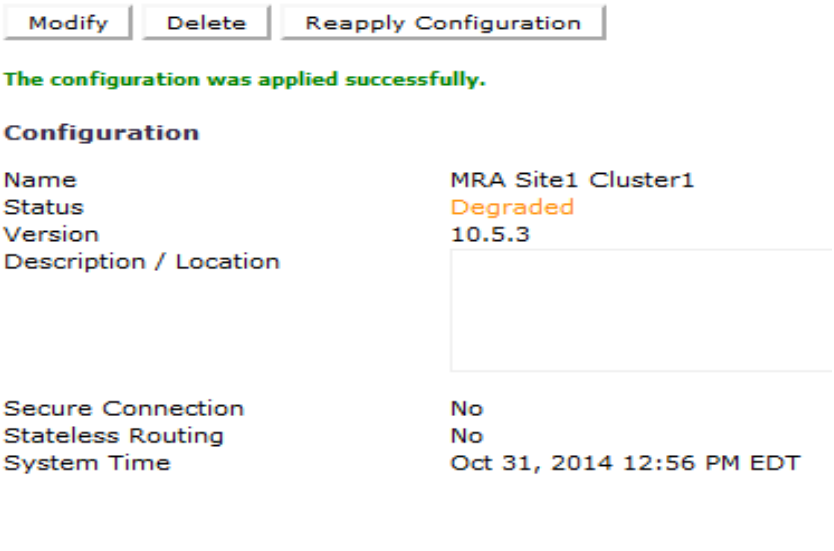
Expected Critical Alarm:
31283 High availability server is offline
70001 The qp_procmgr process has failed. This process manages all pcrf software

Expected Major Alarm:
70004 The QP processes have been brought down for maintenance.

Expected Minor Database replication Alarms:
31100, 31101, 31102, 31107, 31114, 31113

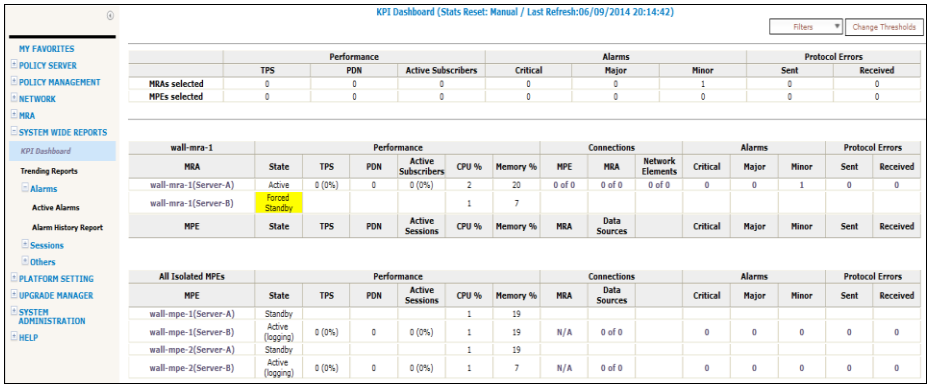
During backout activities, both 'spinner' & 'Sync Broken' indicators are expected to appear.

	CMP GUI: Verify successful Backout status	**Upgrade Manager → System Maintenance** • Verify message under "Upgrade Status" column stating - ***"Completed: backout was completed at ……"*** Save Layout Columns | Name	Appl Type	IP	Server State	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster	CMP Site1 Cluster						
CMP Site2 Cluster	CMP Site2 Cluster						
MPE Site1 Cluster1	MPE						
MRA Site1 Cluster1	MRA						
slak-g6-mra-1a	MRA	10.240.239.22	Force Standby	11.5.0.0.0_27.1.0	10.5.3_6.1.0	Off	Completed: backout was completed at "10/31/2014 16:48:20 UTC"
slak-g6-mra-1b	MRA	10.240.239.23	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/30/2014 01:08:48 UTC"	 • Verify backed out server(s) are running Release 10.5.x (or 9.1.x as the case may be) and are under "Force Standby" status and Replication-OFF.
4. ☐	**In CMP GUI:** Switchover backedout "Force Standby" server with Active Server **IMPORTANT: Service Affecting on MPE/MRA – up to 5 seconds of traffic impact is possible** **This operation should be applied to one MRA/MPE cluster, at a time**	**Upgrade Manager → System Maintenance** • **Select** checkbox for the MRA/MPE cluster being worked on. • Under "Operations menu, select "Switch ForceStandby" Save Layout Columns Filters Operations Push Script Upload ISO Prepare Upgrade Upgrade Completion Undo Upgrade Comple Switch ForceStandby | Name	Appl Type	IP	Server State	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster	CMP Site1 Cluster						
CMP Site2 Cluster	CMP Site2 Cluster						
MPE Site1 Cluster1	MPE						
MRA Site1 Cluster1	MRA						
slak-g6-mra-1a	MRA	10.240.239.22	Force Standby	11.5.0.0.0_27.1.0	10.5.3_6.1.0	Off	Completed: backout was completed at "10/31/2014 16:48:20 UTC"
slak-g6-mra-1b	MRA	10.240.239.23	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/30/2014 01:08:48 UTC"	 • Verify Server State is switched but Replication status remains same After switchover completes, the 'Sync Broken' indicator disappears as expected!

5. ☐	**In CMP GUI:** Reapply Configuration on all cluster(s) being backed out This action can be applied to more than one MRA/MPE cluster	IF MPE, **Policy Server → Configuration →** ***<cluster name>*** **→ System Tab** If MRA, **MRA → Configuration →** ***<cluster name>*** **→ System Tab** • Select "Reapply Configuration" operation • The "Version" is successfully changed to Backout Release 10.5.x (or 9.1.x as the case may be) for MRA/MPE. • Status remains "degraded" as expected. 
6. ☐	**In CMP GUI**: Executing Backout **NOTE:** Backout takes about 30 minutes to complete.	**Repeat step-3 of this procedure for remaining server of the cluster.**

7. ☐ **In CMP GUI:** Verify Traffic Status

Upgrade Manager → KPI Dashboard

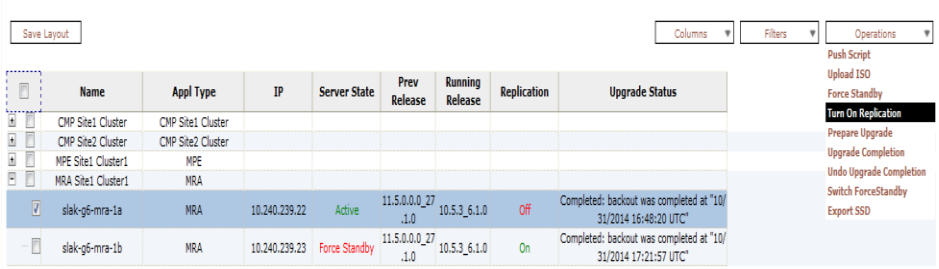


8. ☐ **In CMP GUI:** Turn ON Replication for the Active server(s)

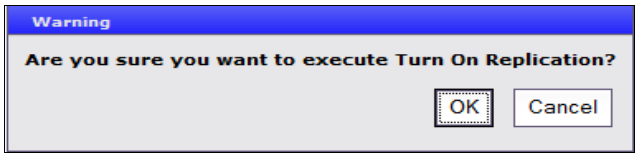
This action can be applied to more than one MRA/MPE cluster

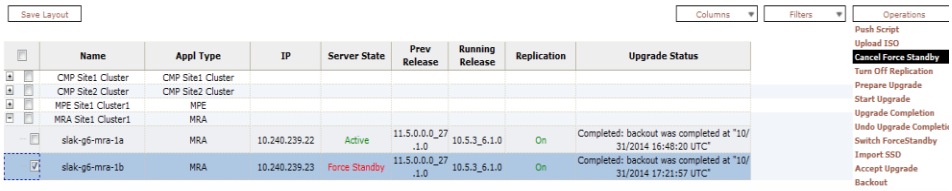
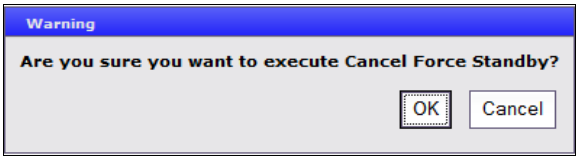
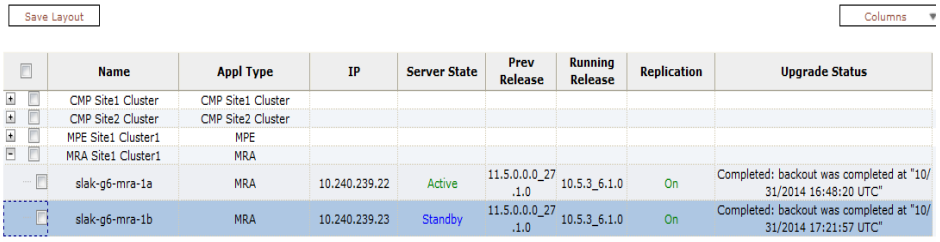
Upgrade Manager → System Maintenance

- Select checkbox for "Active" server(s) and select "Turn ON Replication" under Operations menu



- Select "OK" to continue the operation



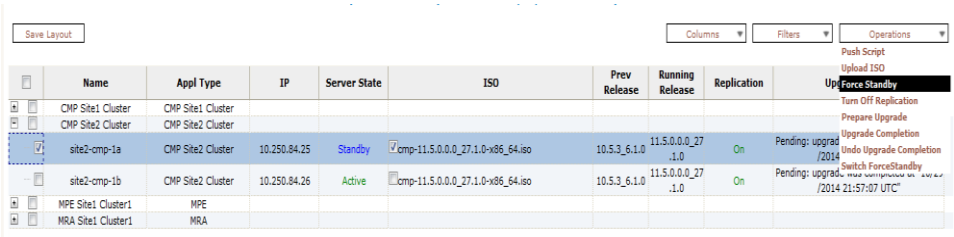
9. ☐	**In CMP GUI:** Cancel all "Forced Standby" back to "Standby" This action can be applied to more than one MRA/MPE cluster	**Upgrade Manager → System Maintenance** • Select checkbox for the "Force Standby" server(s) and under Operations menu and select "Cancel Force Standby"  • Select "OK" to continue the operation   Name | Appl Type | IP | Server State | Prev Release | Running Release | Replication | Upgrade Status CMP Site1 Cluster | CMP Site1 Cluster CMP Site2 Cluster | CMP Site2 Cluster MPE Site1 Cluster1 | MPE MRA Site1 Cluster1 | MRA slak-g6-mra-1a | MRA | 10.240.239.22 | Active | 11.5.0.0.0_27.1.0 | 10.5.3_6.1.0 | On | Completed: backout was completed at "10/31/2014 16:48:20 UTC" slak-g6-mra-1b | MRA | 10.240.239.23 | Standby | 11.5.0.0.0_27.1.0 | 10.5.3_6.1.0 | On | Completed: backout was completed at "10/31/2014 17:21:57 UTC"
10. ☐	**CMP GUI:** Verify KPI dashboard and the Active alarms	**System Wide Reports → Active Alarms** **Expected, temporary Minor Alarms:** 75000: Policy Library loading failed 78001: Transfer of Policy jar files failed
11. ☐	**Repeat!**	**As needed, repeat this procedure for the next MPE/MRA cluster to be backed out.**
THIS PROCEDURE HAS BEEN COMPLETED		

