Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Upgrade Procedure

Policy Management 7.5 to 9.x Upgrade Procedure

E86554-01

March 2017

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

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

Refer to Appendix I Accessing the Oracle customer support site for instructions on accessing this site.

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

TABLE OF CONTENTS

List of Tables

1. INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform a Software upgrade to Release 9.x on in-service Policy 7.5.x servers.

NOTE: Release 9.x includes all the functionality of Release 8.0, plus additional features. This document provides for a upgrade directly to the 9.x Release.

It is assumed that the CMP, MRA and MPE Application media (ISO file, CD-ROM or other form of media) have been delivered to the customer's site(s) before upgrade, in order to have proper preparation for recovery operations. The distribution of the software load is outside the scope of this procedure.

The SDM-SPR Upgrade is not included in this Document.

1.2 References

- *Policy 8.0 Release Notes,* E56020-01
- *Feature Notice Release 8.0,* 910-6405-001
- *Policy Management 9.x Release Notes*
- *Feature Notice Release 9.x*
- *Policy 7.5 Platform Software Installation Guide*, 910-6291-001 Revision B
- *PMAC 3.x/4.x Disaster Recovery Guide*, 909-1638-001

1.3 Software Release Numbering

The Policy Management 9.x is comprised of several software components, the CMP, MPE, MPE-li and the MRA ISO files, each versioned separately. Refer to Policy Management 9.x Release Notes for the target release in order to identify the separate software components included in the release and their version numbers.

1.4 Acronyms

This section describes the acronyms used within this document.

BIOS	Basic Input Output System
BMC	Baseboard Management Controller
CD-ROM	Compact Disc Read-only Media
FRUSDR	Field Replaceable Unit – Sensor Data Record
GPS	Global Product Solutions
HSC	Hot Swap Controller
IP	Internet Protocol
IPM	Initial Product Manufacture
IPMI	Intelligent Platform Management Interface
ISO	ISO 9660 file system (when used in the context of this document)
MOP	Method of Procedure
NEBS	Network Equipment-Building System
PMAC	Platform Management and Configuration
RMM	Remote Management Module

SUP	System Update Package
TPD	Oracle Platform Distribution
UI	User Interface

1.5 Terminology

This section describes terminology as it is used within this document.

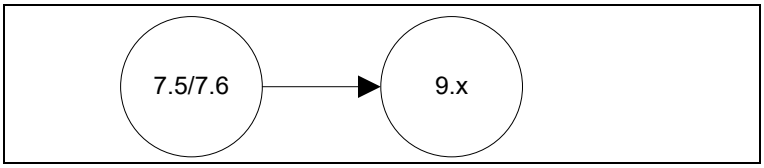
Firmware	Coded instructions and data programmed directly into the circuitry of read-only memory for controlling the operation of the server or one of its devices.
Platcfg	Refers specifically to the Platform Configuration Utility User Interface which is a text-based user interface.
Runlevel	A preset TPD operating state represented by a single-digit integer which designates a different system configuration and allows access to a different combination of processes.
System Health Check	Procedure used to determine the health and status of the server, typically performed using the TPD syscheck utility.
PP5160	The Oracle PP5160 Application Server. An Intel based, 1U NEBS compliant rack-mount server.
Upgrade	The process of converting a TPD based Policy 7.5.x server from its current software release to a newer release.
Upgrade Ready	State that allows for a successful software upgrade of a server. This requires bringing the server out of service and disabling certain processes.
Watchdog	A hardware timing device that triggers the server to reset if the OS, due to some fault condition, such as a hang, neglects to regularly service the watchdog.

2. UPGRADE OVERVIEW

This section lists the required materials and information needed to execute a Policy Management 9.x software upgrade.

2.1 Upgrade Path

The upgrade is supported from the Policy 7.5.x GA software releases.



2.2 New for 9.x

In Release 8.0, a new Upgrade Manager function is provided to improve the upgrade process. In Release 9.x, this function is further enhanced.

The Upgrade Manager function is built into the CMP. It is used to upgrade the MRE/MRAs, after the initial upgrade of the CMPs to the new release. I.e. the upgrade will be done for the CMPs first, and then the new Upgrade Manager is used to upgrade the remaining servers. This tool provides the option to upgrade multiple MPE clusters at a single site in parallel.

There is also an improved data replication service implemented in Release 8.0. Because the replication service extends between servers, it is necessary to upgrade all servers in the Policy system to 9.x, and then activate the new replication service between the servers. This adds new steps to the Upgrade activities, but is also simplified by the Upgrade Manager tool. It also has a specific "roll back" procedure in case of a problem with the new replication service.

NOTE: The new Replication service requires that certain additional tcp ports are open in the customer network between the CMP and MPE/MRAs.

The upgrade to 9.x does not require changes to existing Policies, call flows, or other design activities.[1]

New Features provided in Policy Management 9.x can be activated after the upgrade, on a schedule and plan that is separate from the upgrade. These new feature activations may require planning, but are outside the scope of this document.

For a full list of new features in Policy Release 9.x, see the Policy 8.0 and Policy Management 9.x Feature release notices.

2.3 SPR Upgrade to Rel 8.0 or 9.x

NOTE: Subscriber Profile Repository (SPR) is an optional component of the Oracle Policy Solution. This section only applies to customers that use the Oracle SPR.]

It is recommended to upgrade to SPR 8.0 or 9.x (if SPR is used in the deployment) before the upgrade to Policy Management 9.x.

For a full list of new features in SPR Release 8.0 and 9.x, see the SPR related Feature release notices.

[1] This is the design intent of the release. The user should confirm in the Release notes if there might be exceptions to this that need to be managed before upgrade.

2.4 Upgrade Sequence

This procedure applies to an Active/Standby pair of servers (or a single server, if it is not configured with high availability). This pair of servers will be referred to as a “cluster” or “ha cluster”. The cluster type may be CMP, MRA or MPE. For CMP cluster, the cluster status may also be Primary site or Secondary site.

The customer deployment may consist of multiple clusters.

Required Cluster Upgrade Sequence:

1. CMP Primary site cluster
2. CMP Secondary site cluster
3. MRA and MPE clusters
4. New Replication activation

NOTE: There may be limitations[2] to the CMP management functions during the period when the CMP Active site cluster is on release 9.x and one or more MRA/MPE clusters are on release 7.5.x. For this reason, it is recommended that the deployed policies are not changed during the upgrade period.

2.5 Customer Impacts

The cluster upgrade proceeds by upgrading the standby server, and then switching over from the Active to the Standby, and upgrading the second server. A server boot is part of the Upgrade action.

2.6 Rollback (Backout)

Rollback is the reverse of the upgrade. The full pre-upgrade image is stored on the server during the upgrade, and can be restored from a command line.

2.7 TPD Version

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

2.8 Server Hardware Platforms

The Policy Management 9.x software upgrade can be used on any server that previously had the Policy 7.5.x release. This includes the PP5160, DL360G6, and BL460G6. Policy Management 9.x adds support for DL380G8, and BL460G8.

2.9 Loading Application Software

For upgrade of server Application software, the recommended method is to copy the Application ISO to the servers using scp/ftp. If the system is C-class, the Application software must also be loaded into the PMAC software management library to support new installs and FRU activities (PMAC is not used for Upgrade).

It is also possible to load software from a CD/DVD. The PP5160 and DL360 are Rack Mount servers, and have a front panel CD/DVD Drive. This can be used for the upgrade.

The BL460 is a blade server and does not have a CD/DVD Drive. However, the PMAC server (provided with C-Class solutions) has CD/DVD drive that is used to load and manage Application software (and TPD) versions. Software may be copied from PMAC to a blade server.

---

[2] Specific limitations are to be determined.

2.10 Required Materials

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

- Target-release Policy Management 9.x software media. Either as an ISO image file or in physical CD media format.
- Target-release Policy Management 9.x software Upgrade Release Notes.
- The capability to log into the target server as root.

  NOTE: The login may be through ssh, local console, or iLo/RMM maintenance port.
- The capability to secure copy (scp) from the local workstation being used to perform this upgrade to the target server, or otherwise be able to transfer binary files to the target server.
- User logins, passwords, IP addresses and other administration information. See Section 2.10.2.

VPN access to the customer's network is required if that is the only method to log into the target servers. It must be also possible to access the Policy Manager GUI, and the PMAC GUI (for a BL460 system). The GUI's may be tunneled via VPN for remote console access.

2.10.1 Upgrade Media

You must obtain a copy of the Policy Management 9.x software target release media. The media can be in either ISO image file format or physical DVD media. It is best to have both formats available before going to site.

The Policy Management 9.x software ISO image files will be in the following format:

872-254z-101-9.1.0_x.y.0-mpe-x86_64.iso

Where z is: 4-CMP, 5-MPE, 6-MPE-LI, 7-MRA

The Upgrade Media must be also delivered to the customer site prior to the execution of this upgrade procedure, in case recovery actions from the customer site become necessary. The distribution of media is outside the scope of this procedure.

If using ISO image files, it is assumed that the ISO image files have been delivered to a local workstation being used to perform this upgrade and any user performing the upgrade will have access to the ISO image files.

If the user performing the upgrade is at a remote location, it is assumed that the ISO files are already available to them before starting the upgrade procedure.

2.10.2 Logins, Passwords and Server IP Addresses

The IP Address assignments for each site, from the appropriate Oracle Network IP Site Survey (example: SS005938), must be available. This ensures that the necessary administration information is available prior to an upgrade.

Further, need to confirm login information for key interfaces, and document 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 (each CMP server)	GUI Administrator Login User/Password:
	root password: **NOTE:** This is the password for the root login on the servers. This is not the same login as the GUI or Application Administrator.
MRE/MPA servers (each server)	root password:
Target RMM/iLo (each server)	RMM Administrator Login: User/Password
Target OA (each C-class enclosure)	OA Administrator Login: User/Password
PMAC server (each C-class site)	GUI Administrator Login User/Password:
	root password: **NOTE**: This is the password for the root login on the servers. This is not the same login as the GUI or Application Administrator.
Software Upgrade Pack Target Release[3]	Target Release Number:
	Policy Management 9.x software ISO Image (.iso) file names:

2.11 Upgrade Manager Process

The 9.x CMP supports an Upgrade Manager feature which is used to upgrade MRAs and MPEs.

[3] The ISO image filenames should match those referenced in the Release Notes for the target release. If using physical CD media these ISO images will be extracted from the physical media during the upgrade process.

2.11.1 Overview

The Upgrade Manager collects and displays the Upgrade related status of the MPE and MRA servers, and provides a menu of operations for executing the required upgrade steps.

Like other CMP forms, the user must have privileges to use this tool.

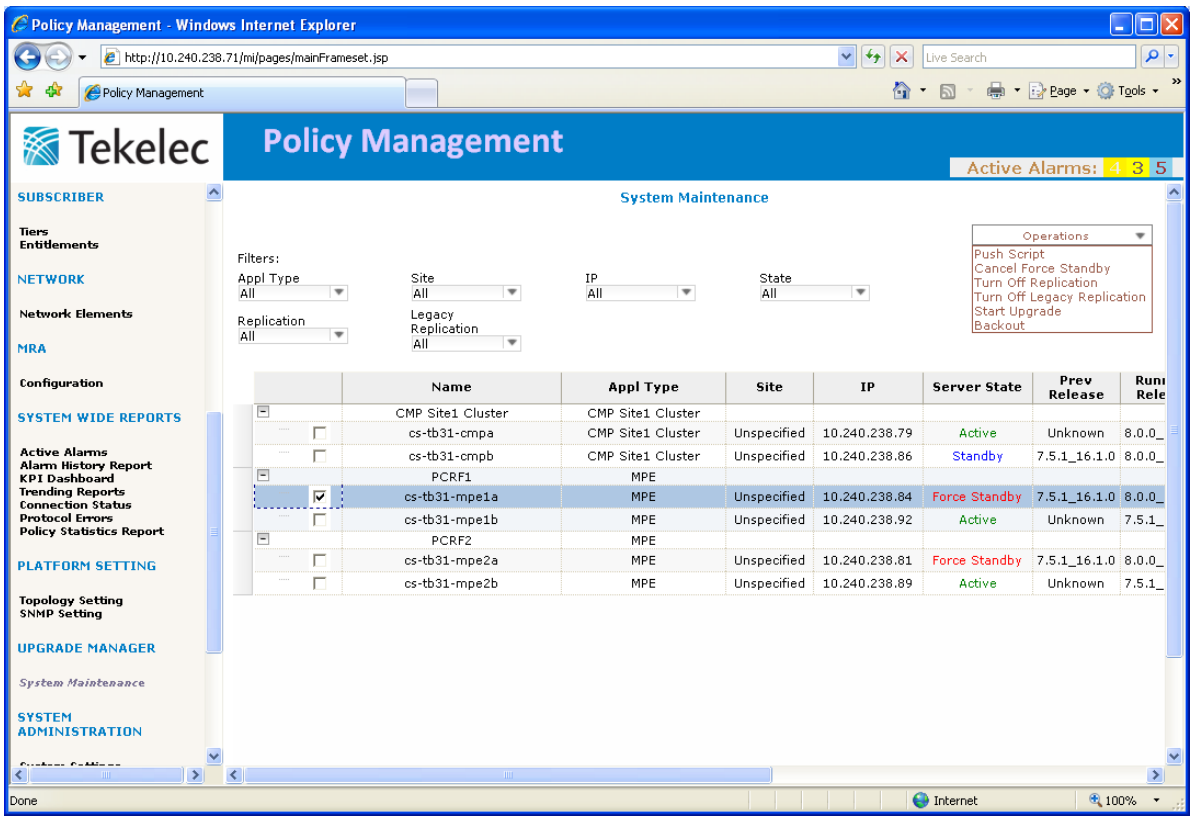
The following operations are supported:

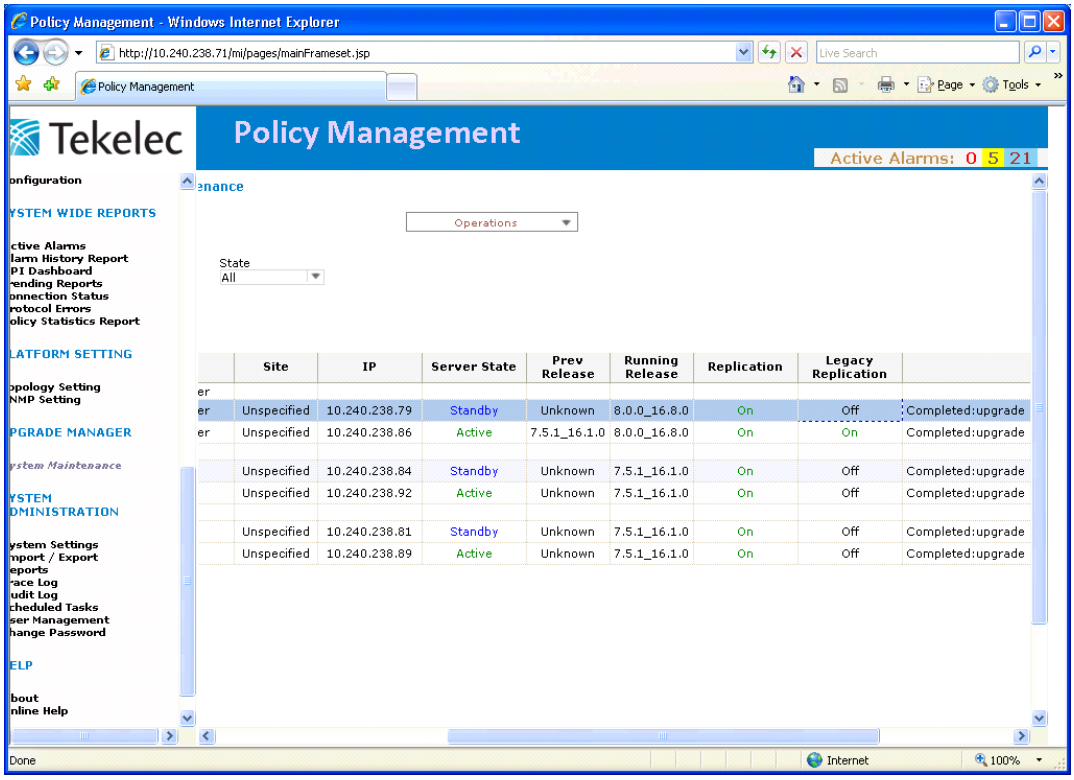
Table 2: Upgrade Manager Operations

Name	Description	Expected outcomes	The command call in remote server
Push Tool	Scp the upgrade script from CMP to the selected remote server(s)	Push Tool - Command returns Successful. Script policyUpgrade.pl is delivered to /opt/camiant/bin	policyUpgrade.pl --pushTool
Force Standby	Force the selected Active or Standby server to Force Standby	Force Standby - Command executed successfully. Status on the Upgrade Manager shows Forced Standby.	SOAP (HTTP/HTTPS)
Switch Force Standby	Make the Active Server to Force Standby, and the Force Standby Server to Active	Switch Force Standby - Command executed successfully. Status on the Upgrade Manager shows that the two servers in the cluster have switched roles.	SOAP (HTTP/HTTPS)
Cancel Force Standby	Cancel the selected server(s) force standby	Cancel Force Standby - Command executed successfully. Status on the Upgrade Manager shows Standby.	SOAP (HTTP/HTTPS)
Upgrade Completion	Turn off the selected server(s) Legacy Replication mode, and turn on new Replication mode	Command executed successfully. Inrepstat shows replication sync, no replication alarms. NodeInfo Exclusions are removed.	
Undo-Upgrade-Completion	Turn on the selected server(s) Legacy Replication mode	Command executed successfully. Inetstat show replication sync, no replication alarms. NodeInfo Exclusions are added.	policyUpgrade.pl --prepareUpgrade
Prepare Upgrade	Turn on the selected server(s) Legacy Replication mode	Command executed successfully. Inetstat shows replication sync, no replication alarms. NodeInfo Exclusions are added.	policyUpgrade.pl --prepareUpgrade
Start Upgrade	Kick off an upgrade on the selected server(s).	Start Upgrade - Command executed successfully. Upgrade Manager shows	policyUpgrade.pl --startUpgrade

Name	Description	Expected outcomes	The command call in remote server
		status of upgrade.	
Backout	Initiate a backout on the selected server(s).	Backout - Command executed successfully. Upgrade Manager shows status of upgrade.	policyUpgrade.pl --backOut

Example View of Upgrade Manager Form:





2.11.2 Operation Sequence for a Site Upgrade

The following is the normal sequence for upgrade at a site (MPEs and MRAs), using the Upgrade Manager. Multiple servers may be upgraded in parallel.

Pre-requisites:

- All CMPs in Topology are already upgraded to 9.x.
- The Application ISO files are deployed to the servers (`/var/TKLC/upgrade` directory).
- Ssh key exchange is completed between CMP and every MPE/MRA
- Ssh key exchange is completed between the 2 servers of each MPE/MRA cluster
- Prior execute of "Prepare Upgrade"
- Push the Upgrade script from CMP to all MPE/MRAs at a site

Upgrade 1st of 2 servers in a cluster:

1. Select some or all standby servers and execute **Forced Standby**

   Force Standby servers will not become Active

2. Select forced standby servers from previous step, and execute **Upgrade**

   This steps takes 20 minutes

   Confirm Upgrade completions for these servers

3. Execute "Switch ForceStandby"

   This step causes a switchover to the 9.x Server for Active traffic, with a several second traffic impact

   Confirm 9.x servers become Active and handle traffic

Upgrade 2nd of 2 servers in a cluster:

1. Select forced standby servers from previous step, and execute **Upgrade**

   Confirm Upgrade completions for these servers

2. Cancel Forced Standby on these servers

   Confirm 9.x servers Standby

Post-requisites (after all sites are upgraded):

1. Select all servers in the network, and execute **Upgrade Completion**
2. Remove Application ISO from the server's /var/TKLC/upgrade directory.

2.12 Firewall

The following protocol ports are used for managing data between Policy servers.

Table 3: Upgrade Manager Firewall requirements

Component	Port/Protocol
Tomcat	80/HTTP 8443/HTTPS
SSH	22/TCP
Comcol	15360/TCP (cmsoapa) 16810/TCP (inetsync) **17398/TCP (inetrep)** **17400/TCP (inetrep)** 17401/TCP (cmha) 16878/TCP (inetmerge) 15616/TCP (Imysqld)

For Policy Management 9.x, the "inetrep" ports are new, and are used by the new Replication software.

The 17400 port is opened for listening on each MPE/MRA blade, and the Active CMP connects to this port for replication.

- Active CMP – connects to -- MPE/MRA Port 17400
- Primary Site Active CMP – connects to – Secondary Site Active CMP Port 17400

The 17400 port is also opened on the Standby MPE/MRA/CMP and for used for replication from Active to Standby servers in a cluster.

- Active MPE– connects to -- Standby MPE Port 17400
- Active MRA– connects to -- Standby MRA Port 17400
- Active CMP– connects to -- Standby CMP Port 17400

The same Firewall rules should also be applied to Port 17389, but this port may not be actively used unless the MPE/MRA Geo-Redundancy feature is enabled.

NOTE: As per PR 227003, if the user encountered the issue mentioned in the PR, i.e. during upgrade, default firewall rules are not applied during upgrade, user may have to Disable firewall before the upgrade and then re-enable firewall after the upgrade.

```
# su - platcfg
```

Select **Camiant Configuration → Firewall → Enable/Disable Firewall → Edit → Disable iptables/Enable iptables**

2.13 Known Limitations

The following is a list of Known Limitations for the operations of the system, during the period that the system is being upgraded (when there is a mix of 9.x and 7.5 servers in the network).

- The Backout of a fully upgraded MPE/MRA cluster will result is the loss of all state data (call sessions) for existing calls in-progress.
- The Backout of a partially upgraded MPE/MRA cluster will result in the resumed use of state data that will be partially out-of-date.
    - The 7.5 server will retain its state data after traffic is switched to the 9.x server of the cluster, but this data will no longer be updated from traffic activity at the 9.x server. If the traffic is switched back to the 7.5 server, it will resume traffic handling with the state data it has, which will be partially out-of-date depending on how long the 9.x server was Active.
- The Mode settings must not be changed during upgrade interval
    - After upgrading the CMP, if you change modes, then 7.5 MPEs are unable to process quota correctly (because UseLocalQuota gets set to true)
    - After upgrading both the CMP and the MPE, then we can no longer terminate Gy sessions (because the quota is all messed up)

3. UPGRADE PREPARATION

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

3.1 Prerequites

This procedure verifies that all required prerequisite steps needed to perform an upgrade have been completed.

3.1.1 Procedure 1: Verify Prerequisites

Step		Procedure	
1	☐	Verify all required materials are present	Materials are listed in Section 2.10: Required Materials. Verify required materials are present.
2	☐	Review Release Notes	Review Policy Management 9.x software Upgrade Release Notes for the target release for the following information: • Individual Software components and versions included in target release • Issues (Oracle PRs) resolved in target release • Known Issues with target release • Any further instructions that may be required to complete the Software Upgrade for the target release
3	☐	Verify all administration data needed during upgrade	Double-check that all information in Section 2.10.2 is filled-in and accurate.
4	☐	Contact Oracle Customer Care Center	Contact My Oracle Support and inform them of your plans to upgrade this system.
This procedure is completed			

3.2 PMAC Upgrade

Policy Release 9.x includes an upgrade to the Management Server (PMAC) for C-class installations to PMAC Rel 5.1. This version of PMAC provides support for HP GEN8 servers, and uses a TVOE virtual OS environment.

The PMAC version is a major upgrade, from release 3 to release 5.1, and includes changes to the look and feel of the GUI, better reliability and improved Software Inventory function. Functionality remains the similar to previous release, and changes are easy to learn.

This upgrade is backwards compatible to Policy 7.5 installations, and can be performed without any risk of network impacts.

NOTE: An additional Management IP Address is required for this PMAC installation.

See Appendix C for instructions to Upgrade PMAC.

3.3 Plan and Track Upgrades

The procedures in this document divide the Upgrade into 3 steps:

- Upgrade CMP clusters
- Upgrade MPE and MRA clusters, 1 site at a time
- Activate the 9.x Replication feature

The following Procedure must be completed before the Upgrade begins, 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.

The MPE Upgrades can be done in parallel.

NOTES:

- No Policy Changes or Configuration change may be made while the system is in mixed-mode.
- Time estimates are for upgrade activity without roll back. Roll back time is typically same or less than upgrade time.
- On C-class systems, the PMAC server must be upgraded before upgrading of the Policy application servers. There is a separate procedure for PMAC Upgrade.

3.3.1 Procedure 2: Plan and Track Cluster Upgrades

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th><th>Init</th><th>Time</th></tr>
<tr><td>1 ☐</td><td>Use the following Checklist to plan the Cluster upgrades for the entire system.</td><td>Maintenance Windows are planned</td><td></td><td></td></tr>
<tr><td>2 ☐</td><td>PRIMARY Site CMP cluster Upgrade</td><td>Site Name _____</td><td></td><td>1 hr</td></tr>
<tr><td>3 ☐</td><td>SECONDARY-Site CMP cluster Upgrade</td><td>Site Name _____</td><td></td><td>30 min</td></tr>
<tr><td>4 ☐</td><td>MPE/MRA clusters Upgraded at Site 1</td><td>Site Name _____

Cluster List:
<table>
<tr><th>Cluster Name</th><th>Hostname 1</th><th>Hostname 2</th><th>Completed?</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table></td><td></td><td>2 hrs</td></tr>
<tr><td>5 ☐</td><td>MPE/MRA clusters Upgraded at Site 2</td><td>Site Name _____

Cluster List:
<table>
<tr><th>Cluster Name</th><th>Hostname 1</th><th>Hostname 2</th><th>Completed?</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table></td><td></td><td>2 hrs</td></tr>
</table>

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th><th>Init</th><th>Time</th></tr>
<tr><td>6 ☐</td><td>MPE/MRA clusters Upgraded

Site 3</td><td>Site Name _____

Cluster List:
<table>
<tr><th>Cluster Name</th><th>Hostname 1</th><th>Hostname 2</th><th>Completed?</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table></td><td></td><td>2 hrs</td></tr>
<tr><td>7 ☐</td><td>MPE/MRA clusters Upgraded

Site 4</td><td>Site Name _____

Cluster List:
<table>
<tr><th>Cluster Name</th><th>Hostname 1</th><th>Hostname 2</th><th>Completed?</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table></td><td></td><td>2 hrs</td></tr>
</table>

3.4 Perform System Health Check (Upgrade Preparation)

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

3.4.1 Procedure 3: Perform System Health Check (Upgrade Preparation)

Step		Procedure	Result
1	☐	Login to Manager (CMP) GUI	
2	☐	View Active Alarms	Identify the cause of any active alarms, and determine if these may have impact on the upgrade. Export current Alarms to file, and save.
3	☐	View KPI Dashboard	Verify that the system is running within expected parameters. Export current KPIs to file, and save.

4	☐	Confirm TSB have been applied (as needed)	Confirm that any needed Technical Service Bulletins (TSB) have been applied.
			Specifically: *Procedure to reset upsynclog configuration parameters back to designed values* must be applied.
			This TSB requires that a command is run on each server in the system to confirm that the configuration is set correctly. If is it not, a procedure must be applied (in a maintenance window) to set the correct configuration value.
			Verify Command (run on each server):
			`iqt -p PartAttrDef where "partDefRecNum='UpSyncLog' and attr='KeepCount'"`
			Correct Result:
			`recNum partDefRecNum attr val`
			`135 UpSyncLog KeepCount 0`
			See the TSB for the procedure to repair, if needed.
			NOTE: This TSB needs to be applied on CMP servers as well only after the all associated MPEs have been applied. When applying this on CMP servers, if there is an error like: schema has mismatched, this will need manual manipulation.

5	☐	Fix for Missing file	On 7.5 MPE/MRA servers, the following file may be missing, and this will (may) cause a Upgrade failure.
			`/opt/camiant/smsr/smscfg/log4j.properties`
			Check if this file exists before upgrade. If not:
			`# touch /opt/camiant/smsr/smscfg/log4j.properties`
			NOTE: In the steps of upgrade, if upgrade has failed immediately, and the upgrade.log shows: Missing Files: camiant-comcol-schemata-xxx `/opt/TKLCcomcol/camiant/prod/maint/loaders/load.dbcfg`.
			`# touch /opt/TKLCcomcol/camiant/prod/maint/loaders/load.dbcfg`

THIS PROCEDURE HAS BEEN COMPLETED			

3.5 Firmware Upgrades

Oracle notifies customers when critical Firmware upgrades are needed. However, other non-critical firmware updates are issued periodically and recommended.

In general, the upgrade of the Policy application does not depend on these firmware upgrades. However, it is strongly recommended deploy any recommended firmware upgrades. This is typically deployed before Policy Management 9.x upgrade.

Current Recommended HP Firmware delivery:

HP Service Pack for ProLiant 2.2.3 ISO	P/N: 875-1124-103	ISO: 872-2488-103-2.2.3-10.29.0.iso
HP Misc Firmware 2.2.2 ISO	P/N: 875-0903-213	ISO: 872-2161-115-2.2.2_10.28.0.iso
Upgrade Procedures Document	P/N: 909-2234-001 Rev A	
Release Notes	P/N: 910-6611-001 Rev A	

This Oracle HP Firmware rev includes Release notes that identify the latest firmware revs for each of the system components.

Firmware upgrade procedures are not included in this document.

NOTE: The firmware upgrade of the Enclosure switches causes a very brief traffic impact, as the switch boots (traffic will failover to the other switch during this activity).

3.6 Deliver Software to Sites

The following media should be shipped to site:

- New PMAC Software
  - PMAC TVOE 2.0 Installation DVD
  - PMAC 5.0 Application ISO (on DVD or USB key)
- Old PMAC Software (for backout)
  - PMAC TPD
  - PMAC 3.x Application ISO
- New Firmware:
  - HP Smart Update Firmware 2.2.3 (on BOTH DVD and USB key)
  - Oracle Misc Firmware Update ISO (on USB key)
- Old Firmware (for backout)
  - HP Smart Update Firmware x.x.x (on BOTH DVD and USB key)
  - Oracle Misc Firmware Update ISO (on USB key)

A local support person must be available to insert the media in the systems, as needed.

Both 9.x and 7.5 Policy Applications will need to be available at the site.

It is assumed that these ISO files can be transferred to PMAC or another on-site server using file transfer, so they are available for upgrade or recovery activities at the site.

(This may take as much as 1 day, depending on the transfer rate.)

3.7 Deploy Software (Upgrade Preparation)

This procedure is intended for remote execution of the Upgrade.

Software should be deployed to each Policy server “upgrade” directory, before the actual upgrade activities. This will typically be done with scp, wget or ftp. Because of the large size of the software ISO files, sufficient time should be planned to accomplish this step.

It is recommended to copy the ISO images to a server at the site, and then re-distribute the ISO images to the other servers at the site. This allows faster transfer times, and allows the host names to be used during the transfer (which reduces the possibility of the wrong image being deployed to a server).

3.8 Deploying Upgrade Software to Servers

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

IMPORTANT: If the deployed image type (CMP, MRA, MPE) 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, and then the new Application type installed.]

3.8.1 Procedure 4: Copy ISO images to Management Servers (PMAC)

If the system has a Management Server (PMAC), then the following procedure must be applied for each PMAC server in the system.

IMPORTANT: PMAC should be upgraded from 3.0 to 5.1 release prior to this step. See Appendix C.

PMAC may be upgraded in advance of the Application upgrade. PMAC 5.0 can manage Policy 7.5 servers.

This procedure transfers software Upgrade ISO files to the PMAC, and loads the ISO files into the PMAC Software Image repository.

NOTES:

- 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.
- Because the ISO images are large, the procedure includes instructions to check space available in the `/var/TKLC/upgrade` directory before copying the ISO files to this directory. After the "Add Image" action on the PMAC, the ISO images are registered in PMAC, and stored in the `/var/TKLC/smac/image/` directory which is very large. After this step, the added images can then be removed from the `/var/TKLC/upgrade` directory.

PRE-REQUISITE: PMAC is upgraded to 4.0 release.

Step	Procedure	Result
1 ☐	**PMAC GUI:** login to pmac as pmacadmin	Open the PMAC GUI, select **Software → Manage Software Images** Determine what Images are installed, and confirm that new images are not yet installed.
2 ☐	WinSCP to PMAC server, login as root	From workstation with ISO Images, open WinSCP (or similar tool), ad login as root.
3 ☐	WinSCP: Change Target Directory to /var/TKLC/upgrade	Change Target Directory to /var/TKLC/upgrade
4 ☐	WinSCP: Remove existing ISO files from /var/TKLC/upgrade	To keep this directory space free, remove any existing ISO files
5 ☐	WinSCP: Copy ISO image to PMAC	Copy a ISO image to PMAC /var/TKLC/upgrade directory

Step	Procedure	Result
6 ☐	PMAC GUI: Add Image	**Software → Manage Software Images** Click **Add Image** Select the ISO that was just copied to the PMAC server.
7 ☐	PMAC GUI: Verify Image is added	**Software → Manage Software Images** The just added image will show in this view after about 1 minute. **NOTE:** Added images are stored in /var/TKLC/smac/image
8 ☐	Repeat above steps for all images	Repeat above steps for all images • TPD Software ISO for Policy • Policy CMP Iso • Policy MPE (or MPE-LI) Iso • Policy MRA Iso
THIS PROCEDURE HAS BEEN COMPLETED		

3.8.2 Procedure 5: Copy ISO Images to Target Servers (PP5160, DL360, c-Class)

This procedure applies to all Server types. For c-Class installations, the previous procedure must also be executed. It is assumed that there is scp access to each server to be upgraded, and that the Application software images are available in a ISO format that can be copied to the servers.

- For PP5160 or DL360, it is also possible to use the CD drive on the server to perform the upgrade, as an alternative to copying the ISO file to the server.
- For C-class servers, the PMAC server may be used to load the ISO files from the PMAC CD drive.

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.

The ISO images are put in the `/var/TKLC/upgrade` directory on each server. Because the ISO images are large, the following procedure includes instructions to check space available before copying the ISO to this directory. The Upgrade command, used later in the procedure, will look in this directory for available upgrades, and present a list to the user.

Step	Procedure	Result
1 ☐	Select Server at the upgrade site to use as Distribution point	This procedure will select a server at the site to copy the ISO images to, and then this server will be used to re-distribute ISO images to the other servers at the site. Distribution Server at site (CMP, MPE, MRA): Example: `cmp_ip_address`
2 ☐	Ssh to Distribution Server:	1. Access the login prompt. 2. Log into the server as the root user on the iLO or RMM. **login as: root** **password: <*enter password*>**

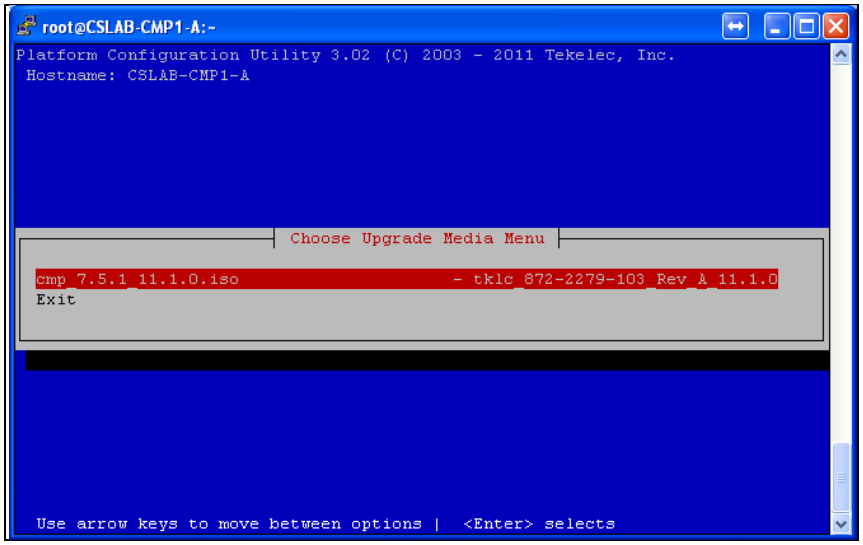
Step	Procedure	Result

3 ☐	Verify enough space exists for ISO	1. Verify that there is at least 1G in the Avail column. If not, clean up files until there is space available.
		2. Make sure you know what files you can remove safely before cleaning up. It is recommended that you only clean up files in the `/var/TKLC/upgrade` directory as this is a platform owned directory that should only contain ISO images. This directory should not be expected to contain images for any length of time as they can get purged.
		Removing files other than those in directory `/var/TKLC/upgrade` is potentially dangerous.
		3. Cleanup un-needed ISO files in upgrade directory.
		`# ls /var/TKLC/upgrade`
		If needed:
		`# rm /var/TKLC/upgrade/*.iso`
		4. Check disk space available
		`# df -h /var/TKLC`
		`Filesystem Size Used Avail Use% Mounted on`
		`/dev/mapper/vgroot-plat_var_tklc`
		`3.9G 174M 3.6G 5% /var/TKLC`

4 ☐	Copy a Policy Management 9.x software ISO image file fromthe local workstation to the target server upgrade directory.
	Image will be one of: CMP, MRA or MPE.
		From the local workstation: (use WinSCP, or equivalent), copy the Policy Management 9.x software ISO to target server
		`# scp <ISO Name> root@<server IP>:/var/TKLC/upgrade`
		Example for CMP ISO:
		`# scp 872-2544-101-9.1.0_x.y.0-cmp-x86_64.iso root@xx.xx.xx.xx:/var/TKLC/upgrade`

5 ☐	Verify ISO image file is copied to correct location. Examine output of the command and verify that the ISO file is present and that file size appears correct.	From the Distribution server: `# ls –l /var/TKLC/upgrade-rw-r--r-- 1 root root 863408128 Jul 24 14:27 872-2544-101-9.1.0_x.y.0-cmp-x86_64.iso`

Step	Procedure	Result

6 ☐	Validate the Policy Management 9.x software ISO
	
	Rel 9.x Application Part Numbers:
	
	CMP – 872-2544-101
	
	MPE – 872-2545-101
	
	MPE-LI – 872-2546-101
	
	MRA – 872-2547-101
		`# su - platcfg`
		
		Maintenance → Upgrade → Validate Media
		
		 
		
		NOTE: The ISO file type may not be shown in the ISO name, as in the example above. In this case, the following part numbers identify the applications types for Rel 9.x:
		
		Select the Iso file to validate, and enter
		
		Expected Result:
		
		…
		`UMVT Validate Utility v2.2.1, (c)Oracle, June 2010`
		`Validating /var/TKLC/upgrade/cmp_9.x_18.2.0.iso`
		`Date&Time: 2011-11-01 09:24:39`
		`Volume ID: tklc_872-2544-101_Rev_A_18.2.0`
		`Part Number: 872-2544-101`
		`Version: 18.2.0`
		`Disc Label: cmp`
		`Disc description: cmp`
		`The media validation is complete, the result is: PASS`
		
		`CDROM is Valid`
		
		Note: Do not continue if ISO image validation reports any errors or is invalid. Instead remove the ISO file and either re-copy it to the target system or regenerate it from physical media.

