Oracle® Communications Policy and Charging Rules Function

PCRF Cable Policy 9.3 to 11.5 Upgrade

Release 11.5

E61663-01

February 2015

ORACLE®

Oracle® Communications Policy and Charging Rules Function, Cable Policy 9.3 to 11.5 Upgrade, Release 11.5

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

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

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

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

1. Introduction

1.1 Purpose and Scope

Due to the recent transition of Cable Policy solution to TPD platform, software upgrade to release 11.5 will only be supportable from TPD based Releases 9.3 and 9.4.
This document describes the procedures to upgrade Cable Policy solution from release 9.3 to release 11.5. The upgrade includes the TPD upgrade.

Cable Policy software 9.3 customers only have it deployed HP ProLiant DL380pG8 RMS equipment accordingly the upgrade to 11.5 is also supported on this Hardware type.

Policy 11.5 is based on Platform 6.7 release and contains the following major components releases:

- Oracle Linux OS 6.5
- TPD 6.7
- COMCOL (In-memory DB) 6.3
- Policy components: MPE, MA, BOD and CMP 11.5

Note: During the upgrade period the Cable Policy system may have configuration where some of CMPs, and MPEs are running Release 9.3 software and some are running Release 11.5 software. This could result in some alarms which will be suppressed after the full solution is upgraded and reaches one coherent release.

1.2 Supporting Documentation

[1] *PD001866 Formal Peer Review Process*
[2] *FE007452 Cable Reference Architecture*
[3] *FD008005 Release 11.5 Upgrade*
[4] *TR007406 Upgrade guide to 11.5 from releases 9.3/9.4*
[5] *FD008102 Policy platform multiple modes*

1.3 9.3 upgrade considerations

- The upgrade is only covering CMP and MPE components' upgrade since those are the components included in 9.3 Cable Policy release so current 9.3 customers only implemented these 2 policy components.

- Back Plane link was not introduced in 9.3 Cable PCRF release, however it should be available and configured (cabled in the correct Ethernet ports "eth04 & eth14") before upgrade since it is a mandatory setup to complete the upgrade process to 11.5 successfully.

Cable Policy solution is upgraded in the following order:

- CMP (Primary Site, then Secondary Site if present)
- MPE-R
- MPE-S

And in case of back out, it should be performed in the reverse order: MPE Clusters → Site2 CMP cluster (if present) → Site 1 CMP Cluster.

1.4 Upgrade infrastructure

Upgrade is supported from Release 9.3 on DL380Gen8 HP rack mount server:

Source	Destination	Hardware	Direct-Link before upgrade	Direct-Link after upgrade
9.3	11.5/Cable	DL380G8	None	Enable

1.5 Required Materials

GA released version of Cable Policy components (CMP, MPE) ISO images on CD/DVD/USB drive or local in the machine used in case of remote installation

1.6 Acronyms

Acronym	Definition
GUI	Graphical User Interface
HA	High Availability
MPE-R	Multimedia Policy Engine (Routing) also known as tier 1 Policy Server
MPE-S	Multimedia Policy Engine (Serving) also known as tier 2 Policy Server
CMP	Camiant Management Platform
OAM	Operation, Administration and Management
SIG	Signaling Network
CD	Compact Disk
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
OS	Operating System (e.g. TPD)
RMS	Rack Mount Server
SFTP	SFTP Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution

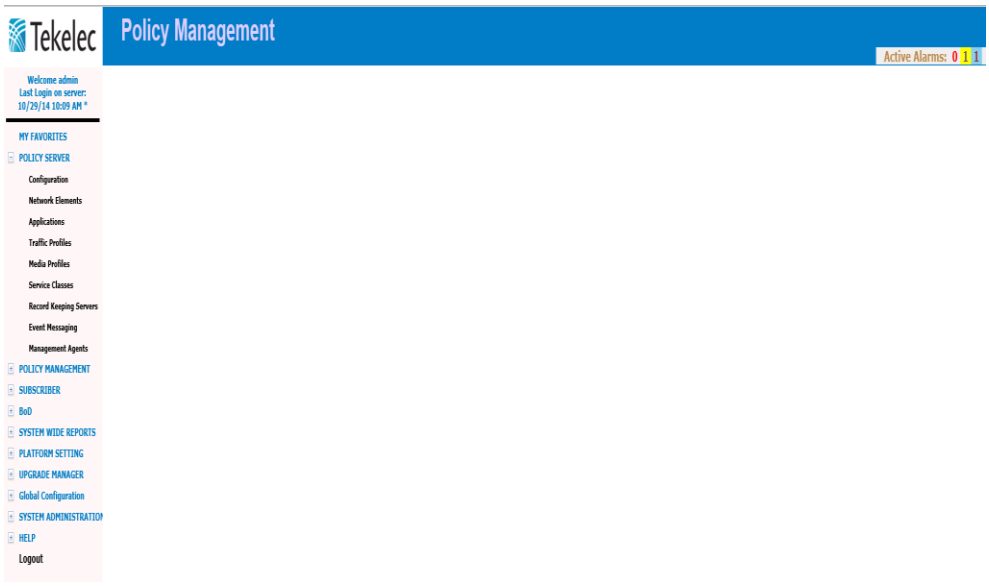
Table 1 Acronyms

2. CMP Cluster(s) Upgrade

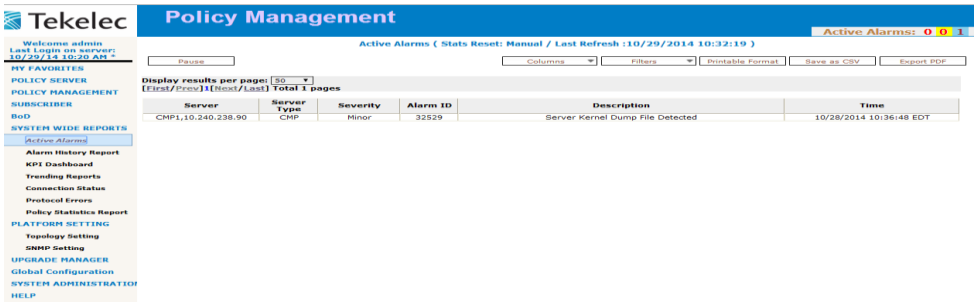
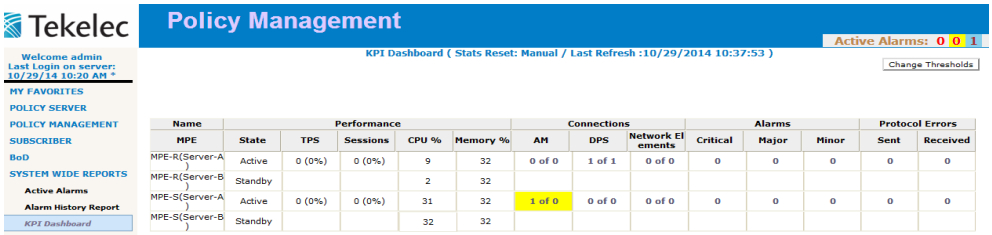
2.1 CMP Pre-Upgrade checks

Procedure 1: CMP pre-Upgrade checks

Procedure 1. CMP Pre-Upgrade checks

S T E P #	This procedure will check the health and state of every component of the Cable Policy solution to ensure the readiness before the upgrade. **Needed material:** - Access to customer's network to access the Cable Policy solution - CMP OAM VIP - Admin login to CMP	
1. ☐	**Computer on solutions' network or remote access to solutions' network:** Login to CMP	Open a browser and enter CMP's OAM VIP to Navigate to CMP GUI:  Enter the password for the admin account and push "Login": 

Procedure 1. CMP Pre-Upgrade checks

2. ☐	**CMP GUI:** Check active alarms	Navigate to System Wide Reports → Active Alarms  Inspect the displayed MAJOR alarms if any and analyze them to confirm they will not impact the upgrade process.
3. ☐	**CMP GUI:** Check KPI Dashboard	Navigate to System Wide Reports → KPI Dashboard  Ensure system is not overloaded and running in an adequate metrics from CPU / Memory / transactions perspective
4.	**BP link preparation:** Connect BP link cables between mates of each cluster	Connect the primary BP link cable on eth04 interface and the secondary BP link cable on eth14 between mates on each of the clusters in the policy management solution. Validate that system works correctly without issues and no major alarms exist after connecting the BP links.

Procedure 2: Exchange SSH Keys

Procedure 2: Exchange SSH keys from Active CMP

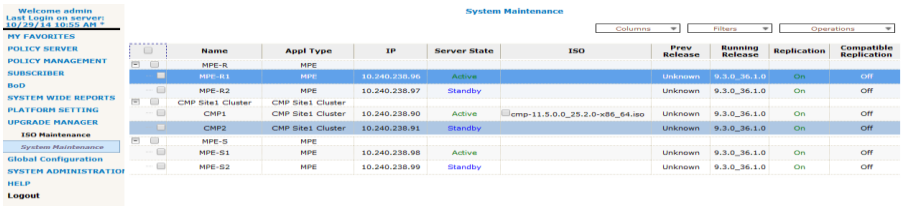
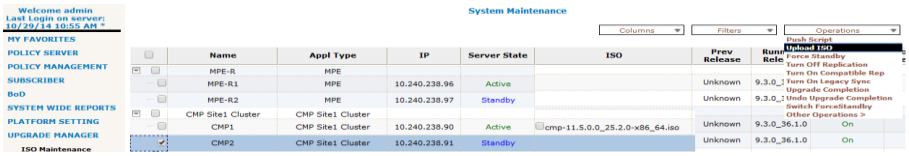
S T E P #	This procedure will make sure SSH keys are exchanged from Active CMP to the different servers of the Cable Policy solution servers. **Needed material:** - Root access to CMP active CLI	
1. ☐	**9.3 Active CMP CLI:** Connect to CLI	SSH to 9.3 Active CMP CLI as root: root@CMP1:~ login as: root root@10.240.238.90's password: Last login: Mon Oct 27 14:40:57 2014 from 10.20.1.36 [root@CMP1 ~]#
2. ☐	**9.3 Active CMP CLI:** Validate if keys are exchanged	Run the following command to check if SSH keys status: [root@CMP1 ~]# policySSHKey.pl --command checkSSHKeys Check SSH Key exchange status with All C level Nodes: Begin to check node:C1484.001 Begin to check node:C1421.100 Begin to check node:C0019.052 Begin to check node:C1421.176 Begin to check node:C0019.102 Begin to check node:C3181.106 Begin to check node:C3181.253 Begin to check node:C1484.088 ---------- NodeID IP Result C1484.001 10.240.238.97 not exchanged C1421.100 10.240.238.99 not exchanged C0019.052 10.240.238.94 not exchanged C1421.176 10.240.238.98 not exchanged C0019.102 10.240.238.95 not exchanged C3181.106 10.240.238.92 not exchanged C3181.253 10.240.238.93 not exchanged C1484.088 10.240.238.96 not exchanged [root@CMP1 ~]#
3. ☐	**9.3 Active CMP CLI:** Exchange the SSH keys	In case the results of the previous step include “not exchanged”, run the following command to perform the SSH keys exchange:

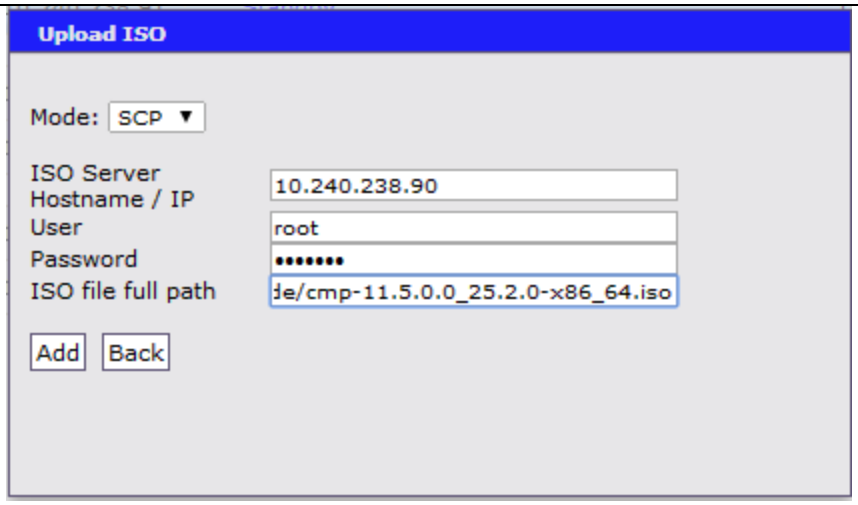
```
[root@CMP1 ~]# policySSHKey.pl --command syncSSHKeys
Sync SSH Key with All C level Nodes:
Begin to sync SSH key with node:C1484.001
Begin to sync SSH key with node:C1421.100
Begin to sync SSH key with node:C0019.052
Begin to sync SSH key with node:C1421.176
Begin to sync SSH key with node:C0019.102
Begin to sync SSH key with node:C3181.106
Begin to sync SSH key with node:C3181.253
Begin to sync SSH key with node:C1484.088
---------------------------------
NodeID          IP                  Result
C1484.001       10.240.238.97       exchanged key successfully
C1421.100       10.240.238.99       exchanged key successfully
C0019.052       10.240.238.94       exchanged key successfully
C1421.176       10.240.238.98       exchanged key successfully
C0019.102       10.240.238.95       exchanged key successfully
C3181.106       10.240.238.92       exchanged key successfully
C3181.253       10.240.238.93       exchanged key successfully
C1484.088       10.240.238.96       exchanged key successfully
[root@CMP1 ~]#
```

2.2 Prepare ISO image

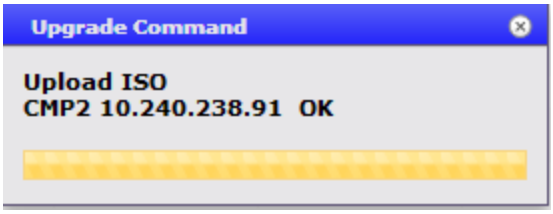
Procedure 3: Prepare ISO image

Procedure 3: Prepare ISO image

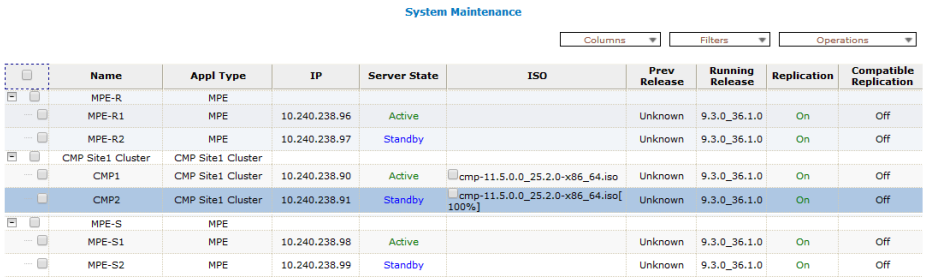
S T E P #	This procedure will transfer the ISO image of 11.5 CMP into the upgrade path in preparation for the upgrade. **Needed material:** - 11.5 CMP iso image file.	
1. ☐	**9.3 Active CMP server:** Transfer 11.5 ISO image file to the upgrade path	Transfer the 11.5 ISO image file into the upgrade path (/var/TKLC/upgrade/) of the 9.3 active CMP server: root@CMP1:/var/TKLC/upgrade [root@CMP1 ~]# cd /var/TKLC/upgrade/ [root@CMP1 upgrade]# ls -ltr total 1077292 -rw-r--r-- 1 root root 1102065664 Sep 30 16:25 cmp-11.5.0.0_25.2.0-x86_64.iso [root@CMP1 upgrade]#
2. ☐	**9.3 CMP GUI:** Upload 11.5 CMP ISO image via CMP GUI	11.5 ISO image file can be copied over to upgrade path via CMP GUI as shown in the below steps: Login to CMP GUI as administrator then navigate to Upgrade Manager → ISO Maintenance:  Check the active CMP server then expand "Operations" menu and select "Upload ISO" :  Fill in the upload ISO window with the details to transfer the ISO image :

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


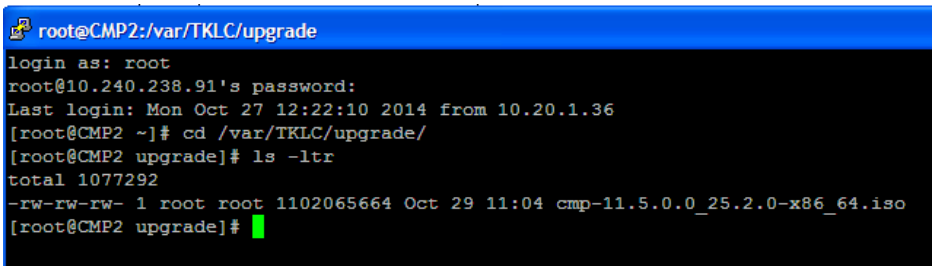
Confirm the process completed successfully :



</td>
</tr>
<tr>
<td>3.
☐</td>
<td>9.3 CMP GUI: Confirm ISO image transfer completion</td>
<td>Navigate to Upgrade Manager → System Maintenance to confirm the 11.5 CMP ISO image appear under ISO column for the CMP cluster



Name	Appl Type	IP	Server State	ISO	Prev Release	Running Release	Replication	Compatible Replication
MPE-R	MPE							
MPE-R1	MPE	10.240.238.96	Active		Unknown	9.3.0_36.1.0	On	Off
MPE-R2	MPE	10.240.238.97	Standby		Unknown	9.3.0_36.1.0	On	Off
CMP Site1 Cluster	CMP Site1 Cluster							
CMP1	CMP Site1 Cluster	10.240.238.90	Active	cmp-11.5.0.0_25.2.0-x86_64.iso	Unknown	9.3.0_36.1.0	On	Off
CMP2	CMP Site1 Cluster	10.240.238.91	Standby	cmp-11.5.0.0_25.2.0-x86_64.iso[100%]	Unknown	9.3.0_36.1.0	On	Off
MPE-S	MPE							
MPE-S1	MPE	10.240.238.98	Active		Unknown	9.3.0_36.1.0	On	Off
MPE-S2	MPE	10.240.238.99	Standby		Unknown	9.3.0_36.1.0	On	Off
</td>
</tr>
<tr>
<td>4.
☐</td>
<td>9.3 CMP CLI: Confirm ISO image exists under upgrade path</td>
<td>Login to 9.3 CMP server as root then validate ISO image file exists under upgrade path (/var/TKLC/upgrade):

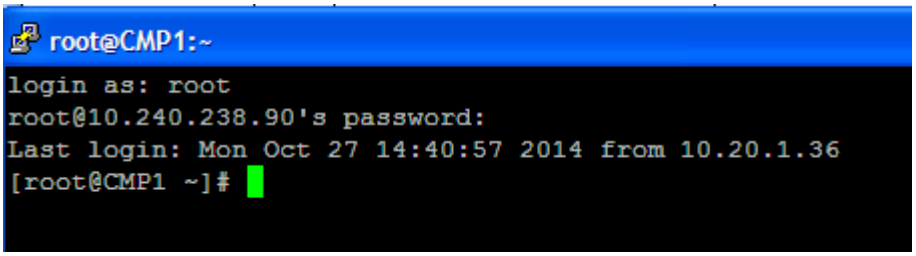
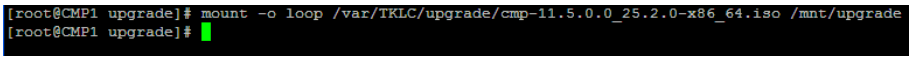
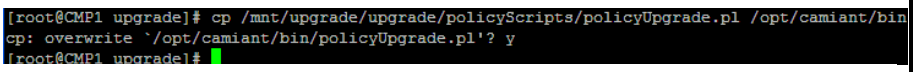
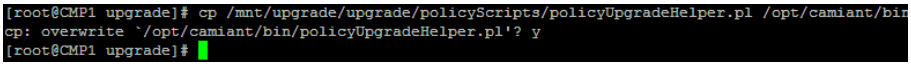
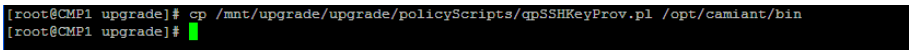