8.5 Procedure-14: Backout Fully Upgraded CMP Clusters

Procedure-14: Backout Fully upgraded CMP Clusters

Pre-requisite and notes:

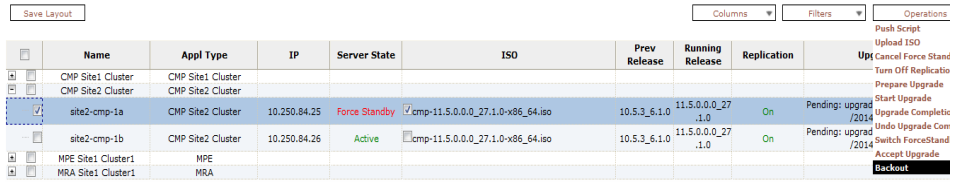
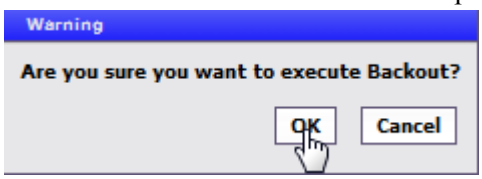
- *Backout steps are same for Site-1 and Site-2 but follow the Backout Sequence, outlined in section 8.2.1.*
- *If the topology has Site-2 Cluster, perform backout steps on Site-2 Cluster followed by Site-1 Cluster.*
- *All other Policy components, such as MRA and MPEs, must have been backed out*

Step	Procedure	Result
1. ☐	**CMP GUI: [Secondary Site, in case of multi-site topology]** Setting "Standby" server to "Force Standby"	**Upgrade Manager → System Maintenance** • Select checkbox for "Standby" server. • Select "Force Standby" under Operations menu.  • Select "**OK**" to continue the operation • Validate "Force Standby" status

Procedure-14: Backout Fully upgraded CMP Clusters

Pre-requisite and notes:

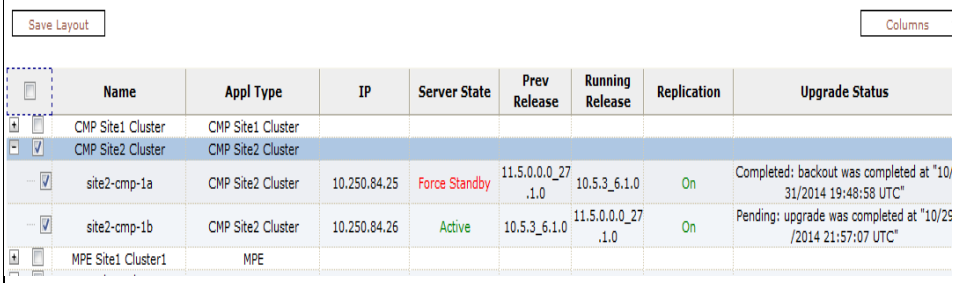
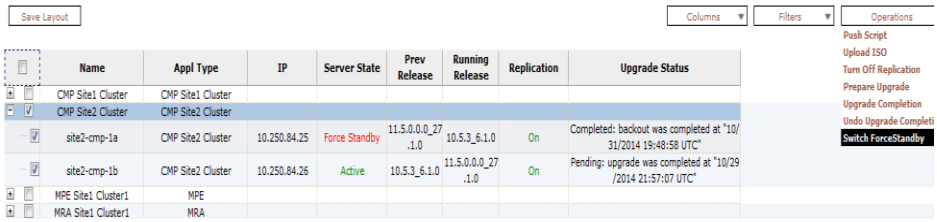
- *Backout steps are same for Site-1 and Site-2 but follow the Backout Sequence, outlined in section 8.2.1.*
- *If the topology has Site-2 Cluster, perform backout steps on Site-2 Cluster followed by Site-1 Cluster.*
- *All other Policy components, such as MRA and MPEs, must have been backed out*

Step	Procedure	Result
2. ☐	**CMP GUI:** Executing Backout **NOTE:** Backout takes about 30 minutes to complete	**Upgrade Manager → System Maintenance** • Select checkbox for Release 11.5 "Force Standby" server • Under Operations menu, select "Backout" operation  • Select "**OK**" to continue the operation  • During Backout activities, the following alarms may be generated as normal reporting events - these are cleared after the whole cluster is completely backed out. Expected temporary critical alarm: **70001** The qp_procmgr process has failed.This process manages all pcrf **software.** **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master Expected, temporary Major Alarm: **31233** High availability path loss of connectivity Expected Minor Database replication Alarms: **31100, 31101, 31102, 31107, 31114, 31113** During backout activities, both 'spinner' & 'Sync Broken' indicators appear as expected.

Procedure-14: Backout Fully upgraded CMP Clusters

Pre-requisite and notes:

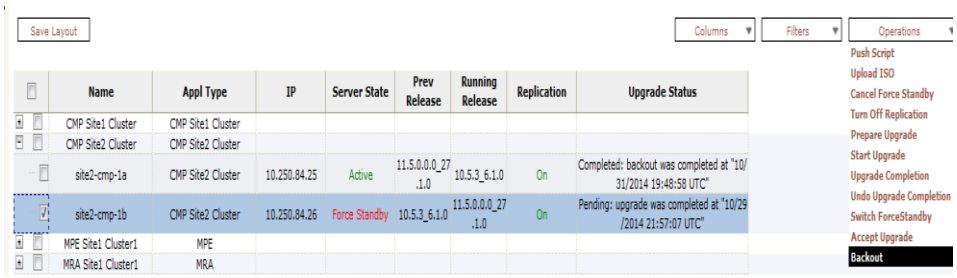
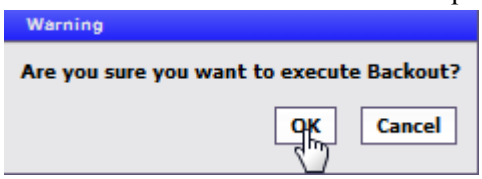
- *Backout steps are same for Site-1 and Site-2 but follow the Backout Sequence, outlined in section 8.2.1.*
- *If the topology has Site-2 Cluster, perform backout steps on Site-2 Cluster followed by Site-1 Cluster.*
- *All other Policy components, such as MRA and MPEs, must have been backed out*

Step	Procedure	Result
3. ☐	**CMP GUI:** Verify successful Backout of "Force Standby"	**Upgrade Manager → System Maintenance** • Verify message under "Upgrade Status" column stating - ***"Completed:backout was completed at ……"*** Verify backed out server is running Release 10.5.x in "Force Standby" status:  Save Layout Columns Name | Appl Type | IP | Server State | Prev Release | Running Release | Replication | Upgrade Status CMP Site1 Cluster | CMP Site1 Cluster CMP Site2 Cluster | CMP Site2 Cluster site2-cmp-1a | CMP Site2 Cluster | 10.250.84.25 | Force Standby | 11.5.0.0.0_27.1.0 | 10.5.3_6.1.0 | On | Completed: backout was completed at "10/31/2014 19:48:58 UTC" site2-cmp-1b | CMP Site2 Cluster | 10.250.84.26 | Active | 10.5.3_6.1.0 | 11.5.0.0.0_27.1.0 | On | Pending: upgrade was completed at "10/29/2014 21:57:07 UTC" MPE Site1 Cluster1 | MPE
4. ☐	**CMP GUI:** Switchover backed out "Force Standby" server with Active server	**Upgrade Manager → System Maintenance** • Select checkbox for CMP cluster to be switched • Under "Operations" menu, select "Switch ForceStandby"  Save Layout Columns Filters Operations Push Script Upload ISO Turn Off Replication Prepare Upgrade Upgrade Completion Undo Upgrade Completi Switch ForceStandby Name | Appl Type | IP | Server State | Prev Release | Running Release | Replication | Upgrade Status CMP Site1 Cluster | CMP Site1 Cluster CMP Site2 Cluster | CMP Site2 Cluster site2-cmp-1a | CMP Site2 Cluster | 10.250.84.25 | Force Standby | 11.5.0.0.0_27.1.0 | 10.5.3_6.1.0 | On | Completed: backout was completed at "10/31/2014 19:48:58 UTC" site2-cmp-1b | CMP Site2 Cluster | 10.250.84.26 | Active | 10.5.3_6.1.0 | 11.5.0.0.0_27.1.0 | On | Pending: upgrade was completed at "10/29/2014 21:57:07 UTC" MPE Site1 Cluster1 | MPE MRA Site1 Cluster1 | MRA • Browser session may be lost at this point and may need to re-login, if the procedure being carried on Primary site CMP cluster**.** • Verify the Server Status is successfully switched **NOTE:** After switchover completes, the 'Sync Broken' indicator disappears as expected Expected Critical Alarm: **70025** The MySQL slave has a different schema version than the master. This alarm is cleared after the whole cluster is completely backed out to the same Release 10.5.x in later steps

Procedure-14: Backout Fully upgraded CMP Clusters

Pre-requisite and notes:

- *Backout steps are same for Site-1 and Site-2 but follow the Backout Sequence, outlined in section 8.2.1.*
- *If the topology has Site-2 Cluster, perform backout steps on Site-2 Cluster followed by Site-1 Cluster.*
- *All other Policy components, such as MRA and MPEs, must have been backed out*

Step	Procedure	Result
5. ☐	**CMP GUI:** Executing Backout **NOTE:** Backout takes about 30 minutes to complete	**Upgrade Manager → System Maintenance** • Select checkbox for Release 11.5 "Force Standby" server • Under Operations menu, select "Backout"  • Select "OK" to continue the operation  • During Backout activities, the following Alarms may be generated and are normal reporting events - these are cleared after the whole cluster is completely backed out Expected Critical Alarm: **70001** The qp_procmgr process has failed. This process manages all pcrf software **31283** High availability server is offline **70025** The MySQL slave has a different schema version than the master Expected Major Alarm: **70004** The QP processes have been brought down for maintenance Expected Minor Database replication Alarms: **31100, 31101, 31102, 31107, 31114, 31113** During backout activities, both 'spinner' & 'Sync Broken' indicators appear as expected.

