Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Upgrade Procedure

Policy Management 11.5/12.0 to 12.1.x Upgrade Procedure, GEO-Redundant Disabled

E69792-03

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

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

EMAIL: support@oracle.com

Copyright © 2013, 2016 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

TABLE OF CONTENTS

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

2. UPGRADE OVERVIEW 7
2.1 Upgrade Status Values 7
2.2 Upgrade Path 7
2.3 Upgrade Information 7
2.3.1 Upgrade Sequence 7
2.3.2 Policy Release Mixed-Version Operation & Limitation 8
2.4 Customer Impacts 9
2.5 Rollback/Backout 9
2.6 TPD Version 9
2.7 Server Hardware Platforms 9
2.8 Loading Application software 9
2.9 Required Materials and Remote Access 9
2.9.1 Upgrade Media 9
2.9.2 Login Users and Passwords 11

3. THEORY OF OPERATION 12
3.1 Upgrade Manager page 12
3.1.1 The upgrade log 13
3.1.2 Optional actions 13
3.1.3 The ISO select 14
3.1.4 Introducing upgrade director behavior 14

4. UPGRADE PREPARATION 16
4.1 Pre-requisites 17
4.2 TVOE and PM&C Server Upgrade 17
4.3 Firmware Upgrade 17
4.4 Plan and Track Upgrades 17
4.5 Perform System Health Check 20
4.6 Deploy Policy Upgrade Software 21
4.6.1 Deploying Policy Upgrade Software to servers 21
4.6.2 Copy ISO image files to Management Server (PM&C) 21
4.6.3 Distribute Application ISO image files to servers 24
4.6.4 Backups and Backup Locations 25
4.6.5 Changing Non-Defauult root and admusr passwords 26

5. SOFTWARE UPGRADE CAUTIONS 30

6. UPGRADE CMP CLUSTERS (11.5 TO 12.1.X) 31
6.1 Upgrade CMP Clusters Overview 31
6.1.1 Upgrade primary CMP Cluster 32
6.1.2 Upgrade Secondary CMP Cluster 41

7. UPGRADE CMP CLUSTERS (12.0 TO 12.1.X) 45

7.1 Upgrade CMP Clusters Overview 45
7.1.1 Upgrade primary CMP Cluster 46
7.1.2 Upgrade Secondary CMP Cluster 54

8. MPE AND MRA UPGRADE 59
8.1 Site/Segment Upgrade Preparation 59
8.1.1 Configuration Preparation 59
8.2 Upgrade MRA and MPEs 60

9. POST UPGRADE HEALTH CHECK 66

10. BACKOUT (ROLLBACK) 67
10.1 Backout Sequence 67
10.2 Pre-requisites 67
10.3 Backout of Fully-upgraded Cluster 68
10.3.1 Backout Sequence 68
10.3.2 Backout Fully Upgraded MPE/MRA Cluster 70
10.3.3 Backout Fully Upgraded Secondary CMP Cluster 75
10.3.4 Backout Fully Upgraded Primary CMP Cluster 79

APPENDIX A. ACCESSING ORACLE'S CUSTOMER SUPPORT SITE & HOTLINES 85

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform Policy Management Release 11.5 or 12.0 Software upgrade to Policy Management Release 12.1.x – Geo-Redundant Disabled.

>Upgrade of the PM&C server including TVoE Host is required, but not covered in this document.

- NOTE: Not all Policy Management systems use a PM&C Server, so this is optional.

>Firmware Upgrades may be required, but will not be covered in this document.

>In-service Policy Release 11.5.x/12.0 CMP, MRA servers and MPE servers.

The audience for this document includes: Software Development, Product Verification, and Consulting Services.

The Non-Geo-Redundant cluster scheme has two servers 'Active & Standby' co-located on a site.

Primary MRA/MPE cluster of 'Active & Standby' resides on Site-1 and Secondary MRA/MPE cluster of 'Active & Standby' resides on Site-2 for disaster recovery.

1.2 References

[1] FD008107 - Upgrade Enhancements

[2] FD008034 - Upgrade Director

[3] TR007572 – Policy Upgrade 12.0 to 12.1.x

[4] TR007573 – Policy Upgrade 11.5 to 12.1.x

[5] E53018 – Tekelec Virtualization Operating Environment (TVOE) upgrade procedure

[6] E54387-03 (CBGU_010617) – PM&C Incremental Upgrade

[7] E59721 – HP Solutions Firmware Upgrade Pack, Upgrade Guide – Release 2.2.8

[8] E59722 – Release Notes for FUP 2.2.8

1.3 Acronyms

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
DSR	Diameter Signaling Router
GUI	Graphical User Interface
LVM	Logical Volume Manager
MPE-Li	PCRF Lawful intercept
MPE	PCRF Product
MRA	Diameter Routing Agent for Policy Applications Product
OCS	On Line Charging System
PC	Policy Counter
PCEF	Policy Control Enforcement Function (GGSN, P-GW, DPI)
PCRF	Policy and Charging Rules Function – Oracle MPE
PM&C	Platform Management and Configuration

Segment	A segment is a collection of HSGWs, P-GWs, DSRs, MPEs and MRAs that provide the PCRF service. A single MPE/MRA cluster may be part of only one PCRF Segment. A CMP manages all the MPE/MRAs at multiple sites. A CMP manages one or more PCRF Segments.
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment
UE	User Equipment
UM	Upgrade Manager – The CMP GUI pages that the operator uses to perform an upgrade
VO	Verification Office

1.4 Terminology

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

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

1.5 Software Release Numbering

- PMAC: 6.0.1.0.0_60.21.0

- TVOE: 3.0.2.0.0_86.28.0

- Policy Management Release 12.1.1.0.0_14.1.0

- Firmware: Firmware Upgrade Pack 2.2.8

2. UPGRADE OVERVIEW

This section lists the required materials and information needed to execute Policy Management Release 12.1.x software upgrades.

2.1 Upgrade Status Values

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

2.2 Upgrade Path

This upgrade document supports the following upgrade path –

1. Policy Management 12.0 to 12.1.x
2. Policy Management 11.5 to 12.1.x

2.3 Upgrade Information

2.3.1 Upgrade Sequence

This procedure applies to Active/Standby pair of servers. This pair of servers is referred to as the “cluster” or “HA cluster”. The cluster involves 3 servers. The cluster types are CMP, MRA or MPE. For CMP cluster, the cluster status may also be Primary site and/or Secondary site.

The customer deployment may consist of multiple clusters.

Required Cluster Upgrade Sequence:

Policy Server Software upgrades will be performed on a cluster by cluster basis at the local and remote sites within the same maintenance window.

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

NOTE: TVOE, PM&C Server, and Firmware upgrades will not be covered in this document, but may be necessary prior to the Policy Management Upgrade.

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

1. Upgrade PM&C Server at Site 1 – Needed If version is older than what is listed in section 1.5
2. Upgrade PM&C Server at Site 2 – Needed If version is older than what is listed in section 1.5
3. Firmware Upgrade – If needed
4. Upgrade Primary CMP
5. Secondary CMP (If applicable)
6. Upgrade MPE and MRA (See note below)

NOTE: An MPE and an MRA cluster can be upgraded in parallel – 4 at a time.

2.3.2 Policy Release Mixed-Version Operation & Limitation

The general expectation is that a system that is running in a mixed version configuration should support features, and perform at a level of the previous version. Thus, the system that is running Release 11.5 or 12.0 and Release 12.1.x mixed configuration would support the performance and capacity of Release 11.5 or 12.0. The mixed version PCRF configuration would support Release 11.5.x or 12.0 features.

Since the CMP is the first PCRF system component that is upgraded to the new version, the Release 12.1.x CMP will be managing the previous release, and Release 12.1.x MRA and MPE servers. In this mixed version configuration Release 12.1.x CMP will not prevent an operator from configuring anything that you could configure in a previous release and all configuration items from the previous release are still available. However, the configuration changes during the upgrade of 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 12.1.x CMP has the following limitations while running in a mixed version environment:

- New features must not be enabled until the upgrades of all servers managed by that CMP are completed. This also applies to using policy rules that include new conditions and actions introduced in the release.
- As a general guideline, policy rules should not be changed while running in a mixed version environment. If it is necessary to make changes to the policy rules while running in a mixed version environment changes that do not utilize new conditions and actions for the release could be installed, but should be jointly reviewed by the customer and Oracle 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
- The CMP running Release 12.1.x software will support IPM'ing an MPE or MRA server with Release 11.5.x or R12.1.x.

Mixed-version configurations supported between Release 11.5.x or 12.0 and Release 12.1.x

PCRF system Components on	CMP R12.1.x	MRA R12.1.x	MPE R12.1.x
CMP R12.0 or 11.5	No	No	No
MRA R12.0 or 11.5	Yes	Yes	Yes
MPE R12.0 or 11.5	Yes	Yes	N/A

Note: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP from Release 11.5.x/12.0 to Release 12.1.x. The replication is automatically enabled once both active CMP and DR-CMP are upgraded to Release 12.1.x.

2.4 Customer Impacts

The cluster upgrade proceeds by upgrading the standby server, then spare, and then switching over from 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 the past releases upgrades.

2.5 Rollback/Backout

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

2.6 TPD Version

The Tekelec Product Distribution (TPD) version needed for this release is included in the Policy Application Software Upgrade ISO, and TPD will be upgraded to version 7.0.2 as part of this procedure.

In the case of IPM or clean install of a new server, the supported baseline TPD version 7.0.2 should have been installed prior to upgrading to Policy Release 12.1.x.

2.7 Server Hardware Platforms

The Policy Release 12.1.x software upgrade can be applied on any server that previously had Policy Release 11.5.x or 12.0.x

2.8 Loading Application software

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

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

2.9 Required Materials and Remote Access

1. Policy 12.1.x software ISO's and TPD software ISO
2. Policy 12.1.x software Upgrade Release Notes.
3. TVOE, PM&C upgrade/installation documentation, software ISOs and TPD ISO. (If applicable)
4. Firmware Upgrade Pack 2.2.8 documentation and ISOs. (If Applicable)
5. The capability to remote login to the target server as admusr.

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

2.9.1 Upgrade Media

The Policy Release 12.1.x software ISO image files will be as the following:

PM&C:	**6.0.1_60.21.0-PMAC-x86_64.iso**
TVOE:	**3.0.2.0.0_86.28.0-TVOE-x86_64.iso**
TPD**:**	**7.0.2.0.0_86.28.0-TPD-x86_64.iso**
CMP:	**12.1.1.0.0_14.1.0_cmp-x86_64.iso**

MPE: **12.1.1.0.0_14.1.0_mpe-li-x86_64.iso**

MPE-LI: **12.1.1.0.0_14.1.0_mpe-x86_64.iso**

MRA : **12.1.1.0.0_14.1.0_mra-x86_64.iso**

FW 2.2.8:

a. FW2_MISC-2.2.8.0.0_10.43.0.iso
b. FW2_SPP-2.2.8.0.0_10.43.0.iso
c. FW2_SPP-2.2.8.0.0_10.43.0.usb

Component	Release
TPD 64 Bit	7.0.2
COMCOL	6.4
PM&C	6.0.1.0_60.20.0
TVOE	3.0.0.0_86.14.0
Firmware	FUP 2.2.8

2.9.2 Login Users and Passwords

Logins, Passwords and Server IP Addresses

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

Further, need to confirm login information for key interfaces, and document in table below.
[It is assumed that the Logins may be common among the customer sites. If not, record for each site.].

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

Table-1: Logins, Passwords and Server IP Addresses

Item	Value
CMP servers	GUI Administrator Login User/Password:
	admusr password:
MRA/MPE servers	**admusr** password:
Target iLO	iLO Administrator Login: User/Password
Target OA	OA Administrator Login: User/Password
PM&C server	GUI Administrator Login User/Password:
	admusr password:
Software Upgrade Target Release[1]	Target Release Number:
	Policy 12.1.x software ISO Image (.iso) filenames.

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

3. THEORY OF OPERATION

3.1 Upgrade Manager page

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

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

There is an important point implicit in the list above:

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

The shift in perspective has a number of ramifications, most noticeably it is no longer possible to select individual servers or bulk select a group of servers. In fact, in order to perform any operation, it is necessary to select a cluster first.

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

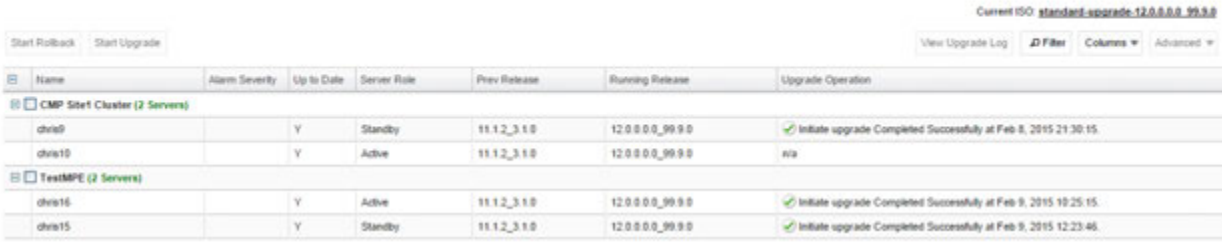


Figure 1: Sample display of the upgrade manager page.

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

- Start Rollback/Start Upgrade buttons (Upper left) – If these buttons are greyed out, it means that there isn't an appropriate action to take at this time. However, if a button isn't greyed out, then it means that there is a 'preferred' action that can be taken to upgrade (or backout) the cluster. Normally, upgrading a cluster is a well defined fixed procedure. However, in some cases there are a number of valid sequences. Selecting the 'preferred' step will simply cause the upgrade director to chose the default sequence. It is strongly recommended to exclusively use these buttons to upgrade/backout a cluster.
- Alarm Severity – This column is used to indicate if there are alarms associated with a server. If so, it displays the severity of the most severe alarm here. It is important to explain the intent of this column. The intent is to

give a visual indication that the particular server is experiencing alarms. This is not a reason to panic: During the upgrade we expect servers to raise alarms:

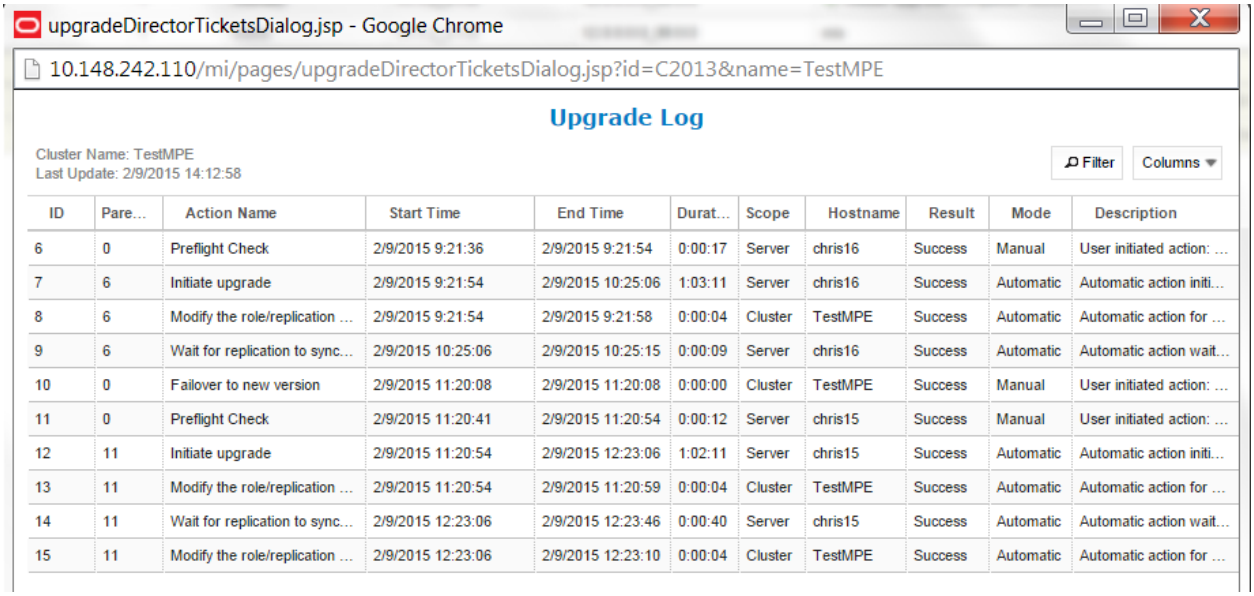
- The CMP will raise alarms simply to indicate that it is initiating upgrade activity.
- Servers will report alarms to indicate that their mate servers are offline.