Step	Procedure	Result

7 ☐	Re-Distribute ISO to other servers of this type at the site
	
	This step will depend on the ISO type.
		From the Distribution server:
		`# cat /etc/hosts | grep <cmp, mpe, mra>`
		Example :
		`[root@slak-cmp-a upgrade]# cat /etc/hosts | grep cmp`
		`10.250.85.25 slak-cmp-a`
		`10.250.84.25 brbg-cmp-a`
		`10.250.84.26 brbg-cmp-b`
		`10.250.85.25 slak-cmp-a`
		`10.250.85.26 slak-cmp-b`
		For the servers of the type for this ISO:
		`# ssh <hostname>`
		`# ls -l /var/TKLC/upgrade`
		Make sure this directory is empty. If not, remove any existing ISO files
		`# exit`
		Copy software to CMPs:
		`# scp 872-2544* <cmp_hostname>:/var/TKLC/upgrade`
		Copy software to MPEs:
		`# scp 872-2545* (or 872-2546*) <mpe_hostname>:/var/TKLC/upgrade`
		Copy software to MRAs:
		`# scp 872-2547* <mra_hostname>:/var/TKLC/upgrade`

8 ☐	Remove ISO from Distribution server (if it is not needed for this server)	If the ISO file is not needed at the Distribution server, delete it.
		[Example: Distribution server is CMP, and ISO is MPE.]
		From the Distribution server:
		`# ls /var/TKLC/upgrade`
		Remove CMP ISO from non-CMP distribution server:
		`# rm /var/TKLC/upgrade/872-2544*`
		Remove MPE ISO from non-MPE distribution server:
		`# rm /var/TKLC/upgrade /872-2545* (or 872-2546*)`
		Remove MRA ISO from non-MRA distribution server:
		`# rm /var/TKLC/upgrade /872-2547*`

9 ☐	Repeat steps 4 – 9 for each server type (CMP, MPE, MRA) at the upgrade site.	Steps 4 – 9 must be repeated for each server type at the target site to be upgraded.
10 ☐	This procedure needs to be repeated for each site to be upgraded.	This procedure needs to be repeated for each site to be upgraded.
Procedure is completed		

3.8.3 Procedure 6: Verify CMP Software Images

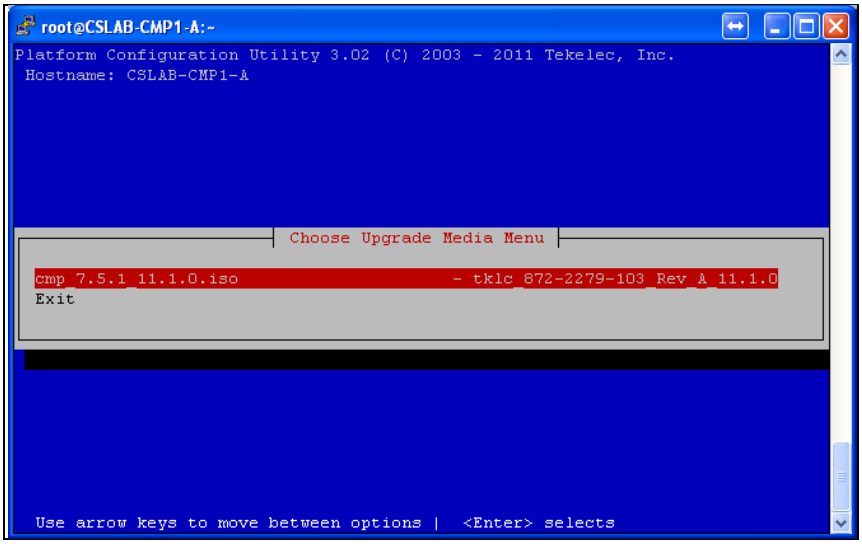
Detailed steps are shown in the procedure below to verify that the image files are correctly deployed and ready for upgrade activity on the CMPs. (A similar step will be done later for the upgrade of the MPE/MRA servers.)

Step	Procedure	Result

1 ☐	SSH: Primary Active CMP
	
	Log into the server as the root user
		`login: root`
		
		`Password: <root_password>`

2 ☐	**SSH:** Verify Image is deployed at Primary CMP cluster
	
	Rel 9.x Application Part Numbers:
	
	CMP – 872-2544-101
	
	MPE – 872-2545-101
	
	MPE-LI – 872-2546-101
	
	MRA – 872-2547-101
		Verify that the correct software ISO is loaded on the server.
		
		IMPORTANT: If the ISO file is the wrong type (example: CMP ISO loaded on a current MRA configured server), the upgrade step for this server will fail and the server will need to be re-installed from the Install OS step.
		
		`# getPolicyRev`
		`7.5.x_x.x.x`
		
		`# getPolicyRev -p`
		`cmp`
		
		`# ls -l /var/TKLC/upgrade`
		`total 706236`
		`-rw-r--r-- 1 root root 863408128 Jul  3 03:04 cmp--9.x.0_18.2.0--872-2544-101--x86_64.iso`
		
		Verify that the ISO matches the correct part number for this server function (CMP), and
		
		Verify there is only one ISO in this directory.

Step	Procedure	Result

3 ☐	Validate ISO image	This step will validate the ISO image:
		`# su - platcfg`
		Maintenance → Upgrade → Validate Media
		 
		
		Choose ISO to validate, and enter
		Expected Result:
		`UMVT Validate Utility v2.2.1, (c)Oracle, June 2010`
		`Validating /var/TKLC/upgrade/cmp_9.x.0_18.2.0.iso`
		`Date&Time: 2011-11-01 09:24:39`
		`Volume ID: tklc_872-2544-101_Rev_A_18.2.0`
		`Part Number: 872-2544-101`
		`Version: 18.2.0`
		`Disc Label: cmp`
		`Disc description: cmp`
		`The media validation is complete, the result is: PASS`
		CDROM is Valid
		Note: Do not continue if ISO image validation reports any errors or is invalid. Instead remove the ISO file and either re-copy it to the target system or regenerate it from physical medi
		`# exit`

4 ☐	If ISO image is not found, or not valid	If ISO image is not found, or not valid, re-deploy the correct ISO image.
5 ☐	Repeat steps 2-4 for each of the remaining CMP servers in the network.	Primary Standby CMP _____ Secondary Active CMP _____ Secondary Standby CMP _____

Step	Procedure	Result

6 ☐	**SSH: Primary Active CMP**
	
	Verify SSH Key Exchange for CMP cluster
		`# ssh <Primary Standby CMP>`
		
		Confirm that there is no password prompt.
		
		If needed, perform ssh Key Exchange:
		
		`# su - platcfg`
		`Camiant Configuration → Exchange SSH keys`
		`OK`

7 ☐	**SSH:** Secondary Active CMP
	
	Verify SSH Key Exchange for CMP cluster
		`# ssh <Secondary Standby CMP>`
		
		Confirm that there is no password prompt.
		
		If needed, perform ssh Key Exchange:
		
		`# su - platcfg`
		`Camiant Configuration → Exchange SSH keys`
		`OK`

Procedure is completed		

3.9 Verify Network Firewall Connectivity

Verify that the additional firewall connectivity needed for Rel 9.x is implemented in the network.

Specifically:

- See detail from Policy Management 9.x Network Architecture Planning Document (NAPD) (see References)

3.10 Backups for Servers and the System

IMPORTANT: Backups for servers, and the system, must be collected and readily accessible for recovery operations.

Consider doing this before each major activity.

Nightly Backup collection should normally be automated for a customer deployment, so identify the location and access method for these backups. If needed, perform manual backups.

3.10.1 Procedure 7: Backups (System and Server) Location and Access

Step	Procedure	Result
1 ☐	Identify Backups Location	Backup location is: _____ Instructions to access to backups are as follows: _____ _____ _____
Procedure is completed		

3.11 Collect Ddata Exports from the System

The Policy system supports Export of key configuration data, such as:

- Policies
- Network Elements
- Quotas

VIdentify what data should be exported, and verify that a recent export of this data is saved to a off-line system.

This may be important for post system upgrade activities.

4. 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.

5. UPGRADE CMP CLUSTERS

This procedure will upgrade the Primary site CMP cluster, and then upgrade the optional Secondary site CMP cluster, in a single maintenance window.

NOTES:

- Once the first CMP at the Active site is upgraded and made active, the other CMPs will report an alarm condition to indicate that they are not able to sync to the Active CMP. As the other CMPs are upgraded, they will re-sync.
- The Upgraded CMPs can perform basic monitoring of the 7.5.x MRAs/MPEs, to allow the migration of these elements to be spaced over several maintenance windows. However, configuration changes must not be performed for these elements.
- New Policies should not be introduced/deployed during the period when the Policy elements are being upgraded. Once all elements are on the new release, Policy activities can resume.
- Rollback option is supported at each step of the upgrade

5.1 Upgrade Active Site CMP Cluster

This procedure should be executed inside of a Maintenance window.

It is assumed that the CMPs may be deployed as 2 geo-redundant clusters, identified as Primary (active) Site and Secondary (non-active) Site. [However, a geo-redundant CMP configuration is not required.]

This section will upgrade the Primary site CMP Cluster, and the next section will upgrade the Secondary Site CMP Cluster. Both may be completed in a single Maintenance window.

Identify the CMPs Sites to be upgraded here, and verify which site is Primary and Secondary:

CMP Site Geo Status	Operator Site Name	Site Designation from Topology Form (aka; 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 _____

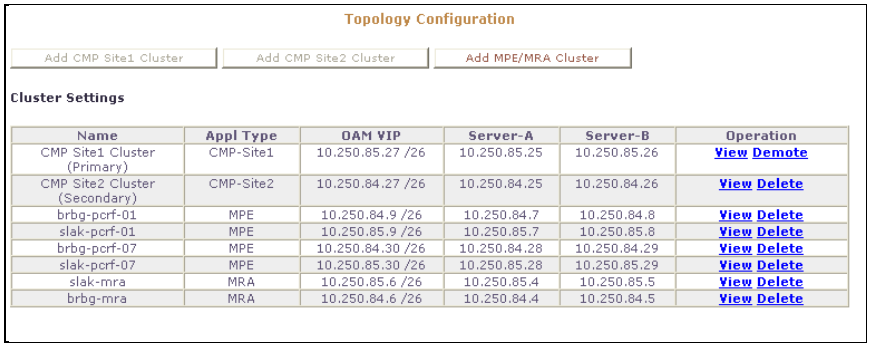
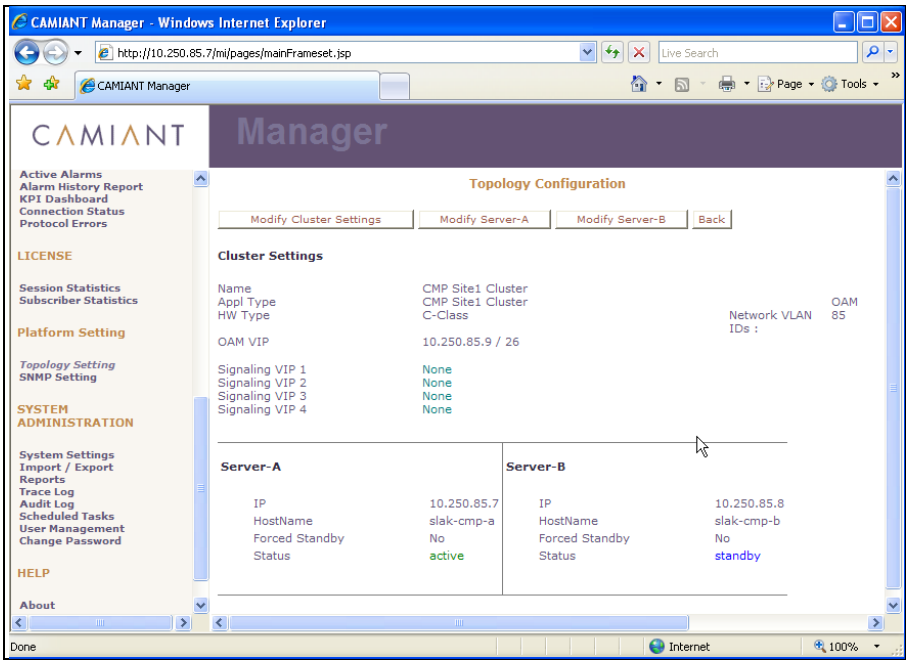
Server-B Status _____

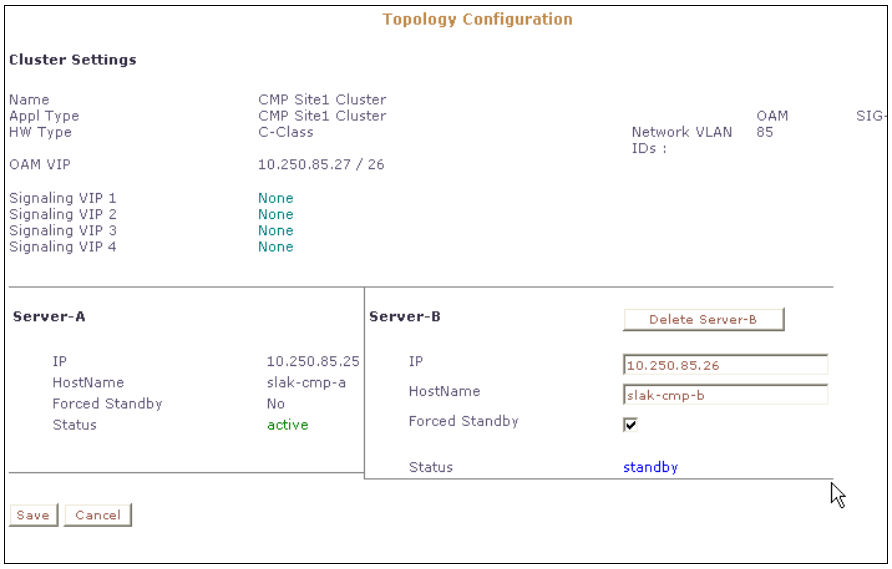
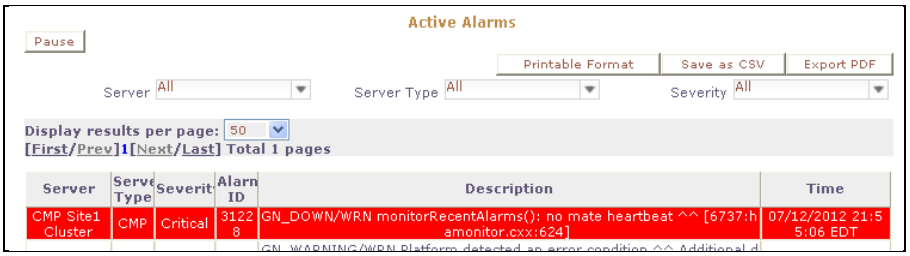
IMPORTANT: CMP servers MUST be upgraded before the MRA or MPE servers.

5.1.1 Procedure 8: Upgrade Standby server at Primary CMP Site

Pre-requisites:

- Procedure 6 is completed – which copies the newest policyUpgrade.pl script onto the Primary Active CMP server

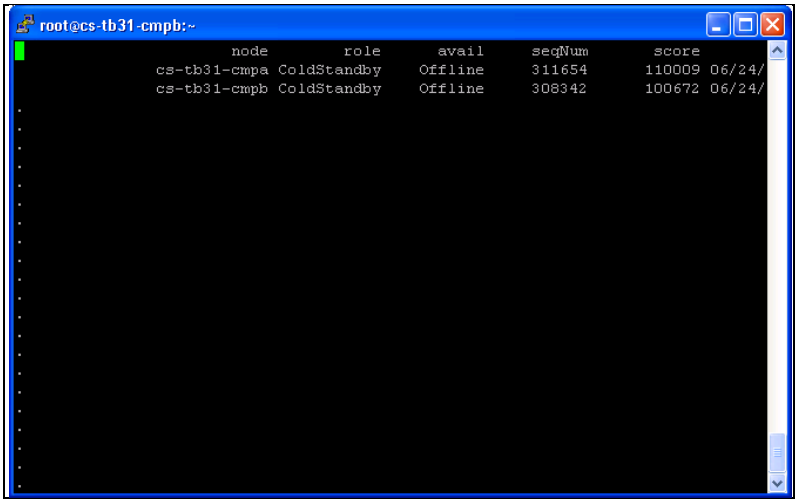
Step	Procedure	Result
1 ☐	**GUI:** Identify the CMP Cluster to be Upgraded	From CMP Manager: **Platform Setting → Topology Setting**  Select the (Primary) CMP Cluster to be Upgraded and View Status (Primary CMP Site): 
2 ☐	**GUI**: Identify the first server in cluster to be Upgraded	Record the CMP Server with Status standby that will be upgraded first. Server to Upgrade First _____

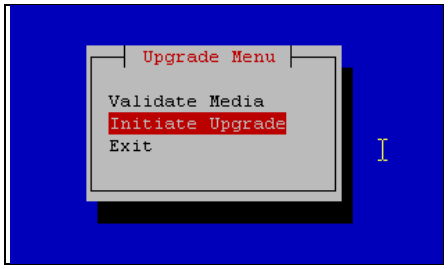
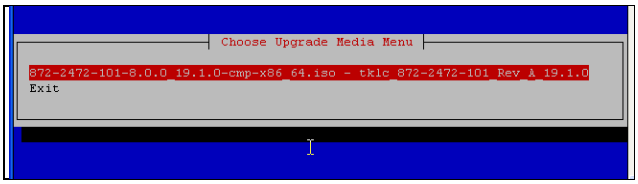
Step	Procedure	Result
3 ☐	**GUI**: Make Standby server Forced Standby	From Manager GUI, Topology view, select Modify for the current **Standby** CMP server **Topology → CMP Primary Site Cluster View → Modify Server –A or –B** Set the Forced Standby checkbox on Standby Server Save the form.  An Alarm will occur to indicate that the Active CMP server has lost sync with the Standby CMP Server. (this may take a minute to appear in the Active Alarms list) 
4 ☐	**SSH:** Login to **Primary Active CMP** server via ssh	``` CentOS release 4.6 (Final) Kernel 2.6.18-1.2849prerel3.3.0_63.1.0 on an i686 localhost login: root Password: <root_password> Verify that this is the Active CMP: # ha.stat ```
5 ☐	**SSH:** Primary Active CMP Extract Upgrade script from CMP ISO	``` # cd /var/TKLC/upgrade # ls 872-2544-101-9.x.0_24.2.0-cmp-x86_64.iso # mount -o loop /var/TKLC/upgrade/872-2544* /mnt/upgrade # cp /mnt/upgrade/upgrade/policyScripts/policyUpgrade.pl /opt/camiant/bin # umount /mnt/upgrade ```

Step	Procedure	Result

6 ☐	**SSH: Primary Active CMP:** Prepare Servers for Upgrade.
	
	Disable replication for certain data tables.
		Execute command to Disable Replication for certain data tables.
		
		`# iqt -p NodeInfo`
		
		`nodeId nodeName hostName inhibitFlag nodeCap excludeTables`
		
		`A3411.121 slak-cmp-b slak-cmp-b,10.250.85.26 MasterCapable`
		
		`A3411.190 slak-cmp-a slak-cmp-a,10.250.85.25 H MasterCapable`
		
		`C1428.038 slak-mpe-07a slak-mpe-07a,10.250.85.28 MasterCapable`
		
		`C1428.073 slak-mpe-07b slak-mpe-07b,10.250.85.29 MasterCapable`
		
		`C3265.167 slak-mra-b slak-mra-b,10.250.85.5 MasterCapable`
		
		`C3265.212 slak-mra-a slak-mra-a,10.250.85.4 MasterCapable`
		
		`C3573.020 slak-mpe-01a slak-mpe-01a,10.250.85.7 MasterCapable`
		
		`C3573.027 slak-mpe-01b slak-mpe-01b,10.250.85.8 MasterCapable`
		
		`# policyUpgrade.pl --prepareUpgrade`
		
		Verify that file is updated with excludeTables “LongParam,AppEventDef”
		
		`# iqt -p NodeInfo`
		
		`nodeId nodeName hostName inhibitFlag nodeCap excludeTables`
		
		`A3411.121 slak-cmp-b slak-cmp-b,10.250.85.26 MasterCapable LongParam,AppEventDef`
		
		`A3411.190 slak-cmp-a slak-cmp-a,10.250.85.25 H MasterCapable LongParam,AppEventDef`
		
		`C1428.038 slak-mpe-07a slak-mpe-07a,10.250.85.28 MasterCapable LongParam,AppEventDef`
		
		`C1428.073 slak-mpe-07b slak-mpe-07b,10.250.85.29 MasterCapable LongParam,AppEventDef`
		
		`C3265.167 slak-mra-b slak-mra-b,10.250.85.5 MasterCapable LongParam,AppEventDef`
		
		`C3265.212 slak-mra-a slak-mra-a,10.250.85.4 MasterCapable LongParam,AppEventDef`
		
		`C3573.020 slak-mpe-01a slak-mpe-01a,10.250.85.7 MasterCapable LongParam,AppEventDef`
		
		`C3573.027 slak-mpe-01b slak-mpe-01b,10.250.85.8 MasterCapable LongParam,AppEventDef`
		
		NOTE: This change is automatically replicated to all 7.5.x servers from the Active CMP, and notifies the servers not to process any further updates to these tables. This step is needed since the upgraded CMPs (8.0) may send table updates to the 7.5.x servers that they will not be able to process correctly.
		
		NOTE: This Minor Alarm may be expected from servers
		
		31101 - GN_WARNING/WRN configuration change forcing re-init [SyncMaster.cxx:587], but will clear itself very quickly.

7 ☐	**SSH/Console/iLo:** Login to CMP Force Standby server
	
	Either:
	
	5. SSH - Access the login prompt.
	6. Log into the server as the root user on the iLO or RMM, and access Remote Console
		`CentOS release 5.5 (Final)`
		`Kernel 2.6.18-194.32.1.el5prerel4.2.3_70.88.0 on an x86_64`
		
		`CMP-02F login:`

Step	Procedure	Result
8 ☐	**SSH/Console/iLo:** Verify ha status at **Standby** CMP	`# ha.stat`  Result will show “ColdStandby” and “Offline”.
9 ☐	**SSH/Console/iLo:** Verify Application is running	`# service qp_procmgr status` `qp_procmgr (pid 13410) is running...`

10 ☐	**SSH/Console/iLo:** Apply Upgrade at Primary Standby CMP
	
	NOTE: the Application is NOT shutdown prior to the upgrade.
	
	This will take approximatelty 20 minutes
		If using ssh, run the `screen` command to prevent hang-ups, and do not exit this screen session until the server reboots.
		`# screen`
		Open platcfg.
		`# su - platcfg`
		Select **Maintenance → Upgrade → Initiate Upgrade**
		 
		
		 
		
		Monitor the ssh window output for the first few minutes, in case the upgrade fails during it’s pre-upgrade checks.
		
		NOTE: If upgrade fails due to the missing files, follow the workaround below (following errors will be logged in upgrade.log):
		
		1369689305:: Checking for any missing packages or files
		
		1369689305:: Checking for missing files...
		
		1369689306::Missing Files:
		
		1369689308:: 0:TKLCsavelogsplat-4.1.17-4.2.3_70.84.0:

Step	Procedure	Result
		/usr/TKLC/plat/etc/savelogs_plat.d/rpms 1369689308:: 1369689308::ERROR: There are files missing from some rpms! 1369689308::ERROR: Will not upgrade the server! 1369689308:: Restarting cron service... **Work Around** Copy the rpms file from `/tmp to the /usr/TKLC/plat/etc/savelogs_plat.d/` directory. After this, output will then show that software packages are being upgraded. This will take 15 - 20 minutes. The SSH session will close as the server re-boots. Re-boot will take several minutes. **Manager GUI Activity** There will be a Major alarm 70005 for CMP cluster. Also multiple Minor Database replication Alarms: 31101, 31102, 31106, 31107, 31114. KPI Dashboard, and PCRF and MRA reports will show that traffic is proceeding as normal.

11 ☐	**SSH/Console/iLo:** Login again to upgraded server.
	
	If login using the Console or Remote Console, verify that server returns to the login prompt after boot.
		`CentOS release 5.5 (Final)`
		`Kernel 2.6.18-194.32.1.el5prerel4.2.3_70.88.0 on an x86_64`
		
		`CMP-02F login:`

12 ☐	**SSH/Console/iLo:** Verify software versions	**`# getPlatRev`** **`5.0.1-72.45.0`** **`# getPolicyRev`** **`9.x.0_x.x.x`**

13 ☐	**SSH/Console/iLo:** Verify success of Upgrade	**`# tail /var/TKLC/log/upgrade/upgrade.log`**
		
		The following indicates SUCCESS of Upgrade.
		
		`[root@CMP-02F ~]# tail /var/TKLC/log/upgrade/upgrade.log`
		`1321039028::  UPGRADE IS COMPLETE`
		`1321039029::`
		`1321039029::  Waiting for reboot`
		`1321039029::DEBUG:  ADDING VAR: UPGRADE_STATUS = SUCCESS`
		`1321039029::DEBUG:  ADDING VAR: UPGRADE_COMPLETED = 11/11/2011 19:17:09 UTC`
		
		IF UPGRADE_STATUS is not equal to SUCCESS, then collect upgrade.log for analysis.
		
		See step 18.

Step	Procedure	Result

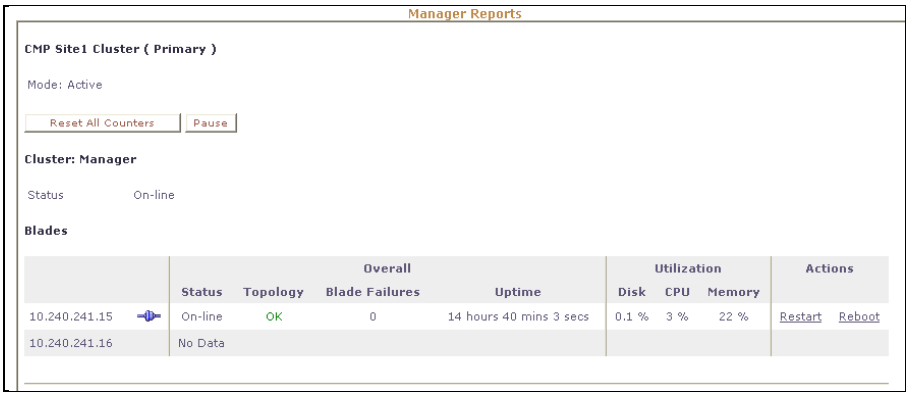
14 ☐	**SSH/Console/iLo:** Verify Status of server processes
	
	(Server is still Forced Standby)
		`# ha.mystate`
		
		`resourceId role node lastUpdate`
		`DbReplication Stby A3411.190 0809:165127.110`
		`VIP Stby A3411.190 0809:165127.123`
		`QP Stby A3411.190 0809:165148.757`
		`DbReplication_old Stby A3411.190 0809:165127.112`
		
		NOTE: It may take a few minutes (after the system has re-booted) for all the processes to reach the Stby state. They may initially be shown as OOS.

15 ☐	**SSH/Console/iLo:** Verify replication is fully ready	`# inetstat`
		
		root@slak-cmp-b:~
		`LT dir nodeId inetsync-State dSeq dTime info`
		`AA To slak-cmp-a Standby 0 0.00`
		`AA From slak-cmp-a Active 0 0.00 ^0.04%cpu 75`
		`AC To slak-mpe-03b Standby 0 0.00`
		`AC To slak-mpe-03a Standby 0 0.00`
		`AC To slak-mra-a Standby 0 0.00`
		`AC To slak-mra-b Standby 0 0.00`
		`AC To slak-mpe-02a Standby 0 0.00`
		`AC To slak-mpe-02b Standby 0 0.00`
		`.`
		`.`
		`.`
		`.`
		`.`
		
		All servers shold show Active or Standby.
		
		If the status is "Audit", wait for the audit to complete.

16 ☐	**SSH:** Primary Active CMP
	
	Verify HA status
		In SSH session with Primary Active CMP server, verify upgraded server is ColdStandby.
		
		`# ha.stat`
		
		`node role avail seqNum score`
		`cs-tb31-cmpa ProvideSvc Available 146282 146282`
		`cs-tb31-cmpb ColdStandby Offline 144723 100687`

17 ☐	**GUI:** Verify Upgraded Standby Server status from CMP Manager Topology Form	From CMP Manager: **Topology → <***CMP Cluster (Primary)***> → View** Upgraded CMP should be in Standby (Force Standby = yes)

18 ☐	**GUI:** Verify Alarms	From CMP Manager:
		
		System Wide Reports → Active Alarms:
		
		Below is an example of alarms that may be seen.
		
		NOTE: It is recommended to sort this view by Severity, to see the most important alarms at the top of the form.
		
		Active Alarms
		Pause
		Printable Format | Save as CSV | Export PDF
		Server: All | Server Type: All | Severity: All
		Display results per page: 50
		[First/Prev]1[Next/Last] Total 1 pages
		
		`Server | Server Type | Severity | Alarm ID | Description | Time`
		`CMP Site1 Cluster | CMP | Critical | 31228 | GN_DOWN/WRN monitorRecentAlarms(): no mate heartbeat ^^ [6717:hamonitor.cxx:624] | 08/09/2012 17:03:49 EDT`
		`CMP Site1 Cluster | CMP | Major | 70005 | The peer server 10.250.85.25 is degraded. | 08/09/2012 16:32:36 EDT`
		`CMP Site1 Cluster | CMP | Critical | 31228 | GN_DOWN/WRN HA cannot connect to remote server ^^ [8248:HaDcCommander.cxx:364] | 08/09/2012 17:01:27 EDT`
		`CMP Site1 Cluster | CMP | Critical | 70025 | The MySQL slave has a different schema version than the master. | 08/09/2012 16:51:56 EDT`

Step	Procedure	Result
19 ☐	**GUI:** Verify System Admin → Reports	Upgraded CMP status shows `No Data`. 
20 ☐	**GUI:** Verify System Wide Reports – KPI Dashboard	**System Wide Reports → KPI Dashboard** Verify that report shows all normal traffic processing for the MPEs/MRAs.
21 ☐	IF UPGRADE Failure – ROLL BACK	If any of the Verifications above fail, then Roll Back the Upgrade. Refer to procedure for Roll back of a Partial Upgrade cluster
22 ☐	Proceed to next Procedure	If Verifications are successful, then one-half of the CMP Primary cluster is now upgraded but the 9.x server not available for service (Forced Standby). Proceed to the next Procedure to complete the CMP Cluster Upgrade.
Procedure is completed		

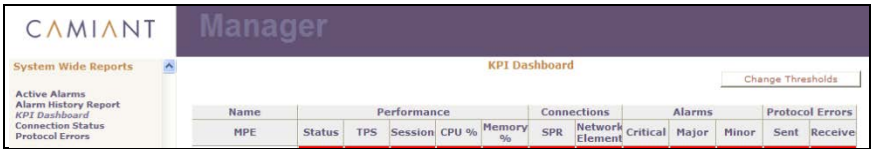
5.1.2 Procedure 9: Make Upgraded Server Active

In this step, the upgraded server will be made to the Active server. The other server in the cluster will be made Forced Standby until it can be upgraded.

IMPORTANT: This step should not be service affecting, but it is recommended to perform this in a Maintenance Window as a precaution.

Pre-requisites:

- Procedure 6 was completed – which copies the newest policyUpgrade.pl script onto the Primary Active CMP server

Step	Procedure	Result
1 ☐	**GUI:** Verify Status of Cluster to be Upgraded	From CMP Manager: **Topology Setting → View Primary CMP Cluster** One Primary Site CMP server will be Active, and the other (Force) Standby
2 ☐	**GUI:** View KPI Dashboard, and make a snapshot	From CMP Manager: **System Wide Reports → KPI Dashboard** Confirm current status is OK. Take a screen shot. 
3 ☐	**SSH:** Login to the Primary Active CMP Server	Ssh to the current Primary Active CMP Server _____

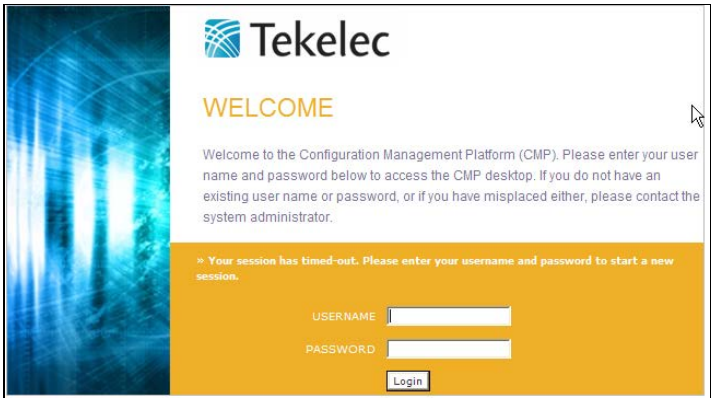
Step	Procedure	Result

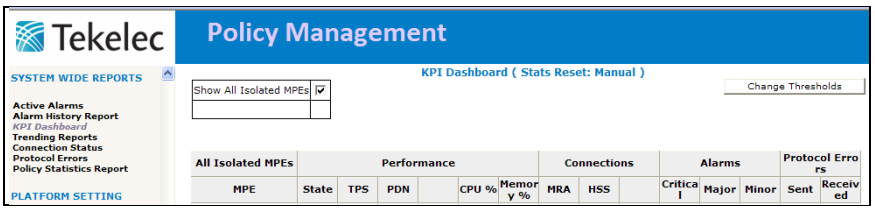
4 ☐	**SSH:** Primary Active CMP - Verify Server is Active	`# ha.stat`
		
		`node role avail seqNum score`
		`cs-tb31-cmpa ProvideSvc Available 146282 146282`
		`cs-tb31-cmpb ColdStandby Offline 144723 100687`
		
		`Cntl-c`

5 ☐	**SSH:** Primary Active CMP - Invoke failover of CMP cluster	**NOTE:** This step will cause the 9.x CMP to become Active, and the 7.5.x server to become Force Standby
		`# policyUpgrade.pl --failover <CMP_Hostname>`
		`<CMP_Hostname> is current Active CMP hostname`
		NOTE: Any ssh sessions to the current CMP VIP address will close when the switchover occurs, and will need to be re-opened.

6 ☐	**SSH:** Login to the New Primary Active CMP Server	Ssh to the New (9.x) Primary Active CMP Server _____

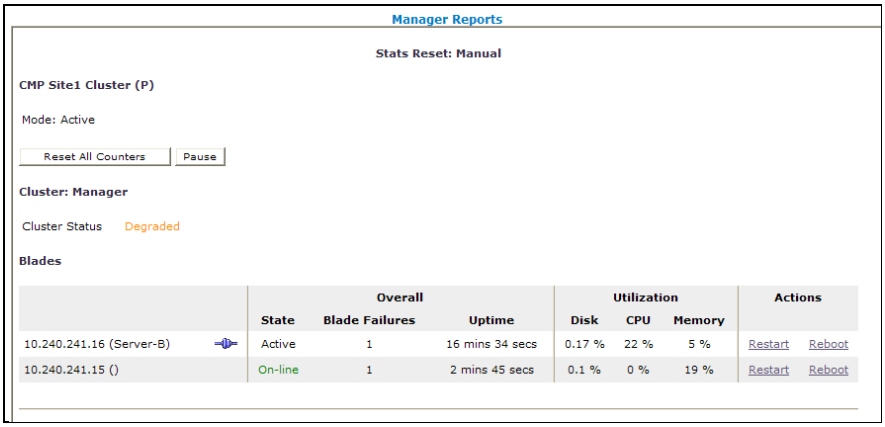
7 ☐	**SSH:** Verify New Primary Active CMP Server is Active, and all resources are Active	`# ha.mystate`
		`resourceId role node subResou lastUpdate`
		`DbReplication Active A2635.240 0 0612:224121.532`
		`VIP Active A2635.240 0 0612:224120.872`
		`QP Active A2635.240 0 0612:224418.295`
		`DbReplication_old Active A2635.240 0 0612:224120.815`

8 ☐	**GUI:** Verify access to 9.x CMP Manager GUI	Close CMP GUI Browser window, and re-open Access CMP Manager GUI using the VIP address Policy Management 9.x Manager login form should be visible. Login credentials are the same as pre-upgrade. 