Procedure-14: Backout Fully upgraded CMP Clusters

Pre-requisite and notes:

- *Backout steps are same for Site-1 and Site-2 but follow the Backout Sequence, outlined in section 8.2.1.*
- *If the topology has Site-2 Cluster, perform backout steps on Site-2 Cluster followed by Site-1 Cluster.*
- *All other Policy components, such as MRA and MPEs, must have been backed out*

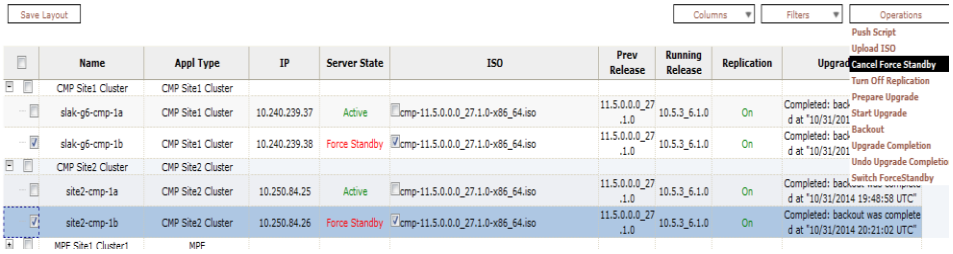
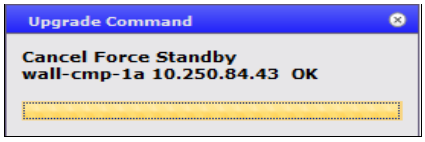
Step	Procedure	Result
6. ☐	**CMP GUI:** Verify successful Backout status	**Upgrade Manager → System Maintenance** • Verify message under "Upgrade Status" column stating - **"Completed:backout was completed at ……"** • Verify this server is now running Release 10.5.x in "Force Standby" status. Save Layout Columns Expected Critical Alarm: ***'70025-** The MySQL slave has a different schema version than the master' is cleared* Wait until the 'Sync Broken' icon disappears as replication synch is successfully completed. **<u>Important:</u>** **If topology is multi-site and if this force Standby server is at Site-2 then leave this server in "Force Standby" status and repeat step 1-6 for Primary-site CMP cluster.**

Name	Appl Type	IP	Server State	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster	CMP Site1 Cluster						
slak-g6-cmp-1a	CMP Site1 Cluster	10.240.239.37	Standby	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/2 /2014 21:13:07 UTC"
slak-g6-cmp-1b	CMP Site1 Cluster	10.240.239.38	Active	10.5.3_6.1.0	11.5.0.0.0_27.1.0	On	Pending: upgrade was completed at "10/2 /2014 19:59:24 UTC"
CMP Site2 Cluster	CMP Site2 Cluster						
site2-cmp-1a	CMP Site2 Cluster	10.250.84.25	Active	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "1 31/2014 19:48:58 UTC"
site2-cmp-1b	CMP Site2 Cluster	10.250.84.26	Force Standby	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "1 31/2014 20:21:02 UTC"
MPE Site1 Cluster1	MPE						
MRA Site1 Cluster1	MRA						

Procedure-14: Backout Fully upgraded CMP Clusters

Pre-requisite and notes:

- *Backout steps are same for Site-1 and Site-2 but follow the Backout Sequence, outlined in section 8.2.1.*
- *If the topology has Site-2 Cluster, perform backout steps on Site-2 Cluster followed by Site-1 Cluster.*
- *All other Policy components, such as MRA and MPEs, must have been backed out*

Step	Procedure	Result
7. ☐	**CMP GUI**: Cancel "Force Standby" server at Site-1 and Site-2(if it exists in the topology)	**Upgrade Manager → System Maintenance** • This can be done in parallel on Site-1 CMP cluster and Site-2 CMP cluster (if it exists in the topology) • Select checkbox for "Force Standby" server(s) • Under Operations menu, select "Cancel Force Standby"  • Click on 'OK' to continue the operation  • Validate CMP cluster on Site-1 and Site-2(if it exists) are now backed out to Release 10.5.x.

Procedure-14: Backout Fully upgraded CMP Clusters

Pre-requisite and notes:

- *Backout steps are same for Site-1 and Site-2 but follow the Backout Sequence, outlined in section 8.2.1.*
- *If the topology has Site-2 Cluster, perform backout steps on Site-2 Cluster followed by Site-1 Cluster.*
- *All other Policy components, such as MRA and MPEs, must have been backed out*

Step	Procedure	Result
8.	View complete backout status of CMP(s),MRA(s),MRA(s)	**Upgrade Manager → System Maintenance** • Confirm all clusters have "Active" and "Standby" status with Replication ON, Running Release as 10.5.x (or 9.1.x as the case may be), *Upgrade Status as Completed: backout…*

Save Layout

Columns

Name	Appl Type	IP	Server State	Prev Release	Running Release	Replication	Upgrade Status
CMP Site1 Cluster	CMP Site1 Cluster						
slak-g6-cmp-1a	CMP Site1 Cluster	10.240.239.37	Active	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 21:59:06 UTC"
slak-g6-cmp-1b	CMP Site1 Cluster	10.240.239.38	Standby	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 22:26:27 UTC"
CMP Site2 Cluster	CMP Site2 Cluster						
site2-cmp-1a	CMP Site2 Cluster	10.250.84.25	Active	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 19:48:58 UTC"
site2-cmp-1b	CMP Site2 Cluster	10.250.84.26	Standby	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 20:21:02 UTC"
MPE Site1 Cluster1	MPE						
slak-g6-mpe-1a	MPE	10.240.239.24	Active	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 17:58:42 UTC"
slak-g6-mpe-1b	MPE	10.240.239.25	Standby	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 18:22:33 UTC"
MRA Site1 Cluster1	MRA						
slak-g6-mra-1a	MRA	10.240.239.22	Active	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 16:48:20 UTC"
slak-g6-mra-1b	MRA	10.240.239.23	Standby	11.5.0.0.0_27.1.0	10.5.3_6.1.0	On	Completed: backout was completed at "10/31/2014 17:21:57 UTC"

THIS PROCEDURE HAS BEEN COMPLETED

8.6 Procedure-15: Finalize Backout

Procedure-15: Finalize backout post CMP Backout		
Step	**Procedure**	**Result**
1. ☐	**CLI:** List out the current Exclusion Tables that were added previously.	Login into Primary/Site-1 Active CMP server (One way to do this is to SSH to CMP VIP) as ***root***, and execute the following command: # iqt -p NodeInfo [root@slak-g6-cmp-1b ~]# iqt -p NodeInfo nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables A0188.078 site2-cmp-1b site2-cmp-1b,10.250.84.26 Active Unspecified PcmmSession,PcmmSessionPhysT A0188.129 site2-cmp-1a site2-cmp-1a,10.250.84.25 Active Unspecified PcmmSession,PcmmSessionPhysT A1041.147 slak-g6-cmp-1a slak-g6-cmp-1a,10.240.239.37 Active Unspecified PcmmSession,PcmmSessionPhysT A1041.203 slak-g6-cmp-1b slak-g6-cmp-1b,10.240.239.38 Active Unspecified PcmmSession,PcmmSessionPhysT C1213.145 slak-g6-mpe-1a slak-g6-mpe-1a,10.240.239.24 Active Unspecified PcmmSession,PcmmSessionPhysT C1213.230 slak-g6-mpe-1b slak-g6-mpe-1b,10.240.239.25 Active Unspecified PcmmSession,PcmmSessionPhysT C2563.007 slak-g6-mra-1a slak-g6-mra-1a,10.240.239.22 Active Unspecified PcmmSession,PcmmSessionPhysT C2563.151 slak-g6-mra-1b slak-g6-mra-1b,10.240.239.23 Active Unspecified PcmmSession,PcmmSessionPhysT [root@slak-g6-cmp-1b ~]#
2. ☐	**CLI:** Cleanup upgrade - to remove all Exclusions in NodeInfo table Note: This step allows the Table Exclusions to be automatically cleared from all servers including the Secondary Active CMP server by the Primary Active CMP existing topology configuration and notifies those servers to start processing further updates to these tables	# policyUpgrade.pl –cleanupUpgrade # iqt -p NodeInfo [root@slak-g6-cmp-1a ~]# iqt -p NodeInfo nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables A0188.078 site2-cmp-1b site2-cmp-1b,10.250.84.26 Active Unspecified A0188.129 site2-cmp-1a site2-cmp-1a,10.250.84.25 Active Unspecified A1041.147 slak-g6-cmp-1a slak-g6-cmp-1a,10.240.239.37 Active Unspecified A1041.203 slak-g6-cmp-1b slak-g6-cmp-1b,10.240.239.38 Active Unspecified C1213.145 slak-g6-mpe-1a slak-g6-mpe-1a,10.240.239.24 Active Unspecified C1213.230 slak-g6-mpe-1b slak-g6-mpe-1b,10.240.239.25 Active Unspecified C2563.007 slak-g6-mra-1a slak-g6-mra-1a,10.240.239.22 Active Unspecified C2563.151 slak-g6-mra-1b slak-g6-mra-1b,10.240.239.23 Active Unspecified [root@slak-g6-cmp-1a ~]#
THIS PROCEDURE HAS BEEN COMPLETED		

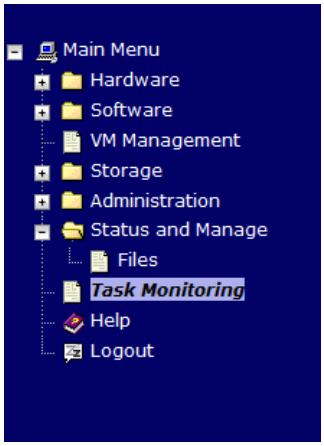
9. APPENDIX

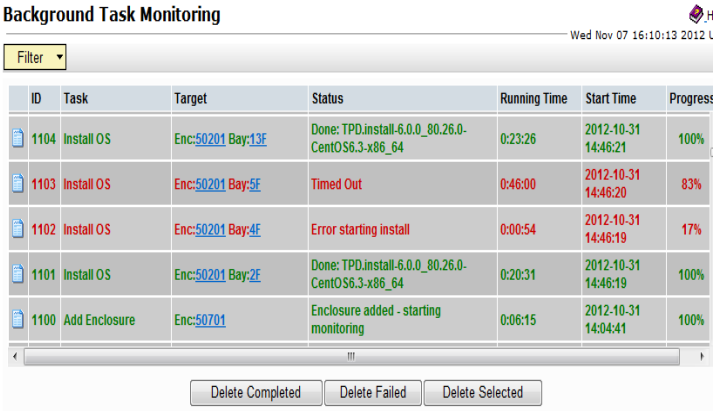
APPENDIX A. TVOE AND PM&C SERVER UPGRADE

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

STEP #		
	NOTE: This procedure (TVOE Upgrade) can be executed either during the same maintenance window as the PM&C Upgrade Procedure or in the separate maintenance window. Please also note that the PM&C upgrade must be upgraded after the TVOE host has been upgraded • TVOE Pre-Upgrade Validation • Pre-Upgrade Backup • Add TVOE software image to TVOE host • Add PM&C Upgrade Software to PM&C Server • Stand Alone TVOE host upgrade • TVOE Post-Upgrade Validation • PM&C upgrade • Stand Alone TVOE Upgrade Accept • PM&C Upgrade Accept **CAUTION:** Do not accept TVOE upgrade until after PM&C upgrade acceptance for the following reasons: - Older PM&C releases, i.e. release 5.5 or less, can't be deployed on upgraded TVOE 2.7.x system. - If an issue occurs during PM&C upgrade it may require disaster recovery for which TVOE upgrade will have to be rejected to allow re-deployment of PM&C 5.7. A reject cannot be performed after an upgrade has been accepted so Accept Upgrade with care following stepwise instructions. **Note: Make sure that the hardware is fault-free. TVOE upgrade won't succeed otherwise!**	
1. ☐		**NOTE:** Upgrade of TVOE host will shutdown all guest OSes – PM&(including PM&C) during the upgrade. Prior to the upgrading of TVOE host, ensure the PM&C server is shutdown.

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

<table>
<tr>
<td>2.
☐</td>
<td>Check and shutdown any in-progress task(s) on PM&C</td>
<td>On a supported web browser like Firefox, login to PM&C GUI as pmacadmin and navigate to Task Monitoring:


Verify all tasks are complete indicated by green 100% Progress
NOTE: If any task shows in-progress (blue or red) then wait for the task to complete prior to continuing the next step.