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

- Up to Date – This column is used to indicate the state of the code on the server.
  - 'N' -> The server is running old code needs to be upgraded
  - 'Y' -> The server is running new code.
  - 'N/A' -> Upgrade is not appropriate and/or the server is in a bad state

3.1.1 The upgrade log

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



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

Figure 2: Upgrade Log

3.1.2 Optional actions

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

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

3.1.3 The ISO select

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

"A standard (full) upgrade to version XXX"

"An incremental upgrade to version XXX"

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

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

3.1.4 Introducing upgrade director behavior

The upgrade director (UD) is a component that tracks the state of the servers, cluster and system during an upgrade. From a user perspective, the UD is largely hidden. However, there are conventions/operating principles that have user visible effects.

3.1.4.1 Alarm philosophy

In general, the upgrade director will raise alarms if

1) A server is somehow impaired
2) There is activity expected of an operator.

The table below summarizes the alarms that can be raised in 12.1.x

Alarm ID	Name	Description
70500	SYSTEM_MIXED_VERSION	The servers in the topology are running different versions of software. Upgrade of the system is not complete.
70501	CLUSTER_MIXED_VERSION	The servers in the specified cluster are running different versions of software. The upgrade of the cluster is not complete.
70502	REPLICATION_INHIBITED	Replication is inhibited to the specified server. It is not receiving session information.
70503	SERVER_FORCED_STANDBY	The specified server has been placed in forced standby and cannot provide service.
70506	UPGRADE_OPERATION_FAILED	An upgrade operation failed on the specified server.
70507	UPGRADE_IN_PROGRESS	An upgrade/backout is currently in progress on the server. It may leave the cluster, become unreachable or even reboot.
70508	ZOMBIE_SERVER	The server is in an indeterminant state and needs to be repaired by support.

3.1.4.2 General upgrade procedure

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

1) Preflight checks – look for certain conditions which guarantee a failed upgrade. If such conditions are detected, fail. There are two principles behind the preflight checks
    a. It is better to fail early in a recoverable way than to fail late in an unrecoverable way.

b. Preflight checks are VERY narrow. We do not want a false positive preventing an otherwise valid upgrade.

2) The upgrade itself

3) Wait for replication to synchronize.

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

3.1.4.3 Unreachable servers

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

3.1.4.4 Reversing directions

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

3.1.4.5 Mixed version and forced standby

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

3.1.4.6 Failure handling and recovery

.

Failures fall into two categories:

- Failures that the upgrade director is able to recover from.
- Failures that the upgrade director can't automatically recover from.

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

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

4. UPGRADE PREPARATION

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

Overview –

1. Upgrade TVOE PM&C Server at Site-1 (If Applicable)
2. Upgrade TVOE PM&C Server at Site-2 (If Applicable)
3. Firmware (If Applicable)
4. Upgrade Primary active CMP
5. Upgrade Secondary CMP (If applicable)

6. Segment 1 Site-1:

   Upgrade MPE clusters
   Upgrade MRA clusters

7. Segment 1 Site-2:

   Upgrade MPE clusters
   Upgrade MRA clusters

8. Segment 2 Site-1:

   Upgrade MPE clusters
   Upgrade MRA clusters

9. Segment 2 Site-2:

   Upgrade MPE clusters
   Upgrade MRA clusters

4.1 Pre-requisites

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

TVOE-PM&C and Firmware will need to be upgraded prior to Upgrade to Policy Management Release 12.1.x. Firmware Upgrade to FUP 2.2.8 will need to be executed prior to the Upgrade to Policy Management Release 12.1.x		
Step	**Procedure**	
1. ☐	Verify all required materials are present	As listed in Section: "Required Materials & Remote Access"
2. ☐	Review Release Notes	Review Policy Release 12.1.x for the following information: - Individual Software components and versions included in target release - New features included in target release - Issues (Oracle BUGs) resolved in target release - Known Issues with target release - Any further instructions that may be required to complete the Software Upgrade for the target release

4.2 TVOE and PM&C Server Upgrade

Policy Release 12.1.x requires PM&C version 6.0 to support IPM'ing TPD 7.0 on c-Class blade.

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

See the following Documents to Upgrade the TVOE and PM&C
1) E53018 - Tekelec Virtualization Operating Environment (TVOE) Upgrade Procedure
2) E54387-03 – PM&C Incremental Upgrade Procedure

4.3 Firmware Upgrade

See the following Documents to Upgrade the TVOE and PM&C
1) E59721 – Upgrade Guide for FUP 2.2.8
2) E59722 – Release Notes for FUP 2.2.8
3) ISOs
    a. FW2_MISC-2.2.8.0.0_10.43.0.iso
    b. FW2_SPP-2.2.8.0.0_10.43.0.iso
    c. FW2_SPP-2.2.8.0.0_10.43.0.usb

4.4 Plan and Track Upgrades

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

Pre-requisite- TVOE and PM&C Server upgraded and FUP 2.2.8 deployed.

1. Upgrade CMP cluster(s)
2. Upgrade MPE/MRA clusters

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

NOTES:

- *Policy Changes or Configuration change should NOT be made while the system is in Mixed-Version operation.*
- *Time estimates are for Upgrade procedure without Backout procedure. Backout procedure time is typically same as, or less than the Upgrade procedure.*

Step	**Procedure**	**Result**	**Engineer**	**Time**
1. ☐	Use the following Checklist to plan the Cluster upgrades for the entire system.	Maintenance Windows are planned		
2.	Upgrade Site A and Site B TVOE/PM&C	Site Names _____ & _____		3 hrs
3. ☐	Upgrade Primary and Site-2s CMP clusters	Site Names _____ & _____		3 hrs
4. ☐	Upgrade Site-1 MPE/MRA clusters for Segment-1 ***NOTE:*** *Maximum of 4 clusters performed in "parallel"*	Site Names _____ Cluster List:		2 hrs
5. ☐	Upgrade Site-2 clusters for Segment-1 ***NOTE:*** *Maximum of 4 clusters performed in "parallel"*	Site Names _____ Cluster List:		2 hrs

Step	**Procedure**	**Result**	**Engineer**	**Time**
6. ☐	Upgrade Site-1 clusters for Segment-2 ***NOTE:*** *Maximum of 4 clusters performed in "parallel"*	Site Names _____ Cluster List:		2 hrs
7. ☐	Upgrade Site-2 clusters for Segment-2 ***NOTE:*** *Maximum of 4 clusters performed in "parallel"*	Site Names _____ Cluster List:		2 hrs

4.5 Perform System Health Check

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

Step	Procedure	Result
1. ☐	CMP GUI Access	Open a browser to access the Primary CMP GUI on its VIP address and login to verify access.
2. ☐	View Active Alarms	Identify the cause of any existing active alarms, and determine if these may have impact on the upgrade. Export current Alarms to save into a file. **IMPORTANT:** *Before starting any upgrade activity, please ensure that all Active Alarms are well understood and resolved.*
3. ☐	View KPI reports	Verify that the system is running within expected parameters. Export current KPIs to save into a file.
4. ☐	Confirm NTP servers reachable from all the Servers (CMP, MPEs & MRAs) to be upgraded ***NOTE:*** *If the time across the servers is out of synch, fix it first and re-validate this step, before starting the upgrade procedures.*	- Validate the IP connectivity between the server and NTP servers by PING. - Confirm that time is synchronized on each server with CLI shell command of '**ntpq –np**' - Confirm that date is correct on each server. - Check that BIOS clock is sync'd with the clock using '**hwclock**' shell command

4.6 Deploy Policy Upgrade Software

Software should be deployed to each Policy server **"/var/TKLC/upgrade"** directory, before the actual upgrade activities. This will typically be done with utilities such as SCP, WGET or SFTP. Because of the large size of the software ISO's, sufficient time should be planned to accomplish this step. For Policy Release 12.1.x, each ISO image size is about 1.0 Gigabytes.

4.6.1 Deploying Policy Upgrade Software to servers

There are 4 possible Software Images in this upgrade (CMP, MPE, MPE-Li, MRA). A single image must be deployed to the Upgrade (/var/TKLC/upgrade) directory of each server to be upgraded, where the image is the correct type for that server. i.e. the new CMP software image must be deployed to the CMP servers, the new MPE image deployed to the MPE servers, the new MPE-Li image deployed to the MPE-Li servers and the MRA image deployed to the MRA servers.

IMPORTANT: *If the deployed image type (CMP, MPE, MPE-LI, 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.* [***NOTE****: To change a server from one application type to another, the server must first be cleaned of all application software by an "Install OS" action via the PM&C GUI, and then the new Application type installed.*]. Or, if multiple images are copied into the /var/TKLC/upgrade directory, the upgrade will fail.

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

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

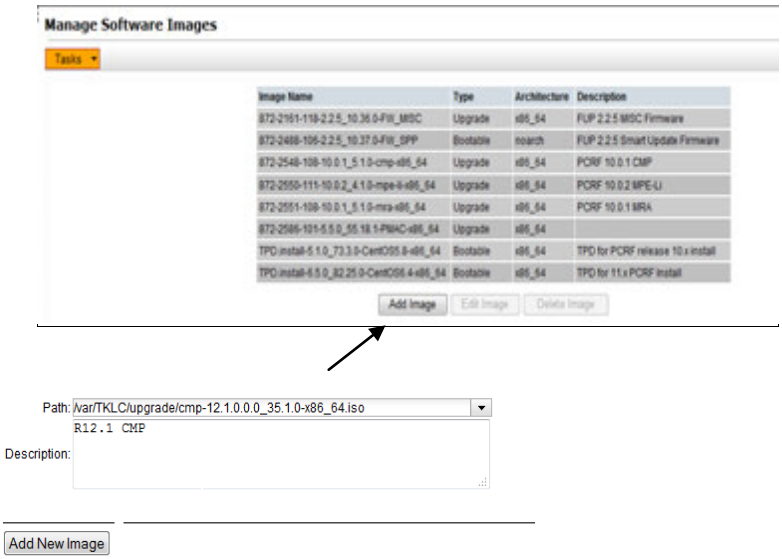
This procedure transfers software Upgrade ISO's to the PM&C servers at each site to be upgraded, and loads ISO's into the PM&C Software Image repository. This is done as a placeholder for future use of the software.

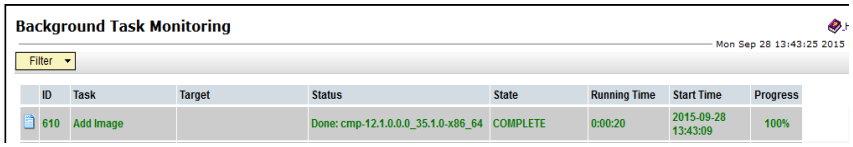
PM&C is not used for the upgrade activities. The purpose of this step is to be prepared for server recovery activities in case a server needs to be re-installed with software.

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

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

Step	Procedure	Result
1. ☐	**PM&C GUI:** Verify no Release 12.1.x ISO files exist.	• Log on to the PM&C Server GUI **Software → Manage Software Images** • Confirm no Release 12.1.x ISO files already exists. If there are, then remove them.

Step	Procedure	Result
2. ☐	SSH to PM&C server as admusr	• Log on as admusr to the PM&C server. • Change Target directory to **/var/TKLC/upgrade** and ensure there is at least of 3.0 GB free disk space available. **$cd /var/TKLC/upgrade** **$df –h /var/TKLC** NOTE: There may be ISOs in the /var/TKLC/upgrade directory, they can be removed to free up disk space or added to the PM&C repository.
3. ☐	Copy Release 12.1.x ISO files to the target directory in the PM&C server	• Transfer all Release 12.1.x ISO files (CMP, MPE/MPE-Li, MRA) into directory **/var/TKLC/upgrade** via either the following methods – - SCP/WGET command in the following steps outline in this Procedure, OR - USB drive
4. ☐	**PM&C GUI:** Adding the new Release 12.1.x ISO files	**Software → Manage Software Images** • Select "**Add Image**" to select the ISO files that are just transferred into PM&C server.  Click OK on the pop-up

Step	Procedure	Result
5. ☐	**PM&C GUI:** Verify the new ISO files are added successfully	**Software → Manage Software Images** • The status of the image being added can be monitored via the "**Task Monitoring**" menu with the screen display as the following –  ***NOTE:*** *the newly added ISO files are now stored in directory* ***/var/TKLC/smac/image/repository***

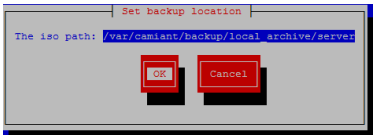
4.6.3 Distribute Application ISO image files to servers

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

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

Step	Procedure	Result
1. ☐	**Transfer ISOs to Policy Servers.**	- Transfer Release 12.1.x ISO files (CMP, MPE/MPE-Li, MRA) into directory **/var/TKLC/upgrade** on the respective server via either of the following methods - - SCP/WGET command OR - USB drive **OR, if the images are on a server on the same network, scp via CLI.** Copy CMP software ISO to ONE of the other CMP servers: **$sudo scp 872-* <*cmp_hostname*>:/var/TKLC/upgrade/** Copy MPE software ISO to ONE of the other MPE servers: **$sudo scp 872-* <*mpe_hostname*>:/var/TKLC/upgrade/** Copy MPE-Li software ISO to ONE of the other MPE-Li servers: **$sudo scp 872-* <*mpe-li_hostname*>:/var/TKLC/upgrade/** Copy MRA software ISO to ONE of the other MRA servers: **$sudo scp 872-* <*mra_hostname*>:/var/TKLC/upgrade/** **NOTE: After copying the ISO to one of the respective servers, the ISO Maintenance will be used to upload to the rest of the servers.**
THIS PROCEDURE HAS BEEN COMPLETED		

4.6.4 Backups and Backup Locations

Step	Procedure	Result
1. ☐	**SSH CLI/ iLO**: Access the server to be backed up **NOTE:System Backup is done on Active CMPs ONLY→**	***IMPORTANT: Server backups (each cmp, mpe, and mra server – active and standby), and the system backup (from Active CMP), must be collected and readily accessible for recovery operations.*** • Login into the ACTIVE Primary CMP server. Navigate to the following through platcfg utility. **$sudo su – platcfg** **Policy Configuration→Backup and Restore→server backup** • Provide the ISO backup filename in default backup location path of */var/camiant/backup/local_archive/serverbackup/<filename.iso>*  Navigate to the following through platcfg utility. **$sudo su – platcfg** **Policy Configuration→Backup and Restore→system backup** • Provide the ISO backup filename in default backup location path of */var/camiant/backup/local_archive/systembackup/<filename.iso>*
2. ☐	**SSH CLI/iLO:** Verify the backup ISO file	• If default location is accepted in the previous step, change directory to the following and verify file exists- $ **cd /var/camiant/backup/local_archive/serverbackup** $ **ls** **<hostname>-mpe-li_x.x.x_x.x.x-serverbackup-2014<xx><xx><xxxx>.iso** $ **cd /var/camiant/backup/local_archive/serverbackup** $ **ls** **<hostname>-mra_ x.x.x_x.x.x-serverbackup-2014<xx><xx><xxxx>.iso** **cd /var/camiant/backup/local_archive/serverbackup** $ **ls** **<hostname>-cmp_ x.x.x_x.x.x-serverbackup-2014<xx><xx><xxxx>.iso** $ **cd /var/camiant/backup/local_archive/systembackup** $ **ls** **<hostname>-cmp_ x.x.x_x.x.x-systembackup-2014<xx><xx><xxxx>.iso**
3.	**Copy backup files.**	An example on where to copy the ISO. **$sudo scp -p /var/TKLC/bkp/xxxxxx -201312091500.iso 10.240.1.1:/var/TKLC/upgrade** Another option is to scp the backup ISO to your local workstation. After copying to remote server/workstation, remove the backup iso from the TVOE Sever. **$sudo rm <backup_filename.iso>**

Step	Procedure	Result
4. ☐	Identify Backups Location	Backup location is: _____ Instructions to access to backups are as follows: _____ _____ _____
THIS PROCEDURE HAS BEEN COMPLETED		

4.6.5 Changing Non-Defauult root and admusr passwords

4.6.5.1 Improve Password Security

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

4.6.5.2 Impact

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

This procedure only addresses root and admusr passwords. Other users should also update their password to benefit from the new hashing. If they are not changed prior to the upgrade to 12.1.x, they will be expired post upgrade.

The following procedure should be executed prior to the upgrade to 12.1.x only if the root or admusr passwords are non-default.