Step	Procedure	Result
9 ☐	**GUI:** View KPI Dashboard	From CMP Manager: **SystemWideReports → KPI Dashboard** Make a snapshot. Compare to prior KPI Dashboard. Verify that service is normal. 
10 ☐	**GUI:** Verify Active Alarms	Open the Active Alarms view. Wait a few minutes for alarms to clear. Certain Alarms are expected: Specifically, the following Critical Alarms are expected from the Active CMP: Active Alarms (Stats Reset: Manual / Last Refresh :10/24/2012 19:00:41) Pause Printable Format Save as CSV Export PDF Columns Filters Display results per page: 50 [First/Prev]1[Next/Last] Total 1 pages Server | Server Type | Severity | Alarm ID | Description | Time cs-tb31-cmp-b,10.240.238.86 | CMP | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10/24/2012 18:57:15 EDT cs-tb31-cmp2-a,10.240.238.83 | CMP | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10/24/2012 18:56:24 EDT cs-tb31-cmp2-b,10.240.238.91 | CMP | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10/24/2012 18:56:27 EDT cs-tb31-cpm-a,10.240.238.79 | CMP | Critical | 31283 | High availability server is offline | 10/24/2012 18:59:26 EDT These will clear as the other CMPs are upgraded. **NOTE:** On the Policy Management 9.x GUI, there is on-line help to get additional alarm information. Click on the alarm ID in the Active Alarm view to get the Alarm details.
11 ☐	**GUI:** Verify Individual MRA/MPE Reports (as desired)	Open and review Reports for the MRAs/MPEs. The reports should show traffic behavior comparable to the pre-upgrade. **NOTE:** Policy Management 9.x Reports are organized differently. The user may need to click a **details** link to see the full report. Protocol Statistics Name | Connections | Total client messages in / out | Total messages timeout Diameter Diameter AF Statistics | 2 | 0 / 0 | 0 Diameter PCEF Statistics | 2 | 583 / 583 | 0 Diameter BBERF Statistics | 2 | 582 / 582 | 0 Diameter TDF Statistics | | | 0 Diameter Sh Statistics | 3 | 0 / 0 | 0 Diameter DRMA Statistics | | | 0

Step	Procedure	Result
		Policy Server Administration Policy Server: slak-pcrf-01 System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sources | Sessi Stats Reset: Manual Diameter BBERF Statistics Mode: Active / Absolute Reset Counters | Show Deltas | Pause | Cancel Connections 2 Currently okay peers 2 Currently down / suspect / reopened peers 0 / 0 / 0 Total messages in / out 582 / 582 CCR messages received / sent 582 / 0 CCR messages timeout CCA success messages received / sent 0 / 582 CCA failure messages received / sent 0 / 0 CCR-I messages received / sent 0 / 0 CCR-I messages timeout CCA-I success messages received / sent 0 / 0 CCA-I failure messages received / sent 0 / 0 CCR-U messages received / sent 292 / 0 CCR-U messages timeout CCA-U success messages received / sent 0 / 292 CCA-U failure messages received / sent 0 / 0 CCR-T messages received / sent 290 / 0 CCR-T messages timeout CCA-T success messages received / sent 0 / 290 CCA-T failure messages received / sent 0 / 0 RAR messages received / sent 0 / 0 RAR messages timeout RAA success messages received / sent 0 / 0 RAA failure messages received / sent 0 / 0 Currently active sessions 39710 Max active sessions 40000 Diameter BBERF connections ID | IP Address : Port | Currently active connections | Currently active sessions | Connect Time | Disconnect Time brbq-mra.tekelec.com | 10.250.84.145 : 43901 | 1 | 0 | Thu Jul 12 22:35:55 EDT 2012 | N/A slak-mra.tekelec.com | 10.250.85.5 : 33111 | 1 | 39710 | Thu Jul 12 22:35:57 EDT 2012 | Thu Jul 12 22:35:56 EDT 2012
12 ☐	**GUI:** Verify System Administration → Reports	**System Administration → Reports** Report status will show with 9.x CMP Active

Step	Procedure	Result
		Manager Reports **Stats Reset: Manual** **CMP Site1 Cluster (P)** Mode: Active Reset All Counters | Pause **Cluster: Manager** Cluster Status Degraded **Blades** Overall: State, Blade Failures, Uptime; Utilization: Disk, CPU, Memory; Actions 10.240.241.16 (Server-B) Active 1 16 mins 34 secs 0.17 % 22 % 5 % Restart Reboot 10.240.241.15 () On-line 1 2 mins 45 secs 0.1 % 0 % 19 % Restart Reboot
13 ☐	**GUI:** Verify **Platform Setting → Topology**	**Platform Setting → Topology Setting → All Clusters** One CMP server will show (FS), or Force Standby in the Cluster view, and Out-of-Ser vice in the Topology Configuration. **Cluster Configuration** Add CMP Site1 Cluster | Add CMP Site2 Cluster | Add MPE/MRA Cluster **Cluster Settings** Name: CMP Site1 Cluster (P); Appl Type: CMP Site1 Cluster; OAM VIP: 10.250.85.9; Server-A: 10.250.85.7 (FS); Server-B: 10.250.85.8; Operation: View slak-mpe-02: MPE; 10.250.85.12; 10.250.85.10; 10.250.85.11; View Delete slak-mpe-03: MPE; 10.250.85.15; 10.250.85.13; 10.250.85.14; View Delete slak-mra: MRA; 10.250.85.6; 10.250.85.4; 10.250.85.5; View Delete View CMP (P) **Topology Configuration** Modify Cluster Settings | Modify Server-A | Modify Server-B | Back **Cluster Settings** Name: CMP Site1 Cluster Appl Type: CMP Site1 Cluster HW Type: C-Class Network VLAN IDs : OAM 85 OAM VIP: 10.250.85.9 / 26 Signaling VIP 1: None Signaling VIP 2: None Signaling VIP 3: None Signaling VIP 4: None **Server-A**: IP 10.250.85.7; HostName slak-cmp-a; Forced Standby Yes; Status out-of-service **Server-B**: IP 10.250.85.8; HostName slak-cmp-b; Forced Standby No; Status active

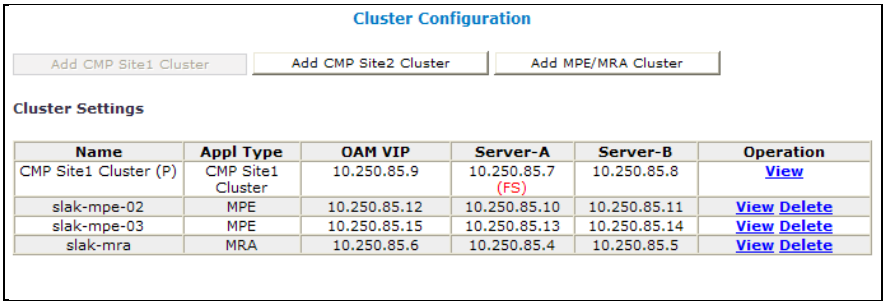
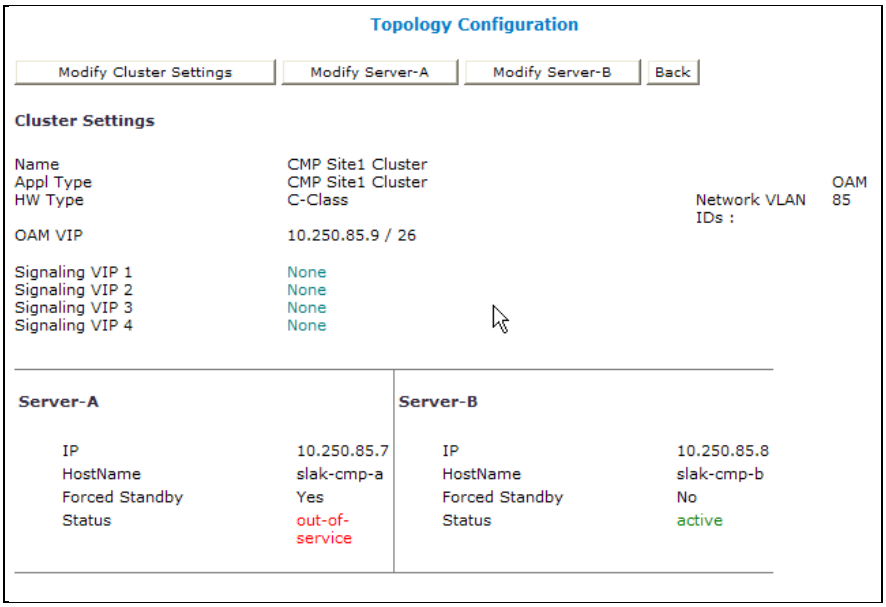
Step	Procedure	Result
14 ☐	**GUI:** Verify **System Administration → Reports**	Upgraded CMP will show Active, Cluster will show degraded. Force Standby CMP (old release) will show on-line.  Manager Reports Stats Reset: Manual CMP Site1 Cluster (P) Mode: Active Reset All Counters | Pause Cluster: Manager Cluster Status Degraded Blades Overall: State, Blade Failures, Uptime Utilization: Disk, CPU, Memory Actions 10.240.241.16 (Server-B) Active 1 16 mins 34 secs 0.17 % 22 % 5 % Restart Reboot 10.240.241.15 () On-line 1 2 mins 45 secs 0.1 % 0 % 19 % Restart Reboot
15 ☐	If Verify Steps Fail	If Verify steps fail, do not proceed. Consult with My Oracle Support. If needed, see Rollback Procedure for Partial Upgraded Cluster, in this document.

16 ☐	**SSH:** Key Exchange from Upgraded CMP server to MPE/MRAs	`# policySSHKey.pl --command syncSSHKeys`
		`Sync SSH Key with All C level Nodes:`
		`Begin to sync SSH key with node:C1975.230`
		`Begin to sync SSH key with node:C1975.137`
		`----------`
		`NodeID IP Result`
		`C1975.230 10.240.241.19 exchanged key successfully`
		`C1975.137 10.240.241.18 exchanged key successfully`
		Verify that all key exchanges are successful. Re-execute if needed.
		NOTE: this tool expects that the root password of the MPE/MRA servers is set to the standard value. If not, the command will fail.
		In this case, use the standard command for keyexchange, for every MPE/MRA:
		`# keyexchange <hostname of MPE/MRA>`

17 ☐	Proceed to next Procedure	One-half of the Primary CMP cluster is now upgraded and Active. The prior-release CMP server is in (Forced Standby). ***IMPORTANT: Do not REMOVE FORCE STANDBY CONDITION on 7.5 CMP server.*** Proceed to the next Procedure to complete the Cluster Upgrade.
Procedure is completed		

5.1.3 Procedure 10: Upgrade Second CMP Server and Primary Site, and Restore Cluster

In this step, the second server of the CMP Site 1 cluster will be upgraded, and the cluster returned to Active/Standby normal condition.

Step	Procedure	Result
1 ☐	**GUI:** Verify Status of Cluster to be Upgraded	**Platform Setting → Topology Setting → All Clusters**  Cluster Configuration Add CMP Site1 Cluster | Add CMP Site2 Cluster | Add MPE/MRA Cluster Cluster Settings Name: CMP Site1 Cluster (P); Appl Type: CMP Site1 Cluster; OAM VIP: 10.250.85.9; Server-A: 10.250.85.7 (FS); Server-B: 10.250.85.8; Operation: View slak-mpe-02: MPE; 10.250.85.12; 10.250.85.10; 10.250.85.11; View Delete slak-mpe-03: MPE; 10.250.85.15; 10.250.85.13; 10.250.85.14; View Delete slak-mra: MRA; 10.250.85.6; 10.250.85.4; 10.250.85.5; View Delete View CMP (P)  Topology Configuration Modify Cluster Settings | Modify Server-A | Modify Server-B | Back Cluster Settings Name: CMP Site1 Cluster Appl Type: CMP Site1 Cluster HW Type: C-Class Network VLAN IDs : OAM 85 OAM VIP: 10.250.85.9 / 26 Signaling VIP 1: None Signaling VIP 2: None Signaling VIP 3: None Signaling VIP 4: None Server-A: IP 10.250.85.7; HostName slak-cmp-a; Forced Standby Yes; Status out-of-service Server-B: IP 10.250.85.8; HostName slak-cmp-b; Forced Standby No; Status active
2 ☐	**SSH:** Login to Primary CMP Force Standby server Either: 7. SSH - Access the login prompt. 8. Log into the server as the "root" user on the iLO or RMM, and access Remote Console	CentOS release 5.5 (Final) Kernel 2.6.18-194.32.1.el5prerel4.2.3_70.88.0 on an x86_64 CMP-02F login:

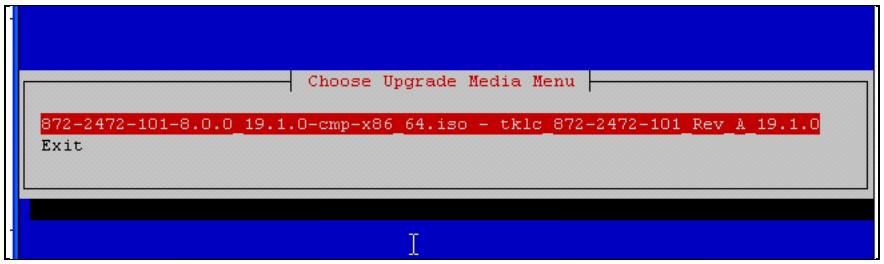
Step	Procedure	Result

3 ☐	**SSH/Console/iLo:** Verify that the server is the correct CMP server for Upgrade	`# getPolicyRev`
		`7.5.x`
		`# ha.stat`
		
		`node role avail seqNum score`
		`CSLAB-CMP1-A ColdStandby Offline 4573326 110010`
		`CSLAB-CMP1-B ColdStandby Offline 4574922 80672`

4 ☐	**SSH/Console/iLo:** Verify qp_procmgr status is running.	`# service qp_procmgr status`
		`[root@CSLAB-CMP1-A ~]# service qp_procmgr status`
		`qp_procmgr (pid 16590) is running...`
		
		NOTE: Do not continue if qp_procmgr is not running. Contact Policy TAC for Assistance.

5 ☐	**SSH/Console/iLo:** Verify comcol database is running	`# prod.state`
		`[root@CSLAB-CMP1-A ~]# prod.state`
		`...prod.state (RUNID=00)...`
		`...getting current state...`
		`Current state: B (product under procmgr)`
		
		Notes:
		• Current state "B" means the system is running and synced.
		• If the Current state does not have a state of B. Do not continue if qp_procmgr is not running. Contact Policy TAC for Assistance.

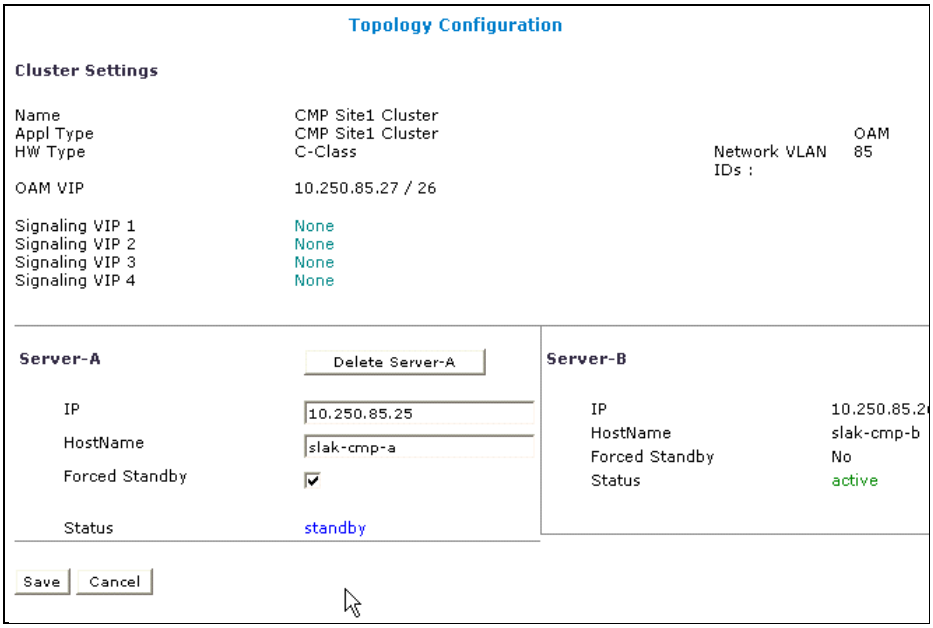
6 ☐	**SSH/Console/iLo:** Verify that the system doesn't have any unexpected qp_procmgr or MySQL alarms	`# ra.stat`
		
		`sev ht timeStamp event instance errInfo`
		`*C 1 09:50:05.796 QP Slave database is a down The MySQL slave has a different schema version than the master.`
		
		Ctrl-c --- to exit command
		
		Note: Do not continue if the system has any unexpected qp_procmgr or MySQL alarms. Contact Policy TAC for Assistance.

7 ☐	**SSH/Console/iLo:** Apply Upgrade
	
	NOTE: the Application is NOT shutdown prior to the upgrade.
	
	This step will take about 20 Minutes, and the server will boot.
		If using ssh, run the `screen` command to prevent hang-ups, and do not exit this screen session until the server reboots.
		`# screen`
		
		`# su - platcfg`
		
		Maintenance → Upgrade → Initiate Upgrade
		 
		This step will take about 20 Minutes, and the server will boot.

Step	Procedure	Result
8 ☐	**SSH/Console/iLo:** Login again to upgraded server. Verify that server returns to the login prompt after boot.	CentOS release 5.5 (Final) Kernel 2.6.18-194.32.1.el5prerel4.2.3_70.88.0 on an x86_64 CMP-02F login:
9 ☐	**SSH:** Verify software versions	**# getPlatRev** **5.0.1-72.45.0** **# getPolicyRev** **9.x.0_x.x.x**
10 ☐	**SSH:** Verify success of Upgrade	**# tail /var/TKLC/log/upgrade/upgrade.log** The following indicates SUCCESS of Upgrade. [root@CMP-02F ~]# tail /var/TKLC/log/upgrade/upgrade.log 1321039028:: UPGRADE IS COMPLETE 1321039029:: 1321039029:: Waiting for reboot 1321039029::DEBUG: ADDING VAR: UPGRADE_STATUS = SUCCESS 1321039029::DEBUG: ADDING VAR: UPGRADE_COMPLETED = 11/11/2011 19:17:09 UTC
11 ☐	**SSH:** Verify that the server processes are running	Verify that all server processes are Stby (Forced Standby) **# ha.mystate** **resourceId role node subResou lastUpdate** **DbReplication Stby A2635.240 0 0612:224121.532** **VIP Stby A2635.240 0 0612:224120.872** **QP Stby A2635.240 0 0612:224418.295** **DbReplication_old Stby A2635.240 0 0612:224120.815** **NOTE:** It takes a minute after the server boot for all server processes to start up. If needed, run the command several times until there is the correct result.
12 ☐	**SSH:** Verify Replication status	**# inetstat** ***<should show Active or Standby>***
13 ☐	**GUI: System Administration → Reports**	Expected information for the Manager Reports Manager Reports Stats Reset: Manual CMP Site1 Cluster (P) Mode: Active Reset All Counters Pause Cluster: Manager Cluster Status Degraded Blades Overall: State, Blade Failures, Uptime Utilization: Disk, CPU, Memory Actions 10.240.241.15 (Server-A) Forced Standby 1 1 min 42 secs 0.17 % 42 % 5 % Restart Reboot 10.240.241.16 (Server-B) Active 1 4 hours 46 mins 31 secs 0.19 % 25 % 5 % Restart Reboot

Step	Procedure	Result
14 ☐	IF Verify steps fail	If Verify steps fail, do not proceed. Consult with My Oracle Support. If needed, see Backout Procedure for a fully upgraded cluster.

15 ☐	**SSH:** Key Exchange from Upgraded Standby CMP server to MPE/MRAs	`# policySSHKey.pl --command syncSSHKeys`
		`Sync SSH Key with All C level Nodes:`
		`Begin to sync SSH key with node:C1975.230`
		`Begin to sync SSH key with node:C1975.137`
		`----------`
		`NodeID  IP  Result`
		`C1975.230  10.240.241.19  exchanged key successfully`
		`C1975.137  10.240.241.18  exchanged key successfully`
		
		Verify that all key exchanges are successful. Re-execute if needed.

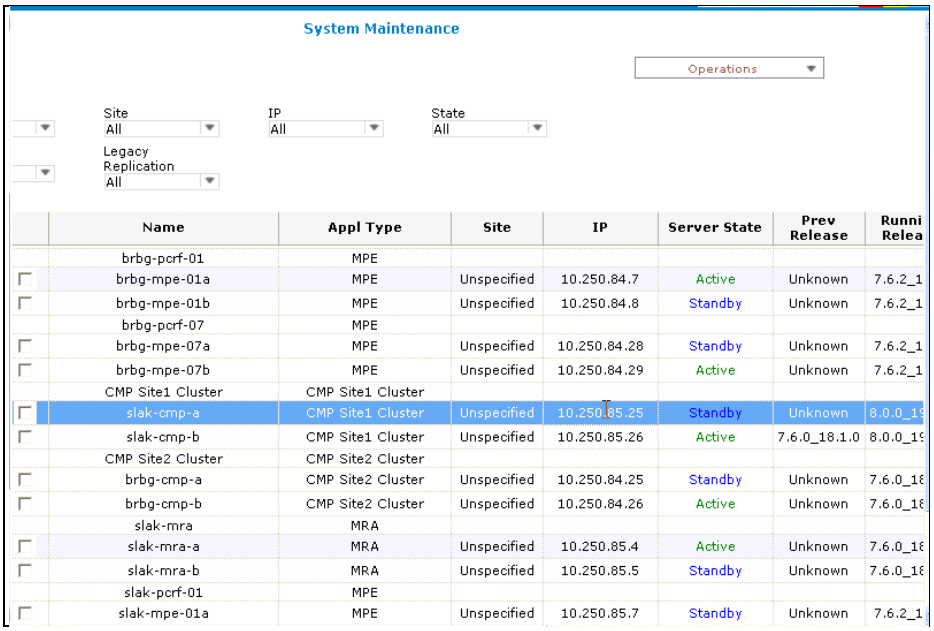
16 ☐	**GUI:** Remove Forced Standby	**Topology Setting → <*Cluster*> → View → Modify** (Primary Site CMP) Remove Forced Standby check mark, and Save. 
17 ☐	**GUI:** Verify Active/Standby Cluster	**Topology Setting → <*CMP Cluster*> → View** CMP Servers will have status of Active and Standby.

Step	Procedure	Result
18 ☐	**SSH:** Verify that the standby server is 'Stby' and Active Server is Active.	

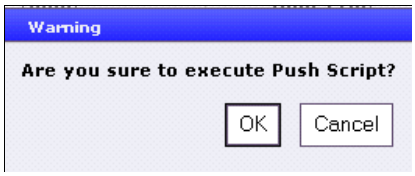
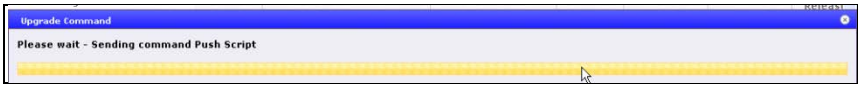
```
# ha.mystate
        resourceId   role         node  subResou      lastUpdate
     DbReplication   Stby    A2635.240         0 0612:224121.532
               VIP   Stby    A2635.240         0 0612:224120.872
                QP   Stby    A2635.240         0 0612:224418.295
DbReplication_old   Stby    A2635.240         0 0612:224120.815

# ha.states
        resourceId   role         node  subResou      lastUpdate
     DbReplication   Stby    A2635.240         0 0612:224121.532
     DbReplication Active    A2635.228         0 0612:224121.247
               VIP   Stby    A2635.240         0 0612:224120.872
               VIP Active    A2635.228         0 0612:224121.355
                QP   Stby    A2635.240         0 0612:224418.295
                QP Active    A2635.228         0 0612:224121.294
DbReplication_old Active    A2635.228         0 0612:224121.245
DbReplication_old   Stby    A2635.240         0 0612:224120.815
```

NOTE: the assigned node Ids for the two servers will depend on the installation. These Ids are internal to the software.

19 ☐	**GUI:** Verify access to **Upgrade Manager → System Maintenance**	Open **Upgrade Manager → System Maintenance** Note status



Name	Appl Type	Site	IP	Server State	Prev Release	Runni Relea
brbg-pcrf-01	MPE					
brbg-mpe-01a	MPE	Unspecified	10.250.84.7	Active	Unknown	7.6.2_1
brbg-mpe-01b	MPE	Unspecified	10.250.84.8	Standby	Unknown	7.6.2_1
brbg-pcrf-07	MPE					
brbg-mpe-07a	MPE	Unspecified	10.250.84.28	Standby	Unknown	7.6.2_1
brbg-mpe-07b	MPE	Unspecified	10.250.84.29	Active	Unknown	7.6.2_1
CMP Site1 Cluster	CMP Site1 Cluster					
slak-cmp-a	CMP Site1 Cluster	Unspecified	10.250.85.25	Standby	Unknown	8.0.0_19
slak-cmp-b	CMP Site1 Cluster	Unspecified	10.250.85.26	Active	7.6.0_18.1.0	8.0.0_19
CMP Site2 Cluster	CMP Site2 Cluster					
brbg-cmp-a	CMP Site2 Cluster	Unspecified	10.250.84.25	Standby	Unknown	7.6.0_16
brbg-cmp-b	CMP Site2 Cluster	Unspecified	10.250.84.26	Active	Unknown	7.6.0_16
slak-mra	MRA					
slak-mra-a	MRA	Unspecified	10.250.85.4	Active	Unknown	7.6.0_16
slak-mra-b	MRA	Unspecified	10.250.85.5	Standby	Unknown	7.6.0_16
slak-pcrf-01	MPE					
slak-mpe-01a	MPE	Unspecified	10.250.85.7	Standby	Unknown	7.6.2_1

Step	Procedure	Result
20 ☐	**GUI: Upgrade Manager -** Get accurate status from all servers by Push of Upgrade status scripts Repeat for all servers until the Upgrade Status column is completed.	Open the **Upgrade Manager → System Maintenance**. Wait for it to fully populate. The 7.5.x servers will typically show an Upgrade Status of unknown. Select a 7.5.x server in the Standby state, using the selection checkbox, and click **Operation**. It will display "Loading", and after a couple of seconds, the list of allowed operations displays:  **NOTE:** The Operations pick list is specific to the current state of the selected server. Select **Operation → Push Script**.   Wait a few seconds for the command to complete and the results to show in the form. Repeat the Push Script action for each server. Multi-select is supported. When done, Verify that the System Maintenance view shows the status of all the deployed servers, at all sites. It should show Completed: upgrade *<from the previous install or upgrade of the server>*. System Maintenance Columns Filters Operations Name / Appl Type / IP / Server State / ISO / Prev Release / Running Release CMP Site1 Cluster / CMP Site1 Cluster slak-cmp-a / CMP Site1 Cluster / 10.250.85.7 / Standby / 872-2472-102-9.0.0_9.1.0-cmp-x86_64.iso / 7.6.0_18.1.0 / 9.0.0_9.1.0 / Completed:upgrade was slak-cmp-b / CMP Site1 Cluster / 10.250.85.8 / Active / 872-2472-102-9.0.0_9.1.0-cmp-x86_64.iso / 7.6.0_18.1.0 / 9.0.0_9.1.0 / Completed:upgrade was slak-mpe-02 / MPE slak-mpe-02a / MPE / 10.250.85.10 / Standby / 872-2474-102-9.0.0_9.1.0-mpe-li-x86_64.iso / Unknown / 7.6.2_1.1.0 / Completed:upgrade was slak-mpe-02b / MPE / 10.250.85.11 / Active / 872-2474-102-9.0.0_9.1.0-mpe-li-x86_64.iso / Unknown / 7.6.2_1.1.0 / Completed:upgrade was slak-mpe-03 / MPE slak-mpe-03a / MPE / 10.250.85.13 / Standby / 872-2474-102-9.0.0_9.1.0-mpe-li-x86_64.iso / Unknown / 7.6.2_1.1.0 / Completed:upgrade was slak-mpe-03b / MPE / 10.250.85.14 / Active / 872-2474-102-9.0.0_9.1.0-mpe-li-x86_64.iso / Unknown / 7.6.2_1.1.0 / Completed:upgrade was slak-mra / MRA slak-mra-a / MRA / 10.250.85.4 / Standby / 872-2475-102-9.0.0_9.1.0-mra-x86_64.iso / Unknown / 7.6.0_18.1.0 / Completed:upgrade was slak-mra-b / MRA / 10.250.85.5 / Active / 872-2475-102-9.0.0_9.1.0-mra-x86_64.iso / Unknown / 7.6.0_18.1.0 / Completed:upgrade was
21 ☐	Procedure is complete.	CMP Active Site Cluster Upgrade is complete. If the Operator has Secondary-CMP site, it may be upgraded in the same maintenance window. CAUTION: it is not supported to Demote/Promote from a Primary CMP cluster (9.x) to a Secondary CMP cluster (7.5.x). CAUTION: No Configuration or Topology changes are supported from 9.x CMPs to 7.5.x MPE/MRA clusters. The GUI does not prevent this, but the actions may not work as expected.
Procedure is completed		

5.2 Upgrade Secondary Site CMP Cluster (if Deployed by Operator)

If the Operator deployment includes a CMP Secondary Site, this procedure must be executed. If not, this procedure can be skipped.

It is possible to upgrade the Secondary Site CMPs in the same maintenance window as the Active Site CMPs, or in a later maintenance window. However, the Secondary-site CMPs should be upgraded before any of the MRAs and MPEs.

For this procedure, CMP Active site (Primary) cluster is already upgraded to 9.x.

The CMP Secondary-site servers will be reporting Critical alarms that they are not able to sync with Active site due to version mismatch.

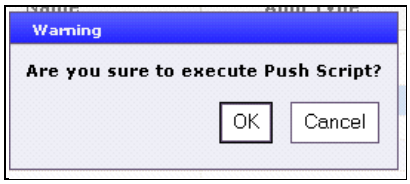
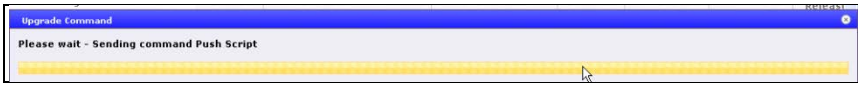
This procedure will use the Policy Management 9.x Upgrade Manager feature.

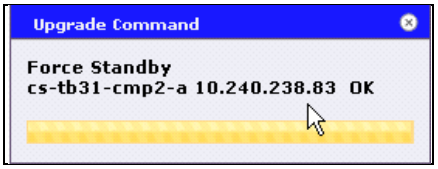
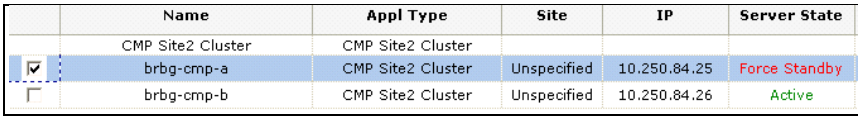
5.2.1 Procedure 11: Upgrade Secondary-Site CMPs

IMPORTANT: This procedure should be performed in a maintenance window.

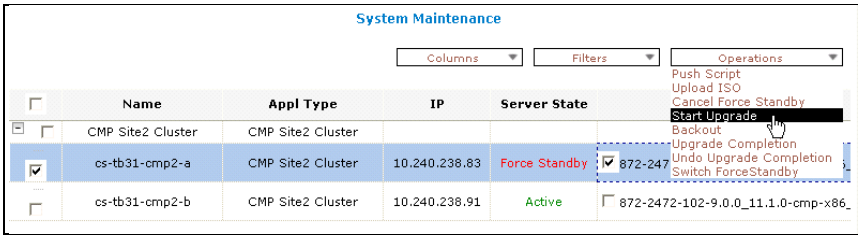
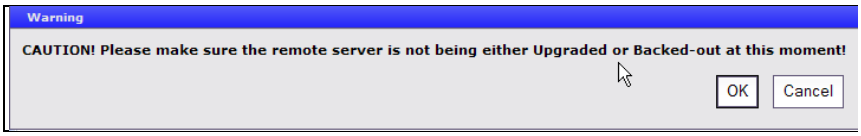
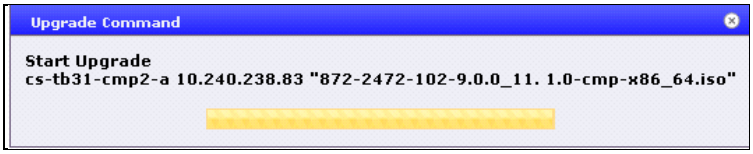
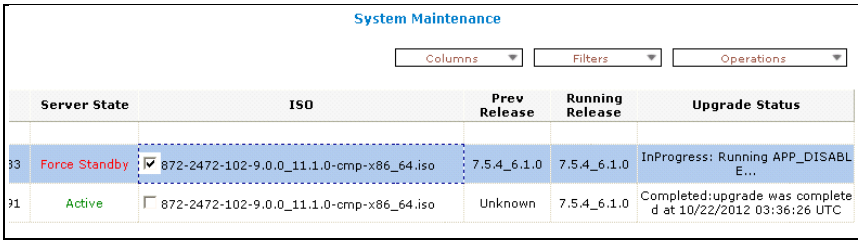
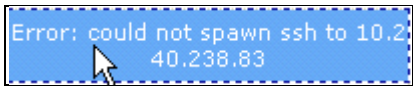
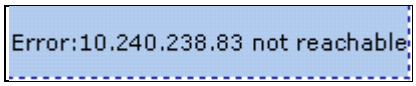
Step	Procedure	Result
1 ☐	**GUI:** Perform Health checks	From the CMP Manager GUI, review the health of the Policy System. • View Active Alarms • View KPI forms • Reset Counters on network elements to provide a baseline for the upgrade. If there are issues in the Policy System, consider if it is wise to proceed.

2 ☐	**SSH:** Open window to Active CMP server (VIP)
	Login to the server as the root user
		`login: root`
		`Password: <enter password>`
		Confirm that this is active server:
		`# ha.mystate`
		`resourceId role node subResou lastUpdate`
		`DbReplication Active A2635.240 0 0612:224121.532`
		`VIP Active A2635.240 0 0612:224120.872`
		`QP Active A2635.240 0 0612:224418.295`
		`DbReplication_old Active A2635.240 0 0612:224120.815`
		This session will be used for executing a switchover command later in this procedure.
		Keep this window open.

Step	Procedure	Result
3 ☐	GUI: Confirm Status for 1st Secondary-CMP	**Upgrade Manager → System Maintenance** WAIT for the form to fully populate. This may take a few seconds. • Review Software Release status • Review Upgrade status Primary site CMPs should be on 9.x. Secondary site CMPs should be on 7.5.x. IF NEEDED: if the Upgrade Status shows an error, it may be needed to execute the Push Script Action, as follows: 9. Select checkbox for a CMP and select **Operation → Push Script**   10. Review Software Release status 11. Review Upgrade status
4 ☐	**GUI:** Push Script – 2nd Secondary-CMP	**Upgrade Manager → System Maintenance** Repeat Push Script operation for **second CMP** at Secondary-site
5 ☐	**GUI:** Verify status of selected CMPs	**Upgrade Manager → System Maintenance** At the top of the form, select Application Filter: the current Secondary site: either Site1 CMP Cluste", or Site2 CMP Cluster. The form will now display only CMPs at the site to be upgraded. **NOTE:** The Secondary site may be either Site1 or Site2. **Example** Name | Appl Type | Site | IP | Server State | Prev Release | Running Release CMP Site2 Cluster | CMP Site2 Cluster brbg-cmp-a | CMP Site2 Cluster | Unspecified | 10.250.84.25 | Standby | Unknown | 7.6.0_18.1.0 brbg-cmp-b | CMP Site2 Cluster | Unspecified | 10.250.84.26 | Active | Unknown | 7.6.0_18.1.0

Step	Procedure	Result
6 ☐	**GUI:** Force Standby on standby Secondary-CMP	**Upgrade Manager → System Maintenance** Select the check box for the Standby CMP server at the site and select the: **Operation → Force Standby** (It takes approximately 15 seconds for the Operations list to load.) There will be the following dialogs:    Confirm that the server state is changed to Force Standby in the form (may take several seconds).  This step will prevent the server from becoming Active. The current Active CMP is un-affected. Alarms are expected.

	Name	Appl Type	Site	IP	Server State
	CMP Site2 Cluster	CMP Site2 Cluster			
☑	brbg-cmp-a	CMP Site2 Cluster	Unspecified	10.250.84.25	Force Standby
☐	brbg-cmp-b	CMP Site2 Cluster	Unspecified	10.250.84.26	Active

Step	Procedure	Result
7 ☐	**GUI:** Upgrade for Force Standby Secondary-CMP **NOTE**: This step requires that the 9.x CMP Software image (.iso) was previously copied to the server and placed in the `/var/TKLC/upgrade` directory. This was done in the Upgrade preparations steps.	**Upgrade Manager → System Maintenance** For the Force Standby CMP server, confirm that the checkbox is set for the server and the desired ISO file, and select - **Operation → Start Upgrade**  Confirm the operation, and verify that the Upgrade request was executed successfully.  
8 ☐	Wait for Upgrade to process This step will take 20 minute or more, and the server will boot during this time	Wait for Upgrade to proceed. Monitor Upgrade Progress, if desired: 1. Follow status on the **Upgrade Manager →System Maintenance** form: Upgrade Status  The Upgrade status will proceed through several status messages. 2. Optional: Login to Server Console via the iLo of the server, and monitor the console output to confirm upgrade progress **NOTE:** The following error messages are seen when the server is re-booting:   3. After the server re-boots, Confirm that status on the GUI form is Completed. 

Step	Procedure	Result

9 ☐	**SSH : Upgraded server –** Verify Upgrade completed sucessfully	SSh to Blade and verify current rev:
		`# getPlatRev`
		`# getPolicyRev`
		
		`View Upgrade log from the server:`
		`# tail /var/TKLC/log/upgrade.log`
		…
		1351126214:: UPGRADE IS COMPLETE
		1351126214::
		1351126214:: Waiting for reboot
		1351126214::DEBUG: ADDING VAR: UPGRADE_STATUS = SUCCESS
		1351126214::DEBUG: ADDING VAR: UPGRADE_COMPLETED = 10/25/2012 00:50:14 UTC

10 ☐	**SSH: Upgraded server -** Verify that the server processes are running	Verify that all server processes are Stby (Forced Standby)
		`# ha.mystate`
		`resourceId role node subResou lastUpdate`
		`DbReplication Stby A2635.240 0 0612:224121.532`
		`VIP Stby A2635.240 0 0612:224120.872`
		`QP Stby A2635.240 0 0612:224418.295`
		`DbReplication_old Stby A2635.240 0 0612:224120.815`
		NOTE: It takes a minute after the server boot for all server processes to start up. If needed, run the command several times until there is the correct result.