<table>
<tr><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr>
<tr><td>1104</td><td>Install OS</td><td>Enc:50201 Bay:13F</td><td>Done: TPD.install-6.0.0_80.26.0-CentOS6.3-x86_64</td><td>0:23:26</td><td>2012-10-31 14:46:21</td><td>100%</td></tr>
<tr><td>1103</td><td>Install OS</td><td>Enc:50201 Bay:5F</td><td>Timed Out</td><td>0:46:00</td><td>2012-10-31 14:46:20</td><td>83%</td></tr>
<tr><td>1102</td><td>Install OS</td><td>Enc:50201 Bay:4F</td><td>Error starting install</td><td>0:00:54</td><td>2012-10-31 14:46:19</td><td>17%</td></tr>
<tr><td>1101</td><td>Install OS</td><td>Enc:50201 Bay:2F</td><td>Done: TPD.install-6.0.0_80.26.0-CentOS6.3-x86_64</td><td>0:20:31</td><td>2012-10-31 14:46:19</td><td>100%</td></tr>
<tr><td>1100</td><td>Add Enclosure</td><td>Enc:50701</td><td>Enclosure added - starting monitoring</td><td>0:06:15</td><td>2012-10-31 14:04:41</td><td>100%</td></tr>
</table>
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>Shutdown PM&C</td>
<td>NOTE: Assuming all tasks are completed (previous step), it is now safe to shutdown PM&C server.
Logon to PM&C CLI as root user
Execute the following command
[root@pmac ~]# halt -p

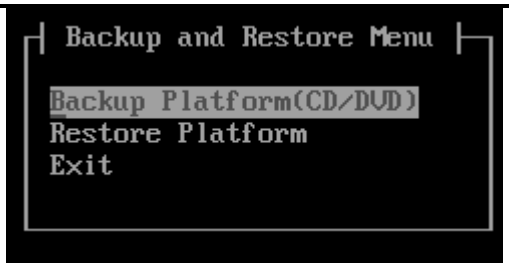
Broadcast message from root@pmac
(/dev/ttyS0) at 11:20 ...

The system is going down for power off NOW!</td>
</tr>
</table>

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

4. ☐	Verify PM&C guest is shutdown	Logon to the TVOE Host Real IP as root user. From TVOE host console execute the following command: [root@tvoe ~]# virsh list - -all Id Name State ---------- - pmac shut off **NOTE:** This should show PM&C guest state as "shut off"
5. ☐	Perform TVOE Pre-upgrade backup	• Login (SSH) to TVOE iLo IP as Administrator user (this is the iLO user account login) and issue following command: </>hpiLO-> vsp login as: Administrator Administrator@10.253.101.140's password: User:Administrator logged-in to ILOUSE925N3ZB.nc.tekelec.com(10.253.101.140) iLO 2 Advanced 2.20 at 12:45:22 May 08 2013 Server Name: wee-tvoe-host Server Power: On </>hpiLO-> vsp Starting virtual serial port. Press 'ESC (' to return to the CLI Session. </>hpiLO-> Virtual Serial Port active: IO=0x03F8 INT=4 [root@wee-tvoe-host ~]# Login as root user (if required!):su - brbgpmac-tvoe login: root Password: Last login: Fri Feb 21 10:56:38 on tty1 [root@brbgpmac-tvoe ~]# • Execute platcfg utility [root@tvoe ~]# su – platcfg Navigate to the following: **Maintenance→Backup and Restore→Backup Platform (CD/DVD)**

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

		 Note: You can click through the warning window as needed • Select **Build ISO file only** option; "*Setting up Staging Area*" and "*Building image…Please wait*" may apear. This step is deemed to take a mere few seconds. The ISO backup file is successfully created by now and saved in /var/TKLC/bkp/ directory. [root@wee-tvoe-host ~]# ls –lrt /var/TKLC/bkp total 56824 -rw-rw----. 1 root platcfg 58185728 Nov 5 10:51 wee-tvoe-host-plat-app-201411051051.iso • Platcfg returns to the Backup TekServer Menu; Select **Exit** until you are out of *platcfg* menu.
6. ☐	Download the new TVOE software to the TVOE host	• Login to TVOE host Real IP CLI as root user. • Verify there is enough space for TVOE software image – 1GB is enough. # df -h /var/TKLC/upgrade/ • Copy the new TVOE ISO image file to the /var/TKLC/upgrade/ director and verify the md5sum #ls /var/TKLC/upgrade [root@weepmac repository]# ls -l /var/TKLC/upgrade/ total 732920 -r-xr-xr-x 1 pmacd pmacd 750505984 Nov 7 12:20 TVOE-2.7.0.0.0_84.20.0-x86_64.iso [root@weepmac repository]# [root@weepmac repository]# [root@weepmac repository]# df -h /var/TKLC/upgrade/ Filesystem Size Used Avail Use% Mounted on /dev/mapper/vgroot-plat_var_tklc 4.0G 901M 2.9G 24% /var/TKLC [root@weepmac repository]#

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

7. ☐

Start TVOE upgrade

NOTE: The upgrade process takes upto 25 minutes

- Execute platcfg utility

#su – platcfg

Platcfg menu: **Maintenance→upgrade→validate upgrade→ Select the new TVOE ISO filename**:

```
#####################################################################
#####################################################################
#####################################################################
#####################################################################
#####################################################################
#####################################################################
#####################################################################
#####################
UMVT Validate Utility v2.3.4, (c)Tekelec, May 2014
Validating /var/TKLC/upgrade/TVOE-2.7.0.0.0_84.20.0-x86_64.iso
Date&Time: 2014-11-10 20:26:06
Volume ID: 2.7.0.0.0_84.20.0
Part Number: N/A
Version: 2.7.0.0.0_84.20.0
Disc Label: TVOE
Disc description: TVOE
The media validation is complete, the result is: PASS

CDROM is Valid



PRESS ANY KEY TO RETURN TO THE PLATCFG MENU.
```

If the result is '**PASS**', proceed ahead, press any key and then **exit** to the **upgrade** window

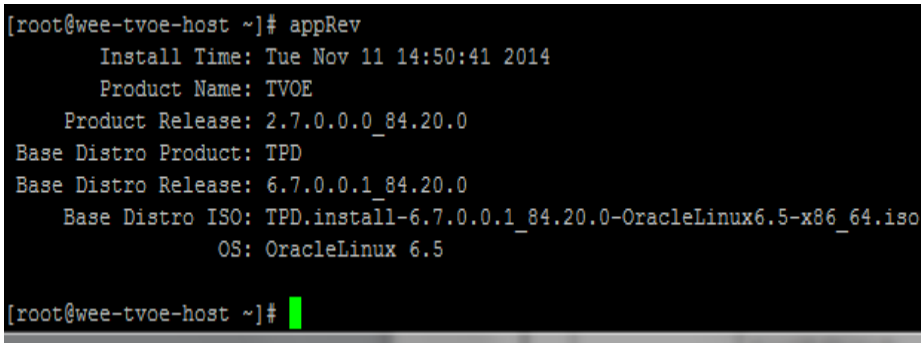
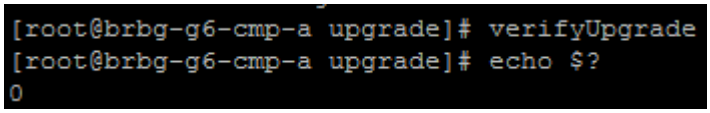
Platcfg menu: **Maintenance→upgrade→initiate upgrade→Select the new TVOE iso filename.**

```
Choose Upgrade Media Menu

TVOE-2.7.0.0.0_84.20.0-x86_64.iso        - 2.7.0.0.0_84.20.0
Exit
```

NOTE: TVOE host will be rebooted by the end of the upgrade process and will return to the login prompt, marking the completion of upgrade.

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

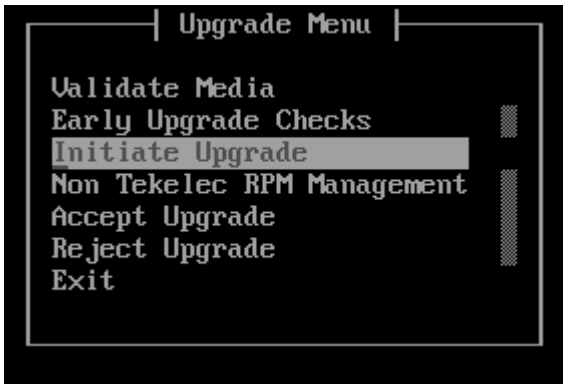
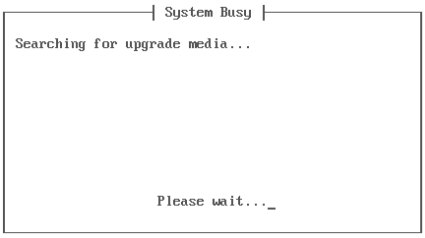
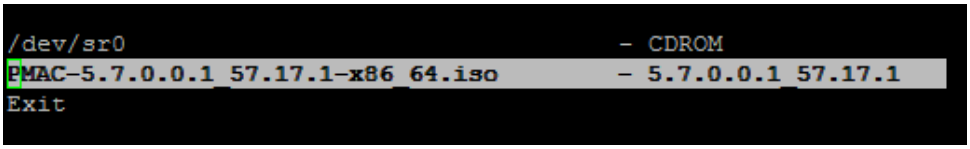
8. ☐	Verify the Upgrade status	• Login again as root to TVOE • Verify the upgraded TVOE revision # appRev  [root@wee-tvoe-host ~]# appRev Install Time: Tue Nov 11 14:50:41 2014 Product Name: TVOE Product Release: 2.7.0.0.0_84.20.0 Base Distro Product: TPD Base Distro Release: 6.7.0.0.1_84.20.0 Base Distro ISO: TPD.install-6.7.0.0.1_84.20.0-OracleLinux6.5-x86_64.iso OS: OracleLinux 6.5 [root@wee-tvoe-host ~]# # verifyUpgrade After verifyUpgrade execute echo $? and the result should be “0” as in the following snapshot:  [root@brbg-g6-cmp-a upgrade]# verifyUpgrade [root@brbg-g6-cmp-a upgrade]# echo $? 0
9.	**Cautionary Note**	DON’T accept TVOE upgrade unless PMAC upgrade has been accepted.

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

10. ☐	Start PM&C guest	If not already logged in to TVOE HOST as root, do so. Using virsh utility on TVOE host, start the PM&C guest if not already started. Query the list of guests until the PM&C guest is "running". **# /usr/bin/virsh list --all** Id Name State ---------- 20 pmac shut off If not running, issue the following command. **# /usr/bin/virsh start<pmac>** Domain pmac started **# /usr/bin/virsh list --all** Id Name State ---------- 20 pmac running
11. ☐	Do not remove the TVOE iso image file at this time	Once the TVOE and the PM&C upgrade have both been accepted the TVOE image file may be removed to clear up disk psace. Important Note: If the TVOER image fiole is removed before the TVOE and PM&C upgrades have been accepted a rololback of the TVOE install will fail as any changes to the disk prior to rollback may invalidate the rollback snapshot.
12. ☐	Proceed with PM&C upgrade	The following procedure beginning with step #1 Will upgrade the PM&C

1. ☐	Preparing PM&C application media	As root on TVOE Host, execute the following to list the PM&C server information #virsh list Id Name State ---------- 1 weepmac running Login to the PM&C Server guest as root by issuing the following command from the TVOE host CLI : #virsh console <pmac> [root@wee-tvoe-host ~]# virsh console weepmac Connected to domain weepmac Escape character is ^] CentOS release 6.5 (Final) Kernel 2.6.32-431.29.2.el6prerel6.5.2_82.37.0.x86_64 on an x86_64 weepmac login: root Password: Last login: Wed Nov 12 12:09:39 from 10.240.239.126 [root@weepmac ~]# Verify the correct ISO file is located in the **/var/TKLC/upgrade** directory. If not, copy PMAC ISO to **/var/TKC/upgrade** using PM&C server's REAL IP. Verify by issuing the following command: #ls –lth /var/TKLC/upgrade ***Validate the upgrade MEDIA:*** From the PM&C Server as *root*, execute: [root@pmac ~]# su – platcfg Navigate to **Maintenance→upgrade→validate media** Select the correct media and click **OK** Make sure validating media result is '**PASS'.** Press any key return to the platcfg menu.