</td>
</tr>
</table>

2.3 Stage upgrade scripts

Procedure 4: Copy over upgrade scripts from 11.5 ISO image

Procedure 4. Copy upgrade scripts from 11.5 ISO image

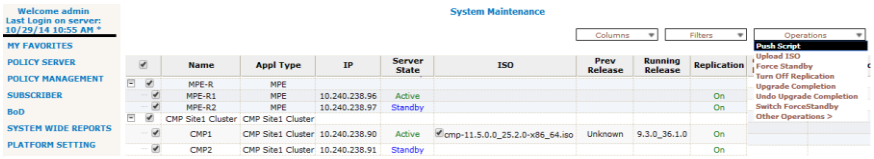
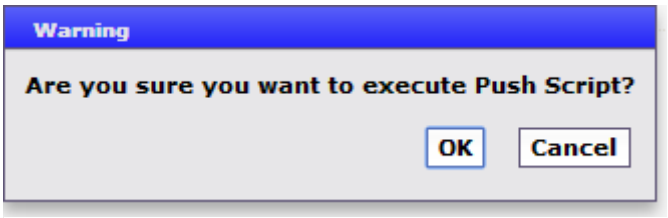
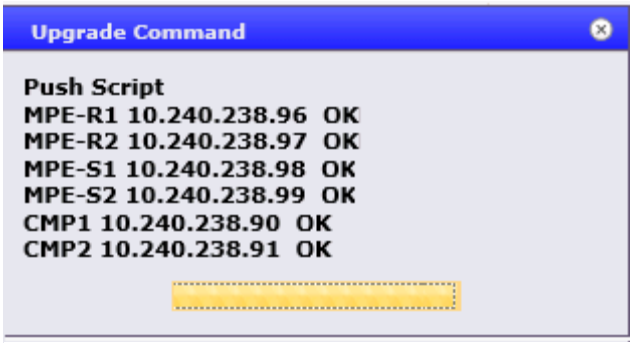
STEP #	This procedure will copy necessary upgrade scripts from 11.5 CMP ISO image overwriting the existing scripts. **Needed material:** - 9.3 Active CMP CLI access	
1. ☐	**9.3 Active CMP CLI:** SSH to the server's CLI	Login to the 9.3 active CMP CLI as root: 
2. ☐	**9.3 Active CMP CLI:** mount ISO image	Run the following command to mount the 11.5 CMP ISO image file: ***mount -o loop /var/TKLC/upgrade/cmp-11.5.0.0_17.1.0-x86_64.iso /mnt/upgrade***  **Note:** change the filename in the command to the CMP ISO image you are using.
3. ☐	**9.3 Active CMP CLI:** Extract needed upgrade scripts	Run the following commands to extract the upgrade scripts overwriting the old scripts: • cp /mnt/upgrade/upgrade/policyScripts/policyUpgrade.pl /opt/camiant/bin  • cp /mnt/upgrade/upgrade/policyScripts/policyUpgradeHelper.pl /opt/camiant/bin  • cp /mnt/upgrade/upgrade/policyScripts/qpSSHKeyProv.pl /opt/camiant/bin 

Procedure 4. Copy upgrade scripts from 11.5 ISO image

4. ☐	**9.3 Active CMP CLI:** unmount ISO image	Run the following command to unmount the 11.5 CMP ISO image file:
		
		umount /mnt/upgrade
		
		`[root@CMP1 upgrade]# umount /mnt/upgrade`
		`[root@CMP1 upgrade]#`

5.	**9.3 Active CMP CLI:** Sync SSH keys to all servers in topology	Run the following command to sync the SSH keys with all servers in the topology:
		
		qpSSHKeyProv.pl --prov --user=root
		
		Note that the root password needs to be supplied for script to run successfully.
		
		`[root@CMP1 bin]# qpSSHKeyProv.pl --prov --user=root`
		
		`The password of root in topology:`
		
		`Connecting to root@MPE-R2 (10.240.238.97) ...`
		`Connecting to root@MPE-S1 (10.240.238.98) ...`
		`Connecting to root@MPE-R1 (10.240.238.96) ...`
		`Connecting to root@MPE-S2 (10.240.238.99) ...`
		`Connecting to root@CMP1 (10.240.238.90) ...`
		`Connecting to root@CMP2 (10.240.238.91) ...`
		
		`[2/10] Provisioning SSH keys on MPE-R2 (10.240.238.97) ...`
		
		`[5/10] Provisioning SSH keys on MPE-S1 (10.240.238.98) ...`
		
		`[6/10] Provisioning SSH keys on MPE-R1 (10.240.238.96) ...`
		
		`[7/10] Provisioning SSH keys on MPE-S2 (10.240.238.99) ...`
		
		`[8/10] Provisioning SSH keys on CMP1 (10.240.238.90) ...`
		
		`[10/10] Provisioning SSH keys on CMP2 (10.240.238.91) ...`
		
		`SSH keys are OK.`
		
		`[root@CMP1 bin]#`

Procedure 4. Copy upgrade scripts from 11.5 ISO image

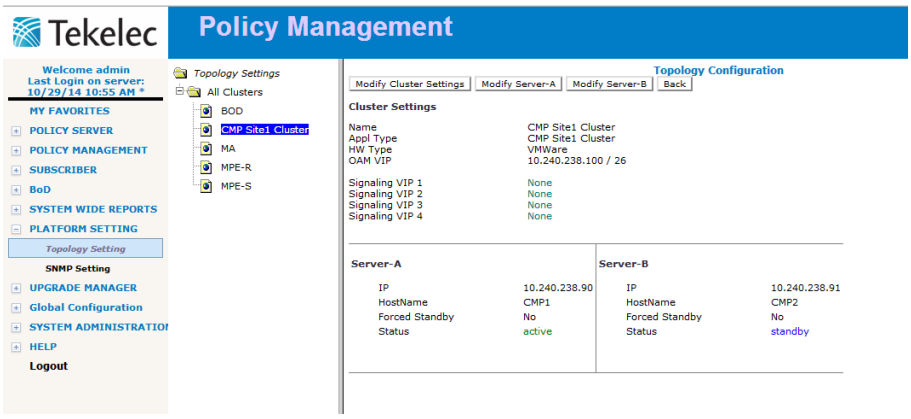
6.	**9.3 CMP GUI:** Push scripts to all servers in the topology	From CMP GUI, navigate to Upgrade Manager → System Maintenance then select "Push Script" from the operations menu:  Confirm the action in the dialog box:  Validate that action completed and script is pushed to all servers in the topology: 

2.4 Upgrade CMP servers

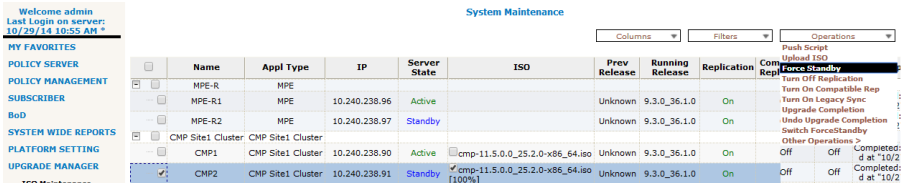
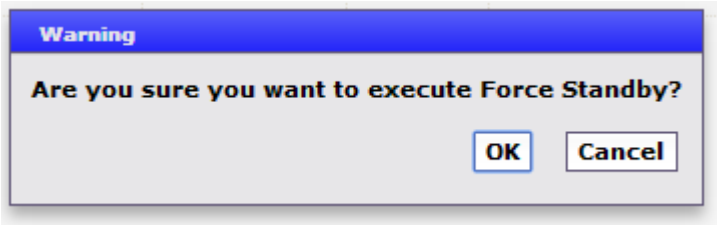
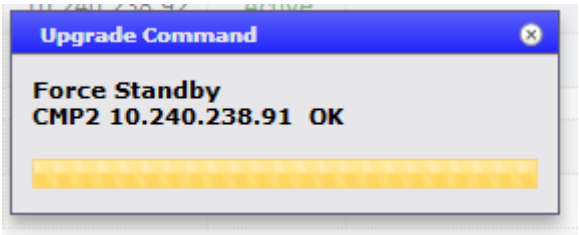
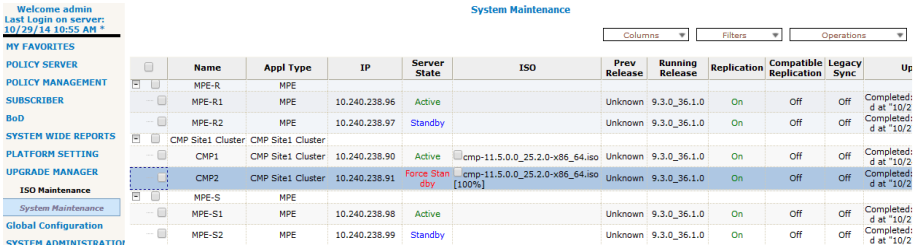
In case Cable Policy solution includes CMP cluster site 2, it should be upgraded after site1 CMP cluster is completed using same steps described in this procedure.

Procedure 5: Upgrade CMP Servers

Procedure 5. Upgrade CMP Servers

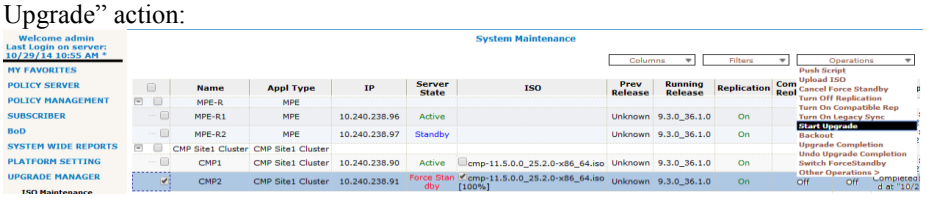
STEP #	This procedure will perform the actual upgrade of the CMP cluster(s) servers. **Needed material:** - Admin access to CMP GUI to perform the upgrade	
1. ☐	**9.3 CMP GUI:** Validate CMP servers status	Login to CMP GUI as admin and navigate to Platform Settings → Topology Setting and choose the CMP cluster  Validate the status of the CMP servers to ensure none of the servers is in OOS (Out Of Service) state.