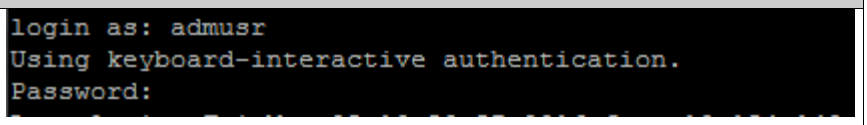
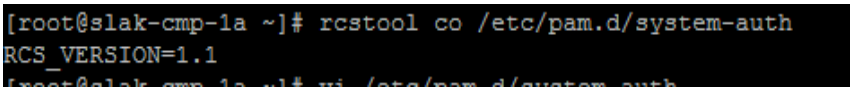
Order to Perform this procedure on an 'In-Service' Policy Management

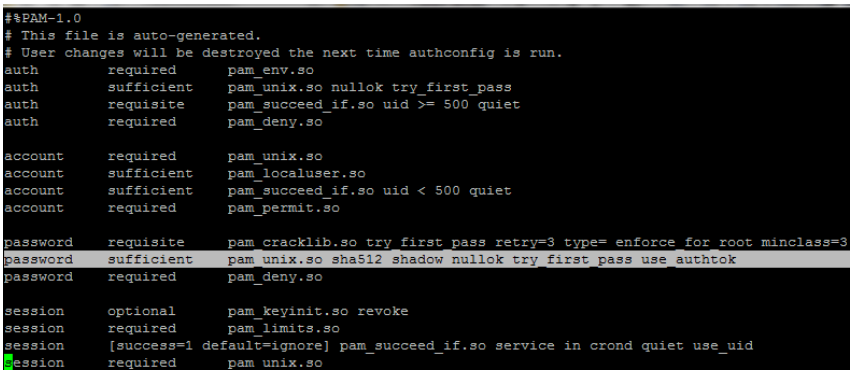
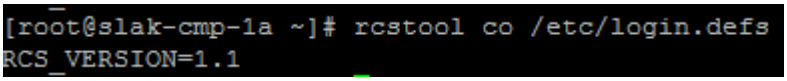
1. Standby CMPs
2. Active CMPs
3. Standby MPEs/MRAs
4. Spare MPEs/MRAs
5. Active MPEs/MRAs

Step	Procedure	Result

1. ☐	Login to the Server (MRA/CMP/MPE) as admusr	`login as: admusr`
		`Using keyboard-interactive authentication.`
		`Password:`

2. ☐	Change to root user	**$sudo su –**

Step	Procedure	Result
3. ☐	Check the password field of root and admusr	Issue the following **#egrep '^(root|admusr)' /etc/shadow** **Example Output.** root:**$6**$mErKrEsA$83n5G8dR3CgBJjMEABi6b4847EXusUnzTaWNJgEi347B.WhLbIc.Cga.nmYCdQYSNwkst1CtUBi.tBSwWujUd.:16825:0:99999:7::: admusr:**$6**$mUstAfa$gn2B8TsW1Zd7mqD333999Xd6NZnAEgyioQJ7qi4xufHSQpls6A5Jxhu8kjDT8dIgcYQR5QlZAtSN8OG.7mkyq/:16825:::::: **If the first two characters after the colon ':' is $6, then this procedure is not needed on this server. Skip to the next section.** **If the first two characters after the colon are not $6, then it is probably $1 (MD5) and this procedure should be followed for this server. Continue on with step 4**
4. ☐	**Order to perform the change**	**Issue steps 5-17 starting with the standby CMPs, then repeat the exact steps for the Active CMPs, then the standby MPEs/MRAs, the spare MPEs/MRAs and lastly the Active MPEs/MRAs**
5. ☐	Login to the Server (MRA/CMP/MPE) as admusr	
6. ☐	Change to root user	**$sudo su –**
7. ☐	Checkout revisions	Issue the following command **#rcstool co /etc/pam.d/system-auth** 

Step	Procedure	Result
8. ☐	Modify 'system-auth' file	**#vi /etc/pam.d/system-auth** **Example below,** Modify the file. Change the following line from md5 to sha512 *Modify the below line with sha512 instead of md5 (Current line indicates currently configured in server. Modified Line indicates modification which needs to be implemented)* *Current Line*: password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok *Modified Line:* password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok  #%PAM-1.0 # This file is auto-generated. # User changes will be destroyed the next time authconfig is run. auth required pam_env.so auth sufficient pam_unix.so nullok try_first_pass auth requisite pam_succeed_if.so uid >= 500 quiet auth required pam_deny.so account required pam_unix.so account sufficient pam_localuser.so account sufficient pam_succeed_if.so uid < 500 quiet account required pam_permit.so password requisite pam_cracklib.so try_first_pass retry=3 type= enforce_for_root minclass=3 password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok password required pam_deny.so session optional pam_keyinit.so revoke session required pam_limits.so session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid session required pam_unix.so
9. ☐	Save the file	*If the file required changing* **#rcstool ci /etc/pam.d/system-auth** *if the file already was configured* **#rcstool unco /etc/pam.d/system-auth**
10. ☐	Checkout revisions for 'login.defs'	**#rcstool co /etc/login.defs**  [root@slak-cmp-1a ~]# rcstool co /etc/login.defs RCS_VERSION=1.1
11. ☐	Edit login.defs	**(**shadow password suite configuration) *Modify the below line with SHA512 instead of MD5* *Current Line*: ENCRYPT_METHOD MD5 *Modified Line:* ENCRYPT_METHOD SHA512 **#vi /etc/login.defs** NOTE: The line to edit is at the bottom of the file NOTE: Comment out the following line if necessary. It will come ***MD5_CRYPT_ENAB yes***

Step	Procedure	Result
12. ☐	Save the File	*If the file required changing* **#rcstool ci /etc/login.defs** *if the file already was configured* **#rcstool unco /etc/login.defs**

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

14. ☐	Edit libuser.conf	***Modify the below line with sha512 instead of md5*** *Current Line:* crypt_style = md5 *Modified Line:* crypt_style = sha512 **#vi /etc/libuser.conf** NOTE: The line to edit is close to the top of the file.
15. ☐	Save the File	*If the file required changing* **#rcstool ci /etc/libuser.conf** *if the file already was configured* **#rcstool unco /etc/libuser.conf**
16. ☐	Set the admusr and root passwords	For root user **#passwd root** For admusr user **#passwd admusr**
17. ☐	Verify	**Logout of the current session and re-login using the new password credentials.**
THIS PROCEDURE HAS BEEN COMPLETED		

5. SOFTWARE UPGRADE CAUTIONS

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.

6. UPGRADE CMP CLUSTERS (11.5 TO 12.1.X)

This procedure will upgrade the Site-1 CMP cluster first, and if needed, upgrade the Site-2 CMP cluster.

6.1 Upgrade CMP Clusters Overview

Upgrade Primary CMP cluster

1) Use the CMP GUI – System Maintenance (11.5.x), to place Primary Standby CMP into Frc-Stby
2) Use the CMP GUI – System Maintenance (11.5.x), to upgrade the Primary Frc-Stby CMP server
3) Use the CMP GUI – System Maintenance (11.5.x), to perform Switch Frc-Stby on the Primary CMP Cluster
4) Log back into the CMP GUI and upgrade the remaining Primary CMP's Frc-Stby server using the 12.1.x Upgrade Manager

Upgrade The Secondary CMP cluster (If applicable)

1) Use the CMP GUI, Upgrade → Upgrade Manager and upgrade the CMP Secondary Site 2
   a. Start Upgrade
   b. Continue Upgrade -- Failover
   c. Continue Upgrade

This procedure should not be service affecting, but it is recommended to perform this in a Maintenance Window

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

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

Identify the CMPs sites to be upgraded here, and verify which sites are Primary and Secondary:

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

Note the Information on this CMP cluster:

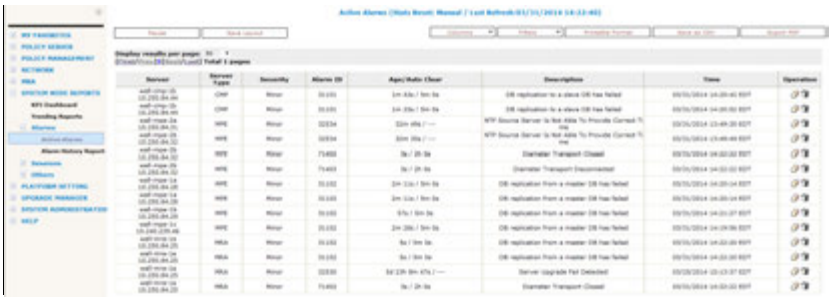
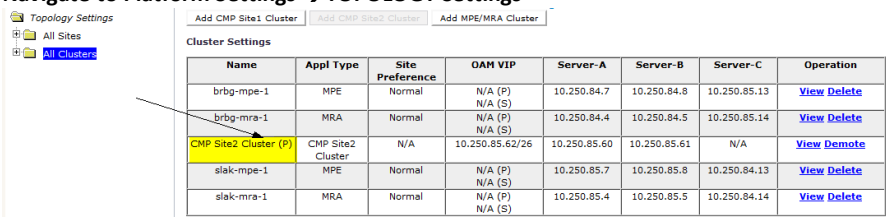
Cluster Name_____
Server-A Hostname _____
Server-A IP _____
Server-A Status _____

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

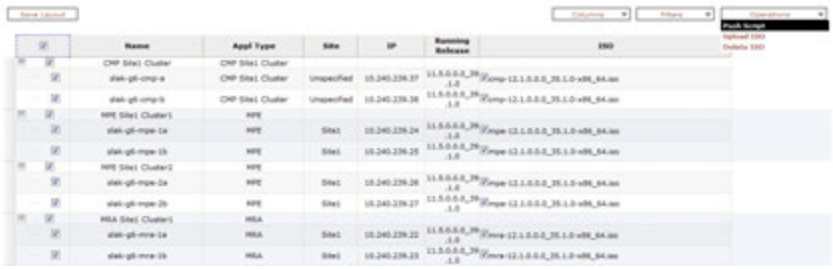
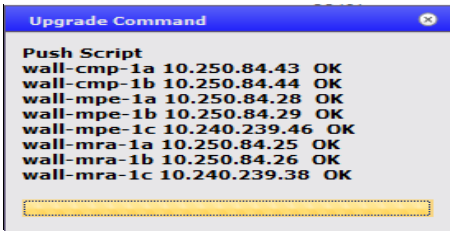
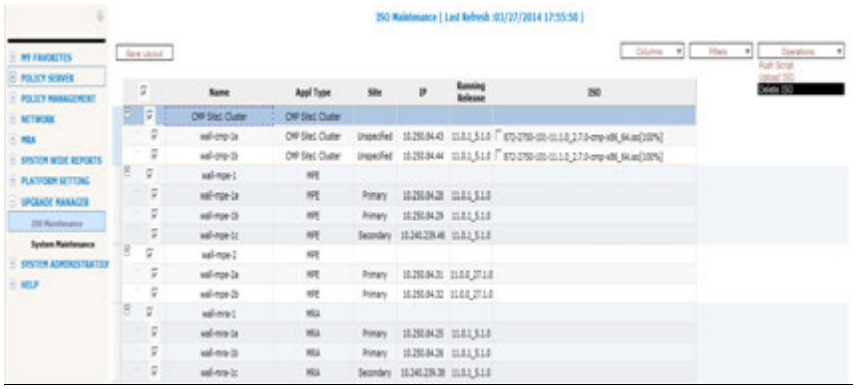
IMPORTANT:

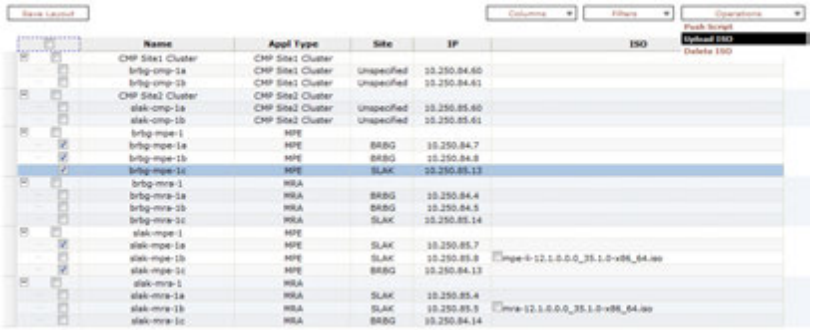
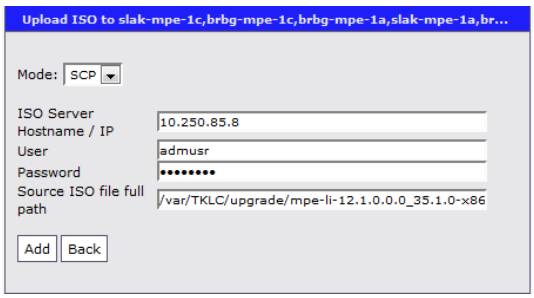
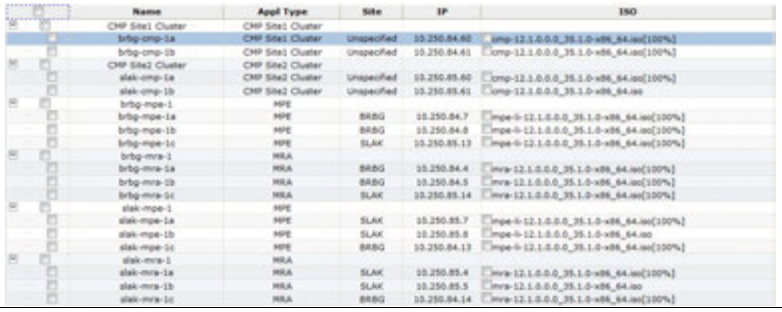
- *CMP servers MUST be upgraded first, before the MPE or MRA clusters*
- *Site-1 CMP MUST be upgraded to the new release first, before the Site-2 CMP(if applicable)*

6.1.1 Upgrade primary CMP Cluster

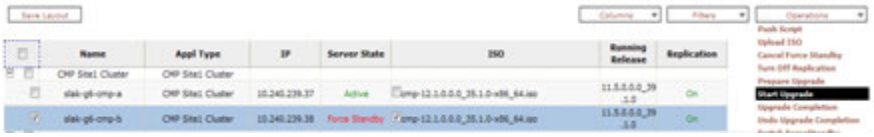
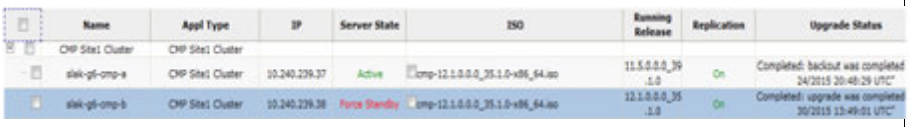
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Alarm Status.	**System Wide Reports →Alarms→ Active Alarms** • Confirm that any existing Alarm is well understood and no impact to the Upgrade procedure. • Capture a screenshot and save it into a file for reference. 
2. ☐	**CMP GUI:** Identify and Record the CMP Cluster(s)	**Navigate to Platform Settings →TOPOLOGY Settings**  • Note which cluster is the primary and which is the secondary. • Save a screenshot for future reference. Primary CMP will be noted with a "(p)'
3. ☐	**CMP GUI**: Verify Status of CMP Clusters	**Upgrade Manager → System Maintenance** • Confirm the CMP clusters have the following – ○ **Active/Standby status** ○ **Running Release of 11.5.x version** ○ **Replication ON** ○ **Corresponding Release 12.1.x ISO files copied to at least one of each server types (CMP/MRA/MPE) – Meaning, a copy of the MPE ISO is on one of the MPE servers, an MRA ISO is on one of the MRA servers and a copy of the CMP ISO is on one CMP server**

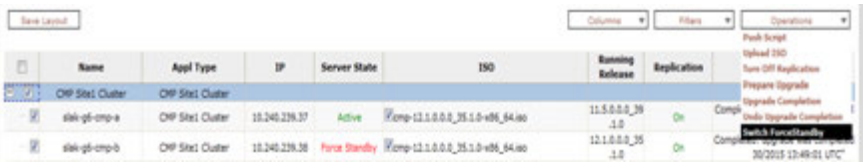
4. ☐	**SSH CLI Primary Active CMP:** exchange keys	• Exchange keys to all servers from the SITE 1 Active Primary CMP. Login as admusr user.
		
		$sudo mount -o loop /var/TKLC/upgrade/cmp-12.1.x..iso /mnt/upgrade/
		
		$sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin
		
		$cd /
		
		$sudo umount /mnt/upgrade
		
		$sudo qpSSHKeyProv.pl --prov
		
		`[admusr@slak-cmp-1b upgrade]$ sudo qpSSHKeyProv.pl --prov`
		
		`The password of admusr in topology:`
		
		• Required to enter the PASSWORD for user admusr
		• Ensure that the Keys are exchanged successfully with all the server clusters –
		
		For example,
		
		Connecting to admusr@slak-mpe-1c (10.250.84.13) …
		Connecting to admusr@slak-cmp-1b (10.250.85.61) …
		Connecting to admusr@slak-mra-1a (10.250.85.4) …
		…….
		….
		[13/16] Provisioning SSH keys on brbg-mra-1b (10.250.84.5) …
		
		[14/16] Provisioning SSH keys on brbg-mra-1a (10.250.84.4) …
		
		[15/16] Provisioning SSH keys on brbg-mpe-1a (10.250.84.7) …
		
		[16/16] Provisioning SSH keys on brbg-cmp-1b (10.250.84.61) …
		
		SSH keys are OK.