11 ☐	**SSH: Upgraded server** - Verify replication	`# inetstat` Status should be Active or Standby for all items.

12 ☐	IF Verify steps have failed, or the Upgrade has gone more than 25 Minutes.
	NOTE: If the upgrade fails, the upgrade software will typically roll back automatically to the prior release and configuration.
		If the Upgrade does not complete sucessfully.
		Do not proceed.
		View/collect Upgrade log and ugwrape.log from the server, if possible:
		`# cp /var/TKLC/log/upgrade/upgrade.log approximatelty`
		`# cp /var/TKLC/log/upgrade/ugwrap.log approximatelty`
		Consult with My Oracle Support.
		If needed, see procedure to Backout a Partial Upgrade Cluster, in this document.

Step	Procedure	Result
13 ☐	**GUI:** Cause Switchover to Upgraded CMP	**Upgrade Manager → System Maintenance** Select the checkbox for the Secondary-Site CMP cluster, and select - **Operation → Switch ForceStandby** System Maintenance Columns Filters Operations Push Script Upload ISO Upgrade Completion Undo Upgrade Completion Switch ForceStandby Name | Appl Type | IP | Server State CMP Site2 Cluster | CMP Site2 Cluster cs-tb31-cmp2-a | CMP Site2 Cluster | 10.240.238.83 | Force Standby | 872-2472-102-9.0.0_11.1.0-cmp-x86_ cs-tb31-cmp2-b | CMP Site2 Cluster | 10.240.238.91 | Active | 872-2472-102-9.0.0_11.1.0-cmp-x86_ **NOTE:** Switch ForcedStandby may be failed due to the primary CMP server not using default password.
14 ☐	**GUI:** Upgrade Manager - Verify switchover	**Upgrade Manager → System Maintenance** After a few seconds (perhaps as many as 15 seconds), the System Maintenance form will update to show that the Active/Force Standby roles have changed. The upgraded 9.x CMP is now Active, and the 7.5.x CMP is Force Standby. Name | Appl Type | IP | Server State | ISO CMP Site2 Cluster | CMP Site2 Cluster cs-tb31-cmp2-a | CMP Site2 Cluster | 10.240.238.83 | Active | 872-2472-102-9.0.0_11.1.0-cmp-x86_ cs-tb31-cmp2-b | CMP Site2 Cluster | 10.240.238.91 | Force Standby | 872-2472-102-9.0.0_11.1.0-cmp-x86_
15 ☐	**GUI:** Verify Alarms	View alarms and confirm status. The following alarms are expected: Server | Server Type | Severity | Alarm ID | Description | Time cs-tb31-cmp2-b,10.240.238.91 | CMP | Critical | 31228 | HA Standby Server Offline | 10/24/2012 21:02:39 EDT cs-tb31-cmp2-b,10.240.238.91 | CMP | Critical | 70025 | The MySQL slave has a different schema version than the master. | 10/24/2012 21:05:16 EDT cs-tb31-cmp2-a,10.240.238.83 | CMP | Critical | 31283 | High availability server is offline | 10/24/2012 21:06:09 EDT cs-tb31-cpm-a,10.240.238.79 | CMP | Critical | 31283 | High availability server is offline | 10/24/2012 21:04:26 EDT DB Replication Alarms may take a few minutes to clear after the switchover.
16 ☐	**GUI:** Upgrade second Secondary-CMP in Cluster This step will take 20 minute or more, and the server will boot during this time.	**Upgrade Manager →System Maintenance** Select the checkbox for the current Force Standby CMP server, and checkbox for the desired ISO, and select – **Operation → Start Upgrade**

Step	Procedure	Result
17 ☐	Wait for Upgrade to process Wait for Upgrade to proceed (up to 25 minutes). Monitor Upgrade Progress, if desired.	Monitor Upgrade Progress. 1. Follow status on the GUI: **Upgrade Manager → System Maintenance: Upgrade Status** Server State / ISO / Prev Release / Running Release / Upgrade Status .83 Active 872-2472-102-9.0.0_11.1.0-cmp-x86_64.iso 7.5.4_6.1.0 9.0.0_11.1.0 Completed:upgrade was complete d at 10/25/2012 00:50:14 UTC .91 Force Standby ☑ 872-2472-102-9.0.0_11.1.0-cmp-x86_64.iso 7.5.4_6.1.0 7.5.4_6.1.0 InProgress: Initializing upgrade... The Upgrade status will proceed through several status messages. 2. Optional: Ssh to Server and run `# tail -f /var/TKLC/log/upgrade/upgrade.log` **NOTE:** the following error messages are seen when the server is re-booting: Error: could not spawn ssh to 10.2 40.238.83 Error:10.240.238.83 not reachable 3. After the server re-boots, Confirm that status on the GUI form is Completed. Completed:upgrade was completed at 07/13/2012 18:23:53 UTC

18 ☐	**SSH:** Verify Upgrade was successful	`# getPlatRev`
		`# getPolicyRev`
		`# ha.mystate`
		`# inetstat`
		
		`# tail -f /var/TKLC/log/upgrade/upgrade.log`

19 ☐	IF Upgrade does not show Completed, or the Upgrade has gone more than 25 Minutes, or the verify step above fails. **NOTE:** If the upgrade fails, the upgrade software will typically roll back automatically to the prior release and configuration.	If the Upgrade does not complete sucessfully. Do not proceed. Consult with My Oracle Support. If needed, see procedure for Backout of Fully Upgraded cluster, in this document.
20 ☐	**CMP:** Upgrade Manager - Remove Forced Standby	**Upgrade Manager → System Maintenance** Select check box for Force Standby CMP server (just upgraded) and select – **Operation → Cancel Force Standby** Follow the dialogs. Confirm that status on the form is updated from Force Standby to Standby after a few seconds.
21 ☐	**CMP:** Verify Alarm Status for Upgraded Cluster	**SystemWideReports → Active Alarms** Verify that Alarms for the upgrade cluster all clear.

Step	Procedure	Result

22 ☐	**SSH:** Active CMP at Secondary Site – verify process status	`# ha.mystate`
		`resourceId role node subResou lastUpdate`
		`DbReplication Active A2635.228 0 0612:224121.532`
		`VIP Active A2635.228 0 0612:224120.872`
		`QP Active A2635.228 0 0612:224418.295`
		`DbReplication_old Active A2635.228 0 0612:224120.815`
		
		`# ha.states`
		`resourceId role node subResou lastUpdate`
		`DbReplication Stby A2635.240 0 0612:224121.532`
		`DbReplication Active A2635.228 0 0612:224121.247`
		`VIP Stby A2635.240 0 0612:224120.872`
		`VIP Active A2635.228 0 0612:224121.355`
		`QP Stby A2635.240 0 0612:224418.295`
		`QP Active A2635.228 0 0612:224121.294`
		`DbReplication_old Active A2635.228 0 0612:224121.245`
		`DbReplication_old Stby A2635.240 0 0612:224120.815`

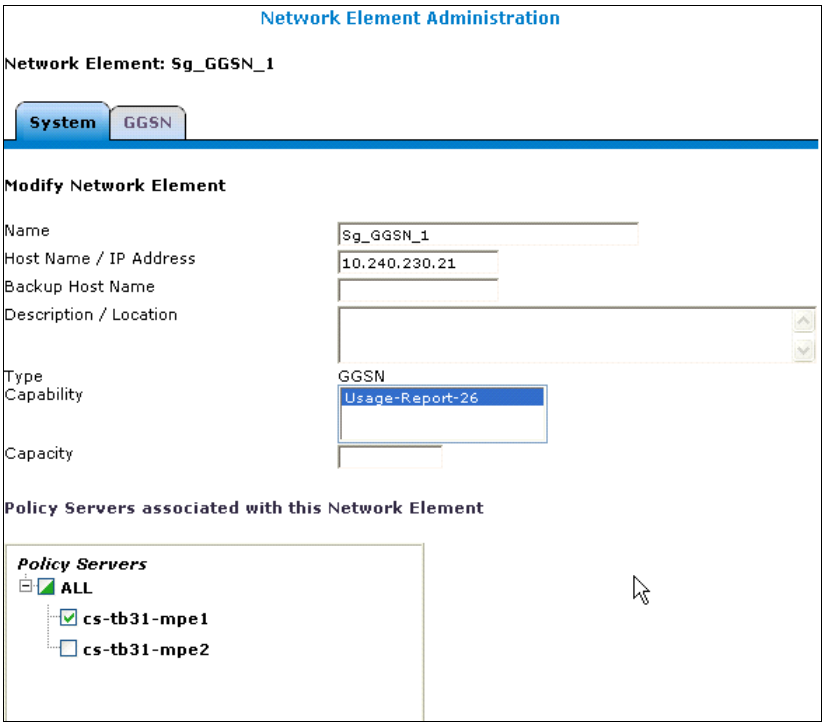
23 ☐	**CMP:** IF problems, rollback	he Upgraded cluster is not in a normal condition, consult with My Oracle Support. IIf need, see procedure to backout a Fully Upgraded Cluster, in this document.
24 ☐	**GUI:** Verify Active Alarms	No Active Alarms are expected
THIS PROCEDURE HAS BEEN COMPLETED		

6. UPGRADE SITES

The following procedures will upgrade a site containing one or more MPE clusters, and (optional) MRA cluster.

6.1 Site Upgrade Preparations

6.1.1 Procedure 12: Configuration Preparations Procedure

Step	Procedure	Result
1 ☐	**GUI:** Open CMP GUI	Login to CMP GUI as Administrator (or as Upgrade Engineer, if an account is defined for this).
2 ☐	**GUI:** Verify Upgrade Manager status display	**Upgrade Manager → System Maintenance** Open form wait a few seconds for the Status of the servers in the managed network to be displayed. • Verify that status is shown for all servers. • Verify that the CMP clusters are upgraded to release 9.x If Upgrade status is not shown, it may be necessary to run the operation to Push Script to the servers. To do this: Select each server at the site (one at a time) using the checkbox, and select the **Operation → Push Script** Confirm that status information on the form (including Upgrade Status) is updated after a few seconds. This step is not service affecting. It must be done before the Upgrade action is applied.
3 ☐	**GUI:** Configure Network Element Capability (if needed)	GUI: **Network → Network Elements → GGSN** For compatibility of Policy Management 9.x with ggsn systems that use Usage-Report-26, select this option and save. 
THIS PROCEDURE HAS BEEN COMPLETED		

6.1.2 Procedure 13: Key Exchanges from CMPs to MPE/MRA

Step	Procedure	Result
1 ☐	**GUI:** Open CMP GUI	Login to CMP GUI as Administrator (or as Upgrade Engineer, if an account is defined for this).
2 ☐	**SSH:** Primary Active CMP Verify Key exchanges to MPE/MRA servers	Ssh to Primary Active CMP Verify key exchanges from CMP to the MPE/MRA servers are completed: `# policySSHKey.pl --command checkSSHKeys` Check output to confirm that key exchanges are completed.

3 ☐	**SSH:** Primary Active CMP
	
	IF keyExchange needs to be updated
		IF the check of Key exchanges (previous step) shows that certain exchanges are not completed, then ex-execute Key Exchange tool:
		
		`# policySSHKey.pl --command syncSSHKeys`
		
		Example output:
		
		`Sync SSH Key with All C level Nodes:`
		`Begin to sync SSH key with node:C1180.027`
		`Begin to sync SSH key with node:C0682.103`
		`Begin to sync SSH key with node:C3474.104`
		`Begin to sync SSH key with node:C0682.146`
		`Begin to sync SSH key with node:C1180.101`
		`Begin to sync SSH key with node:C3474.070`
		`---------------------------------`
		`NodeID  IP  Result`
		`C1180.027  10.240.238.89  exchanged key successfully`
		`C0682.103  10.240.238.92  exchanged key successfully`
		`C3474.104  10.240.238.80  exchanged key successfully`
		`C0682.146  10.240.238.84  exchanged key successfully`
		`C1180.101  10.240.238.81  exchanged key successfully`
		`C3474.070  10.240.238.88  exchanged key successfully`
		`[root@cs-tb31-cmpb approximatelty ]#`
		
		If any key exchanges fail, run this command again.

4 ☐	**SSH:** Primary Standby CMP
	
	Verify Key exchange
		Ssh to Primary Standby CMP
		
		Execute this tool to verify key exchanges from CMP to the MPE/MRA servers:
		
		`# policySSHKey.pl --command checkSSHKeys`
		
		If any key Exchanges are incomplete:
		
		`# policySSHKey.pl --command syncSSHKeys`

5 ☐	**SSH:** Secondary Active CMP
	
	Verify Key exchange
		Ssh to Secondary Active CMP
		
		Execute this tool to verify key exchanges from CMP to the MPE/MRA servers:
		
		`# policySSHKey.pl --command checkSSHKeys`
		
		If any key Exchanges are incomplete:
		
		`# policySSHKey.pl --command syncSSHKeys`

Step	Procedure	Result

6 ☐	**SSH:** Secondary Standby CMP
	
	Verify Key exchange
		Ssh to Secondary Standby CMP
		
		Execute this tool to verify key exchanges from CMP to the MPE/MRA servers:
		
		`# policySSHKey.pl --command checkSSHKeys`
		
		If any key Exchanges are incomplete:
		
		`# policySSHKey.pl --command syncSSHKeys`

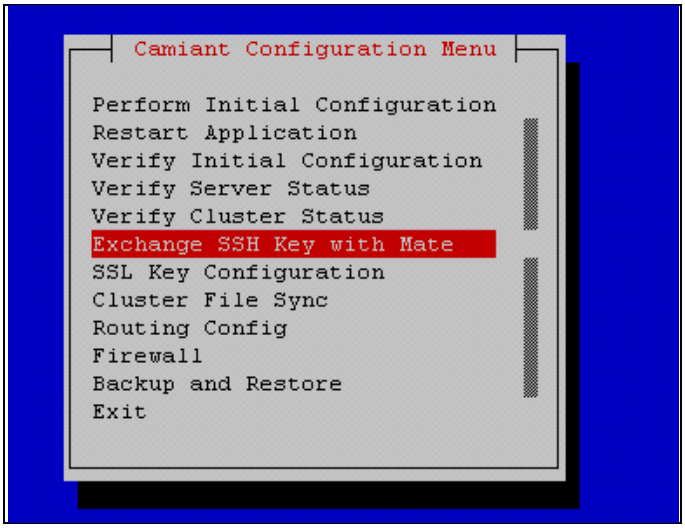
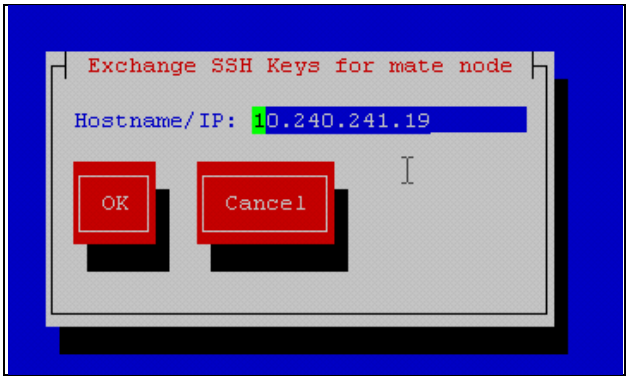
7 ☐	**GUI:** Verify Upgrade Manager status display	GUI: **Upgrade Manager → System Maintenance** Open form wait a few seconds for the Status of the servers in the managed network to be displayed. • Verify that status is shown for all servers. • Verify that the CMP clusters are upgraded to release 9.x **If Upgrade status is not shown**, it may be necessary to execute the operation to Push Script to the servers. To do this: Select each server at the site (one at a time) using the checkbox, and select the **Operation → Push Script** Confirm that status information on the form (including Upgrade Status) is updated after a few seconds. This step is not service affecting. It must be done before the Upgrade action is applied.
THIS PROCEDURE HAS BEEN COMPLETED		

6.1.3 Procedure 14: Key Exchanges Between Servers of MPE/MRA Clusters

This procedure will execute Key Exchanges between servers of MPE/MRA clusters, at the site to be upgraded. Policy Management 9.x requires that a key exchange is performed between MPE/MRA servers in a cluster.

It must be performed for every MPE/MRA cluster.

Step	Procedure	Result
8 ☐	**GUI:** Open CMP GUI	Login to CMP GUI as Administrator (or as Upgrade Engineer, if an account is defined for this).
9 ☐	**SSH:** any CMP server	`# cat /etc/hosts | grep <mpe|mra>`
10 ☐	**SSH:** from CMP server, ssh to a MPE/MRA server	`# ssh <hostname_of_MPE/MRA server>`

Step	Procedure	Result
11 ☐	**SSH:** MPE/MRA – perform Key Exchange using platcfg	At MPE/MRA: `# su - platcfg` **Camiant Configuration → Exchange ssh Key with Mate** 
12 ☐	**SSH:** MPE/MRA – Key Exchange dialog	The Mate IP address will be pre-populated. Select **OK**  There are two successful results: • A Success Dialog (if key is exchanged) • A return to the platcfg menu with no dialog (if key was previously exchanged, and does not need to be exchanged)
13 ☐	Repeat for each cluster	The key exchange is performed on one of the two servers of the cluster. Repeat this procedure for each MPE/MRA cluster at the site.
THIS PROCEDURE HAS BEEN COMPLETED		

6.1.4 Procedure 15: Verify Deployed Software Images at Site MPE/MRA Server

Detailed steps are shown in the procedure below to verify that the image files are correctly deployed and ready for upgrade activity at the MPE/MRA servers. The software ISO files were previously deployed to these servers during upgrade preparation.

Step	Procedure	Result
1 ☐	**SSH:** Active CMP Log into the server as the root user	`login: root` `Password: <root_password>`

2 ☐	**SSH: Active CMP** - Verify Image is deployed at MPE/MRA
	
	Rel 9.x Application Part Numbers:
	
	CMP – 872-2472-101
	MPE – 872-2473-101
	MPE-LI – 872-2474-101
	MRA – 872-2475-101
		`# cat /etc/hostname | grep <mpe/mra>`
		
		`# ssh <MPE/MRA hostname>`
		
		`# getPolicyRev`
		`7.5.x_x.x.x`
		
		`# getPolicyRev -p`
		`mpe or mra`
		
		`# ls -l /var/TKLC/upgrade`
		`total 706236`
		`-rw-r--r-- 1 root root 863408128 Jul 3 03:04 mpe--9.x.0_18.2.0--872-2473-101--x86_64.iso`
		
		Verify that the ISO matches the correct part number for this server function (MRA, MPE, MPE-LI), and
		
		Verify there is only one ISO in this directory.

3 ☐	**SSH:** MPE/MRA Validate ISO image	This step will validate the ISO image at the MPE/MRA server:
		`# su - platcfg`
		Maintenance → Upgrade → Validate
		Note Success of Validation
		exit from platcfg
		`# exit`

4 ☐	Repeat steps 2 and 3 for each MPE and MRA server in the site to be upgraded.	List of MPE _____ List of MRA _____
THIS PROCEDURE HAS BEEN COMPLETED		

6.2 Upgrade MPE Clusters

This procedure will upgrade one or more MPE clusters at a site.

This can be performed before or after MRA upgrade at the site.

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

NOTES:

- CMPs must be upgraded before executing this procedure.
- Application software is previously deployed to the upgrade directory on the servers at the site (see pre-upgrade procedure)
- This procedure will use the Upgrade Manager functionality on the CMP GUI to perform the upgrade of the MPEs.

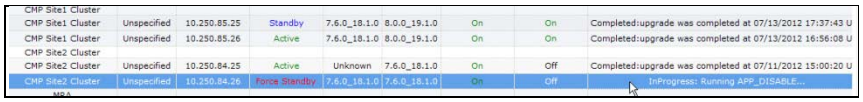
6.2.1 Procedure 16: Upgrade MPEs – Site

Step	Procedure	Result
1 ☐	Health Checks	**GUI:** • Check Active Alarms • (Optional) Reset MPE counters to make a baseline • Check KPI Dashboard (take a snap shot) • Verify current call rates (pre-upgrade) to compare after upgrade

2 ☐	**SSH:** Open ssh session to Primary Active CMP	`login: root`
		`Password: <enter password>`
		This session will be used for ssh access to the servers in the network to verify status.
		Keep this session open.

3 ☐	**GUI:** Verify Upgrade status of selected site from the Upgrade Manager.	**Upgrade Manager →System Maintenance** If desired, filter this form to display MPEs. Verify current Release numbers are the expected values.
4 ☐	**GUI:** Force Standby on standby MPE(s)	**Upgrade Manager →System Maintenance** This Activity can be applied at more than one MPE at a site, in parallel, to reduce time requirements. Select the checkbox for a Standby MPE server at the site and select - **Operation → Force Standby**. Confirm that status on the form is updated after several seconds. This step will prevent the server from becoming Active after the upgrade. Alarm 31228 is expected for each cluster to be upgraded.
5 ☐	**GUI:** Start Upgrade for Force Standby MPE(s) This step will take 20 minute or more, and the server will boot during this time.	**Upgrade Manager →System Maintenance** This Activity can be applied to multiple MPEs at a site, in parallel, to reduce time requirements. Select the checkbox for the Force Standby MPE server(s), and select the checkbox for the ISO to be installed. Then select – **Operation → Start Upgrade**

Step	Procedure	Result

6 ☐	**GUI:** Monitor Upgrade process	Monitor Upgrade Progress.
		1. Follow status on the **Upgrade Manager → System Maintenance: Upgrade Status**
		 
		The Upgrade status will proceed through several status messages.
		2. Optional: ssh to server, run
		`# tail -f /var/TKLC/log/upgrade/upgrade.log`
		NOTE: If upgrade fails due to the missing files, follow the workaround below (following errors will be logged in upgrade.log):
		`1369689305:: Checking for any missing packages or files`
		`1369689305:: Checking for missing files...`
		`1369689306::Missing Files:`
		`1369689308:: 0:TKLCsavelogsplat-4.1.17-4.2.3_70.84.0: /usr/TKLC/plat/etc/savelogs_plat.d/rpms`
		`1369689308::`
		`1369689308::ERROR: There are files missing from some rpms!`
		`1369689308::ERROR: Will not upgrade the server!`
		`1369689308:: Restarting cron service...`
		Work Around:
		Copy the rpms file from `/tmp to the /usr/TKLC/plat/etc/savelogs_plat.d/ directory`.
		NOTE: The following error messages are seen when the server is re-booting:
		Error: could not spawn ssh to 10.240.238.83
		Error:10.240.238.83 not reachable
		After the server re-boots,
		Confirm that status on the GUI form is Completed.
		Completed:upgrade was completed at 07/13/2012 18:23:53 UTC
		The following alarms are expected:
		31283 High Availability Ser ver is off line
		31228 HA Standby Server offline
		70005 One or more servers in the cluster are not at QP Blade Status = Available
		32305 Platform detected an error condition
		311xx *<Minor Replication Alarms>*

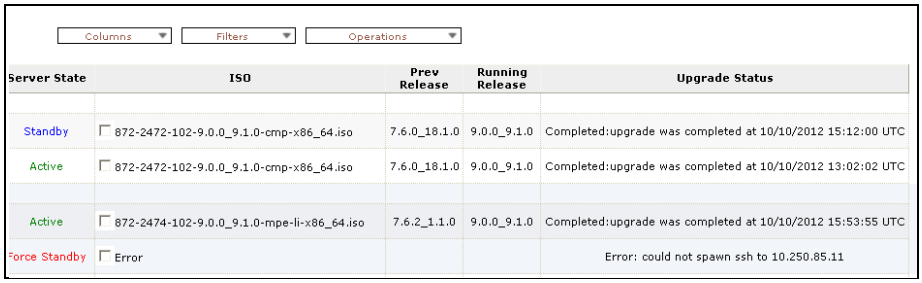
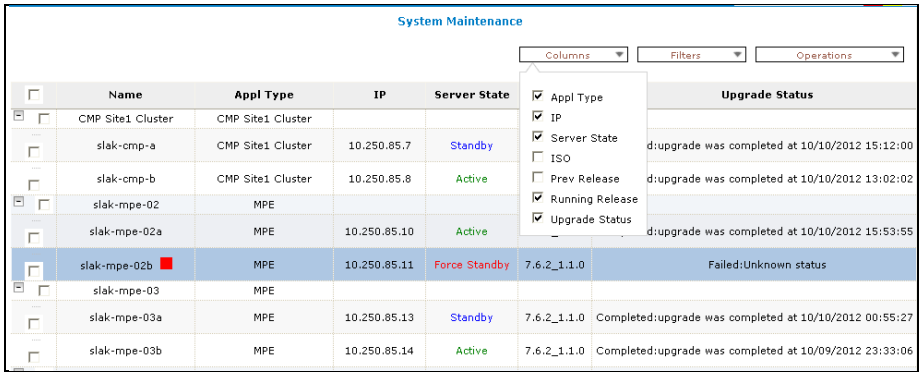
Step	Procedure	Result

7 ☐	**SSH:** Verify upgrade success on upgraded MPE severs	After upgrade shows Completed, ssh session to upgraded server:
		`# getPolicyRev`
		`9.x.0_x.x.x`
		
		`# tail /var/TKLC/log/upgrade/upgrade.log`
		`1343413625:: UPGRADE IS COMPLETE`
		`1343413625::`
		`1343413625:: Waiting for reboot`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_STATUS = SUCCESS`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_COMPLETED = 07/27/2012 18:27:05 UTC`
		`1343413625:: Updating platform revision file...`
		`1343413625::`
		`1343413625::`
		`1343413625:: A reboot of the server is required.`
		`1343413625:: The server will be rebooted in 10 seconds`
		
		`# ha.mystate`
		`resourceId role node lastUpdate`
		`DbReplication Stby C3691.123 0727:143326.003`
		`VIP Stby C3691.123 0727:143326.037`
		`QP Stby C3691.123 0727:143329.774`
		`DbReplication_old Stby C3691.123 0727:143326.104`
		
		NOTE: The state for some services may be OOS for a couple of minutes after upgrade.
		Do not proceed until the status shows Stby for all services.

Step	Procedure	Result
8 ☐	**SSH:** Verify Replication of session data	Once upgraded, the server will get the session data from the Active MPE server via audit. Run this command to monitor completion of this data transfer. It may take several minutes, if there is lot of session data. `# inetstat` **Audit state** root@slak-mpe-02a:~ LT dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 97 AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b Standby 0 0.00 CC From slak-mpe-02b Audit 0 38.24 ^98.01%cpu 6 **Audit Completed State** root@slak-mpe-02a:~ LT dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 82 AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b Standby 0 0.00 CC From slak-mpe-02b Active 0 0.00 ^0.38%cpu 99 ***Do not proceed until status shows that Audit is complete.***
9 ☐	**GUI: Cause Switchover to Upgraded Server** Service Affecting – up to 5 seconds of traffic impact is possible	**Upgrade Manager → System Maintenance** Select the checkbox for the partially upgraded (mixed 7.5/9.x) **cluster**, and select - **Operation → Switch ForceStandby** System Maintenance Columns Filters Operations Push Script Upload ISO Upgrade Completion Undo Upgrade Completion Switch ForceStandby Name Appl Type IP Server State cs-tb31-mpe1 MPE cs-tb31-mpe1-a MPE 10.240.238.84 Active 872-2546-101-9.1.0_15.1.0-mpe-li-x8 cs-tb31-mpe1-b MPE 10.240.238.92 Force Standby 872-2546-101-9.1.0_15.1.0-mpe-li-x8 **NOTE:** Switch ForcedStandby may be failed due to the primary CMP server not using default password. After a several seconds, the following will be shown: System Maintenance Columns Filters Operations Name Appl Type IP Server State ISO cs-tb31-mpe1 MPE cs-tb31-mpe1-a MPE 10.240.238.84 Force Standby 872-2546-101-9.1.0_15.1.0-mpe-li-x8 cs-tb31-mpe1-b MPE 10.240.238.92 Active 872-2546-101-9.1.0_15.1.0-mpe-li-x8

Step	Procedure	Result
10 ☐	**SSH:** Verify KPI Dashboard Status	**System Wide Reports → KPI Dashboard** Status may transition as shown in the following sequence. KPI Dashboard (Stats Reset: Manual) Show slak-mra ☑ Change Thresholds slak-mra: Performance / Connections / Alarms / Protocol Errors MRA: State, TPS, PDN, Active Subscribers, CPU %, Memory %, MPE, MRA, Network Elements, Critical, Major, Minor, Sent, Received slak-mra(active): On-line, 97 (0%), 810790 (3%), 810791 (0%), 0, 6, 2 of 2, 0 of 0, 2 of 3, 0, 0, 0, 204, 0 slak-mra(standby): On-line, 0, 5 MPE: State, TPS, PDN, CPU %, Memory %, MRA, HSS, Critical, Major, Minor, Sent, Received PCRF1(Server-A): No response, ----, ----, ----, ----, ----, ----, ----, ----, ----, ----, ---- PCRF1(null): Active, 55 (1%), 404945 (8%), 0, 19, 1 of 1, 1 of 1, 2, 1, 0, 0, 102 PCRF2(active): On-line, 54 (1%), 405344 (8%), 0, 19, 1 of 1, 1 of 1, 0, 0, 0, 0, 102 PCRF2(standby): On-line, 0, 19 KPI Dashboard (Stats Reset: Manual) Show slak-mra ☑ Change Thresholds slak-mra: Performance / Connections / Alarms / Protocol Errors MRA: State, TPS, PDN, Active Subscribers, CPU %, Memory %, MPE, MRA, Network Elements, Critical, Major, Minor, Sent, Received slak-mra(active): On-line, 96 (0%), 810816 (3%), 810815 (0%), 1, 6, 2 of 2, 0 of 0, 2 of 3, 0, 0, 0, 267, 0 slak-mra(standby): On-line, 0, 5 MPE: State, TPS, PDN, CPU %, Memory %, MRA, HSS, Critical, Major, Minor, Sent, Received PCRF1(Server-A): Active, 24 (0%), 403949 (6%), 0, 7, 1 of 1, 1 of 1, 2, 3, 2, 0, 0 PCRF1(null): Active, 24 (0%), 403949 (6%), 0, 7, 1 of 1, 1 of 1, 2, 3, 2, 0, 0 PCRF2(active): On-line, 89 (2%), 405494 (8%), 1, 19, 1 of 1, 1 of 1, 0, 0, 0, 0, 102 PCRF2(standby): On-line, 0, 19 KPI Dashboard (Stats Reset: Manual) Show slak-mra ☑ Change Thresholds slak-mra: Performance / Connections / Alarms / Protocol Errors MRA: State, TPS, PDN, Active Subscribers, CPU %, Memory %, MPE, MRA, Network Elements, Critical, Major, Minor, Sent, Received slak-mra(active): On-line, 95 (0%), 810840 (3%), 810840 (0%), 0, 6, 2 of 2, 0 of 0, 2 of 3, 0, 0, 0, 267, 0 slak-mra(standby): On-line, 0, 5 MPE: State, TPS, PDN, CPU %, Memory %, MRA, HSS, Critical, Major, Minor, Sent, Received PCRF1(Server-A): Active, 19 (0%), 403863 (6%), 0, 7, 1 of 1, 1 of 1, 2, 2, 2, 0, 0 PCRF1(null): No Data, 0, 0 PCRF2(active): On-line, 93 (2%), 405602 (8%), 1, 19, 1 of 1, 1 of 1, 0, 0, 0, 0, 102 PCRF2(standby): On-line, 0, 19

Step	Procedure	Result
11 ☐	**GUI:** Reapply MPE Cluster Configuration	**PolicyServer → Configuration →** *<cluster>* **→ System** Click **Reapply Configuration**  Verify success of Configuration reapply.
12 ☐	**GUI:** Verify MPE Cluster Traffic	**PolicyServer → Configuration →** *<cluster>* **→ Reports** Verify that Upgraded server is Active and other server is Forced Standby. Verify that the Reports show server is processing traffic.
13 ☐	**GUI:** Verify KPI Dashboard	**SystemWideReports → KPI Dashboard** Compare to pre-upgrade KPI Dashboard. KPI Dashboard (Stats Reset: Manual) Show slak-mra ☑ Change Thresholds slak-mra — Performance / Connections / Alarms / Protocol Errors MRA: slak-mra(active) On-line, TPS 95 (0%), PDN 810840 (3%), Active Subscribers 810840 (0%), CPU 0, Memory 6, MPE 2 of 2, MRA 0 of 0, Network Elements 2 of 3, Critical 0, Major 0, Minor 0, Sent 267, Received 0 slak-mra(standby) On-line, CPU 0, Memory 5 MPE: PCRF1(Server-A) Active, TPS 19 (0%), PDN 403863 (6%), CPU 0, Memory 7, MRA 1 of 1, HSS 1 of 1, Critical 2, Major 2, Minor 2, Sent 0, Received 0 PCRF1(null) No Data, CPU 0, Memory 0 PCRF2(active) On-line, TPS 93 (2%), PDN 405602 (8%), CPU 1, Memory 19, MRA 1 of 1, HSS 1 of 1, Critical 0, Major 0, Minor 0, Sent 0, Received 102 PCRF2(standby) On-line, CPU 0, Memory 19 If possible, confirm with customer that traffic is normal for Network element connected devices.
14 ☐	**IF Verify Step fails - Backout**	If needed, fallback to 7.5/7.5 server: See Procedure of this document for Backout of a Partially Upgraded Cluster.

Step	Procedure	Result
15 ☐	**GUI:** Upgrade second MPE in Cluster This will take 20 Minutes.	This step will take 20 minute or more, and the server will boot during this time. **Upgrade Manager → System Maintenance** Select check box for current Force Standby MPE server(s) and the checkbox for the ISO to be installaed at the site and select – **Operation → Start Upgrade**
16 ☐	Wait for Upgrade to process	Wait for Upgrade to proceed. Monitor Upgrade Progress, if desired: 1. Follow status on the GUI: **Upgrade Manager →System Maintenance** 2. Ssh to server, and run: `# tail -f /var/TKLC/log/upgrade/upgrade.log` 3. Alarms will eventually clear up. Confirm that status on the GUI form is Upgrade Complete. **NOTE:** Final step of the upgrade is a Re-boot of the server. This will appear in the System Maintenance form with a Error message, like below. This is expected.  Columns Filters Operations Server State | ISO | Prev Release | Running Release | Upgrade Status Standby | 872-2472-102-9.0.0_9.1.0-cmp-x86_64.iso | 7.6.0_18.1.0 | 9.0.0_9.1.0 | Completed:upgrade was completed at 10/10/2012 15:12:00 UTC Active | 872-2472-102-9.0.0_9.1.0-cmp-x86_64.iso | 7.6.0_18.1.0 | 9.0.0_9.1.0 | Completed:upgrade was completed at 10/10/2012 13:02:02 UTC Active | 872-2474-102-9.0.0_9.1.0-mpe-li-x86_64.iso | 7.6.2_1.1.0 | 9.0.0_9.1.0 | Completed:upgrade was completed at 10/10/2012 15:53:55 UTC Force Standby | Error | | | Error: could not spawn ssh to 10.250.85.11
17 ☐	IF Upgrade fails	The following indication is shown if a upgrade fails:  System Maintenance Columns Filters Operations Name | Appl Type | IP | Server State | Upgrade Status CMP Site1 Cluster | CMP Site1 Cluster slak-cmp-a | CMP Site1 Cluster | 10.250.85.7 | Standby | d:upgrade was completed at 10/10/2012 15:12:00 slak-cmp-b | CMP Site1 Cluster | 10.250.85.8 | Active | d:upgrade was completed at 10/10/2012 13:02:02 slak-mpe-02 | MPE slak-mpe-02a | MPE | 10.250.85.10 | Active | d:upgrade was completed at 10/10/2012 15:53:55 slak-mpe-02b | MPE | 10.250.85.11 | Force Standby | 7.6.2_1.1.0 | Failed:Unknown status slak-mpe-03 | MPE slak-mpe-03a | MPE | 10.250.85.13 | Standby | 7.6.2_1.1.0 | Completed:upgrade was completed at 10/10/2012 00:55:27 slak-mpe-03b | MPE | 10.250.85.14 | Active | 7.6.2_1.1.0 | Completed:upgrade was completed at 10/09/2012 23:33:06 Appl Type IP Server State ISO Prev Release Running Release Upgrade Status In this case, ssh to the server and view the upgrade log to determine the error. `tail -f /var/TKLC/log/upgrade/upgrade.log` Correct the error, and re-try the upgrade. Or call Oracle support.

Step	Procedure	Result

18 ☐	**SSH:** upgraded MPE server(s), Verify upgrade success	After upgrade shows Completed, ssh session to upgraded server(s):
		`# getPolicyRev`
		`9.x.0_x.x.x`
		
		`# tail /var/TKLC/log/upgrade/upgrade.log`
		`1343413625::  UPGRADE IS COMPLETE`
		`1343413625::`
		`1343413625:: Waiting for reboot`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_STATUS = SUCCESS`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_COMPLETED = 07/27/2012 18:27:05 UTC`
		`1343413625:: Updating platform revision file...`
		`1343413625::`
		`1343413625::`
		`1343413625:: A reboot of the server is required.`
		`1343413625:: The server will be rebooted in 10 seconds`
		
		`# ha.mystate`
		`resourceId role node lastUpdate`
		`DbReplication Stby C3691.123 0727:143326.003`
		`VIP Stby C3691.123 0727:143326.037`
		`QP Stby C3691.123 0727:143329.774`
		`DbReplication_old Stby C3691.123 0727:143326.104`
		NOTE: the state for some services may be OOS for a couple of minutes after upgrade.
		Do not proceed until status shows Stby for all services.