Procedure 5. Upgrade CMP Servers

2. ☐	**9.3 CMP GUI:** Enable Force Stand By on the stand By CMP server	Navigate to Upgrade Manager → System Maintenance, check the CMP stand By server checkbox then from the operations menu click "Force Standby":  Confirm the dialog box to perform the action:  Validate action completed :  Now CMP server should have the "Force Standby" state: 

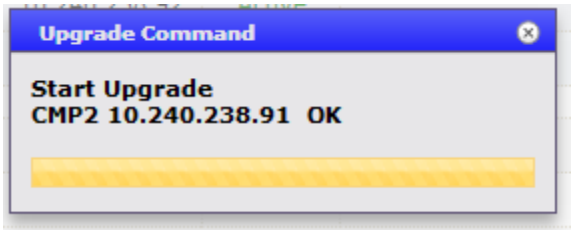
Procedure 5. Upgrade CMP Servers

3. ☐	**9.4 CMP GUI:** Start the upgrade	With the Force Stand By server checked, open the operations menu and choose "Start Upgrade" action:

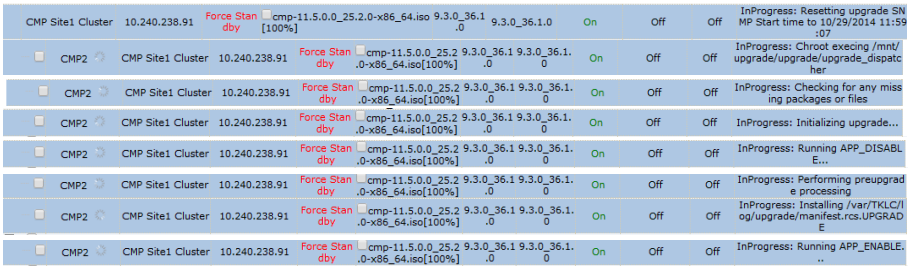


Confirm the action on the next dialog box:

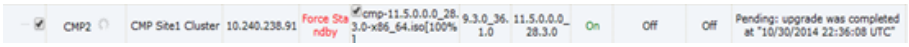
An information message indicating the successful start of the upgrade displays:



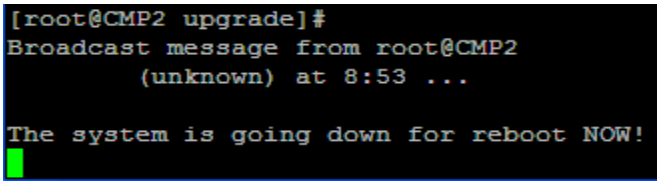
The upgrade will go through multiple phases that would be displayed in the upgrade status field like seen from the following samples:



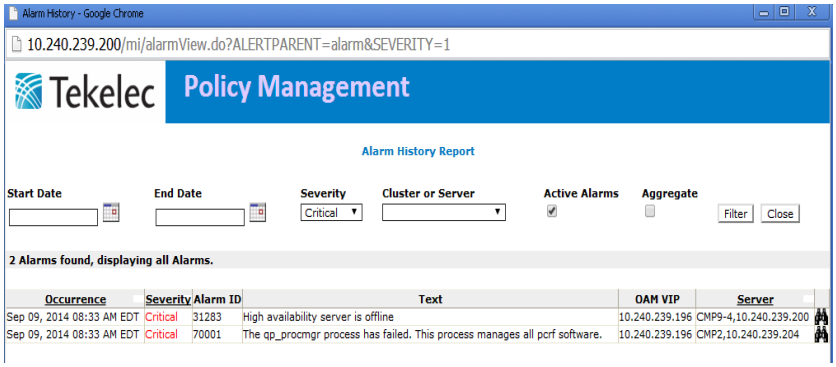
Then when upgrade completes, the upgrade status will reflect that as below:



Note that in case an SSH session is opened to the server while it is being upgraded, the connection will be lost as the server will reboot during the upgrade process:



Procedure 5. Upgrade CMP Servers

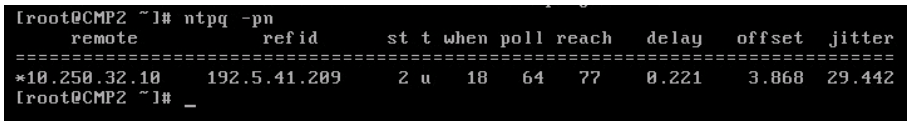
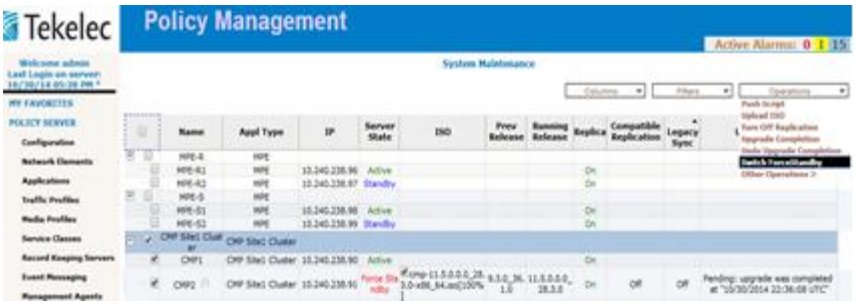
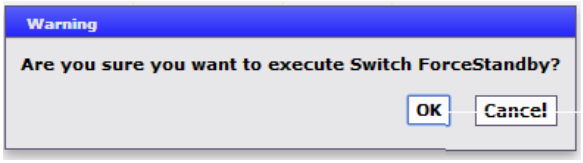
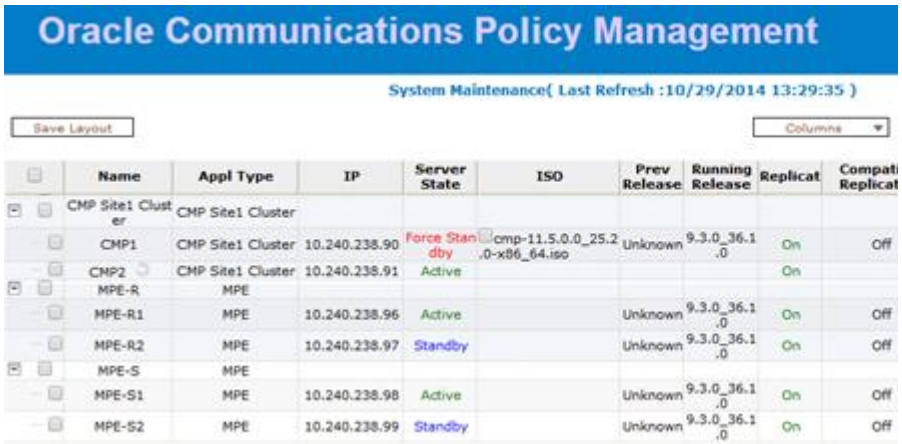
4. ☐	**9.4 CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully

5.	**11.5 upgraded CMP server CLI:** Validate upgrade log file	SSH to upgraded CMP server and login then tail the upgrade log file as follows :
		`|==========|`
		`| This system has been upgraded but the upgrade has not yet |`
		`| been accepted or rejected. Please accept or reject the |`
		`| upgrade soon. |`
		`|==========|`
		`[admusr@CMP2 ~]$ tail /var/TKLC/log/upgrade/upgrade.log`
		`1414708567:: Running postUpgradeBoot() for Upgrade::Policy::QPFirewallFixes upgrade policy...`
		`1414708568:: Running postUpgradeBoot() for Upgrade::Policy::QPIPv6Fixes upgrade policy...`
		`1414708568:: Running postUpgradeBoot() for Upgrade::Policy::QPJDKPolicy upgrade policy...`
		`1414708568:: Running postUpgradeBoot() for Upgrade::Policy::QPMySQLPolicy upgrade policy...`
		`1414708568:: Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy...`
		`1414708568:: Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...`
		`1414708568:: Running postUpgradeBoot() for Upgrade::Policy::TPD5to6Upgrade upgrade policy...`
		`1414708568:: Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy...`
		`1414708568:: Updating platform revision file...`
		`1414708569:: Upgrade returned success!`
		`[admusr@CMP2 ~]$`
		Validate upgrade returned success.

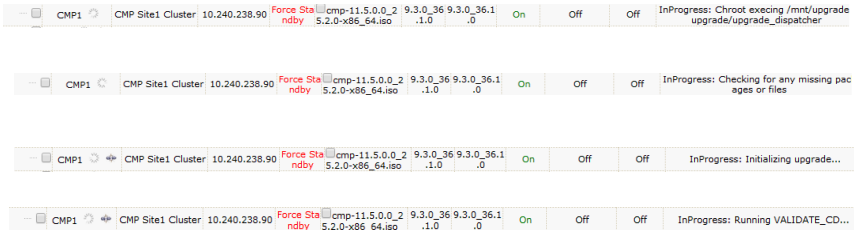
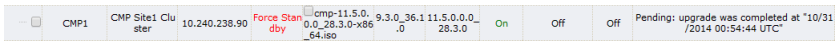
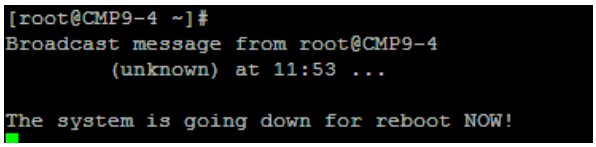
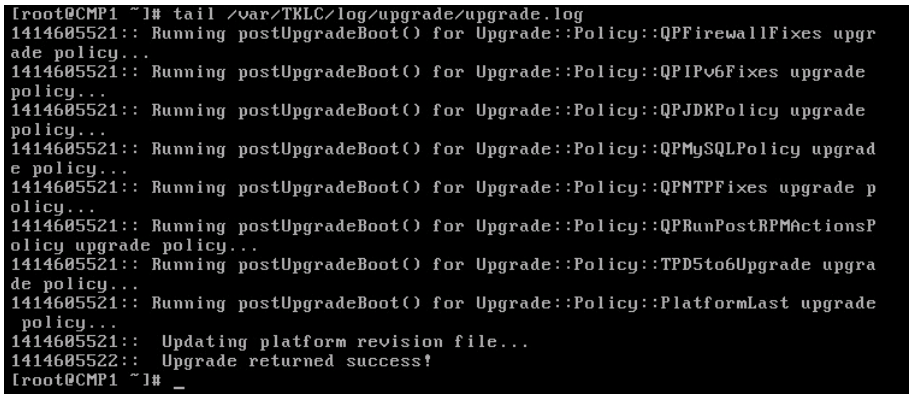
6.	**11.5 Upgraded CMP server CLI:** Validate policy revision	Run the following command to check running policy version:
		`[admusr@CMP2 ~]$ appRev`
		`Install Time: Thu Oct 30 18:36:09 2014`
		`Product Name: cmp`
		`Product Release: 11.5.0.0.0_28.3.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.7.0.0.1_84.20.0`
		`Base Distro ISO: TPD.install-6.7.0.0.1_84.20.0-OracleLinux6.5-x86_64.iso`
		`OS: OracleLinux 6.5`
		`[admusr@CMP2 ~]$`
		Make sure the product Release version is the upgraded version “11.5”