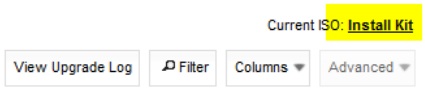
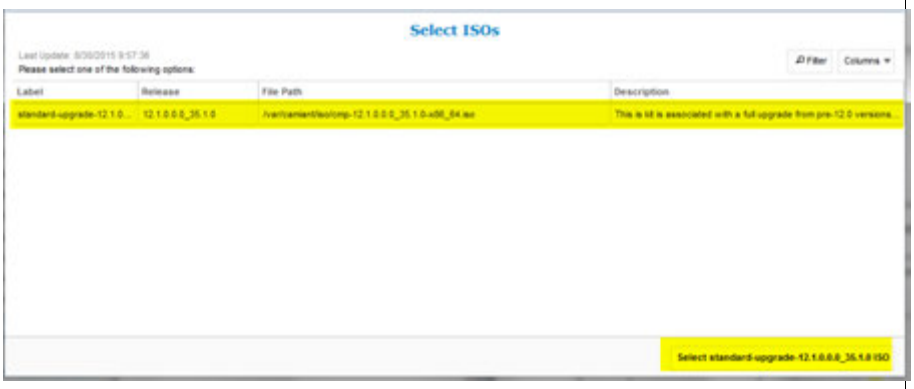
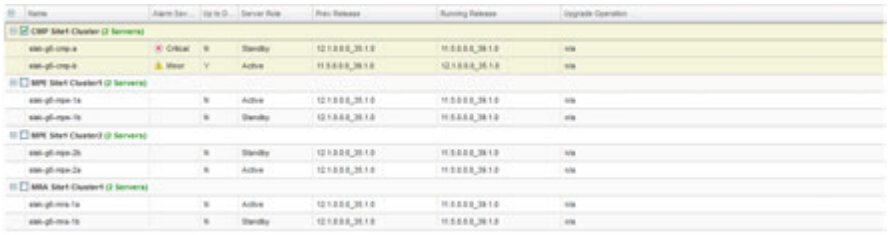
5. ☐	**CMP GUI**: Push the Release 12.1.x upgrade Scripts to all servers in the segment topology	**Upgrade Manager → ISO Maintenance** • Select all the servers in the Topology as shown. • Under **Operations menu, select** "**Push Scripts**" operation. (It is safe to run the push script multiple times as needed)  • Select "OK" to continue the operation. • Operation successful.  **NOTE:** Give the push script a minute to complete
6. ☐	**CMP GUI Access** into Primary CMP Server – Remove old ISO files from servers, if any.	**Upgrade Manager → ISO Maintenance** • Select the server(s) that show any of the OLD ISOs. • Select the server cluster and choose **'delete ISO'** operation to any older ISOs that show.  • Select 'OK' to continue and wait until the successful deletion message appears • Wait until the 'ISO Maintenance' page is refreshed and the ISO column will be blank

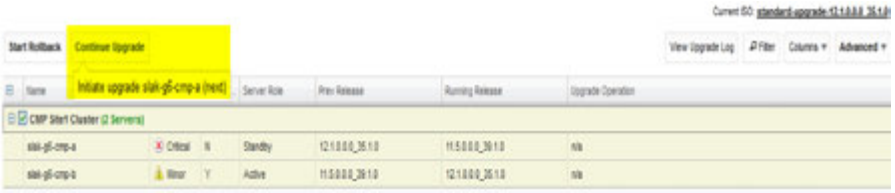
7.	**CMP GUI:** Distribute ISOs to CMP/MPE/MRA servers **NOTE:** This step depends on the ISO type. Distribute ISOs accordingly.	**Upgrade Manager → ISO Maintenance** - (Optional but Preferred) Filter CMP/MPE/MRA servers - One application at a time, check one server type (MPE/MRA/CMP) to be upgraded and perform the '**upload ISOs ' operation** - (this is assumed the ISOs were copied over previously to one of each application type) **Select (CMPs or MPEs or MRAs)-> Operations menu -> upload ISO**  *For example –* **MODE = SCP** **ISO Server IP = <IP address where the ISOs are located >** **USER = admusr** **Password = < admusr password of the server >** **ISO Full Path = /var/TKLC/upgrade/ < server type iso filename >**  • When completed, the ISO column will be populated with the ISO and a notification of "[100%]" 

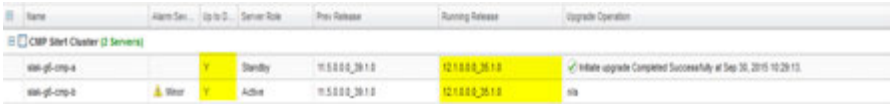
8.	**CMP GUI:** Verify ISO distribution to all the Servers	**Upgrade Manager → ISO Management** • Verify that the Release 12.1.x ISO file of the correct type is shown for each server. • When completed, the ISO column is populated with the ISO and a notification of "[100%]" **NOTE**: For those servers the ISO was copied to from the local machine, there will not be a '100%' indicator. This indicator is only available when transferring ISOs using the ISO management feature.
9.	**CMP GUI**: Set 'Force-Standby' mode on the Standby CMP - Primary Cluster	**Upgrade Manager → System Maintenance** • Select the checkbox for the Standby CMP Server at Primary Site • Under Operations menu, select **Force Standby** operation • Select "OK" to confirm and continue with the operation. • The Standby CMP server state will be changed to "Force Standby"

10.	**CMP GUI:** Upgrade the **Force-Standby** CMP server at the primary site ***NOTE:*** *This will take ~40 minutes to complete.*	**Upgrade Manager → System Maintenance** • Check Force-Standby CMP Server at the Primary Site. • Under **Operation menu**, select '**Start Upgrade'** operation.  • Select "OK" to continue with the operation. • Under "Upgraded Status" column, it will show the In Progress status along with the upgrade activities which typically will take about 40 minutes to complete. • Alarms: **Expected Critical alarm:** **31283** High availability server is offline **Expected Major Alarm:** **31233** HA Path Down **70004** The QP processes have been brought down for maintenance. **70021** The MySQL slave is not connected to the master **Expected Minor Alarms:** **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB replication to slave DB has failed • Wait until "upgrade was completed…." Status message appears  ***Note:*** *If there is other status message appeared other than the "…Upgrade complete…" message, stop here and please contact Oracle Technical Services to troubleshoot and determine if a rollback should be executed.* .
11. ☐	**CMP GUI:** Verify Upgrade Completion is successful	**Upgrade Manager → System Maintenance** • Successful upgrade status will show the Release 12.1.x under the "Running Release" column and the "Upgrade Status" – ***NOTE:*** *Expect the server state role is still shown as "Force Standby" - same as prior to the upgrade.* *Any "Sync Broken" indicator indicates that the data replication between the two servers of the cluster is not synced yet. Do not continue if there is a "sync broken" indicator on the server that was upgraded.*
12. ☐	**CMP GUI:** Verify Alarms	**System Wide Reports → Active Alarms:** Following expected **Alarm(s) ID: 70025** is/are to be seen - • alarm will be cleared after the cluster is fully upgraded to the same release.

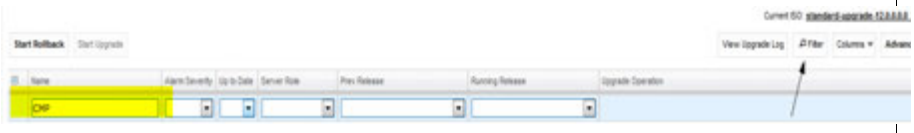
13.	**CMP GUI:** Switch the Upgraded Release 12.1.x CMP server to Active	**Upgrade Manager → System Maintenance** • Select the checkbox for the CMP cluster to be switched – primary cluster only, and • Select the "Switch ForceStandby" operation under Operations menu  • Click on "OK" to continue with the operation and a successful message appears. ***NOTE:*** *At this point, the current CMP GUI browser connection will be lost – if it is the primary CMP cluster, need to re-login as illustrated in the next step.* ***Close the browser and re-open.***
14.	**CMP GUI:** Relogin to the CMP server VIP	• Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. • The Policy Release 12.1.x CMP GUI Login form should appear as shown – Login and password credentials are the same as the pre-upgrade.
15.	**CMP GUI:** verify new Policy Release	**Navigate to help→About. Verify the release number is displayed as 12.1.x**
16.	**CMP GUI:** Critical Alarms	**Critical alarms 70025 will be seen until the SQL Database matches the master (12.1.x) and a minor alarm - 31101.. These alarms are expected and will remain until all CMPs have been upgraded to the same version.** **NOTE: the Upgrade Manager will show the same alarms.**
17.	**CMP GUI:** Verify the Policy Release 12.1.x CMP is Active	**Upgrade→Upgrade Manager** • As noted, the Active CMP server is now on the Running Release of 12.1.x

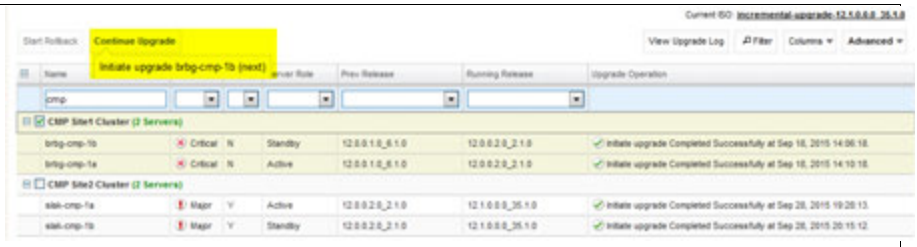
18.	**CMP GUI:** Locate the new 12.1.x Upgrade Manual	**Upgrade → Upgrade Manager** **Select the Current ISO – in this case it is labeled install kit.**  This will pop up a dialog box with a description of the ISO that was just copied into **/var/camiant/iso.** Highlight the available ISO and click the button on the bottom right hand corner of the pop-up window  **Pop-Up confirming – select OK.** Within a few seconds, the 'Up to date' column transition from 'n/a' to 'Y' (meaning up-to-date) or 'N' (meaning needs upgrade). 
19.	**CMP GUI:** New Alarms introduced with 12.1.x	**The Following minor alarms, along with the already active Critical alarms, will now be active.** **Occurrence** | **Severity** | **Alarm ID** | **Text** | **OAM VIP** | **Server** Dec 15, 2015 09:58 AM EST | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10.240.239.16 | kansas-cmp-1a 10.240.239.2 **Occurrence** | **Severity** | **Alarm ID** | **Text** | **OAM VIP** | **Server** Mar 12, 2015 09:22 AM EDT | Minor | 70501 | The Cluster is running different versions of software | 10.250.84.62 | brbg-cmp-1a 10.250.84.60 Mar 12, 2015 09:22 AM EDT | Minor | 70500 | The system is running different versions of software | 10.250.84.62 | brbg-cmp-1a 10.250.84.60

20.	**CMP GUI:** Complete the Upgrade of the Primary CMP Cluster	**Upgrade → Upgrade Manager** Select the Primary Site 1 CMP Cluster The "Continue Upgrade" button will become available, select this button as illustrated below.  Select OK on the POP-UP to continue the upgrade on the remaining server in the CMP cluster Alarms to Note: **Expected Critical alarm:** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm:** **31233** **70004** QP Processes down for maintenance **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **NOTE**: Remaining CMP server will take approximately 40 minutes to complete.

21.	**CMP GUI:** Verify the status of upgraded CMP server.	**Upgrade Manager → Upgrade Manager**  • Successful upgrade status will now show both servers running the Release 12.1.x under the "Running Release" column.- • Active/standby state for both servers in the Primary CMP Cluster. • Active alarms to NOTE **Expected Critical alarm:** **31283** High availability server is offline **70001** QP_procmgr failed **70025** The MYSQL Slave has a different schem version than the master **Expected Major Alarm:** **31233** High Availablity path loss of connectivity **70004** QP Processes down for maintenance **Expected Minor Alarms:** **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **70503** Upgrade Director Server Forced Standby **70507** An Upgrade/Backout action on a server is in progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version
22. ☐	Proceed to next upgrade procedure	• At this point, the Primary Site-1 is running Release 12.1.x • Secondary SITE – if applicable - is on R11.5.x • All 'C' Level Nodes will be on Release 11.5 • Proceed to the next procedure if there is a GR CMP to upgrade. If not, skip to section 8.
THIS PROCEDURE HAS BEEN COMPLETED		

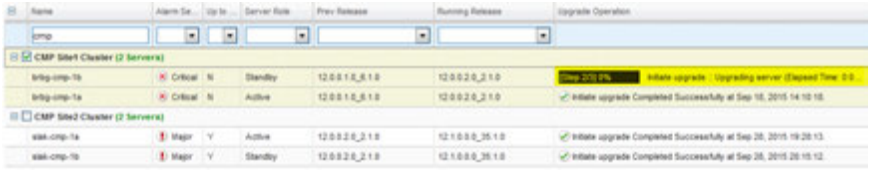
6.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Status of CMP Cluster	**Upgrade → Upgrade Manager** - Primary CMP is completely upgraded to 12.1.x - Secondary CMP Cluster is on 11.5
2. ☐	**CMP GUI**: Upgrade Secondary CMP cluster	**Upgrade → Upgrade Manager** NOTE: The Filter button can be used to show only the CMP servers. Type in CMP under NAME.  • Select the checkbox for the Secondary CMP Server Cluster at Site-2 • Select the 'Start Upgrade' Button.



- Select "OK" to confirm and continue with the operation.

- The specific action taken will be determined by the UM and based on the specific version change being performed.
- This will continue to upgrade the standby server only in the CMP Cluster
- ***NOTE:*** *This will take ~30 minutes to complete.*
- Under "Upgraded Status" column, it will show the In Progress status along with the upgrade activities.



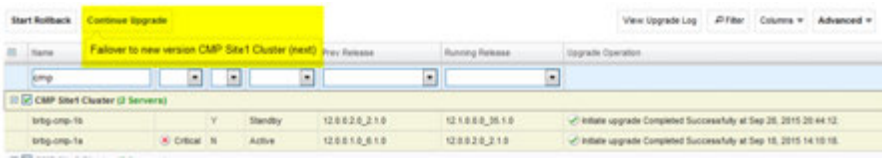
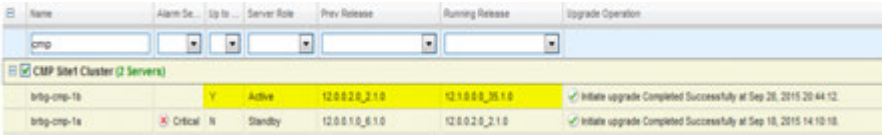
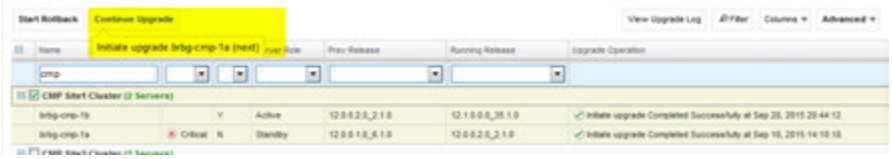
- During the Upgrade activities, the following Alarms may be generated and considered normal reporting events -

Expected Critical alarm:
31283 High availability server is offline
70001 QP_procmgr failed
70025 QP Slave database is a different version than the master

Expected Major Alarm:
70004 QP Processes down for maintenance

Expected Minor Database replication Alarms:
70503 Upgrade Director Server Forced Standby
70507 Upgrade Director In Progress
70500 Upgrade Director System Mixed Version
70501 Upgrade Director Cluster Mixed Version
31114 DB Replication over SOAP has failed
31106 DB Merge To Parent Failure
31107 DB Merge From Child Failure
31101 DB Replication To Slave Failure
31282 HA management fault

LOG FILE from the GUI showing complete on the 1st server on the secondary site.