19 ☐	**SSH:** Verify Replication	Once upgraded, the server will get the session data from the Active MPE server via audit. Run this command to monitor completion of this data transfer. It may take several minutes, if there is lot of session data. `# inetstat` ***Do not proceed until status shows Audit is complete.***
20 ☐	**GUI:** Remove Forced Standby	**Upgrade Manager →System Maintenance** Select checkbox for Standby MRE server at the site and select: **Operation → Cancel Force Standby** Confirm that status on the form is updated to Standby. This step will allow the server to become Active. Active MPE is un-affected. Alarms are expected.

Step	Procedure	Result
21 ☐	GUI: Verify Alarms and Reports	**System Wide Reports → Active Alarms** Confirm if any alarms are unexpected. **NOTE:** Some Alarms have a 30 minute auto clearing time. **System Wide Reports → KPI DashBoard** Compare to pre-upgrade collected reports. **Policy Server → Configuration → Policy Server → Reports** Compare to pre-upgrade collected reports. **Policy Server → Configuration → Policy Server → System** Confirm status
22 ☐	**IF Verify Step fails - Backout**	If needed, fallback to 7.5/7.5 server: See Procedure of this document for Backout of a Fully Upgraded Cluster.
23 ☐	MPE cluster is upgraded	MPE cluster is upgraded.
24 ☐	REPEAT Above steps for next MPE cluster	If Clusters are being upgraded one-at-a-time, then procede with next cluster: MPE Cluster _____ Add rows as needed for all MPEs at a site.
25 ☐	Recommended Soak Period	It is Recommended to let the new release soak for a period of time, to view stability and traffic/policy behavior is as expected.
THIS PROCEDURE HAS BEEN COMPLETED		

6.3 Upgrade Site MRA Clusters

This procedure will upgrade an MRA cluster at a site.

It can be applied before or after the Upgrade of the MPEs at a site.

This section may be replicated or moved to adjust for the customer choice of upgrade order of MPEs and MRAs.

NOTES:

- CMPs must be upgraded before executing this procedure.
- Application software is previously deployed to the upgrade directory on the servers at the site (see pre-upgrade procedure)
- This procedure will use the Upgrade Manager functionality on the CMP GUI to perform the upgrade of the MRA cluster.

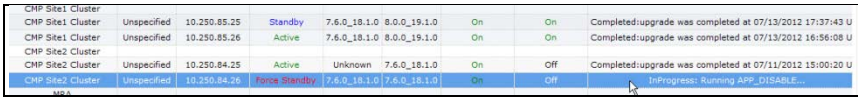
6.3.1 Procedure 17: Upgrade Site MRA

Step	Procedure	Result
1 ☐	**GUI:** Health Checks	GUI: • Check Active Alarms • (Optional) reset MRA/MPE counters to make a baseline • Check KPI Dashboard (take a snap shot) • Verify current call rates to compare after upgrade

Step	Procedure	Result

2 ☐	**SSH:** Open ssh session to Active CMP server at Primary site
	1. Access the login prompt.
	2. Log into the server as the root user
		`login: root`
		`Password: <enter password>`
		This session will be used for ssh to the MRA servers to verify status. Keep this window open.

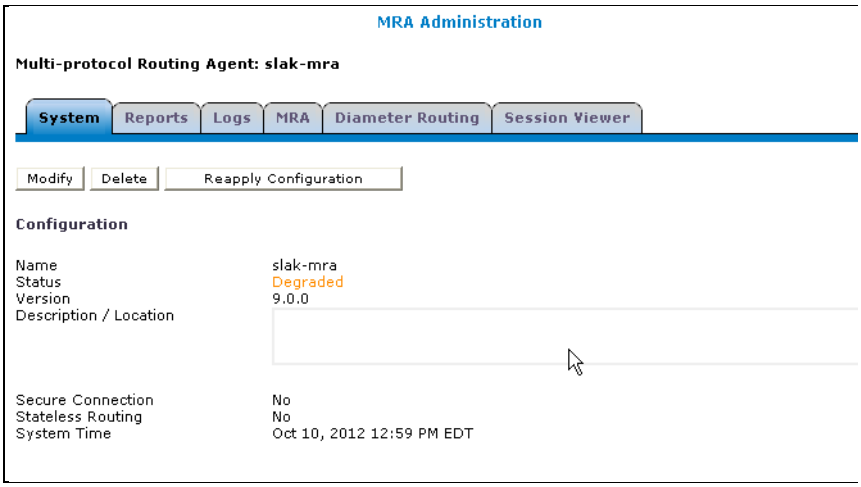
3 ☐	**GUI:** Display Upgrade status of selected site	**Upgrade Manager → System Maintenance** Wait for the form to populate. Select Filter for Appl Type = MRA, to display only MRAs (option). Verify information for the MRAs: • Current Release installed • Upgrade status • Active/Standby status **NOTE:** If the Upgrade status is reporting an Error, it may be needed to select: **Operation → Push Script** to get the current status from the server.
4 ☐	**GUI:** Force Standby on standby MRA	**Upgrade Manager → System Maintenance** Select the checkbox for the Standby MRA server at the site to be upgraded, and select: **Operation → Force Standby** Confirm that status on the form is updated. This step will prevent the server from becoming Active. The Active MRA is un-affected. Active MRA Server will report Alarm 31228.
5 ☐	**GUI:** Upgrade for Force Standby MRA	**Upgrade Manager → System Maintenance** Select the checkbox for the Force Standby MRA server at the site and select: **Operation → Start Upgrade** **NOTE:** The 9.x MRA software image (ISO) should have previously been copied to the /var/TKLC/upgrade directory on the server, and this should be the only image in this directory.

Step	Procedure	Result
6 ☐	Wait for Upgrade to process This step will take 20 minute or more, and the server will boot during this time.	Monitor Upgrade Progress. 1. Follow status on the Upgrade Manager → System Maintenance form: Upgrade Status  The Upgrade status will proceed through several status messages. 2. Optional: ssh to server, run `# tail -f /var/TKLC/log/upgrade/upgrade.log` **NOTE:** The following error messages are seen when the server is re-booting: Error: could not spawn ssh to 10.250.84.26 Error:SSH connection timedout to host 10.250.84.26 3. After the server re-boots, Confirm that status on the GUI form is Completed. Completed:upgrade was completed at 07/13/2012 18:23:53 UTC

7 ☐	**SSH:** Verify upgrade success	After upgrade shows Completed, ssh session to upgraded server(s):
		
		`# getPolicyRev`
		`9.x.0_x.x.x`
		
		`# tail /var/TKLC/log/upgrade/upgrade.log`
		`1343413625:: UPGRADE IS COMPLETE`
		`1343413625::`
		`1343413625:: Waiting for reboot`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_STATUS = SUCCESS`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_COMPLETED = 07/27/2012 18:27:05 UTC`
		`1343413625:: Updating platform revision file...`
		`1343413625::`
		`1343413625::`
		`1343413625:: A reboot of the server is required.`
		`1343413625:: The server will be rebooted in 10 seconds`
		
		`# ha.mystate`
		`resourceId role node lastUpdate`
		`DbReplication Stby C3691.123 0727:143326.003`
		`VIP Stby C3691.123 0727:143326.037`
		`QP Stby C3691.123 0727:143329.774`
		`DbReplication_old Stby C3691.123 0727:143326.104`
		
		NOTE: the state for some services may be OOS for a couple of minutes after upgrade.
		
		Do not proceed until status shows Stby for all services.

Step	Procedure	Result
8 ☐	**SSH:** Verify Replication of session data	Once upgraded, the server will get the session data from the Active MPE server via audit. Run this command to monitor completion of this data transfer. It may take several minutes, if there is lot of session data. `# inetstat` **Audit state** root@slak-mpe-02a:~ LT dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 97 AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b Standby 0 0.00 CC From slak-mpe-02b Audit 0 38.24 ^98.01%cpu 6 **Audit Completed State** root@slak-mpe-02a:~ LT dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 82 AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b Standby 0 0.00 CC From slak-mpe-02b Active 0 0.00 ^0.38%cpu 99 ***Do not proceed until status shows that Audit is complete.***
9 ☐	**GUI:** Verify KPI Dashboard	System Wide Reports → KPI Dashboard In the following example, slak-mra Server B is on 7.5 and Active. slak-mra Server A is 9.x and Force Standby. This is expected. (MPEs are previously upgraded to 9.x.) KPI Dashboard (Stats Reset: Manual) Show slak-mra ☑ Change Thresholds

slak-mra	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
slak-mra(Server-A)	No response	----	----	----	----	----	----	----	----	----	----	----	----	----
slak-mra(null)	Active	104 (0%)	811923 (3%)	811873 (0%)	1	6	2 of 2	0 of 0	2 of 3	2	2	1	3275	41
MPE	**State**	**TPS**	**PDN**		**CPU %**	**Memory %**	**MRA**	**HSS**		**Critical**	**Major**	**Minor**	**Sent**	**Received**
PCRF1(Server-A)	Active	54 (1%)	132 (0%)		0	3	1 of 1	1 of 1		0	0	0	0	293
PCRF1(Server-B)	Standby				0	3								
PCRF2(Server-A)	Standby				0	5								
PCRF2(Server-B)	Active	55 (1%)	404697 (6%)		1	6	1 of 1	1 of 1		0	0	0	21	335

Step	Procedure	Result
10 ☐	**GUI:** Cause Switchover to Upgraded Server ***Service Affecting – up to several seconds of traffic impact is possible***	**Upgrade Manager → System Maintenance** Select the checkbox for the partially upgraded (mixed 7.5/9.x) cluster, and select - **Operation → Switch ForceStandby**
11 ☐	**GUI:** Reapply MRA Configuration	**MRA → Configuration → <*cluster*> → System** Select **Reapply Configuration** 

Step	Procedure	Result
12 ☐	GUI: Verify KPI Dashboard show the transition	**System Wide Reports → KPI Dashboard** The following state transitions for the MPA servers are are expected, over several seconds. In this example, ServerA is 9.x and ServerB 7.5.

KPI Dashboard (Stats Reset: Manual)

Show slak-mra ☑

Change Thresholds

slak-mra	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
slak-mra(Server-A)	Active	0 (0%)	811874 (1%)	811874 (4%)	3	7	2 of 2	0 of 0	1 of 3	2	3	2	0	0
slak-mra(null)	Active	0 (0%)	811874 (1%)	811874 (4%)	3	7	2 of 2	0 of 0	1 of 3	2	3	2	0	0
MPE	State	TPS	PDN		CPU %	Memory %	MRA	HSS		Critical	Major	Minor	Sent	Received
PCRF1(Server-A)	Active	0 (0%)	132 (0%)		3	3	2 of 1	1 of 1		0	0	0	0	293
PCRF1(Server-B)	Standby				1	3								
PCRF2(Server-A)	Standby				0	5								
PCRF2(Server-B)	Active	52 (1%)	404697 (6%)		4	6	1 of 1	1 of 1		0	0	0	21	335

KPI Dashboard (Stats Reset: Manual)

Show slak-mra ☑

Change Thresholds

slak-mra	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
slak-mra(Server-A)	Active	48 (0%)	812197 (1%)	812192 (4%)	1	7	2 of 2	0 of 0	3 of 3	3	3	1	389	0
MPE	State	TPS	PDN		CPU %	Memory %	MRA	HSS		Critical	Major	Minor	Sent	Received
PCRF1(Server-A)	Active	37 (0%)	302 (0%)		0	3	1 of 1	1 of 1		0	0	1	0	515
PCRF1(Server-B)	Standby				0	3								
PCRF2(Server-A)	Standby				2	5								
PCRF2(Server-B)	Active	29 (0%)	404819 (6%)		2	6	1 of 1	1 of 1		0	0	1	21	451

KPI Dashboard (Stats Reset: Manual)

Show slak-mra ☑

Change Thresholds

slak-mra	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
slak-mra(Server-A)	Active	77 (0%)	812397 (1%)	812392 (4%)	1	7	2 of 2	0 of 0	3 of 3	2	3	1	569	0
slak-mra(null)	No Data				0	0								
MPE	State	TPS	PDN		CPU %	Memory %	MRA	HSS		Critical	Major	Minor	Sent	Received
PCRF1(Server-A)	Active	39 (0%)	408 (0%)		0	3	1 of 1	1 of 1		0	0	1	0	628
PCRF1(Server-B)	Standby				0	3								
PCRF2(Server-A)	Standby				4	5								
PCRF2(Server-B)	Active	29 (0%)	404914 (6%)		2	6	1 of 1	1 of 1		0	0	1	21	569

Step	Procedure	Result
13 ☐	**GUI:** Verify KPI Dashboard	**SystemWideReports → KPI Dashboard** Compare to pre-upgrade KPI Dashboard. If possible, confirm with customer that traffic is normal for Network element connected devices. KPI Dashboard (Stats Reset: Manual) Show slak-mra ☑ Change Thresholds

slak-mra	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
slak-mra(Server-A)	Active	29 (0%)	1024401 (2%)	1024398 (5%)	0	7	2 of 2	0 of 0	2 of 2	1	1	0	35	0
slak-mra(null)	No Data				0	0								
MPE	**State**	**TPS**	**PDN**		**CPU %**	**Memory %**	**MRA**	**HSS**		**Critical**	**Major**	**Minor**	**Sent**	**Received**
slak-mpe-02(Server-A)	Standby				0	6								
slak-mpe-02(Server-B)	Active	19 (0%)	14695 (0%)		0	6	1 of 1	1 of 1		0	0	1	0	31
slak-mpe-03(Server-A)	Standby				0	6								
slak-mpe-03(Server-B)	Active	19 (0%)	7571 (0%)		3	6	1 of 1	1 of 1		0	0	1	0	4

Step	Procedure	Result
14 ☐	**GUI:** Verify MPE Cluster Traffic	**MRA → Configuration → <*cluster*> → Reports** Verify that Upgraded server is Active and other server is `On-line` MRA Administration **Multi-protocol Routing Agent: slak-mra** System | Reports | Logs | MRA | Diameter Routing | Session Viewer **Stats Reset: Manual** **Cluster Information Report** Mode: Active Reset All Counters | Rediscover Cluster | Pause **Cluster: slak-mra** Cluster Status Degraded **Blades** | | Overall | | | Utilization | | | Actions | | | State | Blade Failures | Uptime | Disk | CPU | Memory | | | 10.250.85.4 (Server-A) | Active | 1 | 1 hour 26 mins 1 sec | 0.13 % | 2 % | 7 % | Restart Reboot | | 10.250.85.5 () | On-line | 1 | 7 mins 9 secs | 0.07 % | 0 % | 6 % | Restart Reboot | Verify that the Reports show server is processing traffic. **Protocol Statistics** | Name | Connections | Total client messages in / out | Total messages timeout | | **Diameter** | | | | | Diameter AF Statistics | 2 | 0 / 0 | 0 | | Diameter PCEF Statistics | 3 | 3842 / 3842 | 0 | | Diameter CTF Statistics | 2 | 0 / 0 | N/A | | Diameter BBERF Statistics | 3 | 7717 / 7750 | 33 | | Diameter TDF Statistics | 0 | 0 / 0 | 0 | | Diameter DRMA Statistics | 0 | 0 / 0 | 0 | | Diameter DRA Statistics | N/A | N/A | N/A | **Latency Statistics** | Name | Connections | | **Diameter** | | Diameter AF Latency Statistics | 2 | | Diameter PCEF Latency Statistics | 3 | | Diameter BBERF Latency Statistics | 3 | | Diameter TDF Latency Statistics | 0 | | Diameter DRMA Latency Statistics | 0 | **Error Statistics** | Error | Total errors received / sent | | **Diameter** | | Errors By Code | 0 / 33 | | Errors By Remote Identity | 0 / 33 | KPI Interval Statistics
15 ☐	**IF Verify Steps fail: Backout**	If needed, fallback to 7.5 server: See section for Backout of Partial Upgraded Cluster.
16 ☐	**GUI:** Upgrade second MRA in Cluster	**Upgrade Manager → System Maintenance** Select check box for current Force Standby MRA server at the site, and select – **Operation →Start Upgrade**

Step	Procedure	Result
17 ☐	Wait for Upgrade to process This step will take 20 minute or more, and the server will boot during this time.	Wait for Upgrade to proceed. Monitor Upgrade Progress, if desired: 1. Follow status on the **Upgrade Manager →System Maintenance** form: Upgrade Status CMP Site1 Cluster CMP Site1 Cluster Unspecified 10.250.85.25 Standby 7.6.0_18.1.0 8.0.0_19.1.0 On On Completed:upgrade was completed at 07/13/2012 17:37:43 U CMP Site1 Cluster Unspecified 10.250.85.26 Active 7.6.0_18.1.0 8.0.0_19.1.0 On On Completed:upgrade was completed at 07/13/2012 16:56:08 U CMP Site2 Cluster CMP Site2 Cluster Unspecified 10.250.84.25 Active Unknown 7.6.0_18.1.0 On Off Completed:upgrade was completed at 07/11/2012 15:00:20 U CMP Site2 Cluster Unspecified 10.250.84.26 Force Standby 7.6.0_18.1.0 7.6.0_18.1.0 On Off InProgress: Running APP_DISABLE... The Upgrade status will proceed through several status messages. 2. Optional: ssh to server, run `# tail -f /var/TKLC/log/upgrade/upgrade.log` 3. Optional: Login to Server Console via the iLo of the server, and monitor the console output to confirm upgrade progress **NOTE:** The following error messages are seen when the server is re-booting: Error: could not spawn ssh to 10.250.84.26 Error:SSH connection timedout to host 10.250.84.26 4. After the server re-boots, Confirm that status on the GUI form is Completed. Completed:upgrade was completed at 07/13/2012 18:23:53 UTC

18 ☐	**SSH:** upgraded MPE server(s), Verify upgrade success	After upgrade shows Completed, ssh session to upgraded server:
		
		`# getPolicyRev`
		`9.x.0_x.x.x`
		
		`# tail /var/TKLC/log/upgrade/upgrade.log`
		`1343413625:: UPGRADE IS COMPLETE`
		`1343413625::`
		`1343413625:: Waiting for reboot`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_STATUS = SUCCESS`
		`1343413625::DEBUG: ADDING VAR: UPGRADE_COMPLETED = 07/27/2012 18:27:05 UTC`
		`1343413625:: Updating platform revision file...`
		`1343413625::`
		`1343413625::`
		`1343413625:: A reboot of the server is required.`
		`1343413625:: The server will be rebooted in 10 seconds`
		`# ha.mystate`
		`resourceId role node lastUpdate`
		`DbReplication Stby C3691.123 0727:143326.003`
		`VIP Stby C3691.123 0727:143326.037`
		`QP Stby C3691.123 0727:143329.774`
		`DbReplication_old Stby C3691.123 0727:143326.104`
		
		NOTE: the state for some services may be OOS for a couple of minutes after upgrade.
		
		Do not proceed until status shows Stby for all services

Step	Procedure	Result
19 ☐	**SSH:** Verify Replication	Once upgraded, the server will get the session data from the Active MPE server via audit. Run this command to monitor completion of this data transfer. It may take several minutes, if there is lot of session data. `# inetstat` ***Do not proceed until status shows Audit is complete.***
20 ☐	**GUI:** Verify KPI Dashboard Status	**System Wide Reports → KPI Dashboard** Example – Upgraded server now shows force standby KPI Dashboard (Stats Reset: Manual) Show slak-mra ☑ Change Thresholds slak-mra: Performance / Connections / Alarms / Protocol Errors MRA: slak-mra(Server-A) Active, TPS 101 (0%), PDN 81257 7 (1%), Active Subscribers 81257 7 (4%), CPU 0, Memory 7, MPE 2 of 2, MRA 0 of 0, Network Elements 0 of 3, Critical 0, Major 1, Minor 1, Sent 569, Received 0 slak-mra(Server-B) Forced Standby, CPU 0, Memory 7 MPE: PCRF1(Server-A) Active, TPS 54 (1%), PDN 477 (0%), CPU 1, Memory 3, MRA 1 of 1, HSS 1 of 1, Critical 0, Major 0, Minor 1, Sent 0, Received 628 PCRF1(Server-B) Standby, CPU 3, Memory 3 PCRF2(Server-A) Standby, CPU 0, Memory 5 PCRF2(Server-B) Active, TPS 55 (1%), PDN 40500 6 (6%), CPU 4, Memory 6, MRA 1 of 1, HSS 1 of 1, Critical 0, Major 0, Minor 1, Sent 21, Received 569
21 ☐	**GUI:** Remove Forced Standby (second MRA in the cluster)	**Upgrade Manager → System Maintenance** Select check box for just-upgraded Force Standby MRA server at the site and Select - **Operation → Cancel Force Standby** Confirm that status on the form is updated to Standby.
22 ☐	**GUI:** Verify MRA activity at Upgraded site MRA cluster	Perform health checks as in step 1 of this procedure. View Alarms, KPI Dashboard, and MRA reports to verify that the system is healthy. Recommend to make a screen capture of post-upgrade status for these forms.
THIS PROCEDURE HAS BEEN COMPLETED		

6.3.2 Procedure 18: 9.x Replication Activation

For Release 9.x, there is an improved Replication method that needs to be activated after the upgrade. It is recommended that this is done as part of the planned Upgrade activities.

After an upgrade from 7.5 to 9.x, the Policy System will be using "Legacy Replication". This is the Replication method between servers that was supported in release 7.5. This Replication method will be disabled, and the new Replication method enabled.

This Activation should be performed for all servers in the Policy system in a single maintenance window. A roll back procedure is also provided.

IMPORTANT: This is only performed after all servers in the network have been upgraded.

NOTES:

- All servers in the Policy system are previously upgraded to the 9.x Release
- This procedure will use the Upgrade Manager functionality on the CMP GUI to perform the replication feature Activation.

Step	Procedure	Result
1 ☐	**GUI:** Open CMP GUI	Login to CMP GUI as Administrator (or as Upgrade Engineer, if an account is defined for this).

2 ☐	**SSH:** Open ssh session to Active CMP server
	• Access the login prompt.
	• Log into the server as the root user
		`login: root`
		`Password: <enter password>`
		This session will be used for executing command line activities.

3 ☐	**GUI:** Confirm Upgrade status of all sites and servers	**Upgrade Manager → System Maintenance** Confirm in the Running Release column that all servers in the network are upgraded to 9.x.
4 ☐	**GUI:** Change Replication mode: MRAs (One cluster at a time)	**Upgrade Manager → System Maintenance** Select MRA cluster _____ 1. Select the checkbox for the **Standby MRA server**, and execute: **Operation → Upgrade Completion** 2. Select the checkbox for the **Active MRA server**, and execute: **Operation → Upgrade Completion**
5 ☐	**SSH:** MRA Active Server	Verify that the new Replication is active on the cluster: `# irepstat`
6 ☐	**GUI:** Repeat Steps above for each MRA cluster in the Network (One cluster at a time)	Select another MRA cluster _____ Perform steps above (Repeat this row of the table for each MRA cluster in the network.)
7 ☐	**GUI:** Change Replication mode: MPEs (One cluster at a time)	**Upgrade Manager → System Maintenance** Select MPE cluster _____ 1. Select the checkbox for the **Standby MPE server,** and execute: **Operation → Upgrade Completion** 2. Select the checkbox for the **Active MPE server**, and execute: **Operation → Upgrade Completion**
8 ☐	**GUI:** Change Replication mode: Secondary site CMPs	**Upgrade Manager → System Maintenance** Select Secondary-Site CMP cluster _____ 1. Select the checkbox for the **Standby CMP server**, and execute: **Operation → Upgrade Completion** 2. Select the checkbox for the **Active CMP server**, and execute: **Operation → Upgrade Completion**
9 ☐	**GUI:** Change Replication mode: Active site CMPs	Select CMP cluster _____ 1. Select the checkbox for the **Standby CMP server**, and execute: **Operation → Upgrade Completion** 2. Select the checkbox for the **Active CMP server**, and execute: **Operation → Upgrade Completion**
10 ☐	**GUI:** Verify Active Alarms	**System Wide Reports → Active Alarms** All Upgrade related alarms should be cleared.

Step	Procedure	Result
11 ☐	**SSH:** Primary Active CMP, confirm that replication to MPE/MRAs is Active/Standby	`# irepstat` root@slak-cmp-b:~ -- Policy 0 ActStb [DbReplication] ---------- AA To slak-cmp-a Active 0 0.00 0.05%cpu 51B/s AC To slak-mpe-03a Active 0 0.00 0.05%cpu 71B/s AC To slak-mpe-03b Active 0 0.00 0.04%cpu 83B/s AC To slak-mpe-02a Active 0 0.00 0.04%cpu 87B/s AC To slak-mpe-02b Active 0 0.00 0.05%cpu 54B/s AC To slak-mra-a Active 0 0.00 0.05%cpu 67B/s AC To slak-mra-b Active 0 0.00 0.04%cpu 58B/s

12 ☐	**SSH:** Primary Active CMP, confirm that exclustions are removed	Verify that the Replication exclusions “LongParam,AppEventDef” are removed from the NodeInfo Table and output similar to the following is shown:
		`# iqt -p NodeInfo`
		`nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables`
		`A1089.051 tb4-cmp-a tb4-cmp-a,10.240.239.36 Active Unspecified`
		`A1089.106 tb4-cmp-b tb4-cmp-b,10.240.239.x4 Active Unspecified`
		`C0010.058 tb4-mpe-01b tb4-mpe-01b,10.240.239.51 Active Unspecified`
		`C0010.202 tb4-mpe-01a tb4-mpe-01a,10.240.239.x3 Active Unspecified`
		`C0630.121 tb4-mpe-02b tb4-mpe-02b,10.240.239.50 Active Unspecified`
		`C0630.206 tb4-mpe-02a tb4-mpe-02a,10.240.239.x2 Active Unspecified`
		`C1410.098 tb4-mra-a tb4-mra-a,10.240.239.38 Active Unspecified`
		`C1410.135 tb4-mra-b tb4-mra-b,10.240.239.x6 Active Unspecified`

THIS PROCEDURE HAS BEEN COMPLETED		

7. POST UPGRADE ACTIVITIES

To complete an upgrade, complete the procedures in the section 8.1.

7.1 Verify System Upgrade

This procedure is used to verify that the Policy Management 9.x software upgrade was successful.

7.1.1 Procedure 19: Verify System Upgrade

Step	Procedure	Result
1 ☐	Verify System	
2 ☐	1. Access the login prompt. 2. Log into the server as the root user on the iLO or RMM.	`login: root` `Password: <enter password>`
3 ☐	**GUI:** View **Upgrade Manager → System Maintenance**	Add additional Verify steps, based on network specifics and Operator need.
4 ☐		
5 ☐		
THIS PROCEDURE HAS BEEN COMPLETED		

7.2 Additional Instructions

Refer to both the Release Notes for the target release and the Oracle Customer Care Method of Procedure to determine if additional instructions are to be followed to successfully complete the Policy Management 9.x software Upgrade for servers running specific Oracle Applications.

8. BACKOUT (ROLLBACK)

To complete a backout, complete the procedures in this section.

If the Upgrade has succeeded, but an issue is found after upgrade that is causing network impact, then the system can be backed out (rolled back) to the previous release.

NOTE: If an Upgrade fails, it will automatically attempt to backout.

8.1 Backout Order

The backout order is the reverse of the upgrade order:

1. Backout the MRA and MPE clusters
2. Backout the secondary CMP cluster
3. Backout the primary CMP cluster.
    - 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. This MOP uses the 'forced standby' flag to ensure that a server can't become active until the flag is cleared. Setting and clearing the forced standby flag is critical to having an orderly backout. Failing to follow the conventions can lead to loss of service and even possible data corruption.
    - In the case of an MPE/MRA, the upgrade/backout is NOT complete until the operator does a configuration push from the CMP. The MRA/MPE can still operate – to a degree – but it is not fully functional.

8.1.1 Procedure 20: Backout Partially-Upgraded Cluster

This procedure is used to backout a cluster that has been partially upgraded.

Expected Pre-conditions:

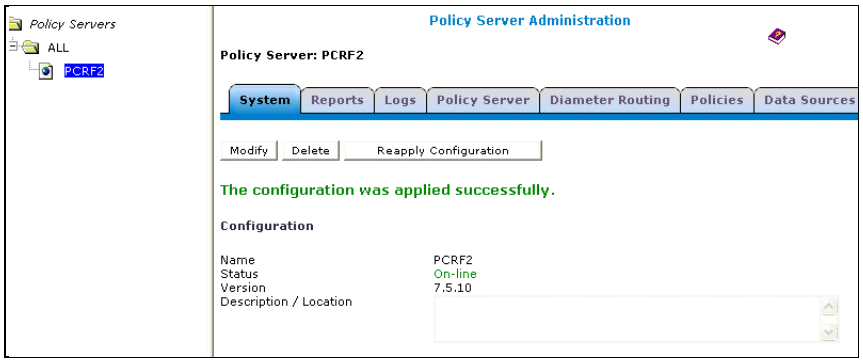
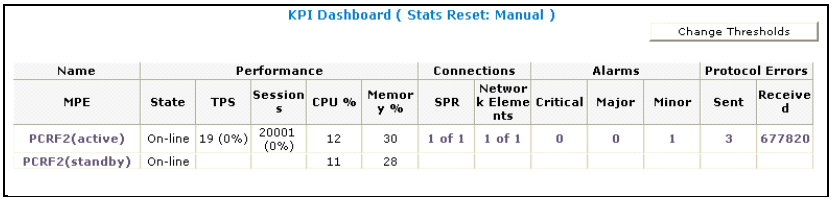
- Primary Active CMP is on 9.x
- Cluster is any of MPE, MRA or Secondary CMP
- One server of target cluster is on 9.x, and Active
- One server of target cluster is on 7.5.x and Force Standby
- At the end of this procedure, both servers of the target cluster will be on 7.5.x, and Active/Standby.

Step	Procedure	Result
1 ☐	**GUI:** Upgrade Manager – Verify cluster status	**Upgrade Manager → System Management** **Confirm status of the cluster to be backed out.**
2 ☐	**GUI:** Upgrade Manager. Switch active server back to 7.5.x Service Affecting for MPE/MRA	IF cluster 9.x server to backout is currently Active -- Execute this step to make 9.x server Force Standby, and make the 7.5.x server Active. [IF 9.x server is already Force Standby, skip this step.] ***IMPORTANT: the current MRA or MPE session data is dropped in this step. The 7.5.x MRA/MPE will start from a clean data set.*** **Upgrade Manager → System Maintenance** Select the checkbox for the partially upgraded (mixed 7.5/9.x) cluster, select - **Operation → Switch ForceStandby**

3 ☐	**GUI:** Upgrade Manager
	Turn off replication
		NOTE: It may need to skip this step for the MRA/MPE backout. Consult TAC to confirm for this step
		GUI:
		Upgrade Manager → System Maintenance View
		Select Checkbox for the standby Server.
		Select **Operation → Turn Off Replication**
		Verify that irepstat shows as Inhibited
		`# irepstat`
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC From cs-tb31-cmp-a  Inhibited  0  0.00 ^`
		`CC From cs-tb31-mpe1-a Inhibited  0  0.00 ^`

4 ☐	**GUI:** Upgrade Manager – Verify cluster status	Verify 7.5.x server is Active.
5 ☐	**GUI:** View KPI Dashboard. Verify 7.5.x server is handling traffic	Verify steps: • KPI Dashboard • View MRA/MPE Report IF there is a problem – Consult with My Oracle Support.

Step	Procedure	Result
6 ☐	**Option 1:** **GUI:** Upgrade Manager. Backout the 9.x server software	Choose Option 1 or Option 2: **Option 1** – use the Upgrade Manager GUI tool to backout 3. **GUI:** Upgrade Manager → System Maintenance 4. Select Checkbox for the Server to be backed out. Current state must be Force Standby 5. Select: **Operation → Backout** Server backout takes several minutes, and the final step will be a re-boot of the server. 6. Verify: **GUI: Upgrade Manager → System Maintenance** Select **Operation → Push Script** - Confirm Upgrade Manager now shows correct release, and - Upgrade status = `Completed: backout was completed at …`
7 ☐	Option 2: SSH: Backout the target 9.x server	**Option 2** – execute backout from ssh root login to target Log into the target 9.x server as root: **# getPolicyRev** **9.x.0_xxx** **# cd /var/TKLC/backout** **# ./ugwrap --backout** **NOTE:** There are two dashs (--) before "backout" **Initializing Upgrade Wrapper...** **Executing any special platform directives** **Setting up application for install/upgrade** **Running backout_server script...** **Starting backout_server...** **Verifying that backout is possible.** **Current platform version: 5.0.1-72.45.0** **Backing out to platform version: 4.2.4-70.90.0** **compare_platform_versions (5.0.1-72.45.0, 4.2.4-70.90.0)** **compare with major upgrade boundary (3.0.0-60.0.0, 4.2.4-70.90.0)** **compare with no backout boundary (4.0.0-70.0.0, 4.2.4-70.90.0)** **Backout Date: 08/10/2012 02:10:24 UTC** **Continue backout? [y/N]:y** **Server backout takes several minutes.** After returning to prompt, verify success: **# tail /var/TKLC/log/upgrade/upgrade.log** **Daemon is not running...** **1344561040::DEBUG: lib/upgrade.sh - app_enable() - APP_ENABLE=[0]** **1344561040::DEBUG: lib/upgrade.sh - app_enable() - MODE_FLAG=[--**

Step	Procedure	Result
		backout] 1344561040:: Enabling applications on the server... 1344561040:: 1344561041:: 1344561042:: 1344561043:: Applications Enabled. 1344561043:: Running /usr/TKLC/plat/bin/service_conf reconfig 1344561045:: Backout is complete. A reboot of the server is now required. # shutdown -r now Verify: After reboot, login and check status of server: # getPolicyRev 7.5_xxx # syscheck # ha.stat
8 ☐	**GUI:** Re-Apply Configuration to MPE/MRA, if needed	• If target is MPE or MRA, Check status on the System Form. • If status shows Mis-Match, re-apply the configuration from the CMP GUI. • For MPE: **Policy Server → Configuration: System → Re-Apply Configuration** • For MRA: **MRA → Configuration: System → Re-Apply Configuration** 
9 ☐	**GUI:** Upgrade Manager – Cancel Force Standby	GUI: **Upgrade Manager → System Maintenance** Select checkbox for the server that is Force Standby **Operation → Cancel Force Standby** Verify status of the server changes to Standby.
10 ☐	**GUI:** Verify cluster is handling traffic as normal	**Verify** • KPI Dashboard  • MPE/MRA Reports • Active Alarms
THIS PROCEDURE HAS BEEN COMPLETED		

8.1.2 Procedure 21: Backout Fully Upgraded MPE/MRA Cluster

This procedure is used to backout a MPE/MRA cluster that has been fully upgraded. i.e. Both servers in the cluster are installed with 9.x and they are Active/Standby.

Pre-conditions:

- Primary Active CMP is on 9.x
- Cluster is any of: MPE, MRA
- One server of target cluster is on 9.x, and Active
- One server of target cluster is on 9.x and either Standby or Force Standby
- At the end of this procedure, both servers of the target cluster will be on 7.5.x, and Active/Standby.

Step	Procedure	Result
1 ☐	**GUI:** Upgrade Manager Set Standby server to Force Standby (Backout first server in cluster)	IF cluster is Active/Standby, set Standby Server to Force Standby. GUI: **Upgrade Manager → System Maintenance View** Select Checkbox for the standby Server. Select **Operation → Force Standby**

2 ☐	**GUI:** Upgrade Manager
	
	Turn off replication
		NOTE: It may need to skip this step for the MRA/MPE backout. Consult TAC to confirm for this step
		
		GUI: **Upgrade Manager → System Maintenance View**
		
		1. Select Checkbox for the standby Server.
		2. Select **Operation → Turn Off Replication**
		3. Verify that irepstat shoes as Inhibited
		
		`# irepstat`
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC From cs-tb31-cmp-a Inhibited 0 0.00 ^`
		`CC From cs-tb31-mpe1-a Inhibited 0 0.00 ^`

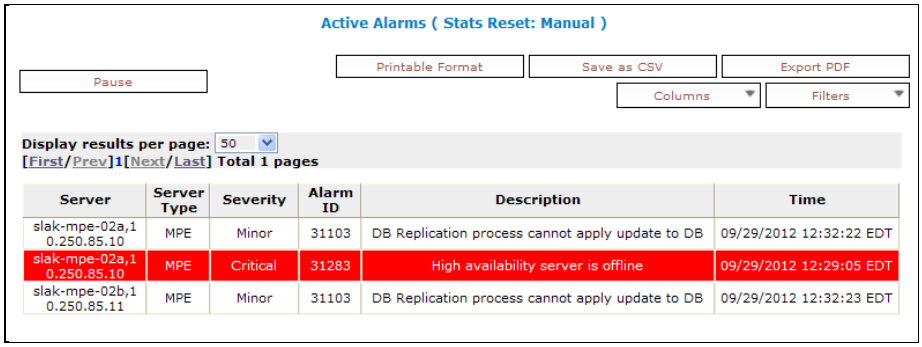
3 ☐	**Option 1:** **GUI:** Upgrade Manager. Backout the 9.x server software (Backout first server in cluster)	Choose Option 1 or Option 2 below, to backout the server: **Option 1** – Use the Upgrade Manager GUI tool to backout GUI: **Upgrade Manager → System Maintenance View** Select checkbox for the Force Standby Server to be backed out. **Operation → Backout** Server backout takes several minutes, and the final step will be a re-boot of the server. Verify: When backout completes, select the server and select: **Operation → Push Script**

Step	Procedure	Result

4 ☐	**Option 2:**
	
	SSH: Backout the target 9.x server
	
	(Backout first server in cluster)
		Option 2 – execute backout from ssh root login to target
		
		Log into the target 9.x server as root:
		
		If using ssh, execute "screen" to prevent hang-ups, and do not exit this screen session until the server reboots.
		
		`# screen`
		
		`# getPolicyRev`
		`9.x.0_xxx`
		`# cd /var/TKLC/backout`
		`# ./ugwrap --backout`
		
		NOTE: There are two dashs (--) before "backout"..
		
		<Answer yes>
		Server backout takes several minutes.
		
		After the backout script completes, it is necessary to reboot the server.
		