7.	**11.5 Upgraded CMP server CLI as root:** Verify the server’s HA role	Run the command “ha.mystate” as root to verify the server has the stand By role:
		`[root@CMP2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby A3706.191 0 1030:183616.931`
		`VIP Stby A3706.191 0 1030:183616.934`
		`QP Stby A3706.191 0 1030:183620.168`
		`DbReplication_old OOS A3706.191 0 1030:183613.060`
		`[root@CMP2 ~]#`

Procedure 5. Upgrade CMP Servers

8.	**11.5 Upgraded CMP server CLI as root:** Verify NTP sync	Run the command “ntpq -pn” to verify the server is in sync with the NTP server:  [root@CMP2 ~]# ntpq -pn remote refid st t when poll reach delay offset jitter ========== *10.250.32.10 192.5.41.209 2 u 18 64 77 0.221 3.868 29.442 [root@CMP2 ~]# _
9.	**9.3 CMP GUI:** Switch Stand By CMP servers	From the System Maintenance screen, check the CMP cluster and choose “Switch Force StandBy” from the operations menu:  Confirm the action on the following dialog box:  Connection to CMP GUI will be lost due to the switch of the CMP servers’ state, you will need to re-login to CMP GUI again which will be on 11.5 release. Navigate to System Maintenance again to confirm the upgraded server assumed the Active state while the other CMP server is in Force Stand By state: 

Procedure 5. Upgrade CMP Servers

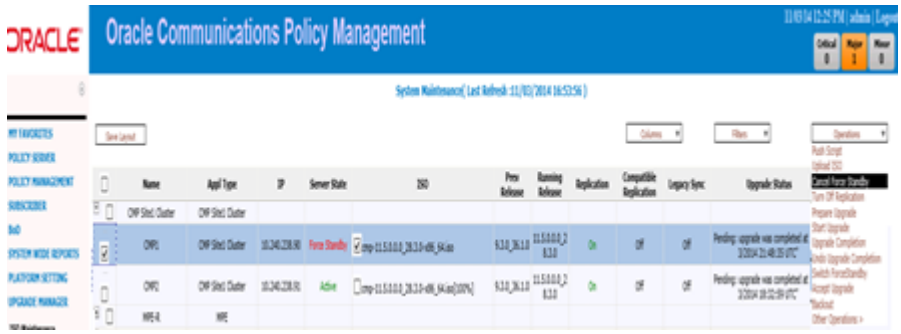
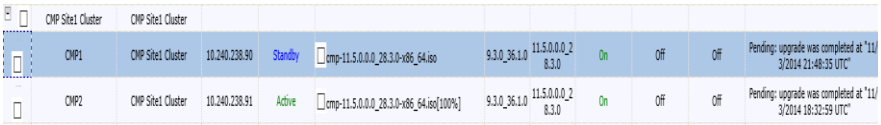
10.	**11.5 CMP GUI:** Upgrade the second server in the CMP cluster	Having the second server checked, click the operations menu and choose start upgrade:  Confirm the action on the following dialog box:  Upgrade will start and goes through several stages which will be reflected in the upgrade status column of the server. Following a sample of those stages:  Then when upgrade completes, the upgrade status will reflect that as below:  Within the upgrade steps, the server will reboot so any opened ssh sessions shall disconnect: 
11.	**11.5 secondly upgraded CMP server CLI:** Validate upgrade log file	SSH to latest Upgraded CMP server and login then tail the upgrade log file as follows : 

Procedure 5. Upgrade CMP Servers

12.	**11.5 secondly upgraded CMP server CLI:** Validate policy revision	Run the following command to check running policy version:
		
		`[root@CMP1 ~]# appRev`
		`Install Time: Wed Oct 29 13:58:42 2014`
		`Product Name: cmp`
		`Product Release: 11.5.0.0_25.2.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.7.0.0.1_84.19.0`
		`Base Distro ISO: TPD.install-6.7.0.0.1_84.19.0-OracleLinux6.5-x86_64.iso`
		`OS: OracleLinux 6.5`
		
		`[root@CMP1 ~]# _`
		
		Make sure the version is the upgraded version “11.5”

13.	**11.5 secondly upgraded CMP server CLI as root:** Verify the server’s HA role	Run the command “ha.mystate” as root to verify the server has the stand By role:
		
		`[root@CMP1 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby A3706.218 0 1030:205451.359`
		`VIP Stby A3706.218 0 1030:205451.360`
		`QP Stby A3706.218 0 1030:205456.286`
		`DbReplication_old OOS A3706.218 0 1030:205448.838`
		`[root@CMP1 ~]#`

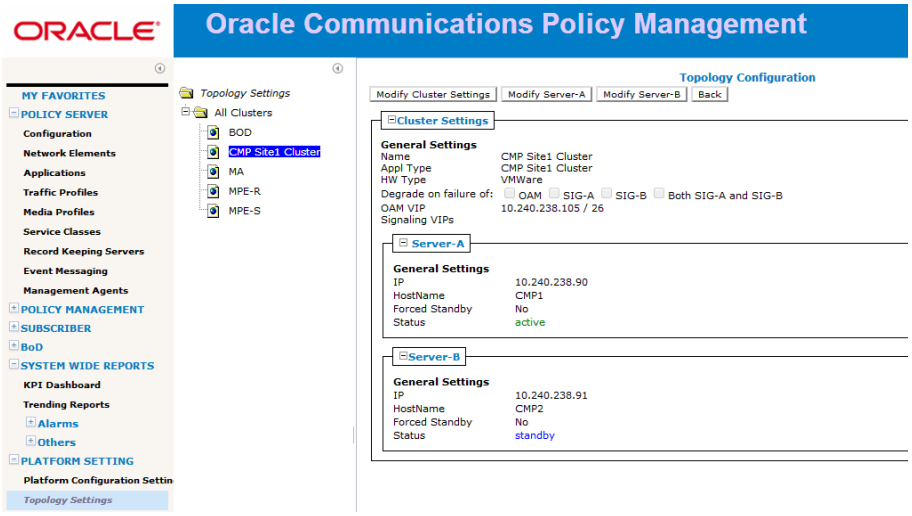
14.	**11.5 secondly upgraded CMP server CLI as root:** Verify NTP sync	Run the command “ntpq -pn” to verify the server is in sync with the NTP server:
		
		`[root@CMP1 ~]# ntpq -pn`
		`remote refid st t when poll reach delay offset jitter`
		`==========`
		`*10.250.32.10 192.5.41.209 2 u 47 64 17 0.232 1.898 14.600`
		`[root@CMP1 ~]# _`

15.	**11.5 CMP GUI:** Cancel the force stand By state	From the system maintenance screen of CMP GUI, check the latest upgraded server then from operations menu choose cancel force standby action:  Now the server state should be changed to “StandBy”: 
16.	**Site2 CMP cluster upgrade (If exists)**	In case Cable Policy solution includes a CMP cluster in secondary site, follow same steps detailed in this procedure to upgrade it similarly to primary site CMP cluster.

2.5 Upgraded CMP cluster validation

Procedure 6: Post Upgrade Validation

Procedure 6. Post CMP cluster Upgrade Validation

STEP #	This procedure will validate the CMP cluster was upgraded successfully. **Needed material:** - Admin access to CMP GUI - Access to SSH to server's CLI	
1. ☐	**11.5 CMP GUI:** Validate CMP servers status in Topology	Login to CMP GUI as admin and navigate to Platform Settings → Topology Setting and choose the CMP cluster  Validate the status of the CMP servers is correct: one in Active state and the other in StandBy state

2.	**11.5 Active CMP server CLI:** Validate BackPlane link state	Run the following command to check BP link is up with the internal IP assigned in the upgrade process (starting with the prefix 169.254.88) :
		
		`[admusr@CMP1 ~]$ ip -4 addr`
		`1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN`
		`inet 127.0.0.1/8 scope host lo`
		`2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000`
		`inet 10.240.238.90/26 brd 10.240.238.127 scope global eth0`
		`inet 10.240.238.105/26 scope global secondary eth0`
		`3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000`
		`inet 169.254.88.2/24 brd 169.254.88.255 scope global eth1`
		`[admusr@CMP1 ~]$`

3.	**11.5 Active CMP server CLI:** Validate MySql database state	Run the following command to check running MySql configuration database state of the server:
		
		`[root@CMP1 ~]# wbAccess mysqlState`
		`MASTER`
		`[root@CMP1 ~]#`

Procedure 6. Post CMP cluster Upgrade Validation

4.	**11.5 Active CMP server CLI:** Verify the server's HA role	Run the following command to verify the server has the Active HA role:
		`[root@CMP1 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Active A3706.218 0 1030:212320.848`
		`VIP Active A3706.218 0 1030:212320.856`
		`QP Active A3706.218 0 1030:212320.866`
		`DbReplication_old OOS A3706.218 0 1030:205448.838`
		`[root@CMP1 ~]#`

5.	**11.5 Active CMP server CLI:** Verify the server's replication role	Run the command ***"# irepstat"*** to verify the server has the Active replication role:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To CMP2 Active 0 0.25 1%R 0.03%cpu 60B/s`
		`AC To MPE-S1 Active 0 0.00 1%R 0.02%cpu 50B/s`
		`AC To MPE-S2 Active 0 0.00 1%R 0.02%cpu 49B/s`
		`AC To MPE-R2 Active 0 0.00 1%R 0.02%cpu 41B/s`
		`AC To MPE-R1 Active 0 0.00 1%R 0.02%cpu 42B/s`