3.	**CMP GUI**: Continue Upgrade Secondary CMP cluster	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP Server Cluster at Site-2 • Select the 'Continue Upgrade' Button. Notice the message "failover to new version"  • Select "ok" to confirm and continue with the operation, • The specific action will take a minute to complete. Wait until the newly upgraded server is active, as shown below.  • Select the checkbox for the Secondary CMP Server Cluster at Site-2 • ***Select the*** 'Continue Upgrade' Button. When hovering over the continue upgrade button, the message will display the next action, which is upgrading the remaining CMP "hostname"  • Select "ok" to confirm and continue with the operation, • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events - **<u>Expected Critical alarm:</u>** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **<u>Expected Major Alarm:</u>** **70004** QP Processes down for maintenance **<u>Expected Minor Database replication Alarms:</u>** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault

4. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	**Upgrade → Upgrade Manager** • Successful upgrade status will show the Release 12.1.x under the "Running Release" column and the "Upgrade Status" –
5. ☐	**CMP GUI:** Verify Alarms	**System Wide Reports → Alarms → Active Alarms:** Following expected Minor Alarm(s) ID: 70500 System in Mixed version

7. UPGRADE CMP CLUSTERS (12.0 TO 12.1.X)

This procedure will upgrade the Site-1 CMP cluster first, then upgrade the Site-2 CMP cluster in a single maintenance window.

7.1 Upgrade CMP Clusters Overview

Upgrade Primary CMP cluster

1) Use the CMP GUI, Upgrade → Upgrade Manager and upgrade the CMP Secondary Site 1
2) Start Upgrade
3) failover
4) Log back into the CMP GUI and upgrade the remaining Primary CMP's Frc-Stby server (continue upgrade)

Upgrade The Secondary CMP cluster

2) Use the CMP GUI, Upgrade → Upgrade Manager and upgrade the CMP Secondary Site 2
   d. Start Upgrade
   e. Failover
   f. Continue Upgrade

This procedure should not be service affecting, but it is recommended to perform this in a Maintenance Window

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

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

Identify the CMPs sites to be upgraded here, and verify which sites are Primary and Secondary:

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

Note the Information on this CMP cluster:

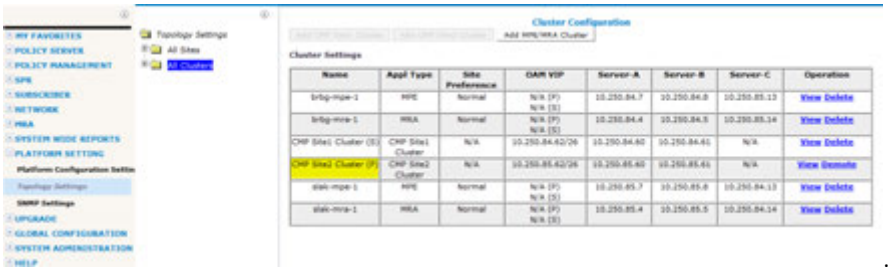
Cluster Name_____
Server-A Hostname _____
Server-A IP _____
Server-A Status _____

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

IMPORTANT:

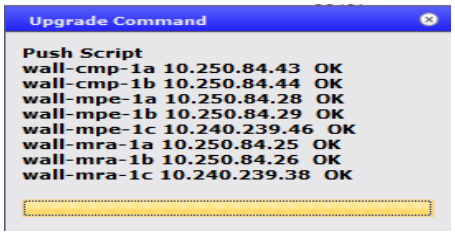
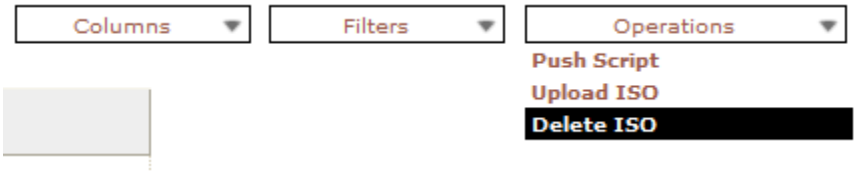
- *CMP servers MUST be upgraded first, before the MPE or MRA clusters*
- *Site-1 CMP MUST be upgraded to the new release first, before the Site-2 CMP*

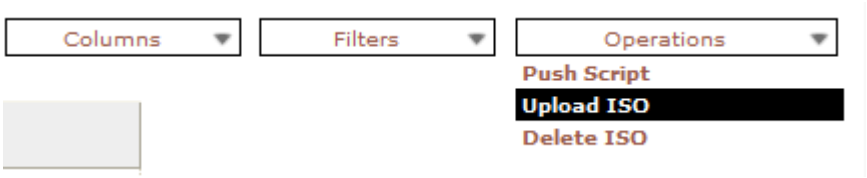
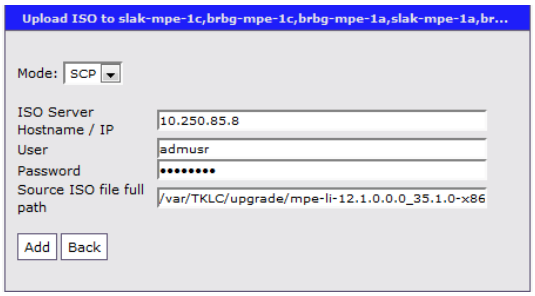
7.1.1 Upgrade primary CMP Cluster

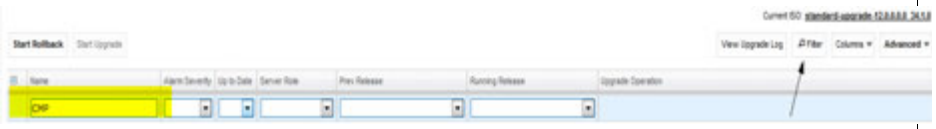
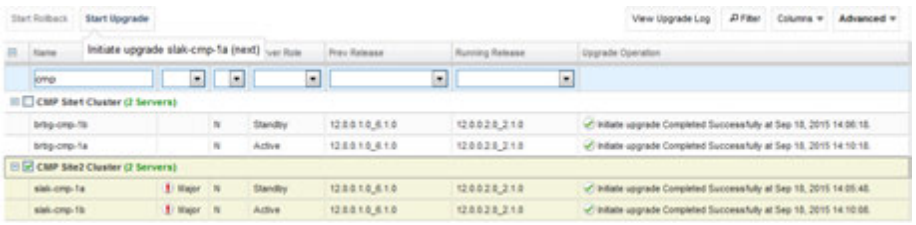
Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Alarm Status.	**System Wide Reports → Alarms→Active Alarms** • Confirm that any existing Alarm is well understood and no impact to the Upgrade procedure. • Capture a screenshot and save it into a file for reference.
2. ☐	**CMP GUI:** Identify and Record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

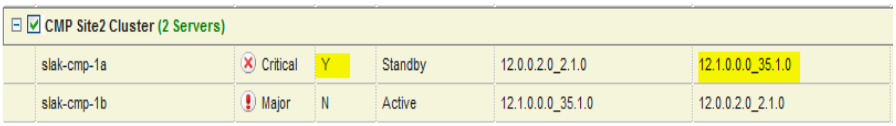
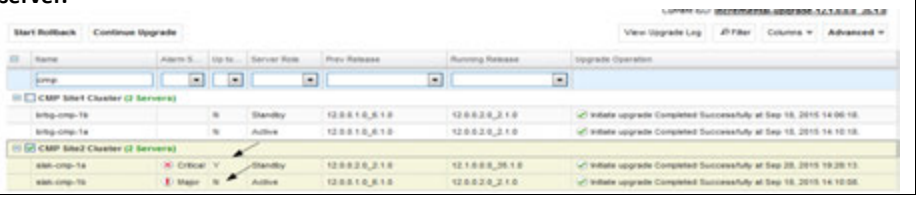
3. ☐	**CMP GUI**: Verify Status of CMP Clusters	**Upgrade Manager → System Maintenance**
		• Confirm the CMP clusters have the following –
		  ○ **Active/Standby status**
		  ○ **Running Release of 12.0.x version**
		  ○ **Replication ON**
		• **Corresponding Release 12.1.x ISO files copied to at least one of each server types (CMP/MRA/MPE)**

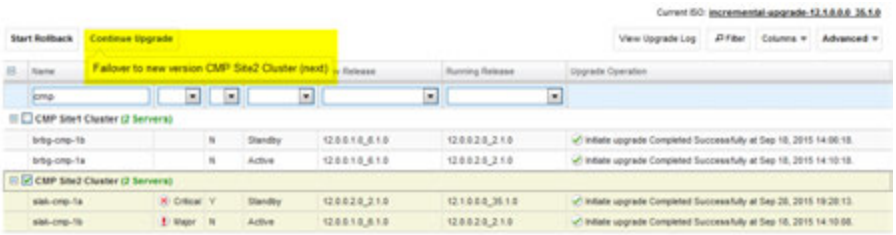
4. ☐	**SSH CLI Primary Active CMP:** exchange keys	• Exchange keys to all servers from the SITE 1 Active Primary CMP. Login as admusr user.
		
		$sudo mount -o loop /var/TKLC/upgrade/cmp-12.1.x _64.iso /mnt/upgrade/
		
		$sudo cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin
		
		$cd /
		
		$umount /mnt/upgrade
		
		$sudo qpSSHKeyProv.pl --prov
		
		`[admusr@slak-cmp-1b upgrade]$ sudo qpSSHKeyProv.pl --prov`
		
		`The password of admusr in topology:`
		
		• Required to enter the PASSWORD for user admusr
		• Ensure that the Keys are exchanged successfully with all the server clusters –
		
		For example,
		
		Connecting to admusr@slak-mpe-1c (10.250.84.13) …
		Connecting to admusr@slak-cmp-1b (10.250.85.61) …
		Connecting to admusr@slak-mra-1a (10.250.85.4) …
		…….
		….
		[13/16] Provisioning SSH keys on brbg-mra-1b (10.250.84.5) …
		
		[14/16] Provisioning SSH keys on brbg-mra-1a (10.250.84.4) …
		
		[15/16] Provisioning SSH keys on brbg-mpe-1a (10.250.84.7) …
		
		[16/16] Provisioning SSH keys on brbg-cmp-1b (10.250.84.61) …
		
		SSH keys are OK.

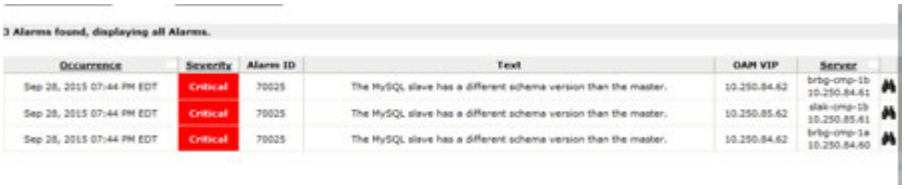
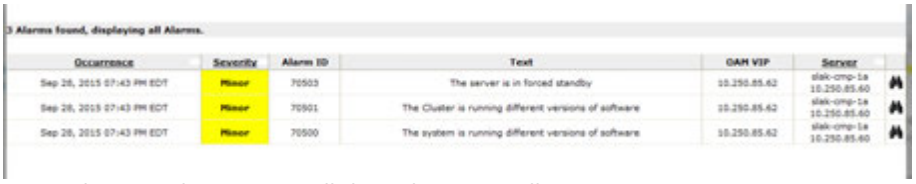
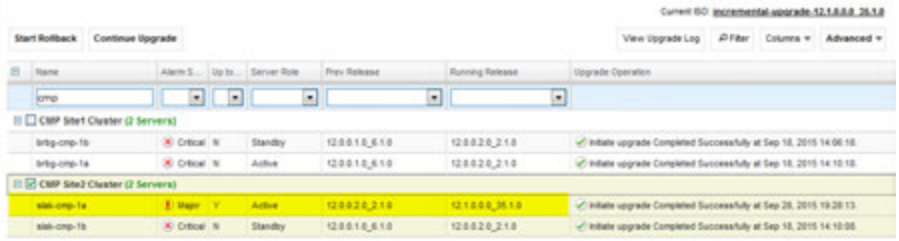
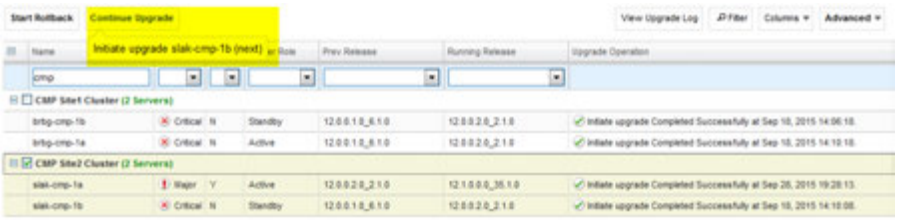
5. ☐	**CMP GUI**: Push the Release 12.1.x upgrade Scripts to all servers in the segment topology	**Upgrade Manager → System Maintenance** • Select all the servers in the Topology as shown. • Under **Operations menu, select** "**Push Scripts**" operation. (It is safe to run the push script multiple times as needed) • Select "OK" to continue the operation. • Operation successful.  **NOTE:** Give the push script a minute to complete
6. ☐	**CMP GUI Access** into Primary CMP Server – Remove old ISO files from servers, if any.	**Upgrade Manager → ISO Maintenance** • Select the server(s) that show any of the OLD ISOs. • Select the server cluster and choose **'delete ISO'** operation to any older ISOs that show.  • Select 'OK' to continue and wait until seeing the successful deletion message • Wait until the 'ISO Maintenance' page is refreshed and the ISO column will be blank

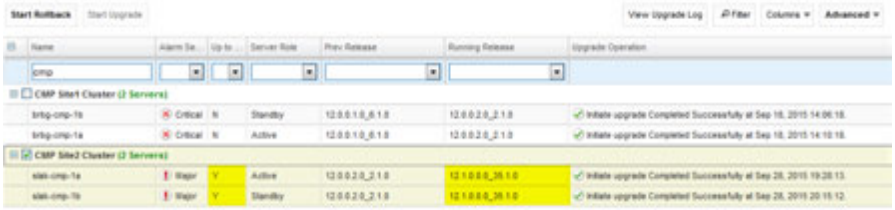
7. ☐	**CMP GUI:** Distribute ISOs to CMP/MPE/MRA servers **NOTE:** This step depends on the ISO type. Distribute ISOs accordingly.	**Upgrade Manager → ISO Maintenance** - (Optional but Preferred) Filter CMP/MPE/MRA servers - One application at a time, check one server type(MPE/MRA/CMP) to be upgraded and perform the '**upload ISOs ' operation** - **Select(CMPs or MPEs or MRAs)-> Operations menu -> upload ISO**  *For example –* **MODE = SCP** **ISO Server IP = <IP address where the ISOs are located >** **USER = admusr** **Password = < admusr password of the server >** **ISO Full Path = /var/TKLC/upgrade/ < server type iso filename >**  • When completed, the ISO column will be populated with the ISO and a notification of "[100%]"
8. ☐	**CMP GUI:** Verify ISO distribution to all the Servers	**Upgrade Manager → ISO Management** • Verify that the Release 12.1.x ISO file of the correct type is shown for each server. • When Completed, the ISO column is populated with the ISO and a notification of "[100%]" **NOTE**: For those servers the ISO was copied to from the local machine, there will not be a '100%' indicator. This indicator is only available when transferring ISOs using the ISO management feature.

9. ☐	**Primary Active CMP:** ssh to primary active CMP and copy iso to /var/camiant/iso	**Logon to the primary active CMP as admusr and copy the 12.1.x ISO to the following directory,** **/var/camiant/iso** **$sudo cp –p /var/TKLC/cmp-12.1.x.iso /var/camiant/iso/** **Verify,** **$ ls /var/camiant/iso/**
10. ☐	**CMP GUI:** Locate the new 12.1.x Upgrade Manual	**Upgrade → Upgrade Manager** **Select the Current ISO – in this case it is labeled install kit.** This will pop up a dialog box with a description of the ISO that was copied into **/var/camiant/iso.** Highlight the available ISO and click the button on the bottom right hand corner of the pop-up window **Pop-Up confirming – select OK.** Within a few seconds, the 'Up to date' column transition from 'Y' (meaning up-to-date) or 'N' (meaning needs upgrade).
11. ☐	**CMP GUI**: Upgrade Primary CMP cluster	**Upgrade → Upgrade Manager** NOTE: The Filter button can be used to show only the CMP servers. Type in CMP under NAME.  • Select the checkbox for the Primary CMP Server Cluster • Select the 'Start Upgrade' Button.  • Select "OK" to confirm and continue with the operation.