		`# shutdown -r now`
		
		Verify:
		
		After reboot, login and check status of server:
		
		`# getPolicyRev`
		`7.5.x_x.x.x`
		`# syscheck`
		`# ha.stat`

5 ☐	**SSH:** Login to active server of the cluster – Wait for Replication sync	`# inetstat`
		
		Before Replication sync
		
		root@slak-mpe-02a:~
		`T dir nodeId inetsync-State dSeq dTime info`
		`AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 71B/s`
		`AC From slak-cmp-a Standby 0 0.00`
		`CC To slak-mpe-02b DownConnecting 0 0.00`
		`CC From slak-mpe-02b DownListening 0 0.00 ^0.01%cpu 0.00B/s`
		
		After Replication sync
		
		root@slak-mpe-02a:~
		`T dir nodeId inetsync-State dSeq dTime info`
		`AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 78B/s`
		`AC From slak-cmp-a Standby 0 0.00`
		`CC To slak-mpe-02b Active 0 0.00 0.00s End Tbl Aud NONE 0.68%cpu 113KB/s`
		`CC From slak-mpe-02b Standby 0 0.00`
		
		Do not proceed until Replication is synced.

6 ☐	**GUI:** Re-Apply Configuration to MPE/MRA	IF target is MPE or MRA, Re-Apply the configuration from the CMP GUI. For MPE: **Policy Server → Configuration: System → Re-Apply Configuration** For MRA: **MRA → Configuration: System → Re-Apply Configuration**

Step	Procedure	Result
7 ☐	GUI: Upgrade Manager	Upgrade Manager → System Maintenance If status is not shown, Select the checkbox for the current Force Standby MPE of the partially upgraded (mixed 7.5/9.x) cluster, and Select **Operation → Push Script** Verify the Upgrade Status: `Completed:backout was completed at 09/29/2012 12:26:22`
8 ☐	**GUI:** Verify Alarms	 Active Alarms (Stats Reset: Manual) Pause Printable Format Save as CSV Export PDF Columns Filters Display results per page: 50 [First/Prev]1[Next/Last] Total 1 pages Server | Server Type | Severity | Alarm ID | Description | Time slak-mpe-02a,10.250.85.10 | MPE | Minor | 31103 | DB Replication process cannot apply update to DB | 09/29/2012 12:32:22 EDT slak-mpe-02a,10.250.85.10 | MPE | Critical | 31283 | High availability server is offline | 09/29/2012 12:29:05 EDT slak-mpe-02b,10.250.85.11 | MPE | Minor | 31103 | DB Replication process cannot apply update to DB | 09/29/2012 12:32:23 EDT
9 ☐	**Cluster is now Partially Upgraded (one server 9.x, and one server 7.5.x)**	The Backed out 7.5.x server is Force Standby. ***IMPORTANT: Do not remove Force Standby.*** ***A 9.x server and a 7.5.x cannot be Active/Standby. One must remain in the Force Standby state.***
10 ☐	**GUI: Upgrade Manager** Switch active server to 7.5.x Service Affecting for MPE/MRA	**Upgrade Manager → System Maintenance** Select the checkbox for the partially upgraded (mixed 7.5/9.x) cluster, and Select - **Operation → Switch ForceStandby** 7.5.x server is made Active ***IMPORTANT: The current MRA or MPE state data is dropped in this step, unless the previous State Data recovery steps were performed.***
11 ☐	**GUI:** Upgrade Manager – Verify cluster status	**Upgrade Manager → System Maintenance** Verify failover is completed, and 7.5.x server is Active.
12 ☐	**GUI:** Verify 7.5.x (Active) server is handling Traffic	The backed out 7.5.x server should be handling traffic. **Verify** View KPI Dashboard on the GUI IF there is a problem – Consult with My Oracle Support.
13 ☐	**Option 1: GUI: Upgrade Manager.** Backout the 9.x server software	Choose Option 1 or Option 2: **Option 1 –** use the Upgrade Manager GUI tool to backout View **Upgrade Manager → System Maintenance** Select checkbox for the server to be backed out, current state must be `Force Standby` **Operation → Backout** Server backout takes several minutes, and the final step will be a re-boot of the server. **Verify** Confirm Upgrade Manager shows server of correct release

Step	Procedure	Result
14 ☐	Option 2: SSH: Backout the target 9.x server	**Option 2** – execute backout from ssh root login to target Log into the target 9.x server as root: If using ssh, run the `screen` command to prevent hang-ups, and do not exit this screen session until the server reboots. **# screen** **# getPolicyRev** **9.x.0_xxx** **# cd /var/TKLC/backout** **# ./ugwrap --backout** **NOTE:** There are two dashes (--) before backout. <Answer yes> Server backout takes several minutes. **….** **mysql stopped** **Installing JDK with option --nomd5** **No JDK backout package found, ignoring...** **#** **# shutdown -r now** **Verify** After reboot, login and check status of server: **# getPolicyRev** **7.5_xxx** **# syscheck** **# ha.stat**
15 ☐	GUI: Re-Apply Configuration to MPE/MRA	IF target is MPE or MRA, re-apply the configuration from the CMP GUI. For MPE: **Policy Server → Configuration: System → Re-Apply Configuration** For MRA: **MRA → Configuration: System → Re-Apply Configuration**
16 ☐	**GUI: Upgrade Manager –** Verify Backout completed	**Upgrade Manager → System Maintenance** If status is not show, Select the checkbox for the current Force Standby MPE of the partially upgraded (mixed 7.5/9.x) cluster, and select **Operation → Push Script** Verify the Upgrade Status: **Completed:backout was completed at 09/29/2012 12:26:22**
17 ☐	**SSH: Primary Active CMP** – Verify replication sync	**# inetstat** root@slak-mpe-02a:~ T dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 57B/s AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b Standby 0 0.00 CC From slak-mpe-02b Active 0 0.00 ^0.27%cpu 134KB/s . . .

Step	Procedure	Result
18 ☐	**GUI: Upgrade Manager –** Verify Backout completed	**Upgrade Manager → System Maintenance** Select Force Standby Server, and select **Operation → Cancel Force Standby** Verify the server state becomes Standby.
THIS PROCEDURE HAS BEEN COMPLETED		

8.1.3 Procedure 22: Backout Fully Upgraded CMP Cluster

This procedure is used to backout a CMP cluster that has been fully upgraded. i.e. Both servers in the cluster are installed with 9.x and they are Active/Standby.

Pre-conditions:

- All MPE/MRA servers in the network are on 7.5
- Cluster is any of: CMP Primary or Secondary site
- One server of target cluster is on 9.x, and Active
- One server of target cluster is on 9.x and either Standby or Force Standby
- At the end of this procedure, both servers of the target cluster will be on 7.5.x, and Active/Standby.

Step	Procedure	Result
1 ☐	**GUI:** Upgrade Manager Set Standby server to Force Standby (Backout first server in cluster)	IF cluster is Active/Standby, set Standby Server to Force Standby. **GUI:** **Upgrade Manager → System Maintenance View** Select Checkbox for the standby Server. Select **Operation → Force Standby**
2 ☐	**Option 1:** **GUI:** Upgrade Manager. Backout the 9.x server software (Backout first server in cluster)	Choose Option 1 or Option 2 below, to Backout the server: **Option 1** – use the Upgrade Manager GUI tool to backout **GUI:** **Upgrade Manager → System Maintenance View** Select Checkbox for the Force Standby Server to be backed out. **Operation → Backout** Server backout takes several minutes, and the final step will be a re-boot of the server. **Verify** When Backout completes, select the server and select: **Operation → Push Script**

Step	Procedure	Result
3 ☐	Option 2: SSH: Backout the target 9.x server (Backout first server in cluster)	**Option 2** – execute backout from ssh root login to target Log into the target 9.x server as root: If using ssh, run the `screen` command to prevent hang-ups, and do not exit this screen session until the server reboots. **# screen** **# getPolicyRev** **9.x.0_xxx** **# cd /var/TKLC/backout** **# ./ugwrap --backout** **NOTE:** There are two dashs (--) before "backout".. <Answer yes> Server backout takes several minutes. After the backout script completes, it is necessary to reboot the server. **# shutdown -r now** **Verify** After reboot, login and check status of server: **# getPolicyRev** **7.5.x_x.x.x** **# syscheck** **# ha.stat**
4 ☐	**SSH:** Login to active server of the cluster – Wait for Replication sync	**# inetstat** Before Replication sync root@slak-mpe-02a:~ T dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 71B/s AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b DownConnecting 0 0.00 CC From slak-mpe-02b DownListening 0 0.00 ^0.01%cpu 0.00B/s . . After Replication sync root@slak-mpe-02a:~ T dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 78B/s AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b Active 0 0.00 0.00s End Tbl Aud NONE 0.68%cpu 113KB/s CC From slak-mpe-02b Standby 0 0.00 . . ***Do Not proceed until Replication is synced.***
5 ☐	**GUI:** Upgrade Manager	**Upgrade Manager → System Maintenance** If status is not shown, Select the checkbox for the current Force Standby MPE of the partially upgraded (mixed 7.5/9.x) cluster, and select **Operation → Push Script** Verify the Upgrade Status: **Completed:backout was completed at 09/29/2012 12:26:22**

Step	Procedure	Result
6 ☐	**GUI:** Verify Alarms	Active Alarms (Stats Reset: Manual) Pause Printable Format Save as CSV Export PDF Columns Filters **Display results per page:** 50 [First/Prev]1[Next/Last] **Total 1 pages** **Server** / **Server Type** / **Severity** / **Alarm ID** / **Description** / **Time** slak-mpe-02a,10.250.85.10 / MPE / Minor / 31103 / DB Replication process cannot apply update to DB / 09/29/2012 12:32:22 EDT slak-mpe-02a,10.250.85.10 / MPE / Critical / 31283 / High availability server is offline / 09/29/2012 12:29:05 EDT slak-mpe-02b,10.250.85.11 / MPE / Minor / 31103 / DB Replication process cannot apply update to DB / 09/29/2012 12:32:23 EDT
7 ☐	Cluster is now Partially Upgraded (one server 9.x, and one server 7.5.x)	The Backed out 7.5.x server is Force Standby. ***IMPORTANT: Do not Remove Force Standby. A 9.x server and a 7.5.x cannot be Active/Standby. One must remain in the Force Standby state.***
8 ☐	**GUI:** Upgrade Manager Switch active server to 7.5.x	• IF cluster 9.x server to backout is currently Active -- Execute this step to make 9.x server Force Standby, and make the 7.5.x server Active. • IF 9.x server is already Force Standby, skip this step. Login to Primary Active CMP as root `# policyUpgrade.pl --failover <target_CMP_Hostname>`

Step	Procedure	Result
9 ☐	SSH: Backout the target 9.x server	Execute backout from ssh root login to target Login to the target 9.x server as root: If using ssh, execute `screen` to prevent hang-ups, and do not exit this screen session until the server reboots. **# screen** **# getPolicyRev** **9.x.0_xxx** **# cd /var/TKLC/backout** **# ./ugwrap --backout** **NOTE:** There are two dashes (--) before "backout".. **<Answer yes>** **Server backout takes several minutes.** **….** **mysql stopped** **Installing JDK with option --nomd5** **No JDK backout package found, ignoring...** **#** **# shutdown -r now** Verify: After reboot, login and check status of server: **# getPolicyRev** **7.5_xxx** **# syscheck** **# ha.stat**
10 ☐	**SSH: Primary Active CMP** – Verify replication sync	**# inetstat** root@slak-mpe-02a:~ T dir nodeId inetsync-State dSeq dTime info AC From slak-cmp-b Active 0 0.00 ^0.02%cpu 57B/s AC From slak-cmp-a Standby 0 0.00 CC To slak-mpe-02b Standby 0 0.00 CC From slak-mpe-02b Active 0 0.00 ^0.27%cpu 134KB/s . . .
11 ☐	**GUI:** Upgrade Manager – Remove Force Standby	**Network → Topology** Select CMP cluster Modify Server – remove Force Standby check
THIS PROCEDURE HAS BEEN COMPLETED		

8.2 Backout of prepareUpgrade Command

This procedure performs a backout of the prepareUpgrade command, that was executed before the first CMP was upgraded. It removes the replication exclusion step. It is only executed after all MPE/MRA servers and all CMPs, are backed out.

Pre-conditions:

- All servers in the Policy system are on 7.5.x
- The "prepareUpgrade" action from procedure to Upgrade the first CMP was previously executed.

8.2.1 Procedure 23: Remove Replication Exclusions (Backout of prepareUpgrade Command)

Step	Procedure	Result

1 ☐	**SSH:** Primary Active CMP
	
	Verify Exclusions need to be removed
		`# iqt -p NodeInfo`
		
		`nodeId nodeName hostName inhibitFlag nodeCap excludeTables`
		
		`A3411.121 slak-cmp-b slak-cmp-b,10.250.85.26 MasterCapable LongParam,AppEventDef`
		
		`A3411.190 slak-cmp-a slak-cmp-a,10.250.85.25 H MasterCapable LongParam,AppEventDef`
		
		`C1428.038 slak-mpe-07a slak-mpe-07a,10.250.85.28 MasterCapable LongParam,AppEventDef`
		
		`C1428.073 slak-mpe-07b slak-mpe-07b,10.250.85.29 MasterCapable LongParam,AppEventDef`
		
		`C3265.167 slak-mra-b slak-mra-b,10.250.85.5 MasterCapable LongParam,AppEventDef`
		
		`C3265.212 slak-mra-a slak-mra-a,10.250.85.4 MasterCapable LongParam,AppEventDef`
		
		`C3573.020 slak-mpe-01a slak-mpe-01a,10.250.85.7 MasterCapable LongParam,AppEventDef`
		
		`C3573.027 slak-mpe-01b slak-mpe-01b,10.250.85.8 MasterCapable LongParam,AppEventDef`
		
		IF the exclusions "LongParam,AppEventDef" are seen, then proceed.

2 ☐	**SSH:** Primary Active CMP Remove Replication table exclusions	Remove Replication exclusions "LongParam,AppEventDef" for all nodes `# ivi NodeInfo` You are now in a "vi" editor session. Use standard "vi" edit commands to proceed.

Step	Procedure	Result

3 ☐	**SSH:** Active CMP
	
	ivi NodeInfo
		Initial edit screen may look like this:
		
		`#!/bin/sh`
		
		`iload -ha -xU -fnodeId -fnodeName -fhostName -finhibitFlag -fnodeCap \`
		
		`-fexcludeTables NodeInfo \`
		
		`<<'!!!!'`
		
		`A0853.107|brbg-cmp-a|brbg-cmp-a,10.250.84.25||MasterCapable| LongParam,AppEventDef`
		
		`A0853.244|brbg-cmp-b|brbg-cmp-b,10.250.84.26||MasterCapable| LongParam,AppEventDef`
		
		`A1408.065|slak-cmp-b|slak-cmp-b,10.250.85.26||MasterCapable|`
		
		`A1408.213|slak-cmp-a|slak-cmp-a,10.250.85.25||MasterCapable| LongParam,AppEventDef`
		
		`C0371.030|brbg-mpe-01b|brbg-mpe-01b,10.250.84.8||MasterCapable| LongParam,AppEventDef`
		
		`C0371.252|brbg-mpe-01a|brbg-mpe-01a,10.250.84.7||MasterCapable| LongParam,AppEventDef`
		
		`C1533.011|slak-mpe-01a|slak-mpe-01a,10.250.85.7||MasterCapable| LongParam,AppEventDef`
		
		`C1533.125|slak-mpe-01b|slak-mpe-01b,10.250.85.8||MasterCapable| LongParam,AppEventDef`
		
		`C1751.030|slak-mra-a|slak-mra-a,10.250.85.4||MasterCapable| LongParam,AppEventDef`
		
		`C1751.145|slak-mra-b|slak-mra-b,10.250.85.5||MasterCapable| LongParam,AppEventDef`
		
		`C2080.054|brbg-mra-a|brbg-mra-a,10.250.84.4||MasterCapable| LongParam,AppEventDef`
		
		`C2080.221|brbg-mra-b|brbg-mra-b,10.250.84.5||MasterCapable| LongParam,AppEventDef`
		
		`C2399.016|brbg-mpe-07a|brbg-mpe-07a,10.250.84.28||MasterCapable| LongParam,AppEventDef`
		
		`C2399.048|brbg-mpe-07b|brbg-mpe-07b,10.250.84.29||MasterCapable| LongParam,AppEventDef`
		
		`C3701.051|slak-mpe-07a|slak-mpe-07a,10.250.85.28||MasterCapable| LongParam,AppEventDef`
		
		`C3701.117|slak-mpe-07b|slak-mpe-07b,10.250.85.29||MasterCapable| LongParam,AppEventDef`
		
		`!!!!`

Step	Procedure	Result

4 ☐	SSH: Active CMP
	
	ivi NodeInfo
	Edit to remove Exclusions for all clusters
		After edit, the screen may look like this:
		
		`#!/bin/sh`
		
		`iload -ha -xU -fnodeId -fnodeName -fhostName -finhibitFlag -fnodeCap \`
		
		`-fexcludeTables NodeInfo \`
		
		`<<'!!!!'`
		
		`A0853.107|brbg-cmp-a|brbg-cmp-a,10.250.84.25||MasterCapable|`
		
		`A0853.244|brbg-cmp-b|brbg-cmp-b,10.250.84.26||MasterCapable|`
		
		`A1408.065|slak-cmp-b|slak-cmp-b,10.250.85.26||MasterCapable|`
		
		`A1408.213|slak-cmp-a|slak-cmp-a,10.250.85.25||MasterCapable|`
		
		`C0371.030|brbg-mpe-01b|brbg-mpe-01b,10.250.84.8||MasterCapable|`
		
		`C0371.252|brbg-mpe-01a|brbg-mpe-01a,10.250.84.7||MasterCapable|`
		
		`C1533.011|slak-mpe-01a|slak-mpe-01a,10.250.85.7||MasterCapable|`
		
		`C1533.125|slak-mpe-01b|slak-mpe-01b,10.250.85.8||MasterCapable|`
		
		`C1751.030|slak-mra-a|slak-mra-a,10.250.85.4||MasterCapable|`
		`C1751.145|slak-mra-b|slak-mra-b,10.250.85.5||MasterCapable|`
		`C2080.054|brbg-mra-a|brbg-mra-a,10.250.84.4||MasterCapable|`
		
		`C2080.221|brbg-mra-b|brbg-mra-b,10.250.84.5||MasterCapable|`
		
		`C2399.016|brbg-mpe-07a|brbg-mpe-07a,10.250.84.28||MasterCapable|`
		`C2399.048|brbg-mpe-07b|brbg-mpe-07b,10.250.84.29||MasterCapable|`
		
		`C3701.051|slak-mpe-07a|slak-mpe-07a,10.250.85.28||MasterCapable|`
		
		`C3701.117|slak-mpe-07b|slak-mpe-07b,10.250.85.29||MasterCapable|`
		
		`!!!!`

5 ☐	**SSH:** ivi NodeInfo Save or Quit the NodeInfo table	IF it was needed to Edit the Table: Save and quit • Exit ivi using the command `'ZZ' or ':wq'` (no quotes) • Answer 'y' to the question: `APPLY THE CHANGES [yn]?` IF no edit was needed: Quit: • Exit ivi using the command `':q'` (no quotes)
6 ☐	**SSH:** Primary Active CMP – Verify Exclusions are removed from previous step.	`# iqt -p NodeInfo`
7 ☐	Verify Health	Verify Alarms
THIS PROCEDURE HAS BEEN COMPLETED		

8.2.2 Procedure 24: Backout of Replication Activation

This procedure performs a backout of the Replication Activation.

It must be applied to all servers, if the Replication Activation procedure was previously performed, and any MPE/MRA server clusters need to be backed out to the 7.5 release.

Pre-conditions:

- All servers in the Policy system are previously upgraded to the 9.x Release
- Some or all servers had the "Upgrade Completion" applied (which activated the new replication).

Step	Procedure	Result
1 ☐	**GUI:** Open CMP GUI	Login to CMP GUI as Administrator (or as Upgrade Engineer, if an account is defined for this).
2 ☐	**SSH:** Open ssh session to Primary Active CMP server 1. Access the login prompt. 2. Log into the server as the root user	`login: root` `Password: <enter password>`

3 ☐	**SSH:** Verify which servers have been set to Upgrade Completion	`# iqt -p NodeInfo`
		`[root@slak-cmp-a approximatelty ]# iqt -p NodeInfo`
		`nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables`
		`A2548.105 slak-cmp-b slak-cmp-b,10.250.85.8 Active Unspecified`
		`A2548.142 slak-cmp-a slak-cmp-a,10.250.85.7 Active Unspecified`
		`C0699.106 slak-mpe-03a slak-mpe-03a,10.250.85.13 Active Unspecified`
		`C0699.238 slak-mpe-03b slak-mpe-03b,10.250.85.14 Active Unspecified`
		`C3238.095 slak-mpe-02a slak-mpe-02a,10.250.85.10 Active Unspecified`
		`C3238.203 slak-mpe-02b slak-mpe-02b,10.250.85.11 Active Unspecified`
		`C3310.177 slak-mra-a slak-mra-a,10.250.85.4 Active Unspecified`
		`C3310.194 slak-mra-b slak-mra-b,10.250.85.5 Active Unspecified`
		The servers with the Exclusions set to "" indicate that these servers had "Upgrade Completion".
		Servers with Exclusions "LongParam,AppEventDef" have not been completed.
		Only servers with Exclusions set to "" need to be backout out. Make a list of these.

4 ☐	**GUI:** Confirm Upgrade status of all sites and servers	**Upgrade Manager → System Maintenance** `Confirm in the "Running Release" column that all servers in the network are upgraded to 9.x.`
5 ☐	**GUI:** Change Replication mode: CMPs (One cluster at a time)	If one of more CMP clusters need to be backout out. Do Primary Site First, then Secondardy Site. **Upgrade Manager → System Maintenance** Select CMP cluster 1. Select the checkbox for the **Standby CMP server**, and execute: **Operation → Undo Upgrade Completion** 2. Select the checkbox for the **Active CMP server**, and execute: **Operation → Undo Upgrade Completion**

Step	Procedure	Result
6 ☐	**SSH:** CMP Active Server	Verify that the Legacy Replication is active on the cluster: `# inetstat`
7 ☐	**GUI:** Change Replication mode: MPEs (One cluster at a time)	**Upgrade Manager → System Maintenance** Select MPE cluster 1. Select the checkbox for the **Standby MPE server**, and execute: **Operation → Undo Upgrade Completion** 2. Select the checkbox for the **Active MPE server**, and execute: **Operation → Undo Upgrade Completion** REPEAT for other MPE clusters to backout.
8 ☐	**GUI:** Change Replication mode: MRAs	**Upgrade Manager → System Maintenance** Select Secondary-Site MRA cluster 1. Select the checkbox for the **Standby CMP server**, and execute: **Operation → Undo Upgrade Completion** 2. Select the checkbox for the **Active CMP server**, and execute: **Operation → Undo Upgrade Completion** REPEAT for other MRA clusters to backout.
9 ☐	**GUI:** Verify Active Alarms	**System Wide Reports → Active Alarms** All Upgrade related alarms should be cleared.
10 ☐	**SSH:** Primary Active CMP, confirm that replication to MPE/MRAs is Active/Standby	`# inetstat` root@slak-cmp-b:~ -- Policy 0 ActStb [DbReplication] ---------- AA To slak-cmp-a Active 0 0.00 0.05%cpu 51B/s AC To slak-mpe-03a Active 0 0.00 0.05%cpu 71B/s AC To slak-mpe-03b Active 0 0.00 0.04%cpu 83B/s AC To slak-mpe-02a Active 0 0.00 0.04%cpu 87B/s AC To slak-mpe-02b Active 0 0.00 0.05%cpu 54B/s AC To slak-mra-a Active 0 0.00 0.05%cpu 67B/s AC To slak-mra-b Active 0 0.00 0.04%cpu 58B/s

Step	Procedure	Result

11 ☐	**SSH:** Primary Active CMP, confirm that exclustions are added	Verify that the Replication exclusions "LongParam,AppEventDef" are added in the NodeInfo Table
		`# iqt -p NodeInfo`
		`nodeId nodeName hostName inhibitFlag nodeCap excludeTables`
		`A3411.121 slak-cmp-b slak-cmp-b,10.250.85.26 MasterCapable LongParam,AppEventDef`
		`A3411.190 slak-cmp-a slak-cmp-a,10.250.85.25 H MasterCapable LongParam,AppEventDef`
		`C1428.038 slak-mpe-07a slak-mpe-07a,10.250.85.28 MasterCapable LongParam,AppEventDef`
		`C1428.073 slak-mpe-07b slak-mpe-07b,10.250.85.29 MasterCapable LongParam,AppEventDef`
		`C3265.167 slak-mra-b slak-mra-b,10.250.85.5 MasterCapable LongParam,AppEventDef`
		`C3265.212 slak-mra-a slak-mra-a,10.250.85.4 MasterCapable LongParam,AppEventDef`
		`C3573.020 slak-mpe-01a slak-mpe-01a,10.250.85.7 MasterCapable LongParam,AppEventDef`
		`C3573.027 slak-mpe-01b slak-mpe-01b,10.250.85.8 MasterCapable LongParam,AppEventDef`

THIS PROCEDURE HAS BEEN COMPLETED		

8.2.3 Procedure 25: Recovery of Server from Backup

This procedure is used to recover a server that is in an unknown state, as a result of Upgrade/Backout activities. In this procedure, the server will be installed again as 7.5.x, and the needed data recovered from a previous backup.

It is assumed that the application on the server is not active (Out-of-Service).

Before taking this step, consult with My Oracle Support.

Expected Pre-conditions:

- Primary Active CMP is 7.5.x or 9.x
- Either both servers of the cluster are Out-of-Service, or just one server is Out-of-Service
- At the end of this procedure, one server will be recovered to 7.5.x from Backup, and may be Active or Standby.

Step	Procedure	Result
1 ☐	Caution	**CAUTION:** Do not remove the affected server from the Topology forms on the CMP GUI. ***Modification of the Topology forms is not supported during upgrade activities.***

Step	Procedure	Result

2 ☐	**Console/iLo/PMAC:** Clean Install server (re-install TPD OS)	At this step, the purpose is clean any disk areas previously used, and re-install the TPD OS.
		Access a login on the server, and perform these commands:
		`# service qp_procmgr stop`
		`# prod.stop`
		`# getPlatRev`
		If the plat rev is 4.0, then:
		`# ./usr/TKLC/plat/sbin removeVG --scrub`
		If the plat rev is 5.0, then:
		`# ./usr/TKLC/plat/sbin storageClean lvm --vgName=vgroot --level=scrub`
		If PMAC is available, use PMAC to Install OS on the server.
		If PMAC is not available, then:
		3. Access iLo/RMM port of server, and start remote Console.
		4. Mount the TPD OS ISO on the server (either CD drive, or iLo Virtual Mount).
		`# shutdown -r now`
		`boot: <enter boot command for the server>`

3 ☐	**Console/iLo/PMAC:** Install the Application	If PMAC is available, use PMAC to install (Upgrade) the Application. If PMAC is not available, Mount the Application ISO on the server (either CD drive, or iLo Virtual Mount). `# su - platcfg` **Maintenance → Upgrade**
4 ☐	**Console/iLo:** Copy server backup to the server.	Use iLo access to transfer the Backup file to the server.
5 ☐	**Console/iLo:** Execute Restore from Backup	`# su – platcfg` Execute Restore Wait for boot
6 ☐	**GUI:** Confirm server is synced to the CMP.	**Platform Administration → Topology** View the cluster from the Topology form, to confirm that the re-installed server is detected.
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX A. MANAGING HA STATUS OF SERVERS

A.1 Understanding the ha.states and ha.mystate commands

IMPORTANT: ha.stat command is no longer supported in Rel 9.x.

It is replaced with 2 commands:

- ha.mystate
- ha.states

The ha.states or ha.mystate command is executed as root on any of the CMP, MRA or MPE servers.

It reports the High Availability status of the clustered servers, or just the single server, respectively.

The ha.states command refreshes the status every second, and will run continually until the user exits with a cntl-C.

The ha.mystate command runs once and exits. Both have the same data format.

This is the example of the normal display of these commands on a server which is fully clustered:

During the upgrade from 7.x to9.x, following will be output as applicable, as DbReplication_old will still be active/standby as per the active/standby server:

Active:

```
root@tb4-mpe-02b:~
[root@tb4-mpe-02b ~]# ha.mystate
          resourceId   role         node       subResources      lastUpdate
       DbReplication Active    C0630.121                  0 0521:070621.781
                 VIP Active    C0630.121                  0 0521:070621.850
                  QP Active    C0630.121                  0 0521:070621.783
   DbReplication_old Active    C0630.121                  0 0521:070621.780
[root@tb4-mpe-02b ~]#
```

Standby:

```
root@tb4-mpe-02a:~
[root@tb4-mpe-02a ~]# ha.mystate
          resourceId   role         node       subResources      lastUpdate
       DbReplication   Stby    C0630.206                  0 0521:071805.158
                 VIP   Stby    C0630.206                  0 0521:071805.070
                  QP   Stby    C0630.206                  0 0521:071805.037
   DbReplication_old   Stby    C0630.206                  0 0521:071935.872
[root@tb4-mpe-02a ~]#
```

ha.states:

```
root@tb4-mpe-02a:~
          resourceId   role         node       subResources      lastUpdate
       DbReplication   Stby    C0630.206                  0 0521:071805.158
       DbReplication Active    C0630.121                  0 0521:070621.781
                 VIP   Stby    C0630.206                  0 0521:071805.070
                 VIP Active    C0630.121                  0 0521:070621.850
                  QP   Stby    C0630.206                  0 0521:071805.037
                  QP Active    C0630.121                  0 0521:070621.783
   DbReplication_old   Stby    C0630.206                  0 0521:071935.872
   DbReplication_old Active    C0630.121                  0 0521:070621.780
```

During upgrade from 9.x.y to 9.z.a.ha.mystate command output will be similar to the following:

```
root@cs-tb31-cmp-bay3:~
[root@cs-tb31-cmp-bay3 ~]# ha.mystate
          resourceId   role         node       subResources      lastUpdate
      DbReplication Active    A0804.231                  0 0529:090223.383
                VIP Active    A0804.231                  0 0529:090223.407
                 QP Active    A0804.231                  0 0529:090226.867
   DbReplication_old    OOS    A0804.231                  0 0529:090328.074
[root@cs-tb31-cmp-bay3 ~]#
```

ha.states command output:

```
root@cs-tb31-cmp-bay3:~
          resourceId   role         node       subResources      lastUpdate
      DbReplication   Stby    A0804.136                  0 0529:090329.994
      DbReplication Active    A0804.231                  0 0529:090223.383
                VIP   Stby    A0804.136                  0 0529:090330.008
                VIP Active    A0804.231                  0 0529:090223.407
                 QP   Stby    A0804.136                  0 0529:090332.502
                 QP Active    A0804.231                  0 0529:090226.867
   DbReplication_old    OOS    A0804.136                  0 0529:090329.675
   DbReplication_old    OOS    A0804.231                  0 0529:090328.074
.
```

There are several key fields in the ha.states.

- Resource – function on the Node that is being reported: QP (Application), Replication, and IP VIP ownership
- Role – Status of HA relationship for the Resource: Active, Standby, OOS
- NodeId – Identifier used in the software for this specific Node instance

In the Normal condition:

- One server will show Active for QP, Replication and VIP
- Other server will show Standby for QP, Replication and VIP
- The same ha.states status will be reported from both servers in the cluster

APPENDIX B. METHODS OF DELIVERING SOFTWARE UPGRADE ISO

There are several methods to deliver the Software ISO to the server.

The above Upgrade procedure assumes scp is used.

In this appendix is a list of several other methods that may be useful.

IMPORTANT: There should be a TPD DVD and Application DVD left on-site, to aid in re-installing a server after a field repair.

B.1 Copy ISO from USB Key

It is possible to put the upgrade ISO on a USB key, and use this to load the ISO to the server.

To do this:

1. USB must be formatted with FAT 32, and at least 1G
2. Copy ISO to USB key, from a laptop or any computer
3. Insert USB key to server
4. Mount to /mnt/upgrade
5. Copy the ISO file to /var/TKLC/upgrade.
6. Unmount USB and remove

B.2 Copy ISO from DVD {PP5160, DL360}

If a three Application DVDs are delivered to a site (CMP, MRA, MPE), but there multiple servers to be upgraded, it may be useful to extract the ISO from the DVD, and copy to the servers that need it, prior to the Maintenance interface.

As long as the ISO is placed in the /var/TKLC/upgrade directory, the Upgrade will find the ISO, and use it for the installation.

B.2.1 Procedure 26: Upgrade from Physical CD media {PP5160, DL360}

Step	Procedure	Result
1 ☐	Insert Policy Management 9.x Upgrade CD	Insert media in CD-ROM tray

2 ☐	1. Access the login prompt.
	2. Log into the server as the root user on the iLO or RMM.
		`CentOS release 4.6 (Final)`
		`Kernel 2.6.18-1.2849prerel3.3.0_63.1.0 on an i686`
		
		`localhost login: root`
		`Password: <root_password>`

3 ☐	Verify ISO images do not already exist by examining contents of /var/TKLC/upgrade directory.	If ISO image files exist you will need to remove them
		`# ls -al /var/TKLC/upgrade`
		`total 16`
		`dr-xr-xr-x  2 root root 4096 Oct 22 16:31 .`
		`dr-xr-xr-x 21 root root 4096 Oct 18 13:40 ..`
		`#`

4 ☐	Determine the physical device name.
	The primary physical device will be the first device listed. In the example it is device hda.
		`# getCDROM`
		`SONY DVD RW AW-G540A|hda`
		`Intel(R) RMM2 VDrive 2|scd0`
		`Intel(R) RMM2 VDrive 3|scd1`
		`Intel(R) RMM2 VDrive 4|scd2`
		`Intel(R) RMM2 VDrive 1|scd3`

5 ☐	Mount the physical media	`# mount /dev/<dev> /mnt/upgrade`
		Example:
		`# mount /dev/hda /mnt/upgrade`

6 ☐	Validate physical media
	Verify that the command output indicates the `CDROM is Valid`.
		`# /mnt/upgrade/upgrade/.validate/validate_cd`
		Below is an example of the command output. Actual values returned may vary depending on version of software and firmware installed.
		`Validating cdrom...`
		`UMVT Validate Utility v1.10.0, (c)Oracle, January 2009`
		`Validating /var/TKLC/upgrade/872-2069-02-1.1.0_70.36.0_SUP35.iso`
		`Date&Time: 2010-03-18 14:21:16`
		`Volume ID: 872-2069-02_Rev_A;70.36.0`
		`Part Number: 872-2069-02_Rev_A`
		`Version: 70.36.0`
		`Disc Label: TPD`
		`Disc description: TPD`
		`The media validation is complete, the result is: PASS`
		
		`CDROM is Valid`
		NOTE: Do not continue if CD validation reports any errors or is invalid until new physical media can be obtained.

Step	Procedure	Result
7 ☐	Change to the upgrade directory	`# cd /var/TKLC/upgrade`

8 ☐	Verify enough space exists for ISO	Verify that there is at least 600M in the Avail column. If not, clean up files until there is space available.
		
		Make sure you know what files you can remove safely before cleaning up. It is recommended that you only clean up files in the `/var/TKLC/upgrade` directory as this is a platform owned directory that should only contain ISO images. This directory should not be expected to contain images for any length of time as they can get purged. Removing files other than those in directory `/var/TKLC/upgrade` is potentially dangerous.
		
		`# df -h /var/TKLC`
		`Filesystem  Size  Used Avail Use% Mounted on`
		`/dev/md8  4.0G  89M  3.7G  3% /var/TKLC`

9 ☐	Copy ISO	`# cp /mnt/upgrade/*.iso /var/TKLC/upgrade`
10 ☐	Remove CD	Remove media in CD-ROM tray
11 ☐	Procedure to ISO image validation	Go to to Procedure 6: Verify CMP Software Images.
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX C. INSTALL PMAC 5.0 ON A C-CLASS SYSTEM

This section includes procedures to perform a new install of PMAC 5.0 on an existing pre-5.0 PMAC server.

PMAC 5.0 is deployed on a Virtual OS (TVOE) environment. The TVOE OS must be installed first, and then the PMAC application ISO is installed. Because there is only a small amout of configuration data needed for PMAC, this approach is recommended over a PMAC Migration procedure.

PMAC install is not service affecting for the Policy system.

NOTE: In Policy Rel 9.x, PMAC is used for Installation activities, growth of new servers and Field repair activities. It is also used for deploying Firmware upgrades.

C.1 Preparations for Installation

The following steps will collect information/data needed for PMAC backout procedure, if needed.

- Prepare Networking Information
- Perform Health checks
- Save Backups

Using the installation site survey or the configuration profile, make note of the network configuration of the Management Server in the Network Layout Workseet below.

This configuration information may be used to re-create the network configuration on the TVOE installation. This is not an exhaustive list of required network settings and may duplicate information in the detailed site survey. Not all of the rows will be filled.

To save the details of a device/bond, execute the following commands at the PMAC 3.x shell.