6.	**11.5 Active CMP server CLI:** Verify HA and replication traffic path	Run the following command to verify the HA and replication traffic path status through the BP link is "OK" :
		`[root@CMP1 ~]# path.test -a CMP2`
		`CMP1 --> CMP2`
		`inetsync = 10.240.238.91 --> OK`
		`inetrep = 10.240.238.91 --> OK`
		`inetmerge = 10.240.238.91 --> OK`
		`cmha = 10.240.238.91 --> OK`
		`SNMP = 10.240.238.91 --> OK`
		`cmsoapa = 10.240.238.91 --> OK`
		`MX = 10.240.238.91 --> OK`
		`cmha2 = 10.240.238.91 --> OK`
		`cmha_cc = 10.240.238.91 --> OK`
		`cmha2_cc = 10.240.238.91 --> OK`
		`inetrep_cc = 10.240.238.91 --> OK`
		`[root@CMP1 ~]#`

7.	**11.5 StandBy CMP server CLI:** Validate BackPlane link state	Run the following command to check BP link is up with the internal IP assigned in the upgrade process:
		`[admusr@CMP2 ~]$ ip -4 addr`
		`1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN`
		`inet 127.0.0.1/8 scope host lo`
		`2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000`
		`inet 10.240.238.91/26 brd 10.240.238.127 scope global eth0`
		`3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000`
		`inet 169.254.88.1/24 brd 169.254.88.255 scope global eth1`
		`[admusr@CMP2 ~]$`

8.	**11.5 StandBy CMP server CLI:** Validate MySql database state	Run the following command to verify the server has the Active HA role:
		`[root@CMP2 ~]# wbAccess mysqlState`
		`SLAVE_SYNCHRONIZED`
		`[root@CMP2 ~]#`

Procedure 6. Post CMP cluster Upgrade Validation

9.	**11.5 StandBy CMP server CLI:** Verify the server's HA role	Run the following command to verify the server has the stand By role:
		`[root@CMP2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby A3706.191 0 1030:212315.182`
		`VIP Stby A3706.191 0 1030:212315.021`
		`QP Stby A3706.191 0 1030:212324.186`
		`DbReplication_old OOS A3706.191 0 1030:183613.060`
		`[root@CMP2 ~]#`

10.	**11.5 StandBy CMP server CLI:** Verify HA and replication traffic path	Run the following command to verify the HA and replication traffic is going to the CMP mate through the BP link successfully:
		`[root@CMP2 ~]# path.test -a CMP1`
		`CMP2 --> CMP1`
		`inetsync = 10.240.238.90 --> OK`
		`inetrep = 10.240.238.90 --> OK`
		`inetmerge = 10.240.238.90 --> OK`
		`cmha = 10.240.238.90 --> OK`
		`SNMP = 10.240.238.90 --> OK`
		`cmsoapa = 10.240.238.90 --> OK`
		`MX = 10.240.238.90 --> OK`
		`cmha2 = 10.240.238.90 --> OK`
		`cmha_cc = 10.240.238.90 --> OK`
		`cmha2_cc = 10.240.238.90 --> OK`
		`inetrep_cc = 10.240.238.90 --> OK`
		`[root@CMP2 ~]#`

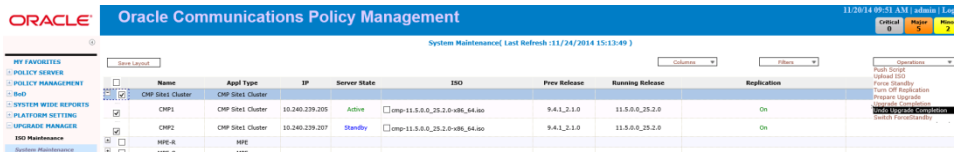
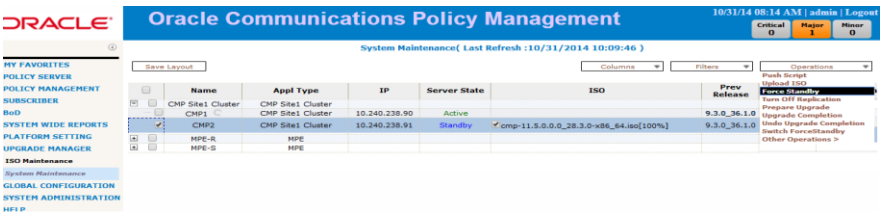
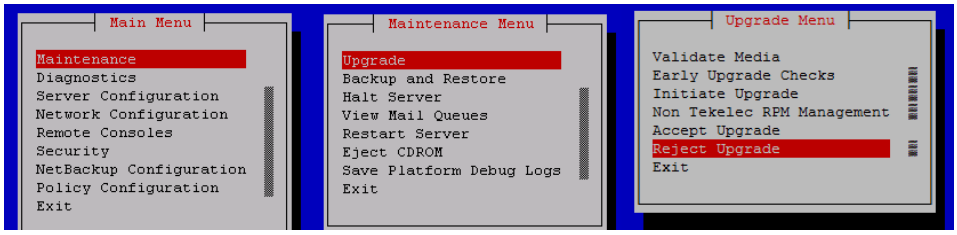
11.	**Validation results**	In case of failure of one or more of the upgrade validation steps in this procedure without a plan for recovery, back out should be performed as in the following procedure. However in case all validation steps passed skip the following procedure (Back out the upgrade) and go directly to accept upgrade procedure in section 2.7.

2.6 Back out the upgrade

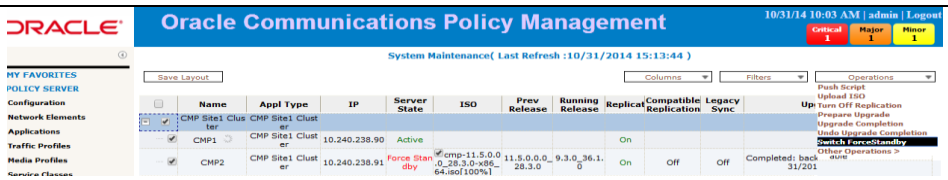
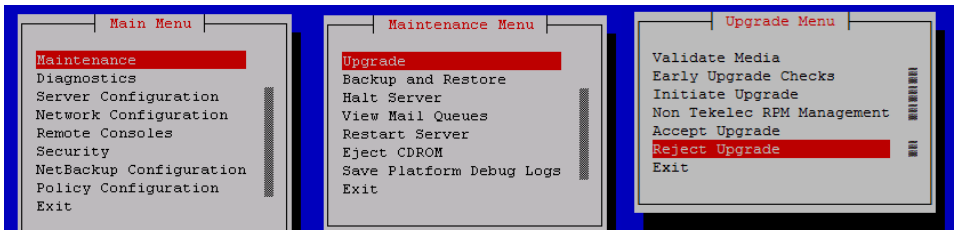
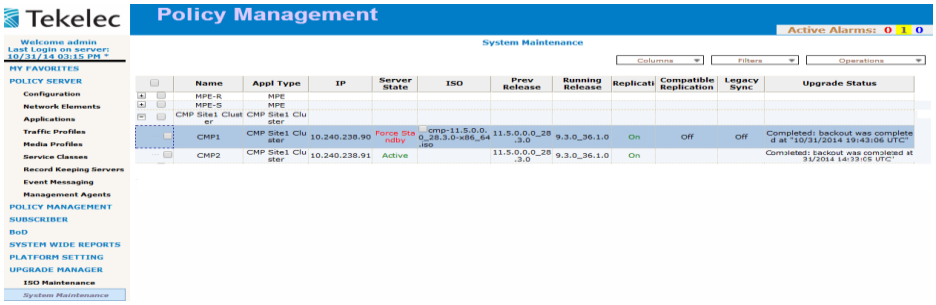
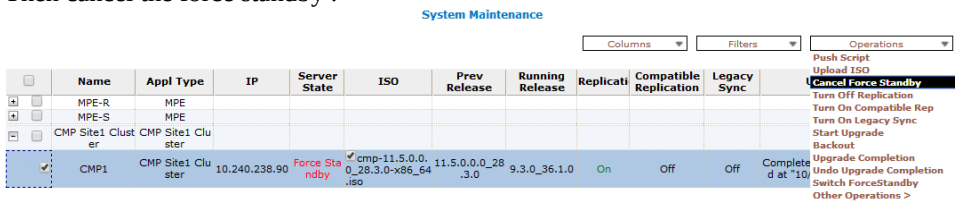
In case all Cable Policy components in the solution were upgraded, back out should start with the MPE cluster(s) first then CMP afterwards.
In case Cable Policy solution includes CMP cluster site 2, it should be backed out first then site1 CMP cluster next using same steps described in this procedure for each site's CMP cluster.