		• The specific action taken will be determined by the UM and based on the specific version change being performed. • This will continue to upgrade the standby server only in the CMP Cluster • ***NOTE:*** *This will take ~30 minutes to complete.* • Under "Upgraded Status" column, it will show the In Progress status along with the upgrade activities. • Upgrade Status will change to completed when done. • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events - **Expected Critical alarm:** 31283 High availability server is offline 31227 The high availability status is failed due to raised alarms 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:** 70503, 70507, 70501, 70500 31101, 31282, 31114, 31106, 31107, • Upgrade is complete on the first server in the cluster when the following message (completed successfully) shows under the 'Upgrade Operation' Column. 
12. ☐	**CMP GUI:** Verify the upgrade is successful	**Upgrade → Upgrade Manager** **View the cluster. At this point, one server is on 12.1.x and the other server in the cluster is on 12.0. The up To Date column will show 'Y' for the 12.1.x server and 'N' for the 12.0 server.** 

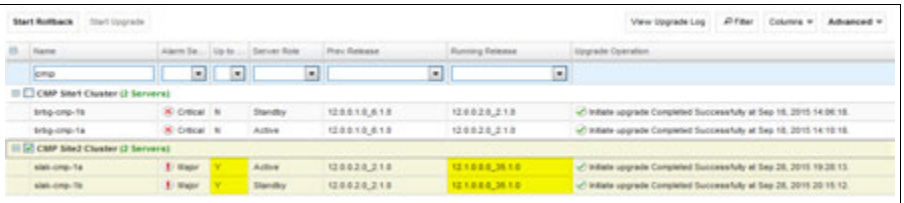
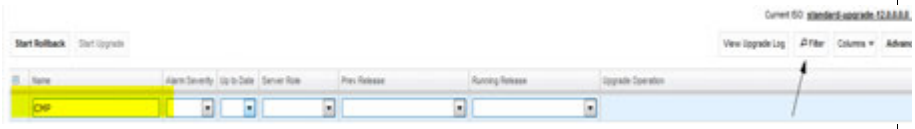
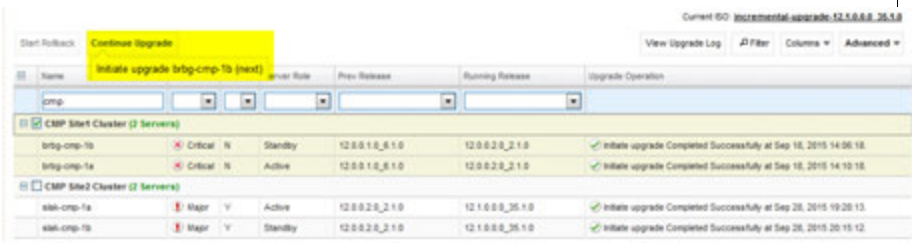
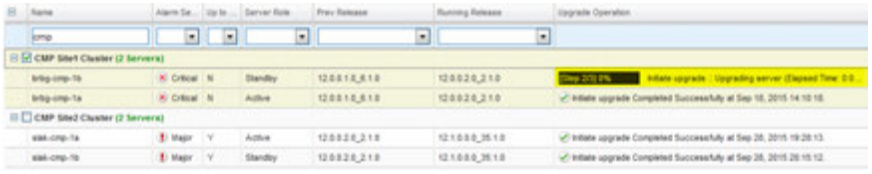
13. ☐	**CMP GUI**: Continue Upgrade CMP cluster	**Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP Server Cluster • Select the 'Continue Upgrade' Button. Notice the message "failover to new version"  • Select "OK" to confirm and continue with the operation, • The specific action will take a minute to complete.
14. ☐	**CMP GUI:** Relogin to the CMP server VIP	• Close the current CMP GUI browser tab and reopen another browser tab with the same CMP VIP address. • The Policy Release 12.1.x CMP GUI Login form should appear as shown – Login and password credentials are the same as the pre-upgrade.
15. ☐	**CMP GUI:** verify new Policy Release	**Navigate to help→About. Verify the release displayed is 12.1.x**

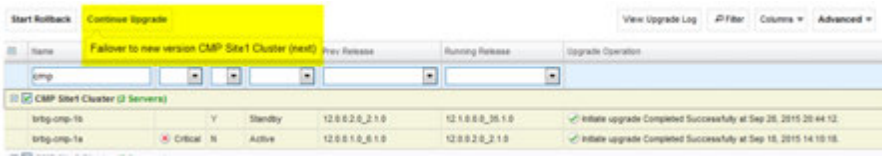
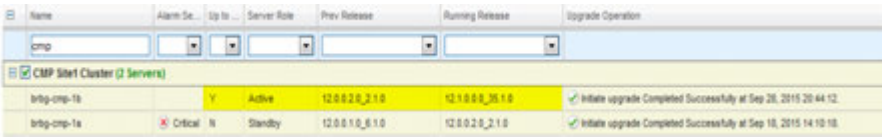
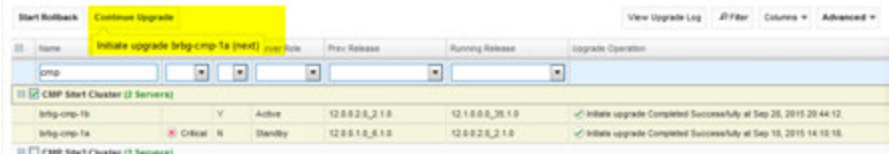
16. ☐	**CMP GUI:** Critical Alarms	**Critical alarms 70025 will be seen until the SQL Database matches the master (12.1.x). These alarms are expected and will remain until all CMPs have been upgraded to the same version.**  3 Alarms found, displaying all Alarms. Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Sep 28, 2015 07:44 PM EDT | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10.250.84.62 | brbg-cmp-1b 10.250.84.61 Sep 28, 2015 07:44 PM EDT | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10.250.85.62 | slak-cmp-1b 10.250.85.61 Sep 28, 2015 07:44 PM EDT | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10.250.84.62 | brbg-cmp-1a 10.250.84.60 **Current Minor Alarms:**  3 Alarms found, displaying all Alarms. Occurrence | Severity | Alarm ID | Text | OAM VIP | Server Sep 28, 2015 07:43 PM EDT | Minor | 70503 | The server is in forced standby | 10.250.85.62 | slak-cmp-1a 10.250.85.60 Sep 28, 2015 07:43 PM EDT | Minor | 70501 | The Cluster is running different versions of software | 10.250.85.62 | slak-cmp-1a 10.250.85.60 Sep 28, 2015 07:43 PM EDT | Minor | 70500 | The system is running different versions of software | 10.250.85.62 | slak-cmp-1a 10.250.85.60 **NOTE: The Upgrade Manager will show alarms as well.**
17. ☐	**CMP GUI:** Verify the Policy Release 12.1.x CMP is Active	**Upgrade→Upgrade Manager** • Verify the following - ○ **Active server is on Running Release 12.1.x** ○ **Standby server is on the previous Release**  Start Rollback | Continue Upgrade | View Upgrade Log | Filter | Columns | Advanced Name | Alarm S... | Up to... | Server Role | Prev Release | Running Release | Upgrade Operation CMP Site1 Cluster (2 Servers) brbg-cmp-1b | Critical | N | Standby | 12.0.0.1.0_6.1.0 | 12.0.0.2.0_2.1.0 | Initiate upgrade Completed Successfully at Sep 18, 2015 14:06:18. brbg-cmp-1a | Critical | N | Active | 12.0.0.1.0_6.1.0 | 12.0.0.2.0_2.1.0 | Initiate upgrade Completed Successfully at Sep 18, 2015 14:10:18. CMP Site2 Cluster (2 Servers) slak-cmp-1a | Major | Y | Active | 12.0.0.2.0_2.1.0 | 12.1.0.0.0_35.1.0 | Initiate upgrade Completed Successfully at Sep 28, 2015 19:28:13. slak-cmp-1b | Critical | N | Standby | 12.0.0.1.0_6.1.0 | 12.0.0.2.0_2.1.0 | Initiate upgrade Completed Successfully at Sep 18, 2015 14:10:08. • As noted, the Active CMP server is now on the Running Release of 12.1.x
18. ☐	**CMP GUI:** Complete the Upgrade of the Primary CMP Cluster	**Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP Server Cluster • Select the 'Continue Upgrade' Button. Notice the message "initiate upgrade"  Start Rollback | Continue Upgrade | Initiate upgrade slak-cmp-1b (next) | View Upgrade Log | Filter | Columns | Advanced Name | Prev Release | Running Release | Upgrade Operation CMP Site1 Cluster (2 Servers) brbg-cmp-1b | Critical | N | Standby | 12.0.0.1.0_6.1.0 | 12.0.0.2.0_2.1.0 | Initiate upgrade Completed Successfully at Sep 18, 2015 14:06:18. brbg-cmp-1a | Critical | N | Active | 12.0.0.1.0_6.1.0 | 12.0.0.2.0_2.1.0 | Initiate upgrade Completed Successfully at Sep 18, 2015 14:10:18. CMP Site2 Cluster (2 Servers) slak-cmp-1a | Major | Y | Active | 12.0.0.2.0_2.1.0 | 12.1.0.0.0_35.1.0 | Initiate upgrade Completed Successfully at Sep 28, 2015 19:28:13. slak-cmp-1b | Critical | N | Standby | 12.0.0.1.0_6.1.0 | 12.0.0.2.0_2.1.0 | Initiate upgrade Completed Successfully at Sep 18, 2015 14:10:08. Select OK on the POP-UP to continue the upgrade on the remaining server in the CMP cluster NOTE: Remaining CMP server will take approximately 30 minutes to complete. **NOTE: Server getting upgraded will go OOS**

19. ☐		**Expected Critical alarm:** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm:** **70004** QP Processes down for maintenance **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault
20. ☐	**CMP GUI:** Tracking the upgrade complete	**Upgrade → Upgrade Manager** **The last step in the upgrade for the first CMP cluster will be to wait for replication to complete.** **From the Upgrade TAB:**
21. ☐	**CMP GUI:** Verify the status of upgraded CMP server.	**Upgrade Manager → Upgrade Manager**  • Successful upgrade status will now show both servers running the Release 12.1.x under the "Running Release" column and 'Y' for both servers under the 'Up To Date' column • Active/standby state for both servers in the Primary CMP Cluster.
22. ☐	Proceed to next upgrade procedure	• At this point, the Primary Site-1 is running Release 12.1.x • Secondary SITE is on R12.0 • Proceed to the next procedure to upgrade the secondary CMP cluster.
THIS PROCEDURE HAS BEEN COMPLETED		

7.1.2 Upgrade Secondary CMP Cluster

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify Status of CMP Cluster	**Upgrade → Upgrade Manager** - Primary CMP is completely upgraded to 12.1.x - Secondary CMP Cluster is on 12.0

		
2. ☐	**CMP GUI**: Upgrade Secondary CMP cluster	**Upgrade → Upgrade Manager** NOTE: The Filter button can be used to show only the CMP servers. Type in CMP under NAME.  • Select the checkbox for the Secondary CMP Server Cluster at Site-2 • Select the 'Start Upgrade' Button.  • Select "OK" to confirm and continue with the operation. • The specific action taken will be determined by the UM and based on the specific version change being performed. • This will continue to upgrade the standby server only in the CMP Cluster • ***NOTE:*** *This will take ~30 minutes to complete.* • Under "Upgrade Operation" column, it will show the In Progress status along with the upgrade activities.  • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events - **<u>Expected Critical alarm:</u>** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **<u>Expected Major Alarm:</u>** **70004** QP Processes down for maintenance **<u>Expected Minor Alarms:</u>**

		70503 Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault **LOG FILE from the GUI showing complete on the 1st server on the secondary site.**
3.	**CMP GUI**: Continue Upgrade Secondary CMP cluster	**Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP Server Cluster at Site-2 • Select the 'Continue Upgrade' Button. Notice the message "failover to new version"  • Select "ok" to confirm and continue with the operation, • The specific action will take a minute to complete. Wait until the newly upgraded server is active, as shown below.  • Select the checkbox for the Secondary CMP Server Cluster at Site-2 • ***Select the*** 'Continue Upgrade' Button. When hovering over the continue upgrade button, the message will display the next action, which is upgrading the remaining CMP "hostname"  • Select "ok" to confirm and continue with the operation, • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events - **Expected Critical alarm:** **31283** High availability server is offline **70001** QP_procmgr failed **70025** QP Slave database is a different version than the master **Expected Major Alarm:** **70004** QP Processes down for maintenance

		Expected Minor Alarms: **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault
4. ☐	**CMP GUI:** Verify Upgrade Completion is successful.	**Upgrade → Upgrade Manager** • Successful upgrade status will show the Release 12.1.x under the "Running Release" column and the "Upgrade Status" – • Also, under Upgrade Operation it will show 'Initiate Upgrade Completed Successfully' with the correct date and time.
5. ☐	**CMP GUI:** Verify Alarms	**System Wide Reports → Alarms → Active Alarms:** **Expected Minor Alarms:** **70500** Upgrade Director System Mixed Version
6.	Procedure is complete.	• All CMP Clusters Upgrade are complete and running Release 12.1.x. • ALL MRAs and MPEs are on Release 12.0 At this point, the PCRF system is running in mixed-version mode.

8. MPE AND MRA UPGRADE

The following procedures will upgrade a site/segment containing one or more MPE cluster(s), and MRA cluster(s).

NOTES:

1. An upgrade of up to 4 clusters can be running at the same time.
2. MPEs and MRAs can be upgraded at the same time.

8.1 Site/Segment Upgrade Preparation

8.1.1 Configuration Preparation

Step	Procedure	Result
1. ☐	**CMP GUI:** Access into CMP server	• Use the supported browser to login as "admin" or user with admin privileges.
2. ☐	**CMP GUI:** Verify Current Upgrade Manager status and Software Release 12.1.x ISO files	**Upgrade → Upgrade Manager** • Verify that all CMP Clusters have both Active, Standb status. • Verify that all MPE & MRA Clusters have both Active, Standby. • Verify that Policy Release 12.1.x ISO files are available for all CMP, MPE & MRA clusters. One ISO per server • Verify that the CMP cluster is upgraded successfully and running Policy Release 12.1.x
THIS PROCEDURE HAS BEEN COMPLETED		

8.2 Upgrade MRA and MPEs

This procedure will upgrade one or more clusters (MPE and/or MRA) at a site/segment.

This procedure is applicable for an 11.5 or 12.0 upgrade to 12.1.x

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

The Upgrade Procedure is essentially the same for an MRA cluster and an MPE Cluster.

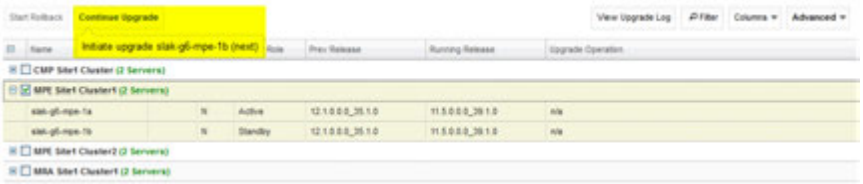
Up to four clusters can be upgraded in parallel (at once).