Table 4. Network Configuration capture

Values	Command
Network Address	`# cat /etc/sysconfig/network-scripts/ifcfg-`*<interface>*
	…
Netmask	`NETMASK=255.255.255.0`
	…
IP Address	`IPADDR=169.254.116.4`
	`NETWORK=169.254.116.0`
Slave Interfaces	`# cat /proc/net/bonding/`*<bond>* `|grep Interface`
	`Slave Interface: eth01`
	`Slave Interface: eth02`
Role	`# pmacadm getNetworkInterfaces`
	`Device Name : bond0`
	`Network Id  : 1`
	`IP Address  : 169.254.116.4`
	`Description : Control network for blades`
	`Device Name : bond0.2`
	`Network Id  : 2`
	`IP Address  : 10.240.4.5`
	`Description : PMC Management`
	`Device Name : bond1`
	`Network Id  : 3`
	`IP Address  : 10.240.6.220`
	`Description : Netbackup interface`
	`# pmacadm getNetworkRoles`
	`NetworkRole Id : 1`
	`Network Role  : control`
	`Network Id  : 1`
	`NetworkRole Id : 2`
	`Network Role  : management`
	`Network Id  : 2`
	`NetworkRole Id : 3`
	`Network Role  : netbackup`
	`Network Id  : 3`
NTP Server IP Address	`# grep ntp /etc/hosts`
	`10.250.32.10  ntpserver1`
SNMP NMS IP address/community string	Using platcfg, navigate to the following configuration form: **Network Configuration → SNMP Configuration → NMS Configuration**

Table 5. Network Layout Worksheet

Bond/Interface	Slave interfaces	Network Address	Netmask	IP address	Role control, management, netbackup, etc.
bond0					control
		_____	_____	_____	
		<Ctrl_net_addr>	**<Ctrl_netmask >**	**<Ctrl_ip_addr>**	**<Ctrl_bridge>**
		For Segregated network environments			
bond1					management
		_____	_____	_____	
		<Mgmt_net_addr>	**<Mgmt_netmask >**	**<Mgmt_ip_addr>**	**<Mgmt_bridge>**
bond2					netbackup
		_____	_____	_____	
		<NB_net_addr>	**<NB_netmask >**	**<NB_ip_addr>**	**<NB_bridge>**
bond3	_____				
	_____				
		For non-segregated network environments			
Tagged bond interface _____					management
		_____	_____	_____	
		<Mgmt_net_addr>	**<Mgmt_netmask >**	**<Mgmt_ip_addr>**	**<Mgmt_bridge>**
Tagged bond interface _____					netbackup
		_____	_____	_____	
		<NB_net_addr>	**<NB_netmask >**	**<NB_ip_addr>**	**<NB_bridge>**
Tagged bond interface _____					

C.1.1 Procedure 27. PMAC Health Check

This procedure provides instructions on how to perform a healthcheck on the Management Server hosting the PMAC application.

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

If this procedure fails, contact My Oracle Support and ask for ASSISTANCE.

Step	Procedure	Result
1 ☐	If necessary, access the PMAC server command prompt	If necessary, access the Management Server command prompt.

2 ☐	At the command prompt, run the `sentry status` command to verify the status of the PMAC application.	`[root@foo-1060101-a approximatelty ]# sentry status`
		`sending status command...`
		`PM&C Sentry Status`
		`------------------`
		
		`sentryd started: Thu May 31 07:47:31 2012`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`------------------ ------ ----------- ------------------------- ----`
		`smacTalk 5932 running Sun Dec 6 07:47:31 2009 1`
		`smacMon 5935 running Sun Dec 6 07:47:31 2009 1`
		`hpiPortAudit 5951 running Sun Dec 6 07:47:31 2009 1`
		`snmpEventHandler 5962 running Sun Dec 6 07:47:31 2009 1`
		`eclipseHelp 5971 running Sun Dec 6 07:47:31 2009 2`
		
		`Thu June 7 11:09:44 2012`
		`Command Complete.`
		`[root@foo-1060101-a approximatelty ]#`

3 ☐	At the command prompt, run alarmMgr.	`[root@foo-1060101-a approximatelty ]#alarmMgr –alarmStatus` `[root@foo-1060101-a approximatelty ]#`
4 ☐	If any error messages are displayed by the alarmMgr command, if sentry shows any PMAC processes not running, or alarmMgr shows any failures, then there is a problem with the Management Server or PMAC application. Contact My Oracle Support for information on how to proceed.	If sentry shows any PMAC processes not running, then the healthcheck was not successful. Contact My Oracle Support for information on how to proceed. Otherwise, if alarmMgr shows no alarms and sentry shows all processes running, then PMAC appears to be running normally.
THIS PROCEDURE HAS BEEN COMPLETED		

C.1.2 Procedure 28. Backup the PMAC Application Data

This procedure backs up all necessary PMAC data.

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

Should this procedure fail, contact My Oracle Support and ask for UPGRADE ASSISTANCE.

Step	Procedure	Result
1 ☐	Optional: Insert a blank optical media	Optional: Insert a blank optical media into the optical drive of the Management Server.
2 ☐	Access the Management Server command prompt	Access the Management Server command prompt as detailed in Appendix A, Accessing the Management Server Command Prompt.

3 ☐	Get special files for backup	`# mkdir /usr/TKLC/smac/etc/4.0migration`
		`# cp /usr/TKLC/plat/etc/vlan.conf /usr/TKLC/smac/etc/4.0migration/`
		NOTE: vlan.conf is an optional file, and my not exist on all servers.
		Although the use of switchconfig, which uses the `vlan.conf` file, is deprecated, there may be useful data in this file. The netConfig tool does not use this file.
		`# hponcfg -a -w ilo_backup`
		`HP Lights-Out Online Configuration utility`
		`Version 4.0.0 Pass 6 (c) Hewlett-Packard Company, 2011`
		`Firmware Revision = 2.09 Device type = iLO 2 Driver name = hpilo`
		`Management Processor configuration is successfully written to file "ilo_backup"`
		`# cp ilo_backup /usr/TKLC/smac/etc/4.0migration/`
		`# pmaccli getProvCabinets > capture_pmac_info`
		`# pmaccli getProvEnclosures >> capture_pmac_info`
		`# pmacadm getNetworkInterfaces > capture_networkInterfaces`
		`# pmacadm getNetworkRoles > capture_networkRoles`
		`# grep ntp /etc/hosts > capture_ntp`
		`# cp capture* /usr/TKLC/smac/etc/4.0migration/`

4 ☐	Perform a backup	Execute only one of the following, based on backup method and blank optical media type.
		For file backup:
		`[root@pmac]# pmacadm backup`
		For CD backup:
		`[root@pmac]# pmacadm backup --media=CD-R`
		For DVD-R backup:
		`[root@pmac]# pmacadm backup --media=DVD-R`
		For DVD+R backup:
		`[root@pmac]# pmacadm backup --media=DVD+R`

Step	Procedure	Result
5 ☐	When the backup is finished, remove and label the PMAC backup disk.	Navigate to the Task Monitoring page on the PMAC GUI. Verify the backup task completes successfully. Copy the backup file to save safe location (usb or another server): `copy the resulting .pef` Or, remove the optical disk from the optical drive of the Management Server and label it `PMAC 3.2 backup`.
6 ☐	Manually back up any ISO images.	The migration will not include ISO images provisioned on the PMAC. Navigate to **Software →Manage Software Images** page in the GUI, to see a list of the software provisioned on the PMAC. If the loss of the existing ISO images is not a problem, then no ISO backups need to be done, they will be removed from the provisioned data (reported in Task Monitoring) if they are not found after the migration. If loss of any of these ISO images is unacceptable, copy the desired ISO images from the PMAC server to a secure remote location using any method available (scp, ftp, sftp, etc.)
7 ☐	Record the host name for later use.	Record the host name of the Management Server for later use.
THIS PROCEDURE HAS BEEN COMPLETED		

C.2 Installation of PMAC 5.0

The following procedure will clean install the PMAC server to use PMAC 5.0. All existing data on the server will be removed.

C.2.1 Procedure c-1. Install TVOE 2.0 on Management Server (DL360/DL380)

This procedure will install TVOE 2.0 on the Management Server

NEEDED MATERIAL:

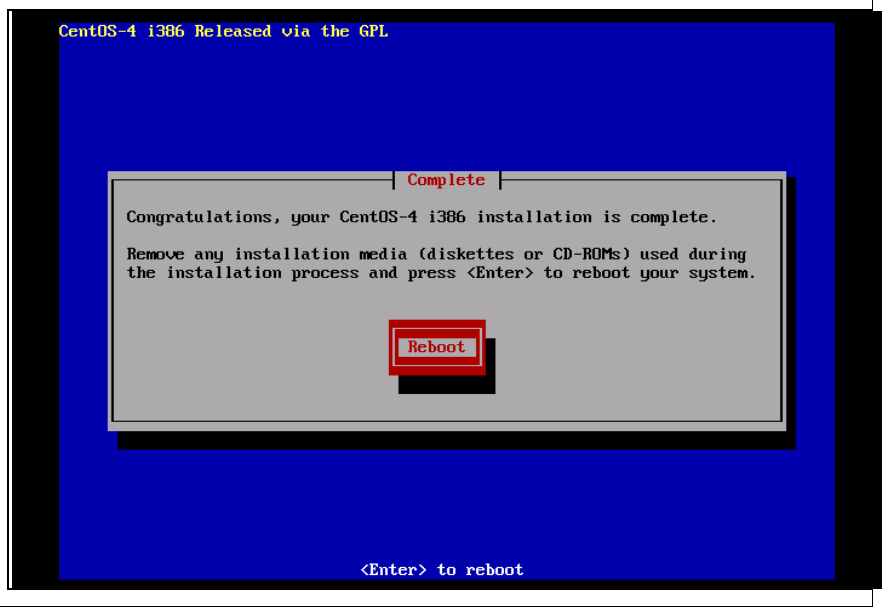
- TVOE 2.0 Media

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

If this procedure fails, contact My Oracle Support and ask for ASSISTANCE.

Step		Procedure	Result
1	☐	Connect to the Server	Connect to the Server using a VGA Display and USB Keyboard, or via the iLO interface using IE.
2	☐	Insert TVOE Media into Server	3. Insert TVOE media in the optical drive. (You can also attach the TVOE ISO to the iLO). 4. Restart the server `# shutdown -r now`

3	☐	Begin IPM Process	Once the Server reboots, it will reboot from the TVOE media and a boot prompt shall be displayed.
			IPM the server using the following command:
			• For a DL360/G5 server:
			`TPDnoraid console=tty0`
			• For a DL360/G6/G7/Gen8 or DL380 G6 server:
			`TPDnoraid diskconfig=HPHW,force console=tty0`

4	☐	IPM Complete	The IPM process takes about 30 minutes, you will see several messages and screens in the process. Once the IPM is complete, you will be prompted to press Enter as shown below. Remove the disk from the drive or unmount the TPD image from the iLO and press **Enter** to reboot the server. The CD may eject automatically. 

5 ☐	**Server Reboot**	Once the Server Reboots, you should see a login prompt. During the first system boot, swap files may be initialized and activated. Each swap file will take about 2 minutes. If no login prompt is displayed after waiting 15 minutes, contact Oracle Customer Support for Assistance.
THIS PROCEDURE HAS BEEN COMPLETED		

C.2.2 Procedure c-2. Upgrade Management Server Firmware

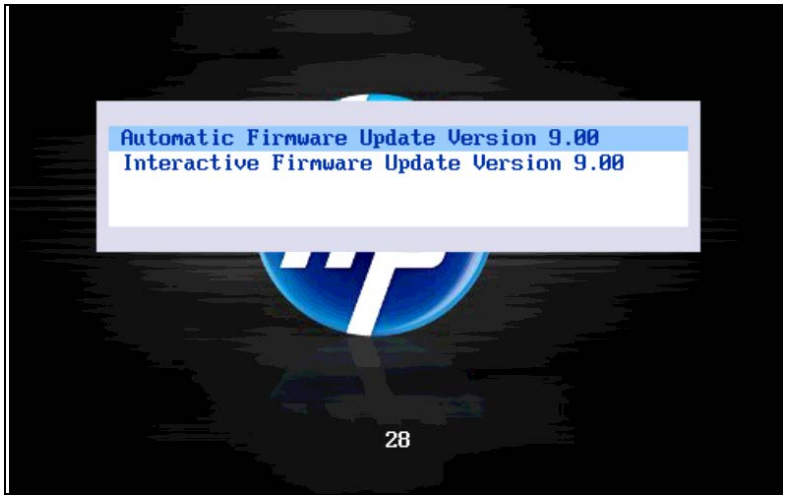
This procedure will upgrade the DL360 or DL380 server firmware

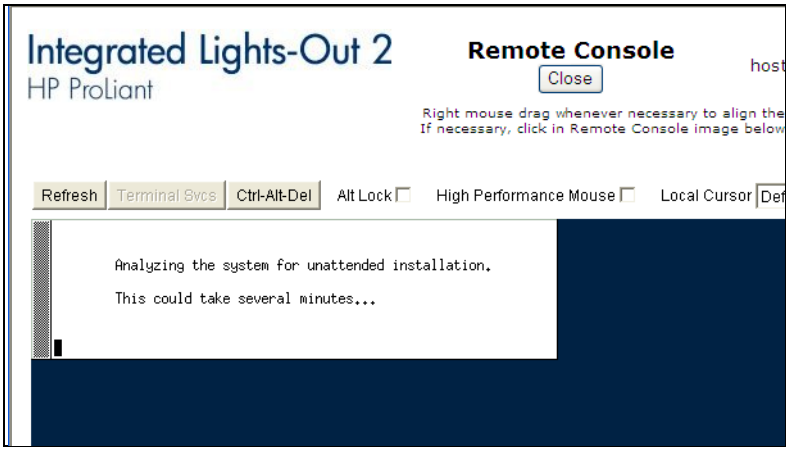
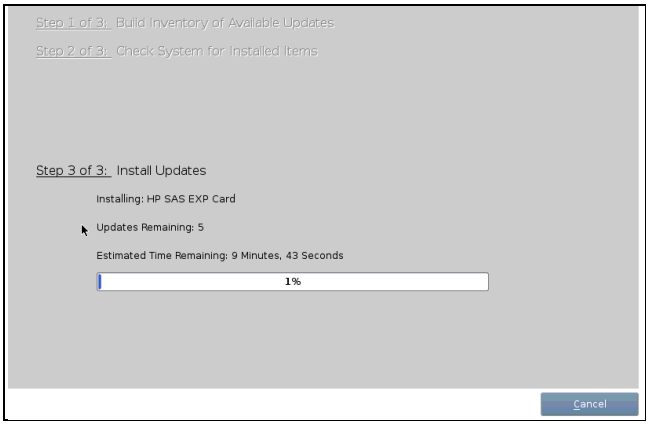
NEEDED MATERIAL:

- HP Firmware Maintenance CD/DVD
- HP Solutions Firmware Upgrade Pack Release Notes

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

If this procedure fails, contact My Oracle Support and ask for ASSISTANCE.

Step	Procedure	Result
1 ☐	**Management server iLO:** Prepare to upgrade DL360 or DL380 server firmware	1. Insert HP Smart Update Firmware DVD into the removable media drive of the DL360 or DL380 server. 2. Launch web based iLO: use IE. 3. Launch the **Integrated Remote Console** on the server. 4. Click **Yes** if the Security Alert pops up.
2 ☐	**Management server iLO:** Restart the DL360 or DL380 server	In the integrated remote console, log into the server as root if needed, and run: `# shutdown -r now`
3 ☐	**Remote Console:** Perform an unattended firmware upgrade	The server will reboot and open the HP Smart Update Firmware ISO and present the following boot prompt. Press **Enter** to select the **Automatic Firmware Update** procedure.  ***If no key is pressed in 30 seconds the system will automatically perform an Automatic Firmware Update.***

Step	Procedure	Result
4 ☐	**Remote Console:** System analysis	The firmware install will perform a system scan of the server in which it will identify all of the firmware components that are eligible for upgrade. This process may take up to 10 minutes and during that time the following screen is displayed on the console.  **NOTE:** No progress indication is displayed during the system scan and analysis stage. In about 10 minutes the installation will automatically proceed to the next step.
5 ☐	**Remote Console:** Monitor installation	Once analysis is complete the installer will begin to upgrade the eligible firmware components. A progress indicator is display at this time as shown below.  **NOTE:** If the iLO2 firmware is to be upgraded it will be upgraded last. At this point the iLO2 session will be terminated and you will lose the remote console, virtual media and Web GUI connections to the server. This is expected and will not impact the firmware upgrade process.
6 ☐	**Local Workstation:** Clean up	Once the firmware updates have been completed the server will automatically be rebooted. At this time you may close the remote console and the iLO2 Web GUI browser session.
7 ☐	**Local Workstation:** Verify server availability	Wait 3 to 5 minutes and verify the server has rebooted and is available by gaining access to the login prompt.
8 ☐	**Management server iLO:** Remove the firmware CD	Remove the HP Smart Update Firmware DVD from the removable media drive. Exit from the **Integrated Remote Console**.
THIS PROCEDURE HAS BEEN COMPLETED		

C.2.3 Procedure c-3. TVOE/Management Server Network Configuration

This procedure will configure the Network on the TVOE/Management Server

PREREQUISITE: *Procedure c-1. Install TVOE 2.0 on Management* Server has been completed.

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

If this procedure fails, contact My Oracle Support and ask for ASSISTANCE.

Refer to the table below to determine the Ethernet port names to use throughout this procedure based on the hardware type and configuration.

Network Interface	DL360 (w/o HP NC364T 4pt Gigabit)	DL360 (with HP NC364T 4pt Gigabit in PCI Slot 2)	DL380	DL380 (with HP NC364T 4pt Gigabit in PCI Slot 3)
<ethernet_interface_1>	eth01	eth01	eth01	eth01
<ethernet_interface_2>	eth02	eth02	eth02	eth02
<ethernet_interface_3>		eth21	eth03	eth03
<ethernet_interface_4>		eth22	eth04	eth04
<ethernet_interface_5>		eth23		eth31

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>1 ☐</td><td>Determine Bridge names and interfaces</td><td>Determine the bridge name to be used on the TVOE management server for the management network and fill in the <TVOE_Management_Bridge> and <TVOE_Management_Bridge_Interface> values in the table below.

If netbackup is to be used, determine the bridge name to be used for the netbackup network and fill in the <TVOE_NetBackup_Bridge> and <TVOE_NetBackup_Bridge_Interface> values in the table below:
<table>
<tr><th>PMAC Interface Alias</th><th>TVOE Bridge Name</th><th>TVOE Bridge Interface</th></tr>
<tr><td>control</td><td>control</td><td>Fill in the appropriate value (default is bond0):
_____
<TVOE_Control_Bridge_Interface></td></tr>
<tr><td>management</td><td>Fill in the appropriate value: (default is management)
_____
<TVOE_Management_Bridge></td><td>Fill in the appropriate value: (example: bond0.2)
_____
<TVOE_Management_Bridge_Interface></td></tr>
<tr><td>Netbackup
(if applicable)</td><td>Fill in the appropriate value: (default is netbackup)
_____
<TVOE_NetBackup_Bridge></td><td>Fill in the appropriate value: (example: bond2)
_____
<TVOE_NetBackup_Bridge_Interface></td></tr>
</table></td></tr>
</table>

Step	Procedure	Result
2 ☐	**Management server iLO:** Login and launch the integrated remote console	5. Log in to iLO in IE using password provided by application: `http://<management_server_iLO_ip>` 6. Click the **Remote Console** tab and launch the **Integrated Remote Console** on the server. 7. Click **Yes** if the Security Alert pops up.

3 ☐	**Management server iLO:** Verify the Control Network	Verify the control network by running the following command
		NOTE: The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		`# netAdm query --type=Bridge --name=control`
		`Bridge Name: control`
		`On Boot: yes`
		`Protocol: dhcp`
		`Persistent: yes`
		`Promiscuous: no`
		`Hwaddr: 00:24:81:fb:29:52`
		`MTU:`
		`Bridge Interface: bond0`
		If the bridge has been configured, skip to the next step.
		If not, add and configure the bridge.
		NOTE: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.
		Add control bridge (<TVOE_Control_Bridge>).
		`# netAdm add --device=bond0`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_Control_Bridge_Interface> added`
		
		`# netAdm set --device=eth01 --type=Ethernet`
		`--master=<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes`
		`Interface <ethernet_interface_1> updated`
		
		`# netAdm set --device=eth02 --type=Ethernet`
		`--master-<TVOE_Control_Bridge_Interface> --slave=yes`
		`--onboot=yes`
		`Interface <ethernet_interface_2> updated`
		
		`# netAdm add --type=Bridge --name=control --bootproto=dhcp --onboot=yes`
		`--bridgeInterfaces=<TVOE_Control_Bridge_Interface>`

Step	Procedure	Result

4 ☐	**Management server iLO:** Create tagged control interface and bridge (optional)	If you are using a tagged control network interface on this PMAC, then complete this step. Otherwise, skip on to the next step.
		`# netAdm set --type=Bridge --name=control --delBridgeInt=bond0`
		`Interface bond0 updated`
		`Bridge control updated`
		
		`# netAdm add --device=<TVOE_Control_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_Control_Bridge_Interface> created`
		
		`# netAdm set --type=Bridge --name=control`
		`--bridgeInterfaces=<TVOE_Control_Bridge_Interface> --bootproto=none --address=192.168.1.2 --netmask=255.255.255.0`

Step	Procedure	Result

5 ☐	**Management server iLO:** Verify the Management Network	Verify if the management network has been configured, by running the following command
		
		NOTE: The output below is for illustrative purposes only. The example output below shows the management bridge configured.
		
		`# netAdm query --type=Bridge --name=management`
		`Bridge Name: management`
		`On Boot: yes`
		`Protocol: none`
		`IP Address: 10.240.4.86`
		`Netmask: 255.255.255.0`
		`Promiscuous: no`
		`Hwaddr: 00:24:81:fb:29:52`
		`MTU:`
		`Bridge Interface: bond0.2`
		
		If the bridge has been configured as needed, skip to the next step.
		
		NOTE: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.
		
		EXAMPLE 1
		
		Create Management bridge using tagged interface on bond0.
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface> --onboot=yes`
		
		`# netAdm add --type=Bridge --name=<TVOE_Management_Bridge>`
		`--address=<Management_Server_TVOE_IP> --netmask=<Management_Server_TVOE_Netmask> --onboot=yes`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`
		
		EXAMPLE 2
		
		Create Management bridge using untagged interfaces (eth03 and eth04) with bonding (<*TVOE_Management_Bridge*>).
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface>`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_Management_Bridge_Interface> added`
		`# netAdm set --device=<ethernet_interface_3> --type=Ethernet`
		`--master=<TVOE_Management_Bridge_Interface> --slave=yes --onboot=yes`
		`Interface <ethernet_interface_3> updated`
		`# netAdm set --device=<ethernet_interface_4> --type=Ethernet`
		`--master-<TVOE_Management_Bridge_Interface> --slave=yes`
		`--onboot=yes`
		`Interface <ethernet_interface_4> updated`
		`# netAdm add --type=Bridge --name=<TVOE_Management_Bridge>`
		`--bootproto=none --onboot=yes --address=<Management_Server_TVOE_IP> --netmask=<Management_Server_TVOE_Netmask>`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`

6 ☐	**Management server iLO:** Verify the NetBackup Network (Optional)	Verify the netbackup network. If the NetBackup feature is not needed, skip to the next step. **NOTE:** The output below is for illustrative purposes only. The example output below shows

Step	Procedure	Result

		the control bridge configured.
		`# netAdm query --type=Bridge --name=netbackup`
		`Bridge Name: netbackup`
		`On Boot: yes`
		`Protocol: none`
		`IP Address: 10.240.6.2`
		`Netmask: 255.255.255.0`
		`Promiscuous: no`
		`Hwaddr: 00:24:81:fb:29:58`
		`MTU:`
		`Bridge Interface: bond2`
		If the bridge has been configured as needed, skip to the next step.
		NOTES:
		• The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.
		• The example below illustrates a TVOE management server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size.
		• The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.
		EXAMPLE 1
		Create NetBackup bridge using tagged interface on bond0.
		`# netAdm add --device=<TVOE_NetBackup_Bridge_Interface>`
		`# netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>`
		`--onboot=yes --MTU=<NetBackup_MTU_size>`
		`--bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>`
		EXAMPLE 2
		For this example, create NetBackup bridge using untagged interfaces (eth05 and eth06) and bonding. (<*TVOE_NetBackup_Bridge*>).
		`# netAdm add --device=<TVOE_NetBackup_Bridge_Interface> --onboot=yes`
		`--type=Bonding --mode=active-backup --miimon=100`
		`--MTU=<NetBackup_MTU_size>`
		`Interface <TVOE_NetBackup_Bridge_Interface> added`
		`# netAdm set --device=<ethernet_interface_5> --type=Ethernet`
		`--master=<TVOE_NetBackup_Bridge_Interface> --slave=yes`
		`--onboot=yes`
		`Interface <ethernet_interface_5> updated`
		`# netAdm set --device=<ethernet_interface_6> --type=Ethernet`
		`--master-<TVOE_NetBackup_Bridge_Interface> --slave=yes --onboot=yes`
		`Interface <ethernet_interface_6> updated`

Step	Procedure	Result

		`# netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>`
		`--onboot=yes --MTU=<NetBackup_MTU_size>`
		`--bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>`

7 ☐	**Management server iLO:** Verify the Default Route	**NOTE:** The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		`# netAdm query --route=default --device=management`
		`Routes for TABLE: main and DEVICE: management`
		`* NETWORK: default`
		`GATEWAY: 10.240.4.1`
		If the route has been configured, skip to the next step.
		NOTE: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.
		For this example add default route on management network.
		`# netAdm add --route=default --device=<TVOE_Management_Bridge>`
		`--gateway=<mgmt_gateway_address>`
		`Route to <TVOE_Management_Bridge> added`

8 ☐	**Management server iLO:** Restart the network interfaces	Restart the network interfaces `# service network restart`
9 ☐	**Management server iLO:** Set Hostname	Set the server hostname by running the following: `# su - platcfg` 1. Navigate to **Server Configuration → Hostname → Edit**. 2. Set TVOE Management Server hostname 3. Click **OK**. 4. Navigate out of Hostname
10 ☐	**Management server iLO:** Set the time zone and/or hardware clock	1. Navigate to **Server Configuration → Time Zone**. 2. Select Edit. 3. Set the time zone and/or hardware clock. 4. Click **OK**. 5. Navigate out of Server Configuration `[Accept H/W clock for GMT]`
11 ☐	**Management server iLO:** Set NTP	1. Navigate to **Network Configuration → NTP**. 2. Set NTP server IP address to point to the customer provided NTP server. 3. Click **OK**. 4. Exit platcfg.
THIS PROCEDURE HAS BEEN COMPLETED		

C.2.4 Procedure c-4. PMAC Deployment Procedure

This procedure will deploy PMAC on the TVOE Host

PREREQUISITE: Procedure c-3. TVOE/Management Server Network Configuration has been completed.

NOTE: Use the following command to delete a TOVE guest (in the example below, the guest name is "pmac"):

```
# guestMgr --remove pmac
```

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

If this procedure fails, contact My Oracle Support and ask for ASSISTANCE.

Step	Procedure	Results
1 ☐	**Management server iLO:** Login and launch the integrated remote console	Log in to iLO in IE using password provided by application: `http://<management_server_iLO_ip>` Click **Remote Console** and launch the Integrated Remote Console on the server. Click **Yes** if the Security Alert pops up.

2 ☐	**Management server iLO:** Mount the PMAC media to the TVOE Management server	If using a DVD media, insert the pmac DVD into the optical drive and execute the following to get the Optical Drive letter and mount it:
		`# getCDROM`
		`DV-W28E-RW|sr0`
		`/dev/sr0`
		`# mount -t iso9660 /dev/sr0 /mnt/upgrade/`
		If using an ISO image, run the following to mount it:
		`# mount -o loop ISO_FILENAME.iso /mnt/upgrade`

Step	Procedure	Results

3 ☐	**Management server iLO:** deploy PMAC	Using the pmac-deploy script, deploy the PMAC instance using the configuration captured during the site survey.
		`# cd /mnt/upgrade/upgrade`
		If deploying PMAC without netbackup feature, run the following command:
		`# ./pmac-deploy --guest=<PMAC_Name>`
		`--hostname=<PMAC_Name>`
		`--controlBridge=<TVOE_Control_Bridge>`
		`--controlIP=<PMAC_Control_ip_address>`
		`--controlNM=<PMAC_Control_netmask>`
		`--managementBridge=<PMAC_Management_Bridge>`
		`--managementIP=<PMAC_Management_ip_address>`
		`--managementNM=<PMAC_Management_netmask>`
		`--routeGW=<PMAC_Management_gateway_address>`
		`--ntpserver=<TVOE_Management_server_ip_address>`
		If deploying PMAC with netbackup feature, run the following command:
		`# ./pmac-deploy --guest=<PMAC_Name>`
		`--hostname=<PMAC_Name>`
		`--controlBridge=<TVOE_Control_Bridge>`
		`--controlIP=<PMAC_Control_ip_address>`
		`--controlNM=<PMAC_Control_netmask>`
		`--managementBridge=<PMAC_Management_Bridge>`
		`--managementIP=<PMAC_Management_ip_address>`
		`--managementNM=<PMAC_Management_netmask>`
		`--routeGW=<PMAC_Management_gateway_address>`
		`--ntpserver=<TVOE_Management_server_ip_address>`
		`--bridge=<TVOE_NetBackup_Bridge>`
		`--nic=netbackup`
		The PMAC will deploy and boot. The management and control network will come up based on the settings that were provided to the pmac-deploy script.

4 ☐	**Management server iLO:** Unmount the media	The media should auto-unmount, if it does not, unmout the media using the following command:
		`# cd /`
		`# umount /mnt/upgrade`
		If using a DVD media, remove it from the optical drive.

Step	Procedure	Results

5 ☐	**Management server iLO:** SSH into the Management Server	Using an SSH client such as putty, ssh to the TVOE host using root credentials.
		Login using `virsh`, and wait until you see the login prompt :
		`virsh # list`
		`Id Name State`
		`----------`
		`13 myTPD running`
		`20 pmacdev7 running`
		
		`virsh # console pmacdev7`
		
		`[Output Removed]`
		
		`Starting ntdMgr: [ OK ]`
		`Starting atd: [ OK ]`
		`'TPD Up' notification(s) already sent: [ OK ]`
		`upstart: Starting tpdProvd...`
		`upstart: tpdProvd started.`
		`CentOS release 6.2 (Final)`
		`Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.14.0.x86_64 on an x86_64`
		`pmacdev7 login:`

6 ☐	**Management server iLO:** Set the PMAC timezone	Determine the TimeZone to be used for the PMAC
		NOTE: Valid time zones can be found on the server in the directory `/usr/share/zoneinfo`. Only the time zones within the sub-directories (i.e. America, Africa, Pacific, Mexico, etc…..) are valid with platcfg.
		`# set_pmac_tz.pl <timezone>`
		For example
		`# set_pmac_tz.pl America/New_York`
		Verify that the timezone has been updated:
		`# date`
		NOTE: CHECK PMAC DATE WITH TVOE DATE – NEED TO MATCH

7 ☐	**Management server iLO:** Reboot the server	Reboot the server by running: `# init 6`
THIS PROCEDURE HAS BEEN COMPLETED		

C.2.5 Procedure c-5. Configure the PMAC Server

This procedure will provide PMAC configuration using the web interface.

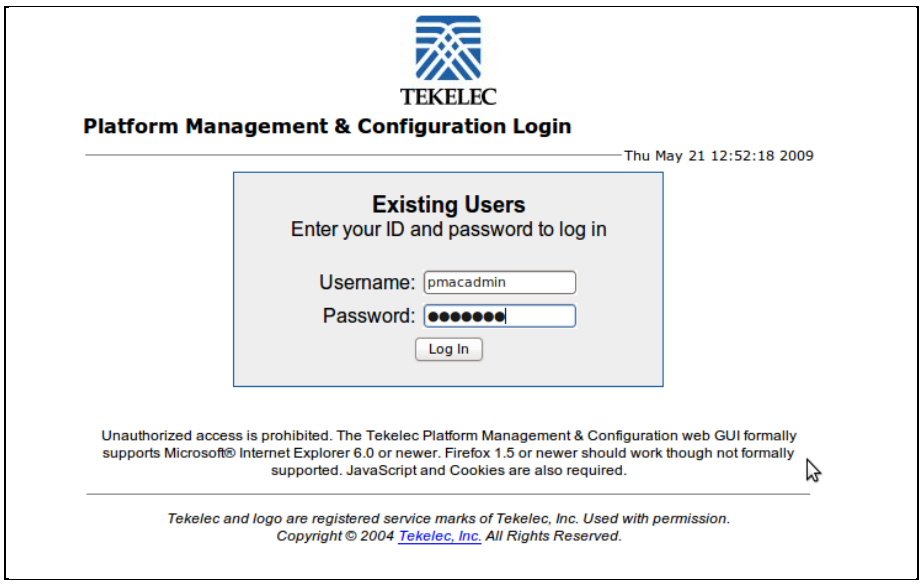
PREREQUISITE: Procedure c-4. PMAC Deployment Procedure has been completed.

NOTES:

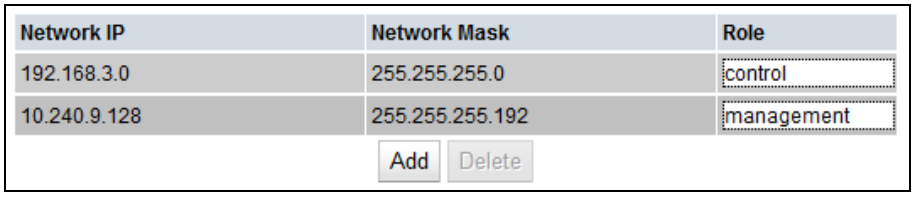
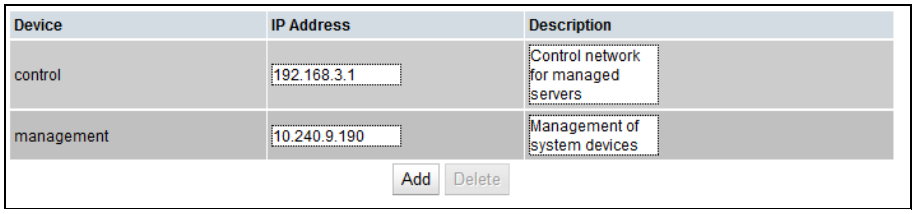
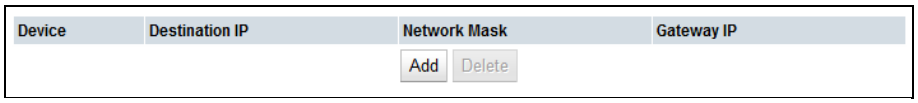
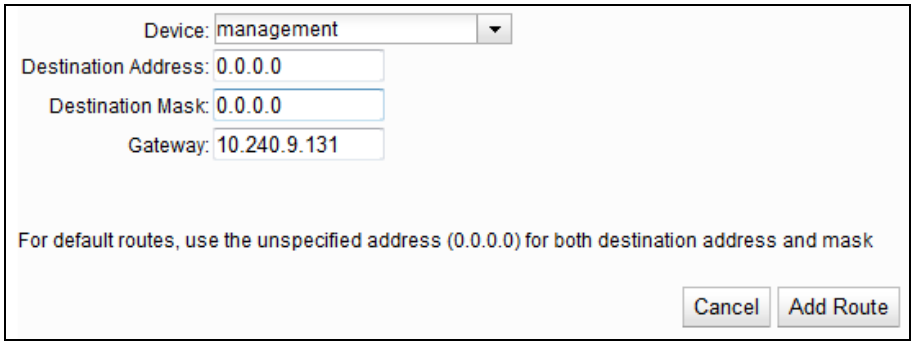
- The installer must be knowledgeable of the network. If you make mistake, click Cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail.
- After you have completed an initialization, the network parameters can no longer be changed through the GUI. If you need to reset any of the network information, you must run the `pmacadm resetProfileConfig` command in the PMAC shell. This will delete the existing configuration and allow you to run through the initialization wizard again. Keep in mind that the reset will not run until all provisioned enclosures and cabinets are deleted

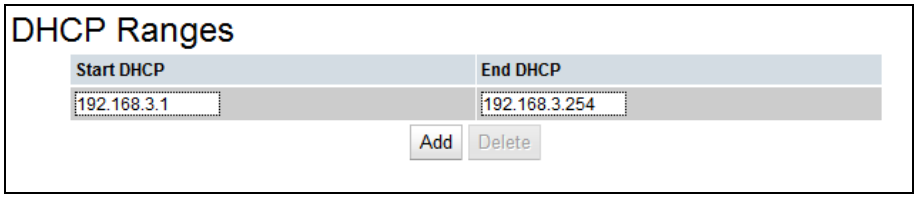
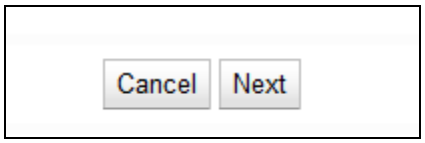
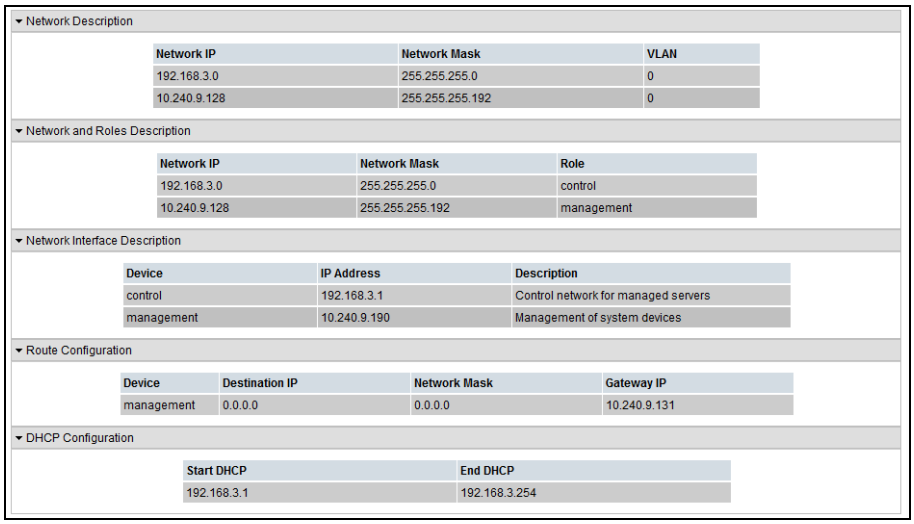
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

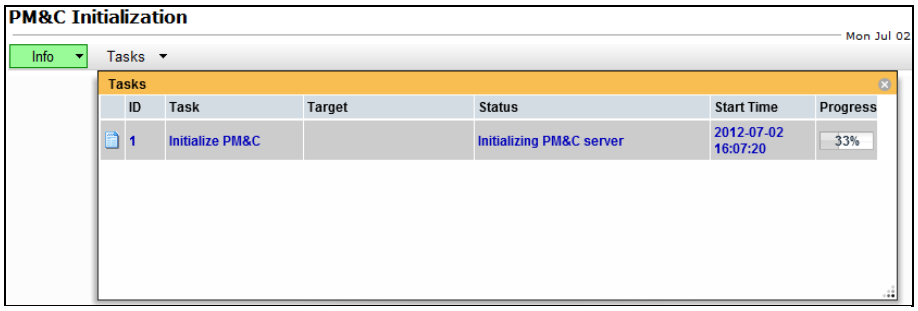
If this procedure fails, contact My Oracle Support and ask for ASSISTANCE.