Procedure 7: Backing out the upgrade

Procedure 7. Back out the upgrade

S T E P #	This procedure is only needed if the upgrade verification fails and back out is decided. This Back out procedures can only be followed successfully if: 1. Upgrade was not accepted 2. No configuration or new features have been set up 3. CMP can be backed out only when all other policy components were backed out first **Needed material:** - Admin access to CMP GUI	
1.	**11.5 CMP GUI:** Undo upgrade completion for the CMP servers	Navigate to Upgrade Manager →System Maintenance, check the CM cluster check box then from the operations menu choose "Undo upgrade completion" : 
2. ☐	**11.5 CMP GUI:** Force Stand By the upgraded Stand By server	Navigate to Upgrade Manager →System Maintenance, set the upgraded server that has the StandBy status to Force StandBy from the operations menu 
3. ☐	**11.5 Stand By CMP CLI:** Reject the upgrade	Login to the stand by server CLI then as root su – platcfg and navigate to Maintenance → Upgrade → Reject Upgrade: 
4.	**11.5 CMP GUI:** Switch Force Stand By	With the cluster checked, choose switch Force standby from the operations menu

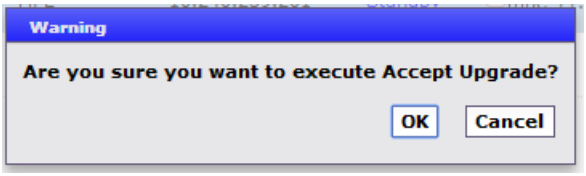
Procedure 7. Back out the upgrade

		 Session to CMP GUI will be lost, re-login to backed out 9.3 CMP GUI.
5.	**11.5 Stand By CMP CLI:** Reject the upgrade	Login to the stand by server CLI then as root su – platcfg and navigate to Maintenance → Upgrade → Reject Upgrade: 
6.	**9.3 CMP GUI:** CMP cluster back out completed	Validate that release running is back to 9.3 release and upgrade status for both servers in the CMP cluster indicates "back out was complete":  Then cancel the force standby : 
7.	**9.3 Active CMP CLI:** Clean up upgrade files	Login to Active CMP CLI as root, run the following command: ***policyUpgrade.pl –cleanupUpgrade***
8.	**9.3 Active CMP CLI:** Remove BP link paths	***After all policy components/clusters were backed out successfully***, login to Active CMP CLI as root then run the following command to clean up BP links configurations: ***irem LogicalPath where "path='BackplanePath'"***

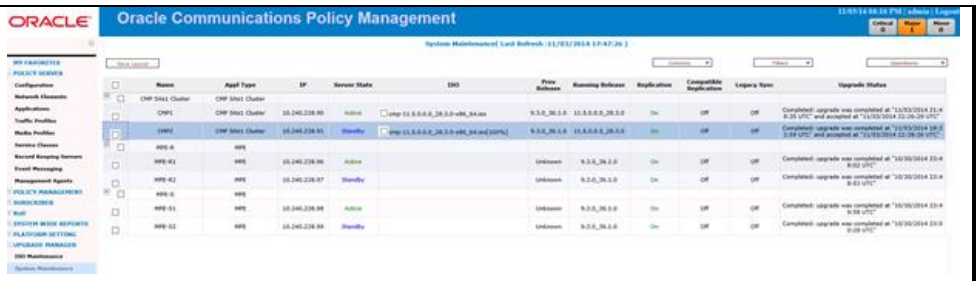
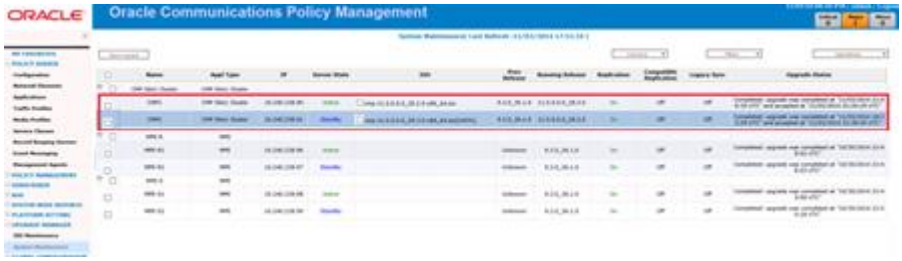
2.7 Accept the upgrade

Procedure 8: Accept the upgrade

Procedure 8. Accept the upgrade

STEP #	This procedure will accept the upgrade. **Needed material:** - Admin access to CMP GUI	
9. ☐	**11.5 CMP GUI:** Force Stand By the upgraded Stand By server	Navigate to Upgrade Manager →System Maintenance, set the upgraded server that has the StandBy status to Force StandBy from the operations menu 
10. ☐	**11.5 CMP GUI:** Accept the upgrade for Stand By server	With the server set to Force StandBy checked, choose "Accept Upgrade" from the operations menu:  Then confirm the action on the next dialog message: 
11.	**11.5 CMP GUI:** Switch Force Stand By	With the cluster checked, choose switch Force standby from the operations menu  Session to CMP GUI will be lost, re-login to CMP GUI then accept the upgrade for the second server  Cancel force stand by for the second server :

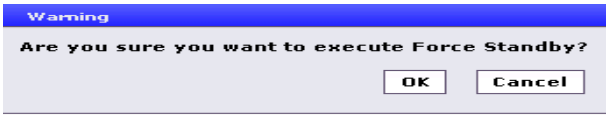
Procedure 8. Accept the upgrade

		
12.	**11.5 CMP GUI:** upgrade completion validation	Validate that upgrade pending alarms are cleared out for the cluster. Also validate that both servers in the cluster are showing completed upgrade status: 

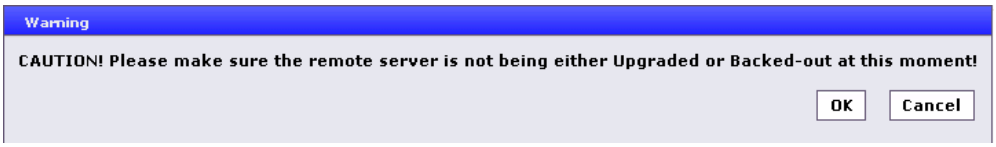
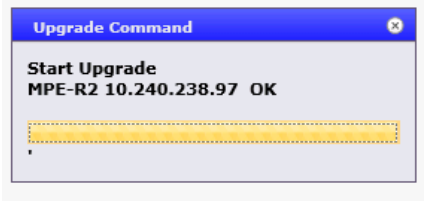
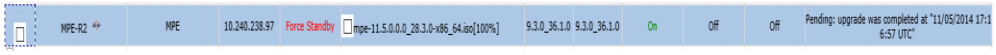
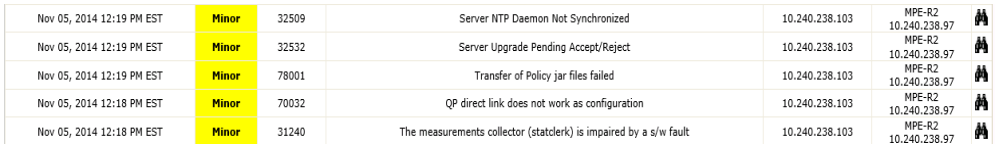
3. MPE-R/MPE-S Cluster Upgrades

Procedure 9: MPE-R/MPE-S Cluster Upgrade

Procedure 9. MPE-R/MPE-S Upgrade

S T E P #	This procedure will perform the upgrade for the MPE-R/MPE-S cluster if exists in the Policy Solution to be upgraded. **Needed material:** - Access to customer's network to access the Cable Policy solution - CMP OAM VIP, MPE-R/MPE-S iLO IP & OAM Real IP - Admin login to CMP, iLO Admin & CLI root login to MPE-R/MPE-S - 11.5 MPE-R/MPE-S ISO image	
1. ☐	**Computer on solutions' network or remote access to solutions' network:** Transfer MPE-R/MPE-S ISO Image	Follow the same procedures outlined in section 2.2 of this document to transfer the 11.5 MPE-R/MPE-S ISO Image into the servers to be upgraded from 9.4 release
2. ☐	**CMP GUI:** Force StandBy the standby server	Navigate to Upgrade Manager → System Maintenance then check the standBy MPE-R/MPE-S server and from the operations menu choose "Force StandBy":  Confirm the action on the next dialog box  An information message indicating the successful execution of Force standby appears then the server state changes to "Force Standby": 

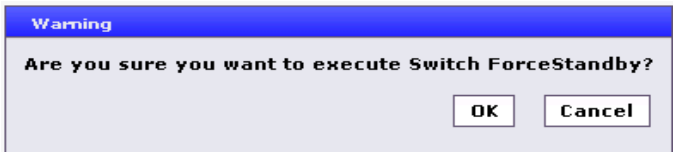
Procedure 9. MPE-R/MPE-S Upgrade

3.	**CMP GUI:** Start the upgrade	Then with the server checked from the operations menu, choose “Start Upgrade”.  Confirm the action on the next dialog box:  An information message indicating the successful start of the upgrade displays:  The upgrade will go through multiple steps including rebooting the server; those steps are reflected in the MPE-R/MPE-S “Upgrade Status” field of the System Maintenance screen.  Wait till the upgrade status indicates upgrade was completed. 
4.	**CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully

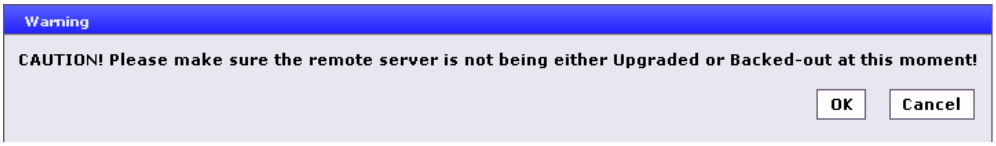
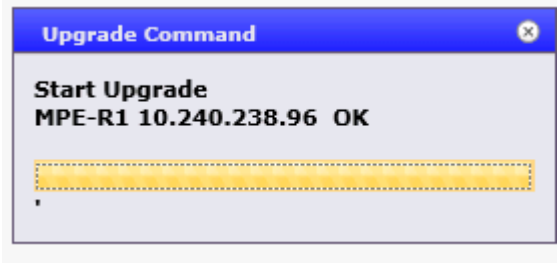
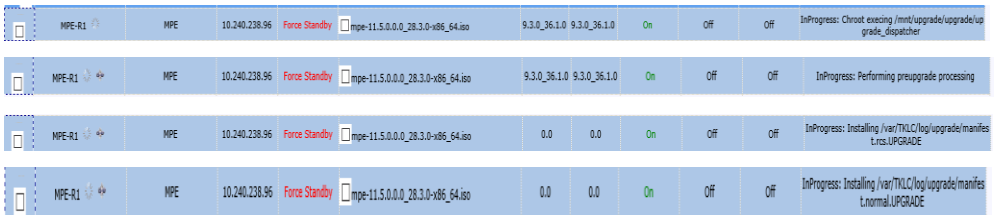
Procedure 9. MPE-R/MPE-S Upgrade