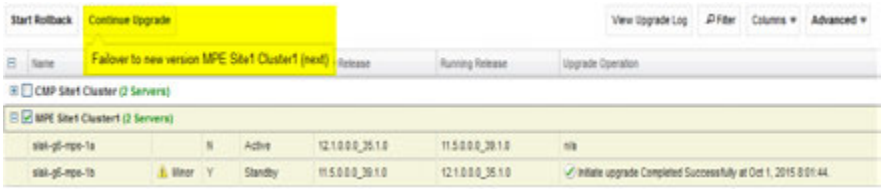
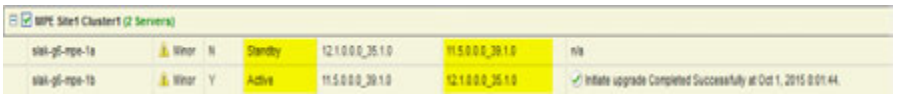
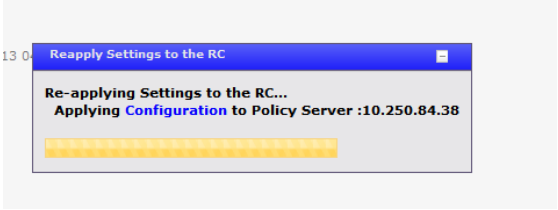
1) Select and start upgrade on Standby server
2) Failover One cluster at a time
3) Re-Apply Configuration one cluster at a time
4) Continue upgrade on remaining server

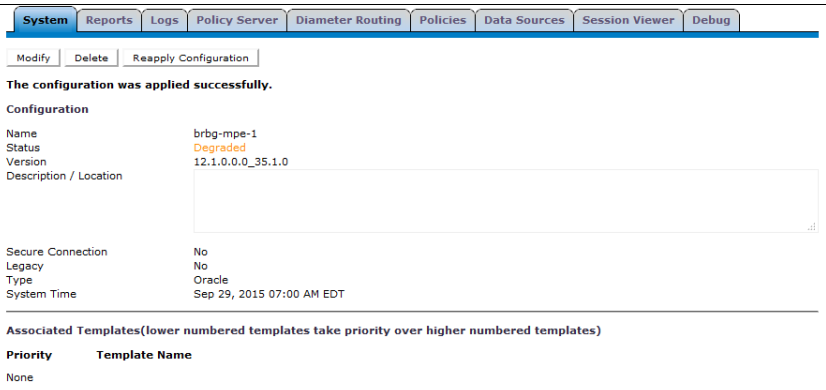
NOTES:

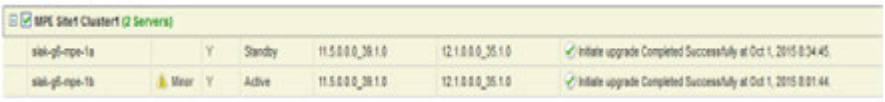
- **All CMP clusters have been upgraded to Policy Release 12.1.x prior executing the following procedures.**
- **The maximum Clusters to be running the upgrade at one time is 4.**
- **Only ONE Cluster can be selected for upgrade activity, 'bulk selection' of servers is not supported in release 12.1.x**

Step	Procedure	Result
1. ☐	**CMP GUI:** Health Checks on the MPE/MRA servers to be upgraded	• Perform the following: - Check for current Active Alarms - Reset MPE/MRA counters to make a baseline For the MPE: **Policy server→configuration→Reports → reset all counters** For the MRA: **MRA→configuration→reports →reset all counters** - Check KPI Dashboard *(capture and save screenshot to a file)*
2. ☐	**CMP GUI:** Verify Upgrade status of selected MPE/MRA site/segment	**Upgrade →Upgrade Manager** • Verify information for the MRAs/MPEs: - **Current Release 11.5.x or 12.0 installed** - **Active/Standby status** - **ISO version to be deployed is 12.1.x** - **Verify Current ISO is 12.1.x using UPGRADE→ISO Maintenance**

Step	Procedure	Result
3.	**CMP GUI**: Upgrade clusters ***NOTE:*** *4 Clusters can be running the upgrade process at one time.* ***NOTE:*** *Each Upgrade of one blade server will take ~35 minutes to complete.*	**Start The upgrade on ONE cluster. Wait for a minute, and then continue with the next cluster and so on. Up to 4 clusters maximum may be running upgrade at any one time.** **Upgrade → Upgrade Manager** • Select the checkbox for the Cluster (One Cluster at a time) (can be an MRA or MPE) • Select the 'Conitnue Upgrade' Button  • Select "OK" to confirm and continue with the operation. It will Begin to Upgrade the standby Server of that cluster. • Wait until the cluster reports "OOS" before selecting the next cluster • Follow the progress status under the "Upgrade Operation" column. • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the MPE cluster is completely upgraded. **Expected Critical Alarms:** **31283** High availability server is offline **70001** QP_procmgr failed **31227** High availability Status Failed **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** High availability path loss of connectivity **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31282** HA management fault **78001** RSYNC Failed • Upgrade is complete on the first server in the cluster when the following message (completed successfully) shows under the 'Upgrade Operation' Column. The server will go back to 'standby' state when the upgrade completes. **Alarms:** **Expected Minor Alarms:** **78001** RSYNC Failed **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **70503** Upgrade Director Server Forced Standby

Step	Procedure	Result
4.	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Next Operation is a **failover** ***NOTE:*** *4 Clusters can be running the upgrade process at one time.*	**Failover ONE cluster at a time. Wait for a minute, before moving on to the next cluster.** **Upgrade → Upgrade Manager** • Select the checkbox for the Cluster (One Cluster at a time) (can be an MRA or MPE) • Select the 'Continue Upgrade' Button. When hovering over the continue upgrade button, it will say 'failover to new version'  • Select "OK" to confirm and continue with the operation. It will Begin to failover the cluster. • Wait until failover completes before failing over the next cluster. And verify the 12.1.x server is now active. Complete is when there is an active/standby 
5.	**CMP GUI:** Reapply Configuration on the MPE/MRA cluster that failed over successfully.	**For MPE: PolicyServer → Configuration → *<MPE cluster name>* → System Tab** **For MRA: MRA→configuration→<MRA cluster>→system tab** • The selected Cluster will have the status shown as "Degraded" with 'Config mismatch' as expected • Select "Reapply Configuration" operation. • NOTE, a progress banner appears for the MPE reapply configuration and NOT the MRA reapply configuration  • Note the "Version" is successfully changed to the upgraded Release 12.1.x

Step	Procedure	Result
		 **NOTE:** *The status still " shown as "Degraded" is a normal reporting event as the servers are in different status.*
6.	**CMP GUI**: Current alarms	**Expected Critical alarm:** **Expected Major Alarm:** **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70502** Upgrade Director cluster replication inhibited **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **71402** Diameter Connectivity Lost **78001** RSYNC Failed **31101** DB Replication To Slave Failure **31113** DB Replication Manually Disabled
7.	***CMP GUI: IF Traffic does not become active within 90 seconds***	**Upgrade Manager → System Maintenance** • Select the checkbox for the partially upgraded cluster, and execute "RollBack" operation. • Release 11.5.x or 12.0 MPE server should become Active and resume handling traffic.
8.	***CMP GUI: Reapply Configuration back to Release 11.5.x or 12.0***	**MPE → Configuration →** *<cluster name>* **→ System Tab** • Select "Reapply Configuration" operation • Verify that the "Version" is changed from 12.1.x to 11.5.x or 12.0, and the action report success. • If NOT, contact Oracle support to consider backout of "Partially Upgraded Cluster" procedure.
9. ☐	**CMP GUI**: Continue Upgrade MRA/MPE clusters. Next Operation is « initiate upgrade». Upgrade on the Standby server	**Continue The upgrade on ONE cluster at a time and when the server goes into OOS, continue with the next cluster and so on. Up to 4 clusters may be running upgrade at one time.** **Upgrade → Upgrade Manager** • Select the checkbox for the Cluster (One Cluster at a time) (can be an MRA or MPE) • Select the 'Continue Upgrade' Button. When hovering over the continue upgrade

Step	Procedure	Result
	***NOTE**: 4 Clusters can be running the upgrade process at one time.*	button, it will say 'initiate upgrade' • Select "OK" to confirm and continue with the operation. It will begin the final server upgrade of the cluster • Wait until the cluster reports "OOS" before selecting the next cluster • Follow the progress status under the "Upgrade Operation" column. • During the Upgrade activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the MPE cluster is completely upgraded. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarm:** **70004** QP Processes down for maintenance **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled • Upgrade is complete when the following message (completed successfully) shows under the 'Upgrade Operation' Column. The server will go back to 'Standby' state and the Up to Date column will show a Y (YES) • Example output of a successful upgrade. • At this point the MPE/MRA Cluster(s) are on Release 12.1.x  **Possible alarms:** **Minor:** 78001, 70500

Step	Procedure	Result
10. ☐	REPEAT the above Steps (1) – (11) for next MPE/MRA cluster(s)	• Proceed with next Cluster(s) – MPE Cluster _____ MPE Cluster _____ MPE Cluster _____ MPE Cluster _____ MRA Cluster _____
11. ☐	**ACCEPT UPGRADE REQUIREMENT**	**with Release 12.1.x, "Accept Upgrade" step is NOT required. It will be embedded as part of the next release upgrade procedure.**
THIS PROCEDURE HAS BEEN COMPLETED		

9. POST UPGRADE HEALTH CHECK

NOTE: This section is executing when the entire Topology is Running Release 12.1.x

Step	Procedure	Result
1. ☐	**CMP GUI:** Verify the upgrade is successful on all CMPs/MRAs/MPEs	**Upgrade → Upgrade Manager** **View the up-to-date, Running release, and Upgrade Operation columns**
2. ☐	**CMP GUI**: View Current alarms	Navigate to System Wide Reports→Alarms→active alarms Only Possible alarms are the following.
3. ☐	**CMP GUI**: View Current KPIs	Navigate to System Wide Reports→KPIDashbord
4.	**CMP GUI:** View trending reports	Navigate to System Wide Reports→Trending Reports
5. ☐	**CMP GUI**: Replication stats	Navigate to System Wide Reports→Others→MPE/MRA Rep Stats
THIS PROCEDURE HAS BEEN COMPLETED		

10. BACKOUT (ROLLBACK)

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

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

Oracle strongly recommends consulting Technical Services & Escalation team before initiating the Backout procedure. They will determine the appropriate course of recovery options.

10.1 Backout Sequence

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

For 11.5, The Upgrade Manager will be used for all of the backouts except the last, or, Primary CMP Server.

1. Backout MRA/MPE - USE UM
2. Backout the Secondary CMP cluster (if applicable). -- USE UM
3. Backout the Primary CMP cluster. -- USE UM and the R11.5.x System Maintenance Manager
4. For 12.0 Backout, the Uprade Manager will be used for all components.

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

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

10.2 Pre-requisites

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

10.3 Backout of Fully-upgraded Cluster

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 backout a cluster that has been fully upgraded. At the end of this procedure, all servers of the target cluster will be on Release 11.5.x or 12.0 (MRA, MPE, CMP) with Active, Standby status.

Expected pre-conditions:

1. Primary Active CMP is on Release 12.1.x
2. Cluster is of MPE, MRA or CMP
3. One server of target cluster is on Release 12.1.x in "Active" role
4. One server of target cluster is on Release 12.1.x in either "Standby" or "Force Standby"

10.3.1 Backout Sequence

This procedure applies to an Active/Standby group of servers. This group of servers will be referred to as a "cluster" or "HA cluster". The cluster types are CMP, MRA or MPE. For CMP cluster, the cluster status may also be Site-1 and/or Site-2.

Required Cluster Backout Sequence (reverse of the Upgrade Sequence) -

1. MRAs and MPEs --- Site 1 and Site-2 clusters – Uses current UM
2. CMP Site-2 cluster (if applicable) -- Uses current UM
3. CMP Site-1 cluster -- Uses current UM and System Maintenance for 11.5, and the UM only for 12.0

NOTE:

It is possible, and desirable, to backout multiple clusters in parallel. However, in order to do this, you must click one cluster at a time, staggering by 1 minute each.

Overview on Backout/Rollback MRA/MPE cluster:
Note: The following procedure should be used to backout a 12.1.x cluster to Policy 11.5/12.0.
This will preserve the cluster as a GR MRA cluster.

1) Use the CMP GUI (Upgrade Manager) to begin the **Backout** of **the MRA/MPE Cluster**
2) **Wait until complete**
3) failover
4) **Use** the CMP GUI (Upgrade Manager) to continue the **Backout** of **the MRA/MPE Cluster**
5) **Use** the CMP GUI (Upgrade Manager) to continue the **Backout** of **the MRA/MPE Cluster**

Backout Secondary CMP(If Applicable):

NOTE:

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

1) Use the CMP GUI (Upgrade Manager) to Backout the Secondary CMP Cluster

Backout Primary CMP (11.5):
NOTE:

Secondary CMP must already be backed out and all of the MPE/MRA Clusters

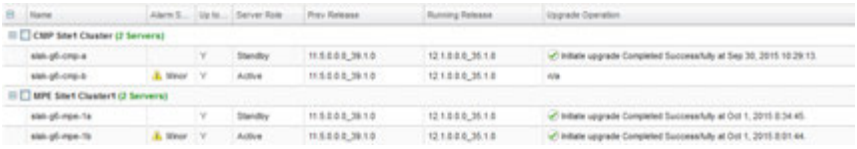
1) Use the CMP GUI (Upgrade Manager) to Backout the Primary standby CMP Cluster
2) Log back in to the Primary CMP VIP
3) Use the 11.5.x System Maintenance to complete backout of the Primary CMP Cluster

Backout Primary CMP (12.0):

1) Use the CMP GUI (Upgrade Manager) to Backout the CMP Cluster

10.3.2 Backout Fully Upgraded MPE/MRA Cluster

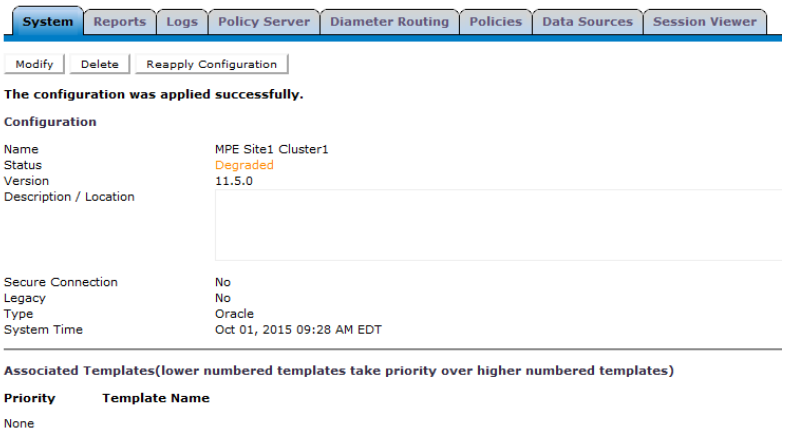
Step	Procedure	Result

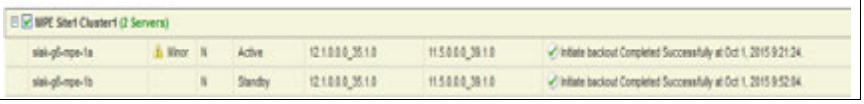
1.	**CMP GUI:** Verify the status of affected Clusters	**Upgrade Manager → Upgrade Manager**
		• Confirm status of the cluster to be backed out –
		  ○ Primary Active CMP is on Release 12.1.x
		  ○ All Standby Servers are on Release 12.1.x
		  ○ Up to Date Column shows 'Y' for all servers
		EXAMPLE:
		 

2.	**CMP GUI**: Rollback standby MPE/MRA clusters ***NOTE:*** *Each backout of one blade server will approximately be completed within 40 minutes time.* ***NOTE:*** *Up to 4 Clusters can be backed out at the same time, selecting one at a time.*	Select the upgraded cluster(s) to backout. **Upgrade → Upgrade Manager** • Select the checkbox for the Cluster (One Cluster at a time) (can be an MRA or MPE) • Select the 'Start Rollback' Button. When hovering over the button, it will inform you of the server to get backed out, in this case it will be the current standby server. • Select "OK" to confirm and continue with the operation. It will Begin to backout. • Follow the progress status under the "Upgrade Operation" column. • At this point, the server backing out will go into 'OOS' state • Wait until the server goes to an OOS state before selecting the next cluster to backout. • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms:**

Step	Procedure	Result
		70503 Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31282** HA Management Fault • Backout of the server is complete when the following message (initiate backout completed successfully) shows under the 'Upgrade Operation' Column. The server will show running release of 11.5.x and return to standby

Step	Procedure	Result
3.	**CMP GUI**: Continue the backout of the MRA/MPE clusters. Next Operation is « failover» to the 11.5.x server. ***NOTE:*** *Up to 4 Clusters can be backed out at the same time, selecting one at a time.*	• Select the cluster to backout. Current state of the cluster needs to be as follows. Active server On Release 12.1.x Standby Server On Release 11.5.x Upgrade → Upgrade Manager • Select the checkbox for the Cluster (One Cluster at a time) (can be an MRA or MPE) • Select the 'Continue Rollback' Button. When hovering over the button, it will inform you to failover to old version, which is 11.5.x • Select "OK" to confirm and continue with the operation. It will Begin to failover. • Wait until the server fails over before selecting the next cluster. This will take a minute or 2. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit Blocked **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31282** HA Management Fault

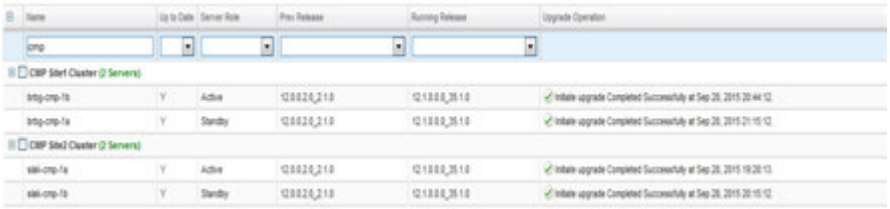
Step	Procedure	Result
4.	**CMP GUI:** Reapply Configuration on MPE/MRA cluster that competed the failover successfully.	**For MPE: PolicyServer → Configuration → *<MPE cluster name>* → System Tab** **For MRA: MRA→configuration→<MRA cluster>→system tab** • The selected Cluster will have the status shown as 'Degraded" as expected • Select "Reapply Configuration" operation. - **The MPE will show a dialog box showing progress of the reapply, the MRA will not show anything.** • Note the "Version" is successfully changed to the previous Release, example shows 11.5 **NOTE:** *The status still " shown as "Degraded" is a normal reporting event as the servers are in different status.* 