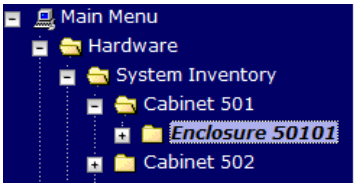
Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

2. ☐	Close any active browser sessions to PM&C	If any open browsers connected to PM&C, close them before proceeding
3. ☐	Entering platcfg menu	From PM&C Server as root, execute the following [root@pmac ~]# su – platcfg
4. ☐	Initiating PM&C upgrade	**Maintenance→upgrade→initiate upgrade**  • Select "**Initiate Upgrade**" to start the upgrade process **NOTE:** The screen displayed below indicates that "platcfg" utility searches for available upgrade media  • Wait for "Choose Upgrade Media Menu" screen to display before proceeding to the next step  • Select the new PM&C 5.7 target iso filename and press the [ENTER] key to start the upgrade process

Description: This procedure will upgrade underlying TVOE host to version 2.7. TVOE host 2.7 is the minimum requirement for PM&C 5.7. To recap, Policy release 11.5 requires PM&C server to be operated at version 5.7, before the other policy components are upgraded!

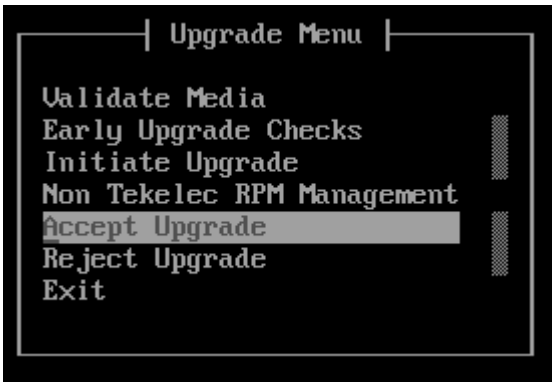
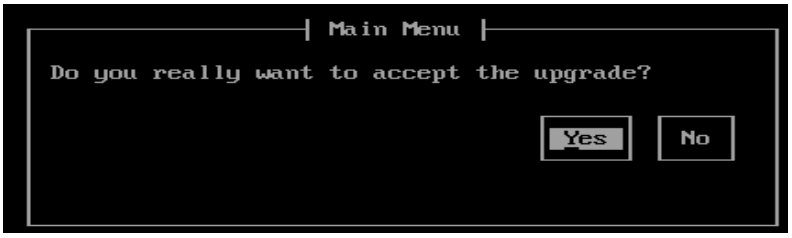
5. ☐	Monitoring the Upgrade process
	
	NOTE: Upgrade process takes up to 20 minutes to complete
		NOTE: The following display output is for illustrative purposes only. Screen similar to the one below is displayed as the upgrade progresses…..
		
		`Running earlyUpgradeChecks() for Upgrade::EarlyPolicy::PMAC upgrade policy...`
		`This is an upgrade of PMAC.`
		`Check for IN-PROGRESS BG Tasks.`
		`No IN-PROGRESS BG Tasks found, we can upgrade.`
		`Running earlyUpgradeChecks() for Upgrade::EarlyPolicy::TPDEarlyChecks upgrade policy...`
		`Verified server is not pending accept of previous upgrade`
		`Hardware architectures match`
		`Install products match.`
		`Verified server is alarm free!`
		`Early Upgrade Checks Have Passed!`
		`Initializing upgrade information...`
		`Shutting down PMAC services: The runlevel transition complete RC file was created as /et`
		`Changing to run-level 3...`
		`**********`
		`* Waiting for run level 3 transistion to finish *`
		`**********`
		`waiting for /etc/rc3.d/S99local_runlevel_transition_complete to disappear.`
		`waiting for /etc/rc3.d/S99local_runlevel_transition_complete to disappear.`
		`waiting for /etc/rc3.d/S99local_runlevel_transition_complete to disappear.`
		`waiting for /etc/rc3.d/S99local_runlevel_transition_complete to disappear.`
		`sending kill command...`
		`please wait up to 60 seconds`
		`waiting for /etc/rc3.d/S99local_runlevel_transition_complete to disappear.`
		`waiting for /etc/rc3.d/S99local_runlevel_transition_complete to disappear.`
		
		The screen shown below will be displayed, if the upgrade completes successfully:
		
		`UPGRADE IS COMPLETE`
		
		`Upgrade command returned success!`
		`Running postUpgrade() for Upgrade::Policy::Platform upgrade policy...`
		`Restarting alarmMgr.`

S T E P #	This procedure provides instructions to verify success of the PM&C upgrade and perform other required post upgrade steps Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.	
1. ☐	Accessing PM&C guest console NOTE: Starting PM&C 5.7, direct SSH login as user root is not permitted, but as admusr.	• Logon to TVOE HOST SSH as root • Verify pmac console is running by issuing the following command #virsh list Id Name State ---------- 1 weepmac running Login to pmac guest console: #virsh console <NAME> Login to the PM&C as ***admusr*** user, then switch to the ***root*** user ¦==========¦ ¦ This system has been upgraded but the upgrade has not yet ¦ ¦ been accepted or rejected. Please accept or reject the ¦ ¦ upgrade soon. ¦ ¦==========¦ [admusr@pmac ~]$ su – root Password:********* ***Informational Note:***To break the guest session to go back to the TVOE Host, enter <ctrl> right bracket
2. ☐	Verify that date/timestamp of the upgrade log aligns with the time of the upgrade	• Execute the following command #ls -l /var/TKLC/log/upgrade/upgrade.log -rw-rw-r-- 1 platcfg root 116198 Nov 12 14:16 upgrade.log
3. ☐	Verify that the release version has been updated	• Execute the following command # appRev [root@weepmac ~]# [root@weepmac ~]# [root@weepmac ~]# appRev Install Time: Wed Nov 12 13:21:43 2014 Product Name: PMAC Product Release: 5.7.0.0.1_57.17.1 Base Distro Product: TPD Base Distro Release: 6.7.0.0.1_84.20.0 Base Distro ISO: TPD.install-6.7.0.0.1_84.20.0-OracleLinux6.5-x86_64.iso OS: OracleLinux 6.5 [root@weepmac ~]# _

4. ☐	Verify successful completion through the upgrade log	• Execute the following commands on PM&C `# grep COMPLETE /var/TKLC/log/upgrade/upgrade.log` **1415816327:: UPGRADE IS COMPLETE**
5.	Restarting network service	• Execute: `# service network restart` *Note that this step is necessary as a workaround to a bug in TVOE 2.7; this bug was fixed in later releases!*
6. ☐	Clear browser cache	• Clear browser cache to ensure that browser has the latest client-side code loaded. Refer to browser documentation if necessary.
7. ☐	Login to PM&C GUI	• Open web browser and enter: https://<PM&C Management Network IP address> • Login with pmacadmin credentials
8. ☐	Verify System Inventory looks correct in PM&C GUI	• Select the System Inventory node and verify the previously provisioned enclosures are present **NOTE:** The hardware discovery may take some time to complete. The screen capture below assumes the discovery is complete for all enclosures. 

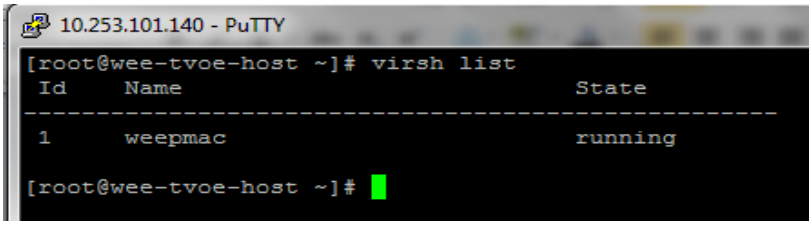
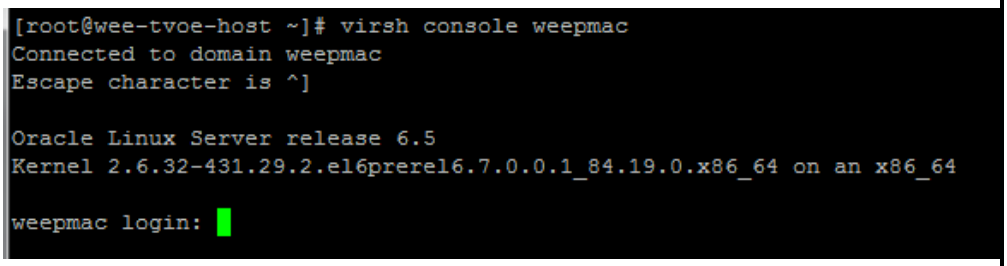
9. ☐	Verify Software Inventory looks correct in PM&C GUI	**PM&C GUI:** Software→ Software Inventory page • Verify all servers are listed and details are filled in (assuming TPD or TVOE is installed on the server) The TVOE and PM&C Server will be listed at the bottom and the APP version column will show pending accept/reject until either one is performed.

10. ☐	**PM&C SSH CLI:** Recreate the ssh_service with admusr creadentials on PM&C guest console	• Delete ssh_service -
		
		# netConfig --repo deleteService name=ssh_service
		If SSH service created already, this command will delete that service and if not, then it will throw an error as show below:
		
		`[root@weepmac ~]# netConfig --repo deleteService name=ssh_service`
		`Service with name ssh_service does not exist.`
		
		• Recreate ssh_service with root user -
		
		# netConfig --repo addService name=ssh_service
		Service type? (tftp, ssh, conserver, oa) ssh
		Service host? <pm&c_mgmtVLAN_ip_address>
		Enter an option name (q to cancel): user
		Enter a value for user: root
		Enter an option name(q to cancel): password
		Enter a value for password: Y-tW******
		Enter an option name(q to cancel): q
		
		`[root@weepmac ~]# netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa)ssh`
		`Service host? 10.240.239.68`
		`Enter an option name <q to cancel>: user`
		`Enter the value for user: admusr`
		`Enter an option name <q to cancel>: password`
		`Enter the value for password:`
		`Verify password:`
		`Enter an option name <q to cancel>: q`
		`Add service for ssh_service successful`
		`[root@weepmac ~]#`
		`[root@weepmac ~]#`
		`[root@weepmac ~]#`
		
		• Ensure the information entered is correct by executing the following command and compare the output with the configuration in the last step -
		
		# netConfig --repo showService name=ssh_service
		`[root@weepmac ~]# netConfig --repo showService name=ssh_service`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 10.240.239.68`
		`Options:`
		`password: C81F6E60ECC2E4F5`
		`user: admusr`
		`[root@weepmac ~]#`