5.	**11.5 upgraded MPE server CLI:** Validate upgrade log file	SSH to upgraded MPE-R/MPE-S server and login then tail the upgrade log file as follows : Validate upgrade returned success. [root@MPE-R2 ~]# tail /var/TKLC/log/upgrade/upgrade.log 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::MBL upgrade policy... 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::QPFirewallFixes upgrade policy... 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::QPIPv6Fixes upgrade policy... 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::QPJDKPolicy upgrade policy... 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy... 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy... 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::TPD5to6Upgrade upgrade policy... 1415207817:: Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy... 1415207817:: Updating platform revision file... 1415207818:: Upgrade returned success! [root@MPE-R2 ~]#
6.	**11.5 upgraded MPE server CLI:** Validate policy revision	Run the following command to check running policy version: [root@MPE-R2 ~]# getPolicyRev -f mpe_11.5.0.0.0_28.3.0 [root@MPE-R2 ~]# Make sure the version is the upgraded version “11.5”
7.	**11.5 upgraded MPE server CLI:** Verify the server’s HA role	Run the command “ha.mystate” to verify the server has the stand By role: [root@MPE-R2 ~]# ha.mystate resourceId role node subResources lastUpdate DbReplication Stby C2411.110 0 1105:121822.304 VIP Stby C2411.110 0 1105:121822.306 QP Stby C2411.110 0 1105:121825.829 DbReplication_old OOS C2411.110 0 1105:121701.873 [root@MPE-R2 ~]#
8.	**11.5 upgraded MPE server CLI:** Verify NTP sync	Run the command “ntpq -pn” to verify the server is in sync with the NTP server: [root@MPE-R2 ~]# ntpq -pn remote refid st t when poll reach delay offset jitter ========== *10.250.32.10 192.5.41.40 2 u 35 64 7 0.316 7.918 3.595

Procedure 9. MPE-R/MPE-S Upgrade

9.	**CMP GUI:** Switch Force StandBy	Navigate to Upgrade Manager → System Maintenance then check the MPE-R/MPE-S cluster and from the operations menu choose "Switch Force StandBy":  Confirm the action on the next dialog box  An information message indicating the successful execution of Switch Force standby appears. 

Procedure 9. MPE-R/MPE-S Upgrade

10.	**CMP GUI:** Start the upgrade	Then with the server checked from the operations menu, choose “Start Upgrade”.  Confirm the action on the next dialog box:  An information message indicating the successful start of the upgrade displays:  The upgrade will go through multiple steps including rebooting the server; those steps are reflected in the MPE-R/MPE-S “Upgrade Status” field of the System Maintenance screen.  Wait till the upgrade status indicates upgrade was completed. 
6.	**CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully

Procedure 9. MPE-R/MPE-S Upgrade

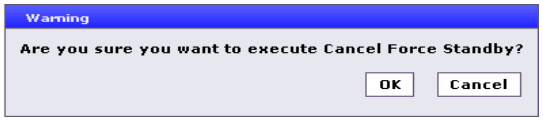
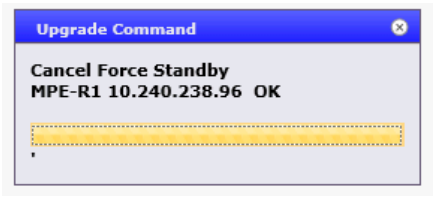
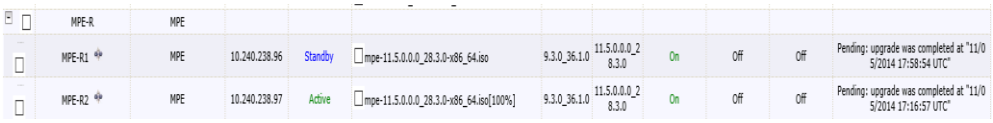
7.	**11.5 upgraded MPE server CLI:** Validate upgrade log file	SSH to upgraded MPE-R/MPE-S server and login then tail the upgrade log file as follows :
		
		Validate upgrade returned success.
		
		`[root@MPE-R1 ~]# tail /var/TKLC/log/upgrade/upgrade.log`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::MBL upgrade policy...`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::QPFirewallFixes upgrade policy...`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::QPIPv6Fixes upgrade policy...`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::QPJDKPolicy upgrade policy...`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy...`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::TPD5to6Upgrade upgrade policy...`
		`1415210334:: Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy...`
		`1415210335:: Updating platform revision file...`
		`1415210335:: Upgrade returned success!`
		`[root@MPE-R1 ~]#`

10.	**11.5 upgraded MPE server CLI:** Validate policy revision	Run the following command to check running policy version:
		
		`[root@MPE-R1 ~]# getPolicyRev -f`
		`mpe_11.5.0.0.0_28.3.0`
		`[root@MPE-R1 ~]#`
		
		Make sure the version is the upgraded version “11.5”

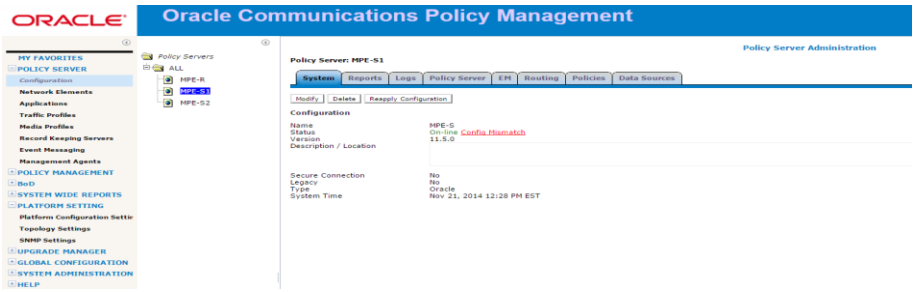
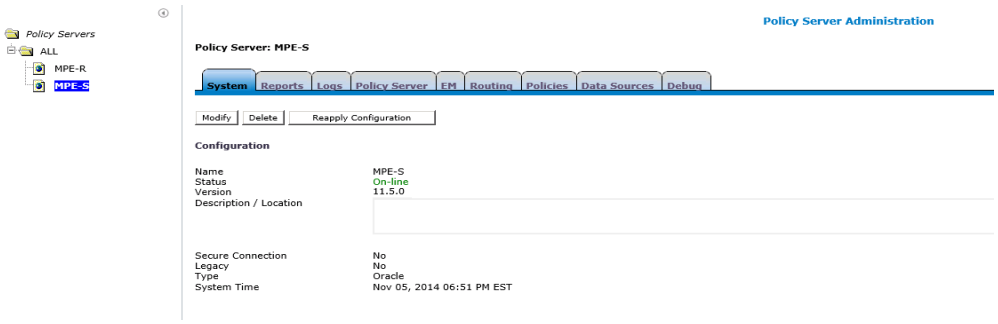
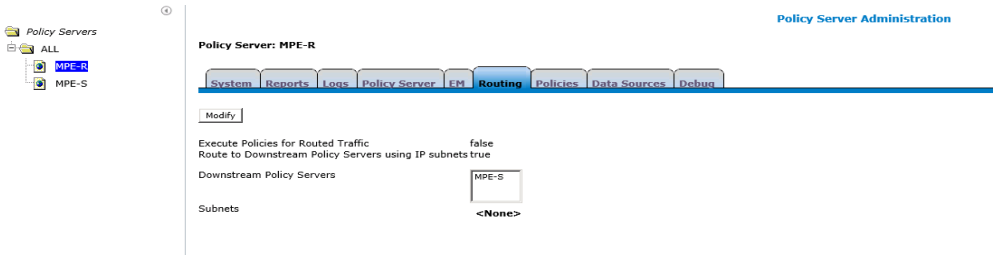
11.	**11.5 upgraded MPE server CLI:**
	
	Verify the server’s HA role
		Run the command “ha.mystate” to verify the server has the stand By role:
		
		`[root@MPE-R1 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby C2411.214 0 1105:130037.402`
		`VIP Stby C2411.214 0 1105:130037.404`
		`QP Stby C2411.214 0 1105:130037.406`
		`DbReplication_old OOS C2411.214 0 1105:125859.321`
		`[root@MPE-R1 ~]#`

12.	**11.5 upgraded MPE server CLI:**
	
	Verify NTP sync
		Run the command “ntpq -pn” to verify the server is in sync with the NTP server:
		
		`[root@MPE-R1 ~]# ntpq -pn`
		`remote refid st t when poll reach delay offset jitter`
		`==========`
		`*10.250.32.10 192.5.41.40 2 u 52 64 17 0.347 2.022 0.988`

Procedure 9. MPE-R/MPE-S Upgrade

13.	**CMP GUI:** Cancel force standby	After upgrade completes, cancel Force Standby from the operations menu :  Confirm the action on the next dialog box  An information message indicating the successful cancellation of Force standby 
14.	**CMP GUI:** MPE servers status check	Validate that now one of the MPE-R/MPE-S servers is in “Active” State and the other is in “StandBy” state:  MPE-R MPE MPE-R1 MPE 10.240.238.96 Standby mpe-11.5.0.0.0_28.3.0-x86_64.iso 9.3.0_36.1.0 11.5.0.0.0_28.3.0 On Off Off Pending: upgrade was completed at "11/05/2014 17:58:54 UTC" MPE-R2 MPE 10.240.238.97 Active mpe-11.5.0.0.0_28.3.0-x86_64.iso[100%] 9.3.0_36.1.0 11.5.0.0.0_28.3.0 On Off Off Pending: upgrade was completed at "11/05/2014 17:16:57 UTC"

Procedure 9. MPE-R/MPE-S Upgrade

15.	**CMP GUI:** MPE-R/MPE-S cluster configuration	Navigate to Policy Server → Configuration  Click on "Reapply Configuration" to clear out the config mismatch status of MPE, then validate the state of the MPE-R/MPE-S cluster is "On-line" and that the version reflects the upgraded release.  Then switch to the "Routing" tab in the MPE-R/MPE-S administration:  Validate configurations are maintained for MPE-R/MPE-S after the upgarde. Switch to the "Policy Server" tab in the MPE-R/MPE-S administration:, validate that associations of MPE-S with CMTS are intact after the upgrade. Then switch to the "Reports" tab in the MPE-R/MPE-S administartion :  Validate both servers of the cluster are displayed and with correct "Active" and "StandBy" state.
16.	**Post upgrade checks**	Follow the same procedures outlined in section 2.5 of this document to validate the upgrade completed successfully.

Procedure 9. MPE-R/MPE-S Upgrade

17.	**Back out the upgrade**	In case post upgrade checks failed and back out is decided, follow the same procedures outlined in section 2.6 of this document to back out the MPE clusters
18.	**Accept the upgrade**	Follow the same procedures outlined in section 2.7 of this document to accept the upgrade.