Step	Procedure	Result
5.	**CMP GUI**: Complete Backout of cluster(s) ***NOTE:*** *Each backout of one blade server will approximately be completed within 35 minutes time.* ***NOTE:*** *Up to 4 Clusters can be backed out at the same time, selecting one at a time.*	**Select the partially Backed out cluster** **Upgrade → Upgrade Manager** • Select the checkbox for the Cluster (One Cluster at a time) (can be an MRA or MPE) • Select the 'Continue Rollback' Button. When hovering over the button, it will inform you of the server to get backed out. • Select "OK" to confirm and continue with the operation. It will Begin to backout. • Follow the progress status under the "Upgrade Operation" column. • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit Blocked **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31282** HA Management Fault • Backout of the server is complete when the following message (initiate backout completed successfully) shows under the 'Upgrade Operation' Column. **All of the servers will be on Release 11.5.x or 12.0 at this point and show active/standby** 

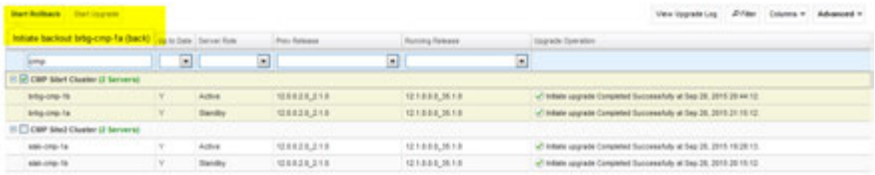
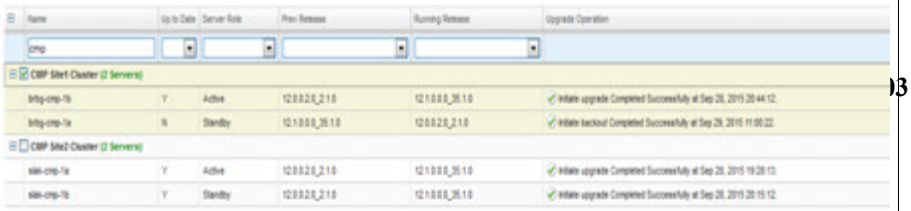
Step	Procedure	Result
6.		**Repeat this Procedure for remainder of MPE/MRA servers, if not fully backed out yet.**
THIS PROCEDURE HAS BEEN COMPLETED		

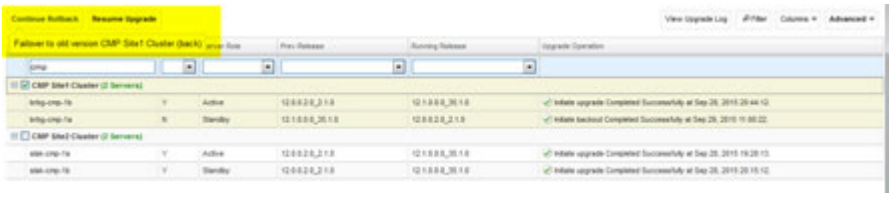
10.3.3 Backout Fully Upgraded Secondary CMP Cluster

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For Rollback to R12.0, the Upgrade Manager is used.

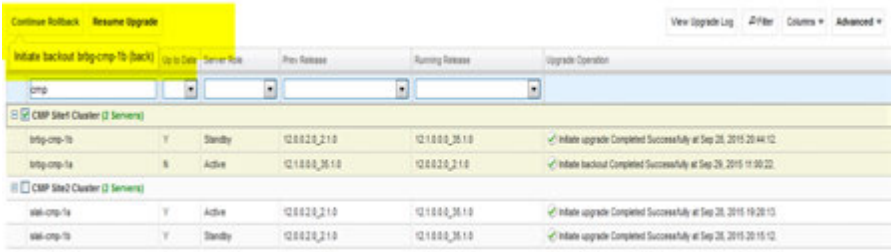
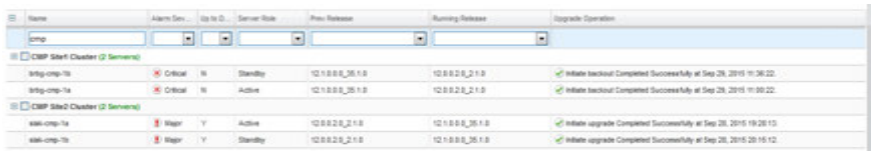
Step	Procedure	Result
1.	**CMP GUI:** Verify the status of the CMP Clusters	**Upgrade Manager → System Maintenance** • Confirm status of the cluster to be backed out – o Primary Active CMP is on Release 12.1.x o Standby Servers are on Release 12.1.x o Up to Date Column shows 'Y' for all servers o Use the Filter button and enter 'cmp' in the box as shown below *EXAMPLE:* 

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For Rollback to R12.0, the Upgrade Manager is used.

Step	Procedure	Result
2.	**CMP GUI**: backout secondary cmp cluster ***NOTE:*** *Each backout of one server will take ~40 minutes to complete.*	**Select Secondary CMP cluster to backout.** **Upgrade → Upgrade Manager** • Select the checkbox for the secondary CMP Cluster • Select the 'Start Rollback' Button. When hovering over the button, it will inform you of the server to get backed out.  • Select "OK" to confirm and continue with the operation. It will Begin to backout. Server will go in an 'OOS' server Role • Follow the progress status under the "Upgrade Operation**"** column. • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **<u>Expected Critical Alarms:</u>** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **<u>Expected Major Alarm:</u>** **70004** QP Processes down for maintenance **31233** HA Path Down **31126** Audit Blocked **<u>Expected Minor Alarms:</u>** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31282** HA Management Fault • Backout of the server is complete when the following message (initiate backout completed successfully) shows under the 'Upgrade Operation' Column. The server will go back to standby state and show the previous release 

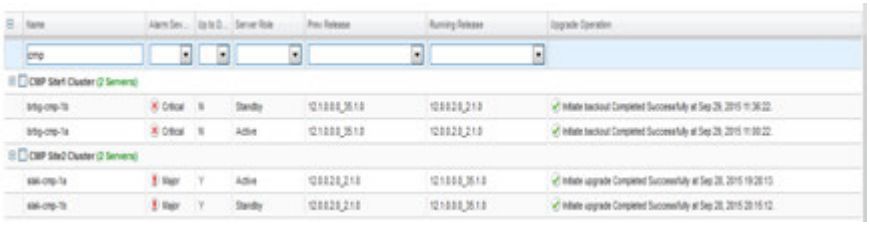
NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For Rollback to R12.0, the Upgrade Manager is used.		
Step	**Procedure**	**Result**
3.	**CMP GUI**: Continue the backout. Next Operation is « failover»	**Select Secondary CMP Cluster.** **Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP cluster • Select the 'Continue Rollback' Button. When hovering over the button, it will inform you to failover."  • Select "OK" to confirm and continue with the operation. It will Begin to failover. • Wait until the previous release becomes active before continuing **Expected Critical alarm:** **70025** QP Slave database is a different version than the master **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70500** Upgrade Director System Mixed Version

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For Rollback to R12.0, the Upgrade Manager is used.

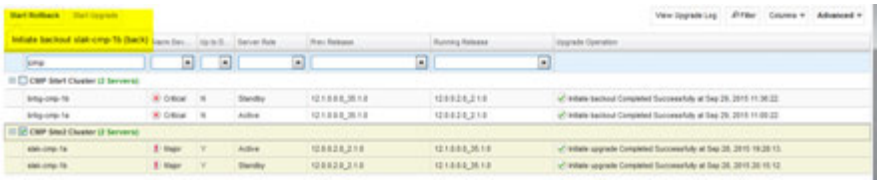
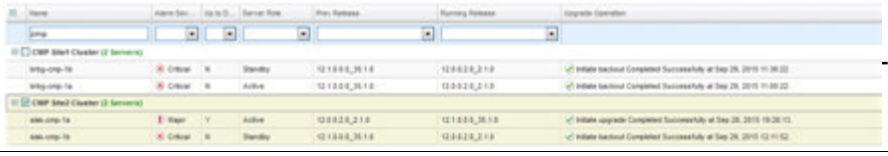
Step	Procedure	Result
4.	**CMP GUI**: Continue the backout. Next Operation is « initiate backout»	**Select Secondary CMP Cluster.** **Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP cluster • Select the 'Continue Rollback' Button. When hovering over the button, it will inform you to rollback  • Select "OK" to confirm and continue with the operation. It will Begin to failover. • Follow the progress status under the 'Server Role' Column.  **Expected Critical alarm:** **70025** QP Slave database is a different version than the master **Expected Minor Alarms:** **70500** Upgrade Director System Mixed Version
THIS PROCEDURE HAS BEEN COMPLETED		

10.3.4 Backout Fully Upgraded Primary CMP Cluster

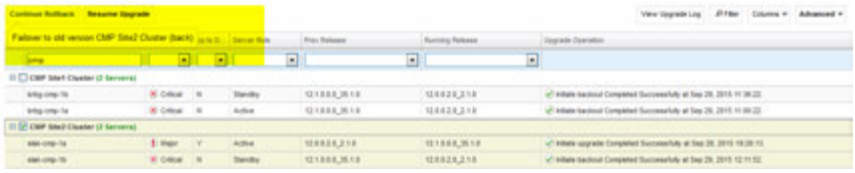
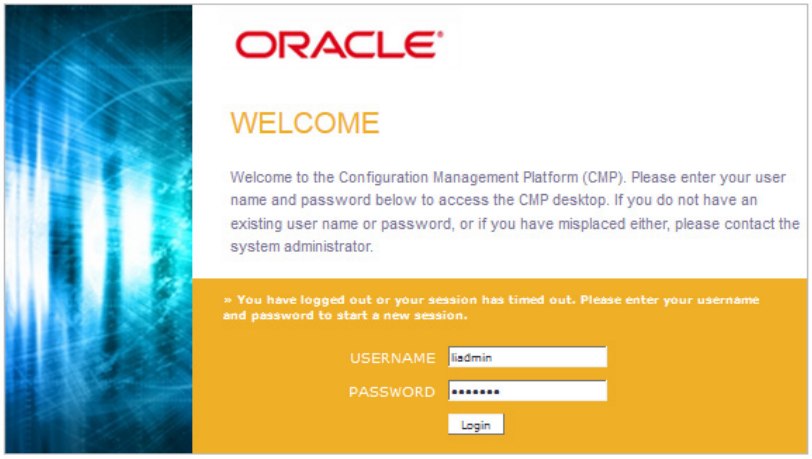
NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For rollback to R12.0, only use the Upgrade Manager.

Step	Procedure	Result
1.	**CMP GUI:** Verify the status of the CMP Clusters	**Upgrade Manager → System Maintenance** • Confirm status of the cluster to be backed out – o Primary Active CMP is on Release 12.1.x o Secondary CMP Cluster is on Release 11.5.x or 12.0 o Up to Date Column shows 'Y' for all servers in Primary CMP Cluster o Use the Filter button and enter 'cmp' in the box *EXAMPLE:* 

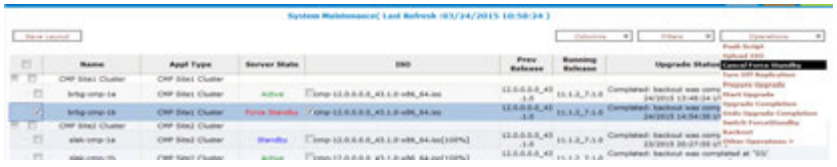
NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For rollback to R12.0, only use the Upgrade Manager.

Step	Procedure	Result
2.	**CMP GUI**: backout standby Primary CMP cluster ***NOTE:*** *backout of one server will take ~40 minutes to complete.*	**Select Primary CMP cluster to backout.** **Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP Cluster • Select the 'Start Rollback' Button. When hovering over the button, it will inform you of the server to get backed out.  • Select "OK" to confirm and continue with the operation. It will Begin to backout. Server will go in an 'OOS' server Role • Follow the progress status under the "Upgrade Operation**"** column. • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **31236** HA Link Down **Expected Major Alarm:** **70004** QP Processes down for maintenance **31233** HA Path Down **Expected Minor Alarms:** **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited • Backout of the server is complete when the following message (initiate backout completed successfully) shows under the 'Upgrade Operation' Column. The server will go back to standby state and show the previous release. 

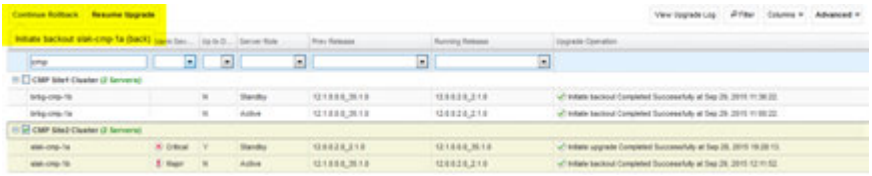
NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For rollback to R12.0, only use the Upgrade Manager.

Step	Procedure	Result
3.	**CMP GUI**: Continue the backout. Next Operation is « failover»	**Select Primary CMP Cluster.** **Upgrade → Upgrade Manager** • Select the checkbox for the Secondary CMP cluster • Select the 'Continue Rollback' Button. When hovering over the button, it will inform you to failover."  • Select "OK" to confirm and continue with the operation. It will Begin to failover. • **Failover takes a couple minutes.**
4.	**CMP GUI**: Log back in to the Primary CMP VIP	**After failover, you will be required to log back in to the CMP GUI using the Primary CMP VIP.** 
5.	**CMP GUI:** Verify release	**Navigate to help→About. Verify the release number is displayed as either 11.5 or 12.0** **If Rollback is for release 11.5, continue with step 6.** **If Rollback is for Release 12.0, continue with step 8**

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For rollback to R12.0, only use the Upgrade Manager.

Step	Procedure	Result
6.	**CMP GUI (Release 11.5)**: Continue the backout of the Primary CMP Cluster ***NOTE:*** *backout of one server will take ~30 minutes to complete.*	**Upgrade → System Maintenance** • Select the checkbox for the remaining server in the Primary CMP Cluster. The server will be on 12.1.x and show 'Forced Standby' • Select operations→backout • Click on "OK" on the pop up to continue • Follow the progress status under the Upgrade Status' Column. Wait until the server to backout comes to backout complete. • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **Expected Major Alarm:** **31233** High availability path loss of connectivity **31236** HA Link Down **70004** QP Processes down for maintenance **Expected Minor Alarms:** **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled **31284** HA remote subscriber heartbeat
7.	**CMP GUI**: Remove Forced standby	**Upgrade → System Maintenance** • Select the checkbox for the remaining server in the Primary CMP Cluster. The server will be on 11.5.x and show 'Forced Standby' • NOTE: A refresh of the current screen may be necessary at the 40 minute mark. • **Select operations→cancel forced standby** 

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For rollback to R12.0, only use the Upgrade Manager.

Step	Procedure	Result
8.	**CMP GUI (Release 12.0)**: Continue the backout of the Primary CMP Cluster ***NOTE:*** *backout of one server will take ~40 minutes to complete.*	**Select Primary CMP cluster to complete the backout.** **Upgrade → Upgrade Manager** • Select the checkbox for the Primary CMP Cluster • Select the 'Start Rollback' Button. When hovering over the button, it will inform you of the server to get backed out. At this point it will be the remaining standby server  • Select "OK" to confirm and continue with the operation. It will Begin to backout. Server will go in an 'OOS' server Role • Follow the progress status under the "Upgrade Operation**"** column. • During the backout activities, the following Alarms may be generated and considered normal reporting events – these will be cleared after the cluster is completely backed out. **Expected Critical Alarms:** **31283** High availability server is offline **31227** High availability Status Failed **70001** QP_procmgr failed **Expected Major Alarm:** **70004** QP Processes down for maintenance **Expected Minor Alarms:** **70503** Upgrade Director Server Forced Standby **70507** Upgrade Director In Progress **70500** Upgrade Director System Mixed Version **70501** Upgrade Director Cluster Mixed Version **78001** RSYNC Failed **70502** Upgrade Director Cluster Replication Inhibited **31114** DB Replication over SOAP has failed **31106** DB Merge To Parent Failure **31107** DB Merge From Child Failure **31101** DB Replication To Slave Failure **31102** DB Replication from Master Failure **31113** DB Replication manually Disabled • Backout of the server is complete when the following message (initiate backout completed successfully) shows under the 'Upgrade Operation' Column. The server will go back to standby state and show the previous release

NOTE: The Secondary CMP Site-2 cluster to be backed out first using the Upgrade Manager -- followed by the Primary CMP Site-1 cluster using both the upgrade Manager and the 11.5.x System maintenance Option. For rollback to R12.0, only use the Upgrade Manager.		
Step	**Procedure**	**Result**
9.		**This completes the RollBack**
THIS PROCEDURE HAS BEEN COMPLETED		

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

Access to Oracle's Customer Support site is restricted to current Oracle customers only. This section describes how to log into Oracle's Customer Support site and link to 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 and http://www.oracle.com/us/corporate/acquisitions/tekelec/support/index.html