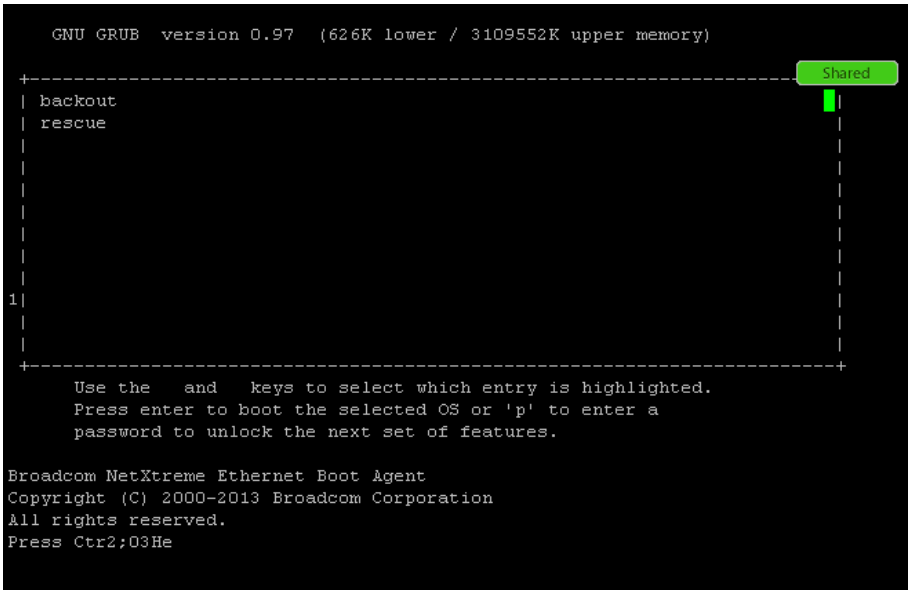
11. ☐	Check!	**If ALL Health checks passed, accept PM&C server and TVOE upgrades.** **If Health Checks do not pass or a backout is needed, skip to Appendix B to reject/backout the Upgrade in entirety. This will include both the PM&C server and the TVOE HOST.**
12. ☐	Accept the upgrade for PM&C	• Logon to PM&C guest console • Run the platcfg utility – # su – platcfg PM&C GUI: **Maintenance→Upgrade→Accept Upgrade**  • Select "Accept Upgrade" and press the [ENTER] key  • Select 'Yes' to start accept upgrade process. This take should take mere few seconds.
13. ☐	Accept the upgrade for TVOE.	Login as root to TVOE HOST CLI and execute the following command: # /var/TKLC/backout/accept This '***accept'*** command will take mere few seconds to complete.

14. ☐	Monitoring "Accept Upgrade" process	**NOTE:** The following image is only for illustrative purposes Called with options: --accept Loading Upgrade::Backout::LVM Accepting Upgrade snapmgr: Logical volume "smac_root_snap" successfully removed snapmgr: Logical volume "smac_var_snap" successfully removed snapmgr: Logical volume "plat_usr_snap" successfully removed snapmgr: Logical volume "smac_backup_snap" successfully removed snapmgr: Logical volume "plat_root_snap" successfully removed snapmgr: Logical volume "plat_var_tklc_snap" successfully removed snapmgr: Logical volume "plat_var_snap" successfully removed snapmgr: Removed snapshot lv's related to tag "@upgrade" Executing common accept tasks Setting POST_UPGRADE_ACTION to ACCEPT in upgrade info. Cleaning backout directory. Clearing Upgrade Accept/Reject alarm. Cleaning message from MOTD. Cleaning up RPM config backup files... Checking / Checking /boot Checking /tmp Checking /usr Checking /var Checking /var/TKLC Checking /usr/TKLC/smac

TVOE AND PM&C SERVER BACKOUT

S T E P #	This procedure provides instructions to backout/reject the PM&C server upgrade. **NOTE: Upgrade 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.	
1. ☐	Close any active browser sessions of PM&C	Close any open browsers connected to PM&C before proceeding.
2. ☐	If necessary, access PM&C guest console	• Logon to TVOE iLo HOST SSH as Administrator • Verify PM&C console is running by issuing the following command #virsh list  Login to PM&C guest console by issuing the following command #virsh console <NAME>  Logon to pmac as root if needed – may not require a login. Last login: Wed Jun 6 08:39:14 on ttyS0 |==========| | This system has been upgraded but the upgrade has not yet | | been accepted or rejected. Please accept or reject the | | upgrade soon. | |========== [admusr@pmac ~]$ **NOTE: To break the guest session to go back to TVOE Host, enter <ctrl> right bracket.**

3. ☐	Run "platcfg" utility on the PM&C Server	At the prompt execute: # su – platcfg Navigate to **Maintenance→Upgrade** Upgrade Menu Validate Media Early Upgrade Checks Initiate Upgrade Non Tekelec RPM Management Accept Upgrade Reject Upgrade Exit Select "Reject Upgrade" and press the [ENTER] key to start the reject process. The following window will pop up; enter yes to begin the backout. Main Menu Do you really want to reject the upgrade? Yes No **NOTE**: 5 minutes into the backout, a reboot will be required.
4. ☐	Backout requires reboot	The following image is only for illustrative purposes Message The reject has completed. The system will now be rebooted. Press any key to continue... **NOTE:** From this point on, it will take 25 minutes to complete the backout
5. ☐	Wait for PM&C login prompt	Upon successful completion of backout, the user should be returned to a login prompt. Login as root.

6. ☐	Verify backout completed	Execute the following command to verify source PM&C release : [root@pmac ~]# appRev Output should reflect older release! If correct Product Release is not displayed, contact Tekelec Customer Service and do not proceed until instructed by a Tekelec Customer Care representative.
7.	TVOE iLo SSH	As root on the TVOE CLI – logged in through the iLO execute the following command to check the logical drives that will be used for thebackout. #/sbin/lvs -o lv_name,snap_percent @upgrade *Typical* output: **LV Snap%** **plat_root_snap 27.52** **plat_usr_snap 7.70** **plat_var_snap 5.08** **plat_var_tklc_snap 19.14**
8.	**TVOE Server iLO:** **manually backout upgrade**	Initiate the backout by running the following command: # /var/TKLC/backout/reject --noprompt **[↵](carriage return)** The system will undergo a backout. As part of the process the system will reboot several times. On reboot you may be prompted to select backout or rescue. Use the up/down arrow on the keyboard to choose backout.  After completing the final reboot the login prompt will be presented. Some of the final startup output will reflect older TVOE release numbers.

9.	**TVOE Server iLO:** **check server health**	Execute: # appRev # /usr/TKLC/plat/bin/alarmMgr --alarmStatus [↵] If any output is produced, an alarm is present on the system. Contact Oracle for information about how to proceed.
10. ☐	Clear browser cache	Clear browser cache to ensure that browser has the latest client-side code loaded. Refer to browser documentation if necessary.
11.	Browsing PM&C GUI	It might be necessary to restart network service on PM&C server before browsing PM&C GUI: # service network restart PM&C GUI could be opened now!

APPENDIX B. COPY UPGRADE ISOS FROM USB DRIVE

Copy ISO images to Policy Management & Configuration Server (PM&C)		
Step	**Procedure**	**Result**
1. ☐	**USB drive specification**	• Minimum of 8 GB size • Formatted with FAT-32 file system for broader compatibility with various Operating Systems
2. ☐	**Copy ISO files into USB drive**	• Perform and validate the server ISO files have been transferred successfully into the USB drive

Copy ISO images to Policy Management & Configuration Server (PM&C)		
Step	**Procedure**	**Result**
3. ☐	**Determining USB drive Device-id**	• SSH CLI into TVoE (Host of PM&C server) control IP address • Insert the USB drive to any available USB slot on this server • There are 2 methods of performing the following steps - **Either:** # cd /var/log # tail –f messages 1) Monitor the 'tail' outputs and look for the following to determine the USB device-id highlighted below - Mar 7 11:19:03 localhost kernel: usb 1-1.3: new high speed USB device number 7 using ehci_hcd Mar 7 11:19:03 localhost kernel: usb 1-1.3: New USB device found, idVendor=0781, idProduct=5530 Mar 7 11:19:03 localhost kernel: usb 1-1.3: New USB device strings: Mfr=1, Product=2, SerialNumber=3 Mar 7 11:19:03 localhost kernel: scsi5 : SCSI emulation for USB Mass Storage devices Mar 7 11:19:04 localhost kernel: sd 5:0:0:0: Attached scsi generic sg3 type 0 Mar 7 11:19:04 localhost kernel: sd 5:0:0:0: [sdb] 15633408 512-byte logical blocks: (8.00 GB/7.45 GiB) Mar 7 11:19:04 localhost kernel: sd 5:0:0:0: [sdb] Write Protect is off Mar 7 11:19:04 localhost kernel: sd 5:0:0:0: [sdb] Assuming drive cache: write through ***Mar 7 11:19:04 localhost kernel: sdb: sdb1*** ***OR:*** # **lsblk** NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT sda 8:0 0 838.3G 0 disk |-sda1 8:1 0 256M 0 part /boot |-sda2 8:2 0 819.1G 0 part ... |-vgroot-plat_usr (dm-3) 253:3 0 3G 0 lvm /usr |-vgroot-plat_tmp (dm-4) 253:4 0 1G 0 lvm /tmp `-vgroot-plat_var_tklc (dm-5) 253:5 0 3G 0 lvm /var/TKLC sdb 8:16 1 7.5G 0 disk ***-sdb1 8:17 1 7.5G 0 part /media/sdb1*** • To confirm the new device-id on this server – Filesystem Size Used Avail Use% Mounted on /dev/mapper/vgroot-plat_root 756M 434M 285M 61% /tmpfs ***/dev/sdb1 7.5G 3.0G 4.6G 40% /media/sdb1***

Copy ISO images to Policy Management & Configuration Server (PM&C)		
Step	**Procedure**	**Result**
4. ☐	**Copy ISO files to PM&C server**	• SSH CLI into TVoE (Host of PM&C server) control IP address again, if previously logged out • Create a new directory and call it 'test' as example • Mount USB directory /dev/sdb1 to the directory 'test' # cd / # mkdir test # mount /dev/sdb1 test # ls –la total 24 drwxrwxr-x. 3 root admgrp 4096 Mar 7 11:31 . dr-xr-xr-x. 16 root root 4096 Nov 24 19:50 .. ***drwxr-xr-x. 2 root root 16384 Feb 31 1969 test*** • Determine the mounted directory and check on the ISO files as in the example - # cd test [test]# ls –la total 3067300 drwxr-xr-x. 2 root root 16384 Feb 27 19:69 . drwxrwxr-x. 3 root admgrp 4096 Mar 7 11:31 .. -rwxr-xr-x. 1 root root 1170579456 Mar 7 09:58 **cmp-11.5.0.0.0_27.1.0-x86_64.iso** -rwxr-xr-x. 1 root root 999618560 Mar 7 09:58 **mpe-11.5.0.0.0_27.1.0-x86_64.iso** -rwxr-xr-x. 1 root root 970686464 Mar 7 10:10 **mra-11.5.0.0.0_27.1.0-x86_64.iso** • Perform SCP file transfer to PM&C server – [test]# scp -p *.iso <PM&C server control IP address>:/var/TKLC/upgrade Password: < *enter the password* > 872-2750-101-11.5_2.7.0-cmp-x86_64.iso 100% 1116MB 21.1MB/s 00:53 872-2752-101-11.5_2.7.0-mpe-li-x86_64.iso 100% 953MB 21.2MB/s 00:45 872-2754-101-11.5_2.7.0-mra-x86_64.iso 100% 926MB 21.0MB/s 00:44 • Logout the session

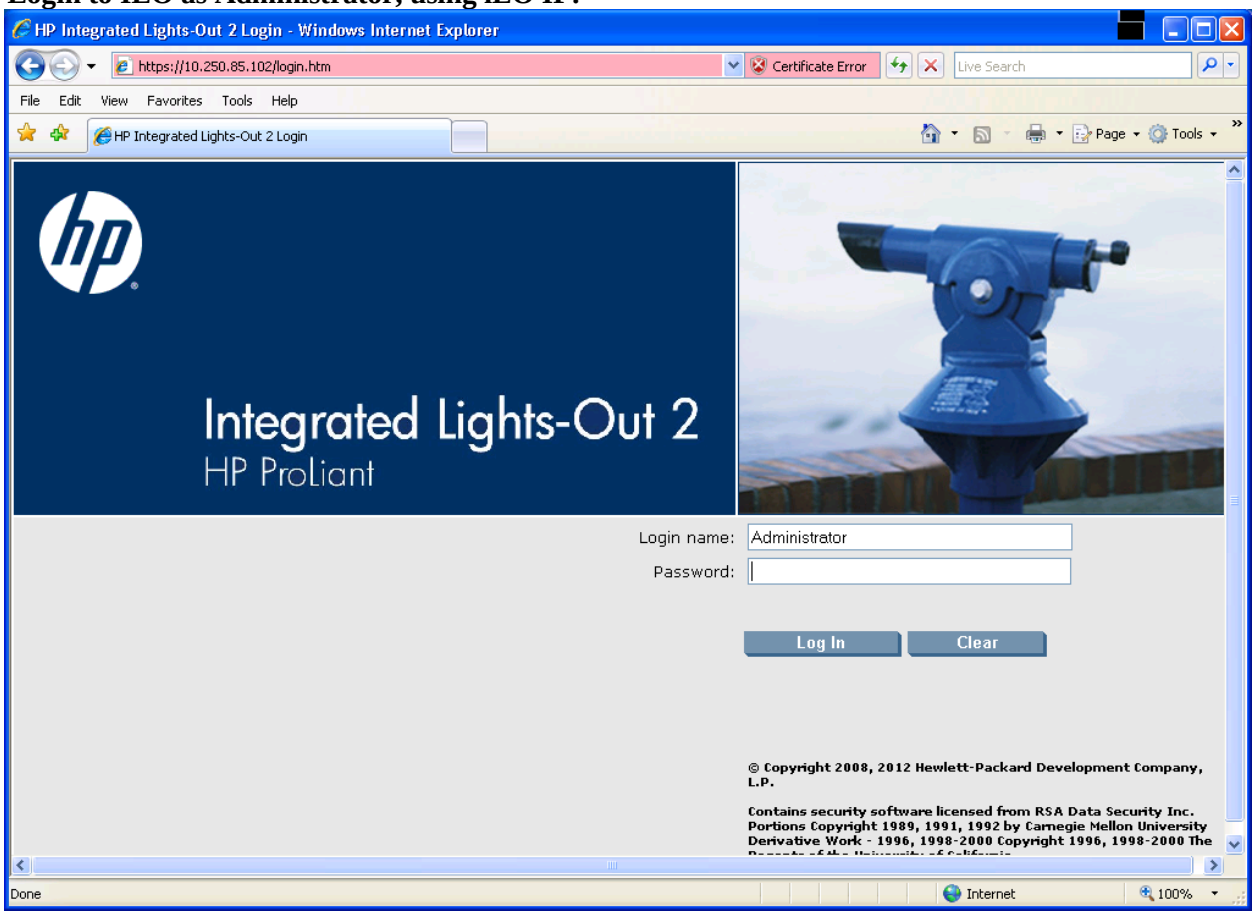
Copy ISO images to Policy Management & Configuration Server (PM&C)		
Step	**Procedure**	**Result**
5. ☐	**Validate the ISO files in PM&C server**	• SSH CLI into PM&C server control IP address and perform the following commands – # cd /var/TKLC/upgrade # ls –la total 3898852 drwxrwxr-x. 2 root admgrp 4096 Mar 7 12:05 . dr-xr-xr-x. 20 root root 4096 Feb 9 17:52 .. -rwxr-xr-x 1 root root 1170579456 Mar 7 09:58 872-2750-101-11.5_2.7.0-cmp-x86_64.iso -rwxr-xr-x 1 root root 999618560 Mar 7 09:58 872-2752-101-11.5_2.7.0-mpe-li-x86_64.iso -rwxr-xr-x 1 root root 970686464 Mar 7 10:10 872-2754-101-11.5_2.7.0-mra-x86_64.iso
6. ☐	**Unmount and remove the USB drive**	• SSH CLI into TVoE (Host of PM&C server) control IP address again and perform the following – # cd / # umount /test # rmdir test # ls -la total 8 drwxrwxr-x. 2 root admgrp 4096 Mar 7 11:37 . dr-xr-xr-x. 16 root root 4096 Nov 24 19:50 .. • Logout the session

APPENDIX C. USING ILO TO REMOTELY ACCESS A SERVER

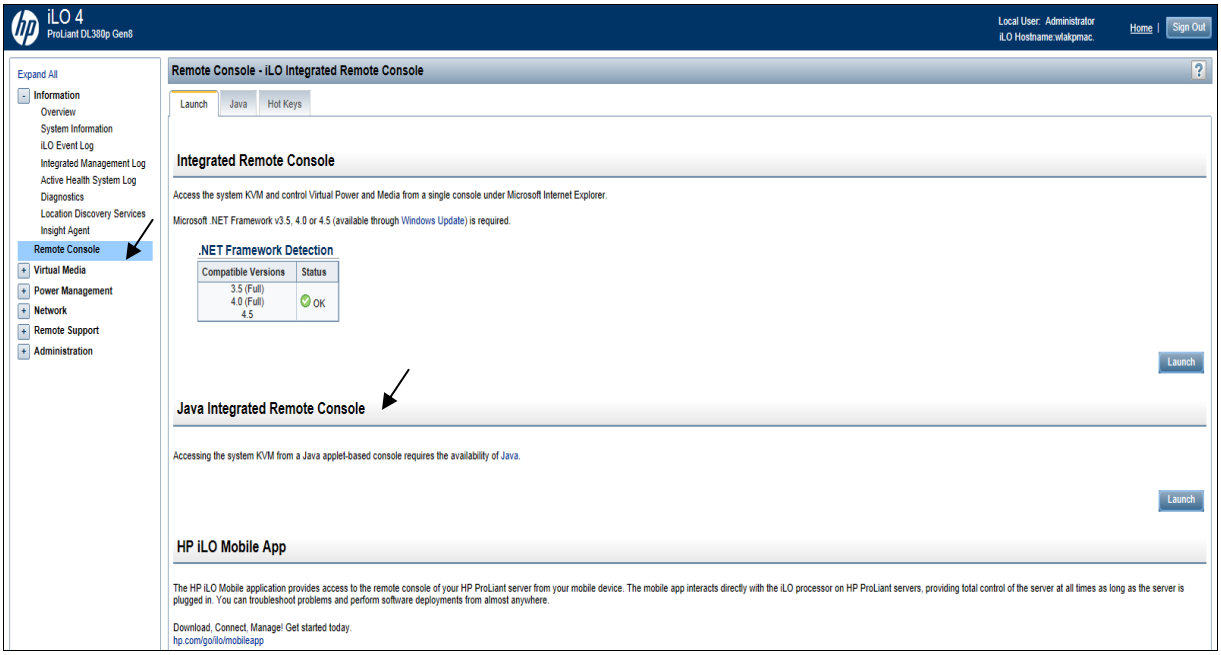
The "Remote Console" access option of the iLO can be used to get console access to the server. This has the following benefits:

- User can track the server's activity under all circumstances, even when the server is booting.
- The "Remote Console" access can also be used in case the server IP interfaces are down and the server state is unknown.
- From this interface it is also possible to mount an ISO located on your computer to the server using the iLO "Virtual Mount utility".
- One can also remotely boot the server if needed.

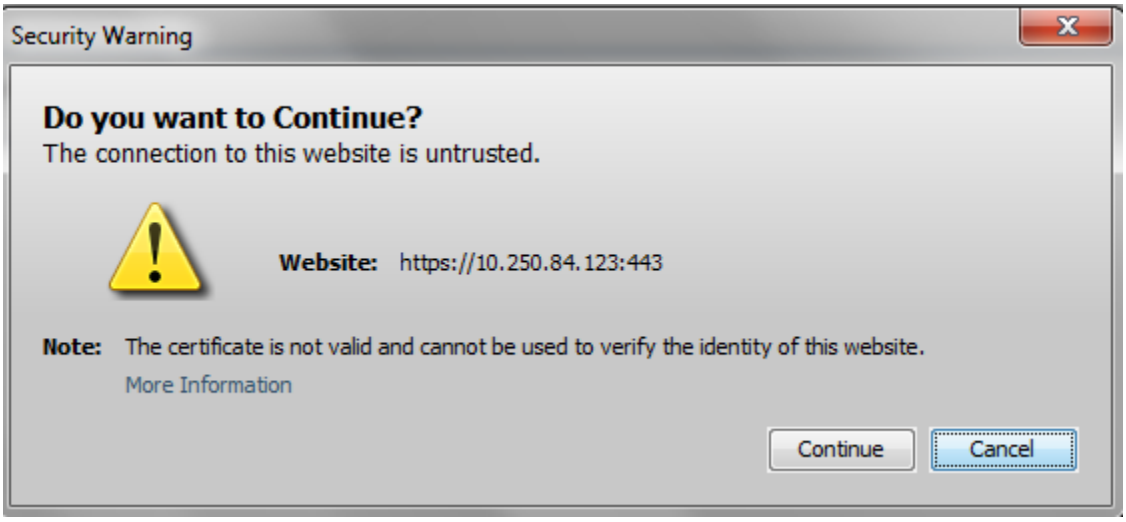
Login to ILO as Administrator, using iLO IP:



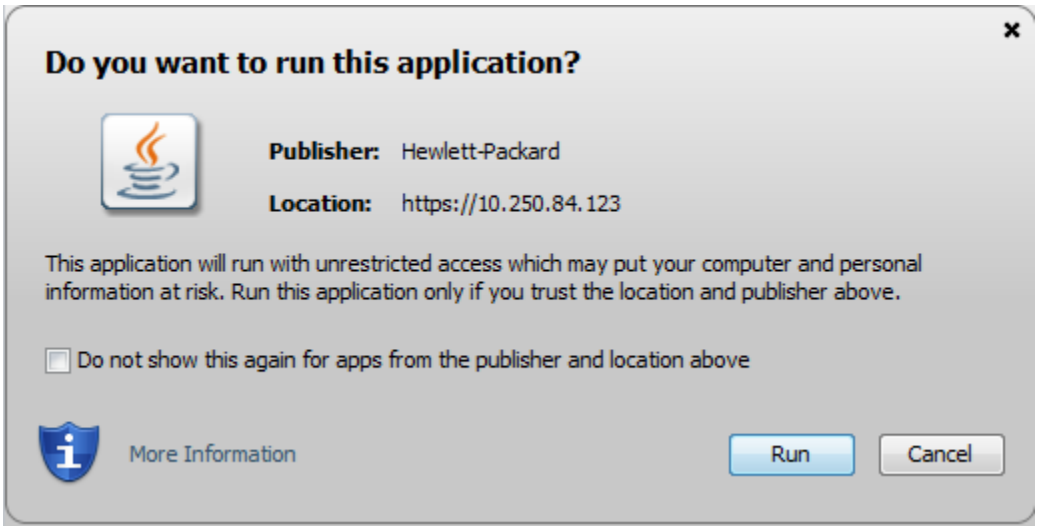
- Select “Remote Console” option
- Before doing the next step to launch “Java Integrated Remote Console”, some Java Configuration may be required by adding IP of PM&C iLO to JAVA security and then launching the Remote Console:
    - On your computer, go to Start->All Programs->Configure Java
    - Click Security tab
    - Click on Edit Site List
    - Enter the required IPs for ILOs, including “https” for example https://1.1.1.1
    - Click Apply and OK and you should be good to launch the “Java Integrated Remote Console”



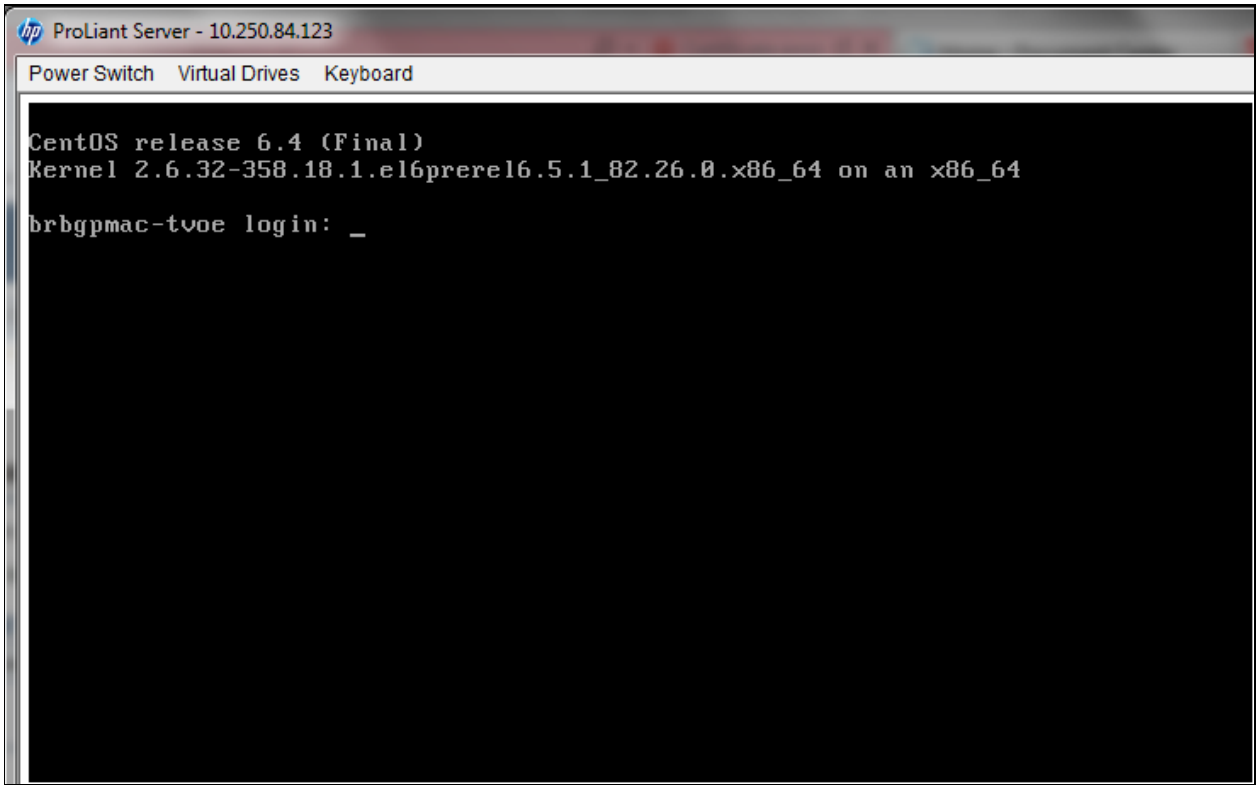
    - Launch “Java Integrated Remote Console” in the above screen
    - Select Continue



- Select Run



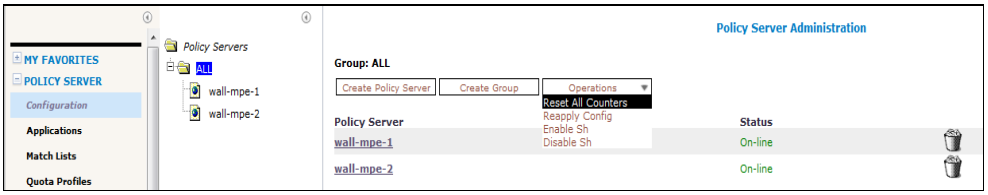
- ILO Remote Console appears



APPENDIX D. RESETTING COUNTERS

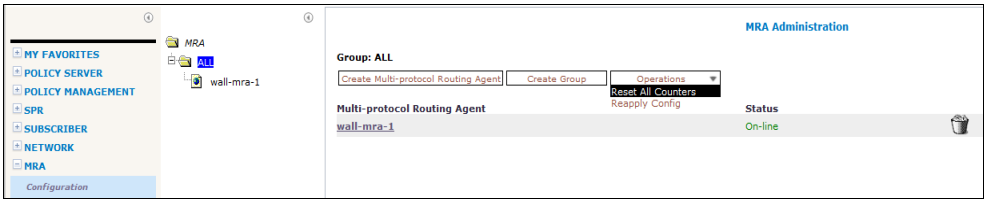
To reset the counters associated with a group of MPE servers in CMP GUI:

Browse to **POLICY SERVER->Configuration->Policy Servers** and select one group, default group is ALL: **ALL->->Operations menu->Select Reset Counters or Reset All Counters**



To reset the counters associated with a group of MRA servers in CMP GUI:

Browse to MRA->Configuration->**MRA** and select one group, default group is ALL: **ALL-> ->Operations menu->Select Reset Counters or Reset All Counters**

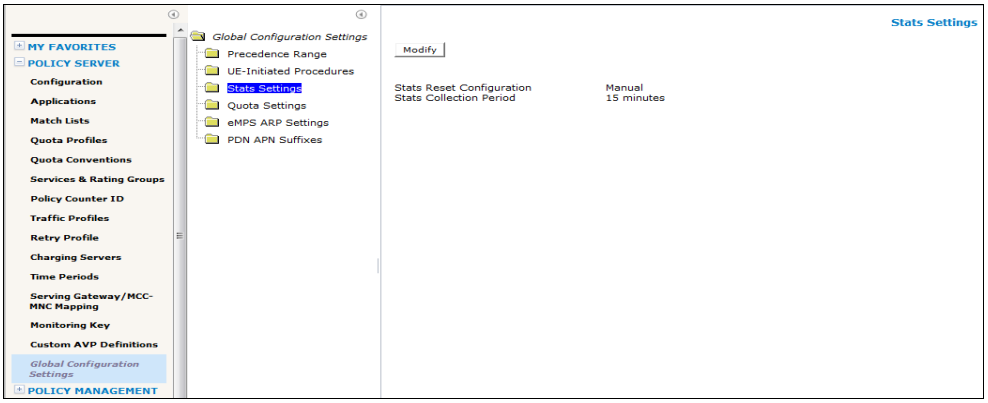


Note:

Operations menu shows either Reset Counters or Reset All Counters depending on Stats Reset Configuration setting
When Stats Reset Configuration = Interval, then Operations menu shows Reset Counters option
When Stats Reset Configuration = Manual, then Operations menu shows Reset All Counters option

Reset Counters option resets counters on the current screen to the initial values
Reset All Counters option resets all counters of the selected server group to the initial values

Stats Reset Configuration value can be set under **POLICY SERVER->Global Configuration Settings->Stats Settings->click Modify**



The default Stats Reset Configuration value is Manual.
When in Manual mode, counter values can only reset when the system restarts (for example, on failover Or initial startup) or when you issue a reset command.
When configured for Interval mode, counter values are reset at regular intervals, controlled by the Stats Collection Period variable.

APPENDIX E. EXPORT KPIS FROM CMP GUI USING OSSI XML INTERFACE

- Configuration Management Platform (CMP) OSSI XML interface allows an operator or third-party system to programmatically push configuration information to and retrieve operational statistics from the policy server deployment using XML over HTTP(s) for requests and responses.

- XML allows the data to be represented in a portable, vendor-neutral and readable format.

- The OSSI XML interface provides XML schema definitions for specific request and response messages to enable message validation and to accurately specify the syntax of each of the messages.

Example OssiXmlOm.xsd — defines the schema for the OM interface and the OSSI OM stats query and response type defintion.

- For an application desiring to use the OSSI XML interface, the only requirement is the ability to send an HTTP POST request and to process any response.

Request-
Specifically an HTTP POST message is sent containing the specific request message.

Response-
The HTTP response contains a response message indicating status and returning any data as required.

- This example shows the command line utility wget to send an HTTP POST request that contains data specified in an XML file as input and returns an output XML file.

Additional options to wget are available but not described here.
Please note that the request URL is case sensitive and must be entered as seen here.

> wget --post-file=input.xml --output-document=output.xml
http://1.2.3.4/mi/xmlInterfaceRequest.do?user=test&pwd=test

Where the following describes each parameter:
--post-file=input.xml (Required) —> This parameter indicates the request input XML file.

--output-document=output.xml (Optional) —> This parameter is used to name the output file. If unspecified, the default filename is the URL string indicated in the wget request.

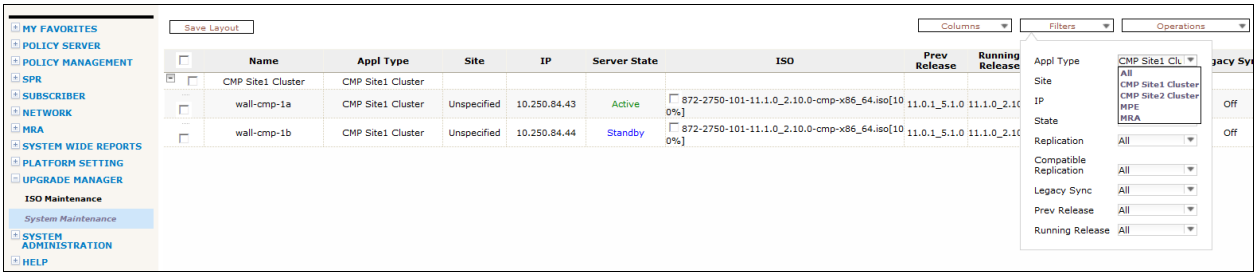
http://1.2.3.4/mi/ xmlInterfaceRequest.do ?user=test&pwd=test (Required) —>
The HTTP request URL, including the authentication credentials.

--timeout=0 (Optional) —> This parameter sets the network timeout to seconds. The default for this value is 900 (15min). A value of 0 disables timeout checking completely.

--progress=dot (Optional) —> This parameter is used to display the progress bar on the request.

APPENDIX F. CMP GUI FILTERS

Upgrade Manager →System Maintenance →Filters →select the required Application Type(CMP,MPE,MRA,ALL)



APPENDIX G. ACCESSING ORACLE'S CUSTOMER SUPPORT SITE & HOTLINES

My Oracle Support

My Oracle Support MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*.

When calling, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

1) For the first set of menu options, select 2, "New Service Request". You will hear another set of menu options.
2) In this set of menu options, select 3, "Hardware, Networking and Solaris Operating System Support". A third set of menu options begins.
3) In the third set of options, select 2, " Non-technical issue". Then you will be connected to a live agent who can assist you with MOS registration and provide Support. Identifiers. Simply mention you are a Tekelec Customer new to MOS.

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*.. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.
A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.