Step	Procedure	Results
1 ☐	**PMAC GUI:** Load GUI initialization wizard	5. Open web browser and enter: `http://<management_network_ip>/gui` 6. Login as pmacadmin user. 

Step	Procedure	Results
2 ☐	**PMAC GUI:** Select a profile	The first screen will be similar to image below. Profiles File Name: TVOE; Name: PM&C TVOE Guest; Comment: Manage systems from a TVOE hosted PM&C; Version: 6.0.0 Initialize Select the TVOE profile and click on **Initialize**, the following features screen will display Feature / Description / Role / Enabled DEVICE.NETWORK.NETBOOT — Network device PXE initialization — control — ☑ DEVICE.NTP — PM&C as a time server — management — ☑ SERVER.IPM — Server Initial Product Manufacturing — control — ☑ PMAC.MANAGED — Remote management of PM&C server — management — ☐ PMAC.REMOTE.BACKUP — Remote server for backup — management — ☑ PMAC.NETBACKUP — NetBackup client — management — ☐ Add Role Make sure that the role for DEVICE.NETWORK.NETBOOT and SERVER.IPM are set to **control** while the roles for all other features is set to **management**. Also make sure that the enabled checkbox is checked for the following: DEVICE.NETWORK.NETBOOT DEVICE.NTP PMAC.REMOTE.BACKUP SERVER:IPM PMAC.NETBACK (only if NetBackup is used) And click on **Next**. Cancel Next
3 ☐	**PMAC GUI:** Network Description	You will see this default screen similar to: Network IP / Network Mask / VLAN 192.168.3.0 / 255.255.255.0 / 0 10.240.9.128 / 255.255.255.192 / 0 Add Delete Enter the Network IPs and Netmasks for the control and Management Networks and set their VLAN IDs to 0. Click **Next**.

Step	Procedure	Results
4 ☐	**PMAC GUI:** Network Roles	You will see this default screen similar to:  Verify the Roles and update if necessary. Click **Next**.
5 ☐	**PMAC GUI:** Network Interface	You will see this default screen similar to:  Verify the IP addresses for each Device and update if necessary. Click **Next**.
6 ☐	**PMAC GUI:** Network Route	You will see this default screen similar to:  Click **Add** to create new routes. At a minimum a default route should be defined. The following screen will be displayed. For the default route, select the “management” Device, enter “0.0.0.0” for both Destination Address and Destination Mask, and enter the gateway IP under Gateway as shown below  Click **Add Route**. Repeat to define more route. Click **Next** when done.

Step	Procedure	Results
7 ☐	**PMAC GUI:** DHCP Ranges	You will see this default screen similar to:  DHCP Ranges Start DHCP: 192.168.3.1 End DHCP: 192.168.3.254 Add Delete  Cancel Next Set address range: Start - 192.168.1.5 End – 192.168.1.254. [192.168.1.1 – 192.168.1.4 are reserved for PMAC] If you need to define additional DHCP ranges, press Add (most deployments do not require additional DHCP Ranges, Otherwise, click **Next**.
8 ☐	**PMAC GUI:** Settings summary	The following summary screen will be displayed.  Network Description Network IP / Network Mask / VLAN 192.168.3.0 / 255.255.255.0 / 0 10.240.9.128 / 255.255.255.192 / 0 Network and Roles Description Network IP / Network Mask / Role 192.168.3.0 / 255.255.255.0 / control 10.240.9.128 / 255.255.255.192 / management Network Interface Description Device / IP Address / Description control / 192.168.3.1 / Control network for managed servers management / 10.240.9.190 / Management of system devices Route Configuration Device / Destination IP / Network Mask / Gateway IP management / 0.0.0.0 / 0.0.0.0 / 10.240.9.131 DHCP Configuration Start DHCP / End DHCP 192.168.3.1 / 192.168.3.254 Verify the values and click **Finish**.

Step	Procedure	Results
9 ☐	**PMAC GUI:** Complete the configuration	The following summary screen will be displayed, click on Tasks to view the Initialization Progress.  Click **Task Monitoring** for status of this task. ID Task Target Status Running Time Start Time Progress 2 Initialize PM&C PM&C initialized 0:00:39 2011-09-19 14:19:30 100% Wait until the Progress bar turns green, that signifies that the PMAC Initialization was successful.
10 ☐	Add Cabinet and Enclosure	Add the Cabinets and Enclosures to be managed by this PMAC. Wait for these tasks to complete.
11 ☐	Verify Software and Hardware Inventory	Open GUI forms for Hardware and Software Inventory. Confirm that the hardware and software are correctly shown for the added Enclosures.
12 ☐	Add ISO Images to Storage	Add the software ISO images needed for both 7.5 and 9.x. Add the Misc Firmware ISO image.
THIS PROCEDURE HAS BEEN COMPLETED		

C.2.6 Procedure c-6. Define netConfig Repositiry, and Store Switch Configuration Backups

This procedure configures the netConfig repository, and stores the switch config backups.

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

Should this procedure fail, contact My Oracle Support and ask for UPGRADE ASSISTANCE.

Step	Procedure	Results

1 ☐	Setup conserver serial access on TVOE Host	**Management Server:** Setup conserver serial access for switch1A and switch1B and open the firewall to allow for future tftp use in this procedure.
		
		NOTE: If there are no aggregation switches in this deployment, skip to the next step.
		
		From Management Server/TVOE Host, configure the conserver service to enable serial access to the switches:
		
		For switch1A:
		
		`# conserverAdm --addConsole --name=switch1A_console --device=/dev/ttyS4`
		
		For switch1B:
		
		`# conserverAdm --addConsole --name=switch1B_console --device=/dev/ttyS5`
		
		Open the conserver port on the firewall of the TVOE Management Server:
		
		`# iptables -I INPUT -s 10.240.238.4/255.255.255.255 -p all -j ACCEPT`
		`# service iptables save`
		
		You should be returned to the command line prompt. If so, continue to the next step; if not, contact Customer Care Center for assistance.

2 ☐	Login to the PMAC guest console	TVOE Management Server:
		
		`# virsh list`
		`# virsh console <PMAC_Name>`

Step	Procedure	Results

3 ☐	Add 4948 switch Devices on Virtual PMAC	**NOTE**: If there are no aggregation switches in this deployment, skip to the next step.
		`# netConfig --repo listDevices`
		
		`# netConfig --repo addDevice name=switch1A --reuseCredentials`
		`Device Vendor? Cisco`
		`Device Model? 4948E`
		`Should the init oob adapter be added (y/n)? y`
		`Adding consoleInit protocol for switch1A using oob...`
		`What is the name of the service used for OOB access? console_service`
		`What is the name of the console for OOB access? switch1A_console`
		`What is the device console password? <switch_console_password>`
		`Verify Password: <switch_console_password>`
		`What is the platform access username? <switch_platform_username>`
		`What is the platform user password? <switch_platform_password>`
		`Verify Password: <switch_platform_password>`
		`What is the device privileged mode password? <switch_enable_password>`
		`Verify Password: <switch_enable_password>`
		`Should the live network adapter be added (y/n)? y`
		`Adding cli protocol for switch1A using network...`
		`What is the address used for network device access? <switch1A_mgmtVLAN_ip_address>`
		`Should the live oob adapter be added (y/n)? y`
		`Adding cli protocol for switch1A using oob...`
		`OOB device access already set: console_service`
		`Device named switch1A successfully added.`
		
		REPEAT for other switches
		
		NOTE: The platform user password and the privileged mode password must be the SAME.

Step	Procedure	Results

4 ☐	IF Needed – reset 6120 switch login credentials and assign hostname	NetConfig tool requires certain additional setup steps on the switches.
		• Unique hostname
		• ssh enabled
		• The password for operation and manager access must be the same.
		PMAC CONSOLE: Modify the logon credentials for all 6120 switches
		For ALL HP6120XG switches in the deployment, **ssh** or **telnet** to the switch using the current login credentials. If ssh is already enabled, telnet will then be automatically disabled. i.e. only one option will work. If ssh does not work, you will need to enable it.
		On the switch, enter config mode:
		`6120XG_1002# config`
		`6120XG_1002(config)# hostname <switch_hostname>`
		`6120XG_1002(config)# password manager user-name <manager_user_name> plaintext <password>`
		`6120XG_1002(config)# password operator user-name <operator_user_name> plaintext <password>`
		`6120XG_1002(config)# ip ssh filetransfer`
		`6120XG_1002(config)# exit`
		`6120XG_1002# write mem`
		NOTES:
		• <*password*> must be the same for both users.
		• standard <*manager_user_name*> = manager
		• standard <*operator_user_name*> = operator
		• *switch_hostname* = a unique name, which will also be the device name in netConfig

Step	Procedure	Results
5 ☐	Add 6120 switch Devices on Virtual PMAC	

```
# netConfig --repo listDevices


# netConfig --repo addDevice name=<switch_hostname> --reuseCredentials
Device Vendor? HP
Device Model? 6120
Should the live network adapter be added (y/n)? y
Adding cli protocol for 6120XG_IOBAY1 using network...
What is the address used for network device access? <enclosure_switch_IP>
What is the platform access username? <manager_user_name>
What is the platform user password? <6120_password>
Verify Password: <6120_password>
What is the device privileged mode password? <6120_password>
Verify Password: <6120_password>
Should the live oob adapter be added (y/n)? n
Should the init network adapter be added (y/n)? y
Adding sshInit protocol for SLAK_6120XG_Enc2b using network...
Network device access already set: <enclosure_switch_IP>
What is the platform access username? root
What is the platform user password? <pmac_root_password>
Verify password: <pmac_root_password>

What is the device privileged mode password?
Verify password: <6120_password>



Device named SLAK_6120XG_Enc2b successfully added.
REPEAT for other switches
```

Step	Procedure	Results

6 ☐	Configure console_service on Virtual pmac	**PMAC Console:** Setup netConfig repository with necessary console information.
		
		NOTE: If there are no aggregation switches in this deployment, skip to the next step.
		
		Use netConfig to delete the console_service prior to the migration:
		
		`[root@pmac approximatelty ]# netConfig --repo deleteService name=console_service`
		
		Use netConfig to create a repository entry that will use the conserver service that was configured in the previous steps. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.
		
		`[root@pmac approximatelty ]# netConfig --repo addService name=console_service`
		`Service type? (tftp, ssh, conserver, oa) conserver`
		`Service host? <management_server_mgmtVLAN_ip_address>`
		`Enter an option name (q to cancel): user`
		`Enter a value for user: platcfg`
		`Enter an option name(q to cancel): password`
		`Enter a value for password: <platcfg_password>`
		`Verify password: <platcfg_password>`
		`Enter an option name(q to cancel): q`
		`Add service for console_service successful`
		
		To check that you entered the information correctly, use the following command:
		
		`[root@pmac approximatelty ]# netConfig --repo showService name=console_service`
		
		Check the output, which will be similar to the one shown below:
		
		`[root@pmac approximatelty ]# netConfig --repo showService name=console_service`
		`Services:`
		`Service Name: console_service`
		`Type: conserver`
		`Host: 10.240.8.4`
		`Options:`
		`password: D8396824B3B2B9EE`
		`user: platcfg`
		`[root@pmac approximatelty ]#`

Step	Procedure	Results

7 ☐	Configure tftp_service on Virtual PMAC	**PMAC Console:** Check for the tftp_service, and add it if necessary
		
		NOTE: If there are no aggregation switches in this deployment, skip to the next step.
		
		`[root@pmac approximatelty ]# netConfig --repo listServices`
		
		SAMPE OUTPUT
		
		`Services:`
		`  Service Name:  tftp_service`
		`  Type:  tftp`
		`  Host:  10.240.8.4`
		`  Options:`
		`  dir: /var/TKLC/smac/image`
		
		If the tftp_service IS listed in the output of **'listServices'** skip to the next step.
		
		If the tftp_service is NOT listed in the output of **'listServices'** add the service:
		
		`[root@pmac approximatelty ]# netConfig --repo addService name=tftp_service`
		`Service type? (tftp, ssh, conserver, oa) tftp`
		`Service host? <pmac_mgmtVLAN_ip_address>`
		`Enter an option name (q to cancel): dir`
		`Enter a value for dir: /var/TKLC/smac/image/`
		`Enter an option name(q to cancel): q`
		`Add service for tftp_service successful`
		
		To check that you entered the information correctly, use the following command:
		
		`[root@pmac approximatelty ]# netConfig --repo showService name=tftp_service`
		
		Check the output, which will be similar to the one shown below
		
		NOTE: Only the tftp service info has been shown in this example. If the previous step and this step were done correctly, both the console_service and tftp_service entries would show up.
		
		`[root@pmac approximatelty ]# netConfig --repo showService name=tftp_service`
		`Services:`
		`Service Name: tftp_service`
		`Type: tftp`
		`Host: 10.240.8.4`
		`Options:`
		`dir: /var/TKLC/smac/image`
		`[root@pmac approximatelty ]#`

Step	Procedure	Results

8 ☐	Configure ssh_service on Virtual PMAC	**PMAC Console:** Check for the ssh_service, and add it if necessary
		`[root@pmac approximatelty ]# netConfig --repo listServices`
		SAMPLE OUTPUT
		`Services:`
		`  Service Name:  ssh_service`
		`  Type:  ssh`
		`  Host:  10.240.8.4`
		`  Options:`
		`  password: D5477140ECECECEB`
		`  user: root`
		If the ssh_service IS listed in the output of '**listServices'** skip to the next step.
		If the ssh_service is NOT listed in the output of '**listServices'** add the service:
		`[root@pmac approximatelty ]# netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <pmac_mgmtVLAN_ip_address>`
		`Enter an option name <q to cancel>: user`
		`Enter the value for user: root`
		`Enter an option name <q to cancel>: password`
		`Enter the value for password: <pmac_root_password>`
		`Verify Password: <pmac_root_password>`
		`Enter an option name <q to cancel>: q`
		`Add service for ssh_service successful`
		`[root@pmac approximatelty ]#`
		To ensure that you entered the information correctly, use the following command and inspect the output, which will be similar to the one shown below.
		`[root@pmac approximatelty ]# netConfig --repo showService name=ssh_service`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 10.250.62.85`
		`Options:`
		`password: C20F7D639AE7E7`
		`user: root`
		`[root@pmac approximatelty ]#`

9 ☐	Verify switch access.	**PMAC CONSOLE:** Verify netConfig access to HP6120 switches
		Verify that netConfig can access all HP6120 switches:
		`[root@pmac approximatelty ]# netConfig getVersion --device=<switch_name>`
		SAMPLE OUTPUT:
		`Firmware Version: Z.14.32`
		If this step fails, see the following step to re-set the switch credentials.

Step	Procedure	Results

10 ☐	Backup all 4948 switches	`[root@pmac approximatelty ]# mkdir -p /usr/TKLC/smac/etc/switch/backup`
		
		`[root@pmac approximatelty ]# cd /usr/TKLC/smac/etc/switch/backup`
		
		`[root@pmac approximatelty ]# netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup`
		
		REPEAT command for each switch

11 ☐	Backup all 6120 switches	`[root@pmac approximatelty ]# cd /usr/TKLC/smac/etc/switch/backup`
		
		`[root@pmac approximatelty ]# netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup`
		
		REPEAT command for each switch

12 ☐	End PMAC console session. Close iLO console session.	Press **<ctrl>]** to exit the PMAC guest console. In the iLO console session, execute: `# exit`
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX D. BACKUP CONFIG OF THE SWITCHES TO PMAC

The following procedures will backup the switch configurations to the PMAC, so these are available for future recovery actions or replacement activities.

D.1 Backup 6120XG Enclosure Switch

This procedure should be executed after every change to the switch configuration.

Prerequisites:

- IPM DL360 or DL380 Server must be completed
- Install PMAC on DL360 or DL380 must be completed
- Configure HP 6120XG switch (netConfig)

Procedure Reference Tables:

Variable	Value
<switch_name>	hostname of the switch

1. Verify netConfig Devices and Services are setup

```
# netConfig --repo listDevices
Devices: <the 2 enclosure switches>

# netConfig --repo listServices
Services: <the ssh_service>
```

   If Devices and Services are not setup, see procedure to setup netBackup Devices and Services before proceeding.

2. Verify netConfig is setup

   Verify switch is at least initialized correctly, and verify connectivity, by verifying hostname:

```
# netConfig --device=<switch_name> getHostname
Hostname: 6120_IOBAY3
```

   NOTE: The value beside Hostname should be the same as the *<switch_name>* variable.

3. Verify the ssh service is configured by running the `netConfig --repo showService name=ssh_service` and look for ssh service.

```
# netConfig --repo showService name=ssh_service
Service Name: ssh_service
Type: ssh
Host: 10.240.8.4
Options:
password: C20F7D639AE7E7
user: root
```

4. Ensure the directory where the backups will be stored exists.

```
# ls -l /usr/TKLC/smac/etc/switch/backup
```

   If you receive an error such as the following:

```
-bash: ls: /usr/TKLC/smac/etc/switch/backup: No such file or directory
```

   Then the directory must be created by issuing the following command

```
# mkdir -p /usr/TKLC/smac/etc/switch/backup
```

5. Navigate to the backup directory.

```
# cd /usr/TKLC/smac/etc/switch/backup
```

6. Execute the backup command

```
# netConfig --device=<switch_name> backupConfiguration service=ssh_service
filename=<switch_name>-backup
```

7. Verify switch configuration was backed up by cat <switch_name> and inspecting its contents to ensure it reflects the latest known good switch configurations.

```
# ls <switch_name>-backup*


# cat <switch_name>-backup
```

8. Go back to the home directory

```
# cd approximatelty
```

9. Repeat steps 2, 5-8 for each HP 6120XG switch to be backed up.

D.2 Backup Cisco 4948/4948E/4948E-F Aggregation Switch

This procedure should be executed after every change to the switch configuration.

Oracle Provided Aggregation Switch Prerequisites for c-Class system:

- IPM DL360 or DL380 Server must be completed
- Install PMAC on DL360 or DL380 must be completed
- Configure Cisco 4948/4948E/4948E-F aggregation switches (c-Class system) (netConfig)

Procedure Reference Tables:

Variable	Value
<switch_backup_user> (also needed in switch configuration procedure)	
<switch_backup_user_password> (also needed in switch configuration procedure)	
<switch_name>	hostname of the switch
<switch_backup_directory>	/usr/TKLC/smac/etc/switch/backup

1. Verify switch is at least initialized correctly and connectivity to the switch by verifying hostname

```
# netConfig --device=<switch_name> getHostname
Hostname: switch1A
```

NOTE: The value beside "Hostname:" should be the same as the <switch_name> variable.

2. Run command "netConfig --repo showService name=ssh_service" and look for ssh service.

```
# netConfig --repo showService name=ssh_service
Service Name: ssh_service
Type: ssh
Host: 10.250.62.85
Options:
password: C20F7D639AE7E7
user: root
```

In the ssh_service parameters, the value for 'user:' will be the value for the variable <switch_backup_user>.

3. Navigate to the `<switch_backup_user> home` directory.

```
# cd approximatelty <switch_backup_user>
```

Verify your location on the server

```
# pwd

/some/user/home/dir/path
```

4. Execute the backup command

```
# netConfig --device=<switch_name> backupConfiguration service=ssh_service

filename=<switch_name>-backup
```

5. Verify switch configuration was backed up by cat <switch_name>-backup and inspect its contents to ensure it reflects the latest knwon good switch configurations. Then, copy the files over to the backup directory.

```
# ls <switch_name>-backup*


# cat <switch_name>-backup


# mv <switch_name>-backup* <switch_backup_directory>/
```

6. Repeat steps 1, 3-5 for each switch to be backed up.

APPENDIX E. BACKOUT OF PMAC 5.0 TO PMAC 3.2

The following procedure will re-install the PMAC 3.2 application from backups.

E.1 Procedure 29. PMAC Backout Procedure

This procedure backs out the PMAC 5.0 software by reinstalling the PMAC 3.x software and recovering the data.

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

Should this procedure fail, contact My Oracle Support and ask for UPGRADE ASSISTANCE.

Step		Procedure	Results
1	☐	Install TPD 4.0 and PMAC on the Management Server.	1. PM the Management Server using the instructions and installation disks: TPD.install-4.2.1_70.71.0-CentOS5.5-i386 PMAC -- 872-2288-103-3.2.2_31.13.0-i386.iso 2. Perform the Installation and Setup of the PMAC Server procedure in the Policy System Platform Software Installation Guide: 910-6291-001 Rev B **NOTE:** Reconfigure the hostname of this server to be the same as that of the system manager it is replacing.
2	☐	Restore the configuration data.	Restore the PMAC 3.2 configuration data using the Restore PMAC Server From Backup Media procedure in *PMAC 3x/4x Disaster Recovery,* 909-1638-001 Rev B, September 2012
3	☐	Verify Inventory Views	Verify PMAC sync with Enclosures: • Hardware Inventory • Software Inventory
4	☐	Verify Inventory Views	Add Software Images to Image Storage on the PMAC server Perform the procedure in the *Policy System Platform Software Installation Guide*: 910-6291-001 Rev B
5	☐	Execute the system healthcheck.	Perform the PMAC Healthcheck procedures. If any error or failure conditions are discovered, contact My Oracle Support to work to resolve the failure conditions.
THIS PROCEDURE HAS BEEN COMPLETED			

APPENDIX F. TRANSFER FILES OR ISO FILES TO PMAC 5.0

Below discussion of how transfer files/ISO files from a USB key (FAT32) to the PMAC (Policy Management 9.x).

When the USB key is inserted to PMAC, it is mounted to /media (automatic).

- Login to the TVOE shell.
- cd to `/media/sdb1/`<*directory on the USB that you need*>.

Two options:

- Copy the files to the PMAC environment using the scp command.
  - scp <*file*> `pmac:/var/TKLC/upgrade`

    Note: Adding a `/etc/hosts` entry for pmac on the TVOE makes this easier to do.

    Please note that the `/var/TKLC/upgrade` partition has a space limit of about 3G.

```
[root@pmacTVOE238 ~]# sd 3:0:0:0: [sdb] Assuming drive cache: write through
sd 3:0:0:0: [sdb] Assuming drive cache: write through
sd 3:0:0:0: [sdb] Assuming drive cache: write through

[root@pmacTVOE238 ~]# cd /mediia
-bash: cd: /mediia: No such file or directory
[root@pmacTVOE238 ~]# cd /media
[root@pmacTVOE238 media]# ls
sdb1
[root@pmacTVOE238 media]# cd sdb1
[root@pmacTVOE238 sdb1]# ls
7.6.4  9.0  Other
[root@pmacTVOE238 sdb1]# cd 9.0
[root@pmacTVOE238 9.0]# ls
909-1620-001.pdf  909-2208-001.docx  909-2209-001.pdf  FW  PMAC  Policy  UP006207_1-3.docx
[root@pmacTVOE238 9.0]# cd Policy
[root@pmacTVOE238 Policy]# ls
872-2472-102-9.0.0_11.1.0-cmp-x86_64.iso     872-2475-102-9.0.0_11.1.0-mra-x86_64.iso
872-2473-102-9.0.0_11.1.0-mpe-x86_64.iso     TPD.install-5.1.0_73.3.0-CentOS5.8-x86_64.iso
872-2474-102-9.0.0_11.1.0-mpe-li-x86_64.iso
[root@pmacTVOE238 Policy]# scp *mra* pmac:/var/TKLC/upgrade
The authenticity of host 'pmac (10.240.238.4)' can't be established.
RSA key fingerprint is 75:8f:12:5f:e3:c5:33:68:57:3e:ff:aa:35:d6:08:51.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'pmac,10.240.238.4' (RSA) to the list of known hosts.
root@pmac's password:
872-2475-102-9.0.0_11.1.0-mra-x86_64.iso                                    17%  118MB  23.4MB/s   00:23 ET
```

- ftp ISO files from TVOE to pmac repository directory
  - Using sftp, connect to the PMAC management server

```
> sftp pmacftpusr@<pmac_management_network_ip>

> put <image>.iso
```

  - After the image transfer is 100% complete, close the connection

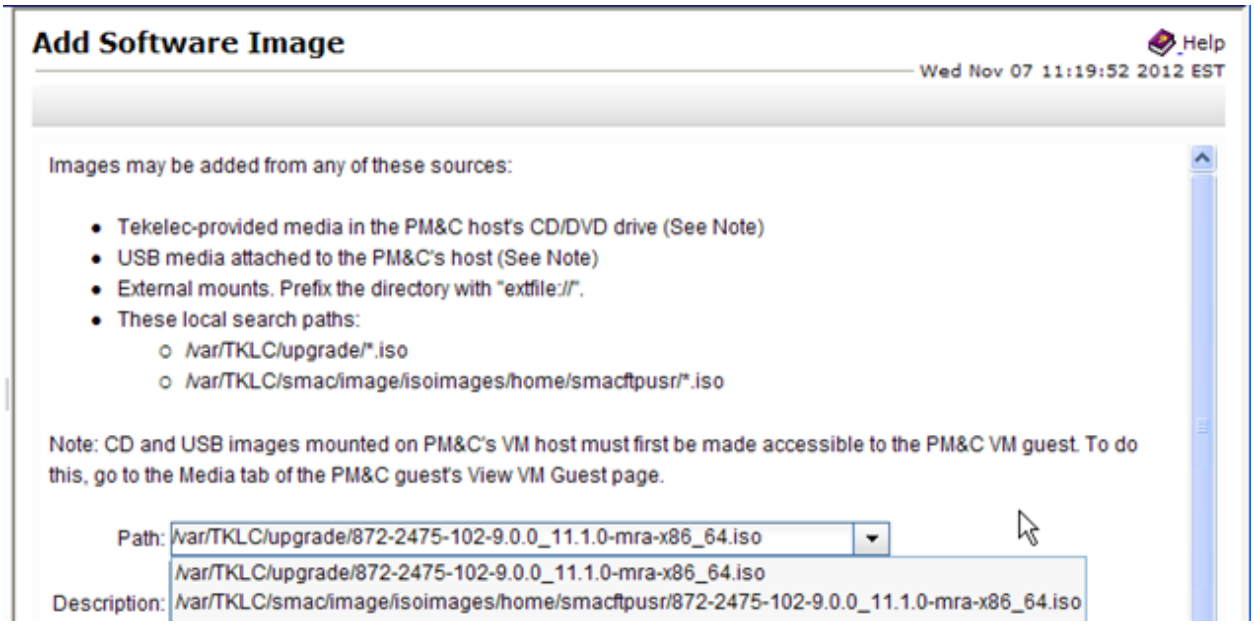
```
> quit
```

File is placed in `/var/TKLC/smac/image/isoimages/home/smacftpusr/`directory.

```
[root@pmacTVOE238 Policy]# pwd
/media/sdb1/9.0/Policy
[root@pmacTVOE238 Policy]# ls
872-2472-102-9.0.0_11.1.0-cmp-x86_64.iso     872-2475-102-9.0.0_11.1.0-mra-x86_64.iso
872-2473-102-9.0.0_11.1.0-mpe-x86_64.iso     TPD.install-5.1.0_73.3.0-CentOS5.8-x86_64.iso
872-2474-102-9.0.0_11.1.0-mpe-li-x86_64.iso
[root@pmacTVOE238 Policy]# sftp pmacftpusr@pmac
Connecting to pmac...
pmacftpusr@pmac's password:
sftp> put *mra*
Uploading 872-2475-102-9.0.0_11.1.0-mra-x86_64.iso to /home/smacftpusr/872-2475-102-9.0.0_11.1.
872-2475-102-9.0.0_11.1.0-mra-x86_64.iso                                                      1
sftp> quit
[root@pmacTVOE238 Policy]#
```

```
root@pmac238:/var/TKLC/smac/image/isoimages/home/smacftpusr
login as: root
root@10.240.238.4's password:
Access denied
root@10.240.238.4's password:
Last login: Wed Nov  7 10:25:48 2012 from 10.25.110.73
[root@pmac238 ~]# cd /var/TKLC/smac/image/isoimages/home/smacftpusr/
[root@pmac238 smacftpusr]# ls
872-2475-102-9.0.0_11.1.0-mra-x86_64.iso
[root@pmac238 smacftpusr]# ls
872-2475-102-9.0.0_11.1.0-mra-x86_64.iso
[root@pmac238 smacftpusr]#
```

Add Image to PMAC Repository:



APPENDIX G. ADDING ISO IMAGES TO THE PMAC FROM MEDIA

This procedure provides the steps for adding ISO images to the PMAC repository from Media.

1. **PMAC GUI:** Login

   Open web browser and enter:

   ```
   Error! Hyperlink reference not valid.>
   ```

   Login as pmacadmin user.

2. **PMAC GUI:** Attach the software image to the PMAC guest

   If the image is on a CD or USB device, continue with this step.

   In the PMAC GUI, nevigate to **Main Menu ➢ VM Managmenet.**. In the VM Entities list, select the PMAC guest. On the resulting View VM Guest page, select the **Media** tab.

   Under the **Media** tab, find the ISO image in the Available Media list, and click **Attach**.

   After a pause, the image will appear in the Attached Media list.

3. **PMAC GUI:** Navigate to Manage Software Images

   Navigate to **Main Menu ➢ Software ➢ Manage Software Image**s

4. **PMAC GUI:**Add image

   Click **Add Image**.

5. **PMAC GUI:** Add the ISO image to the PMAC image repository.

   Select an image to add:

   - If in Step 1 the image was transferred to PMAC via sftp it will appear in the list as a local file `/var/TKLC/....`
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device (`device://`…). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the ISO image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.

     Enter an appropriate image description and click **Add New Image**.

6. **PMAC GUI** Monitor the Add Image status

   The Manage Software Images page is then redisplayed with a new background task entry in the table at the bottom of the page.

7. **PMAC GUI** Wait until the Add Image task finishes

   When the task is complete, its text changes to green and its Progress column indicates "100%".

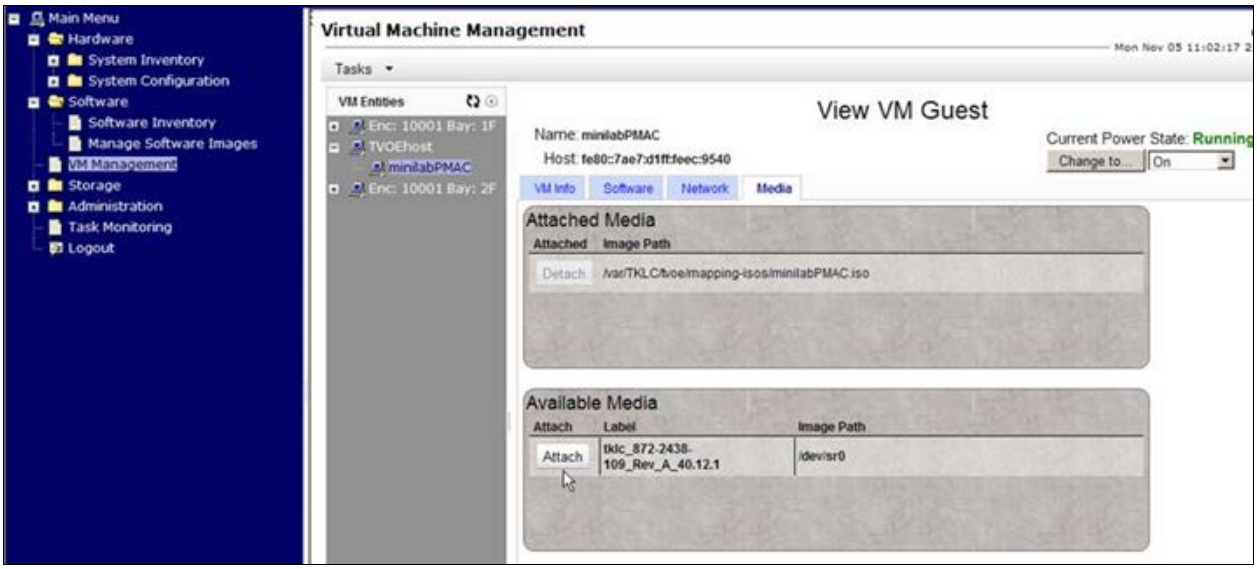
   Check that the correct image name appears in the Status column:

8. **PMAC GUI:** Detach the image from the PMAC guest

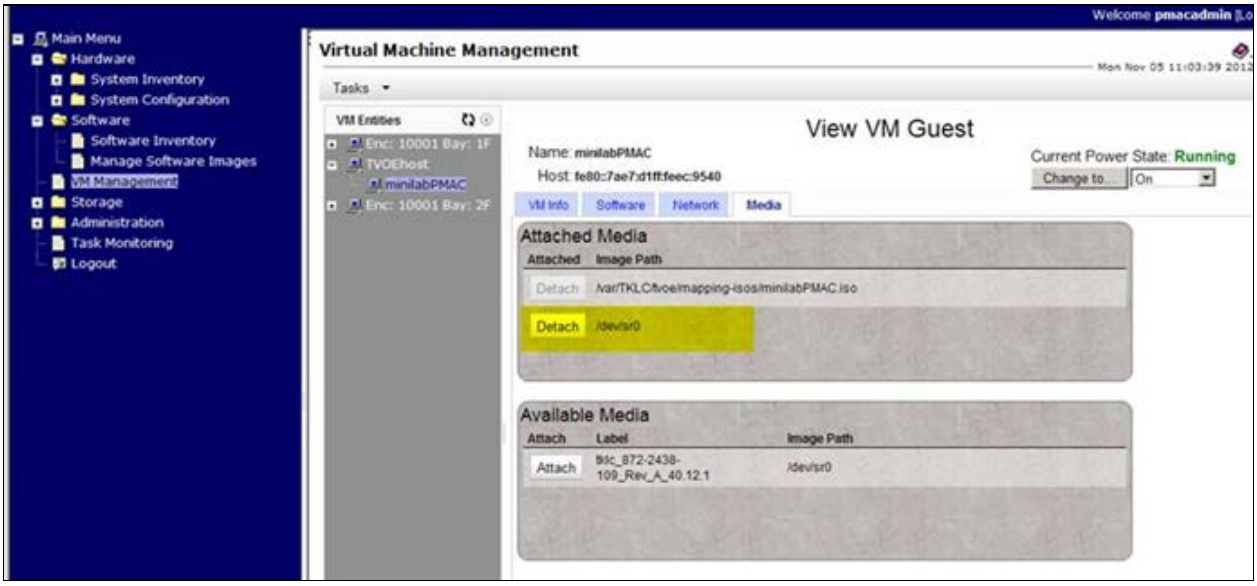
   If the image was supplied on CD or USB, return to the PMAC guest's **Media** tab used in Step 3, locate the image in the Attached Media list, and click **Detach**. After a pause, the image will be removed from the Attached Media list. This will release the virtual device for future use.

   Remove the CD or USB device from the Management Server.

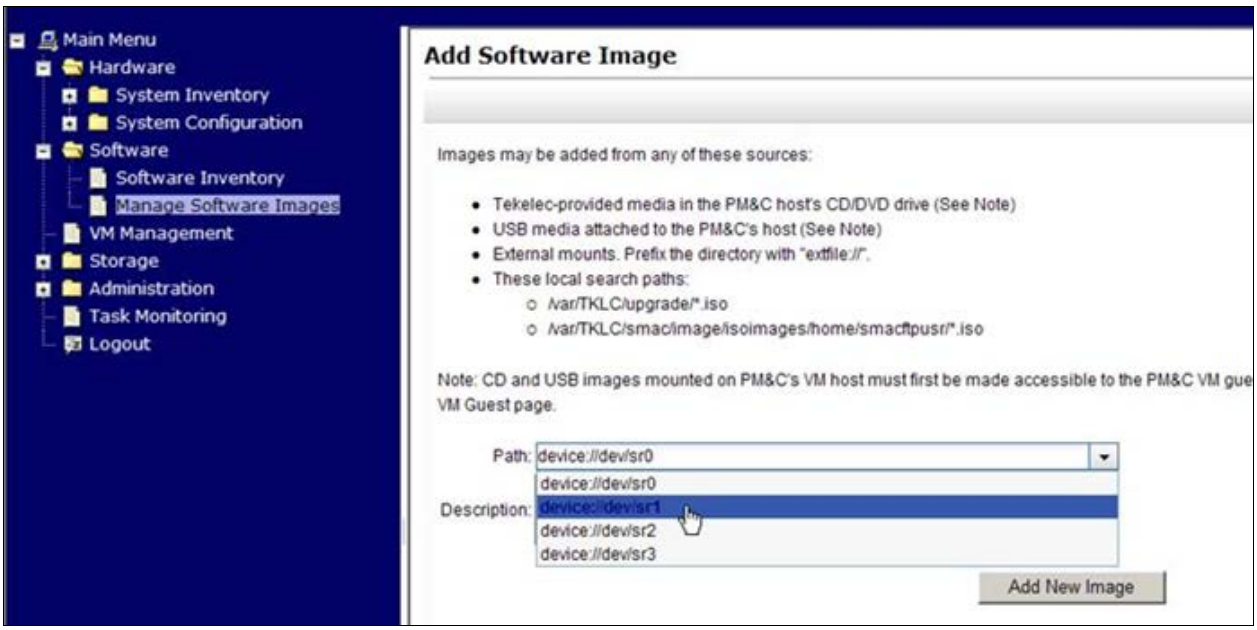
Below are the screen captures:

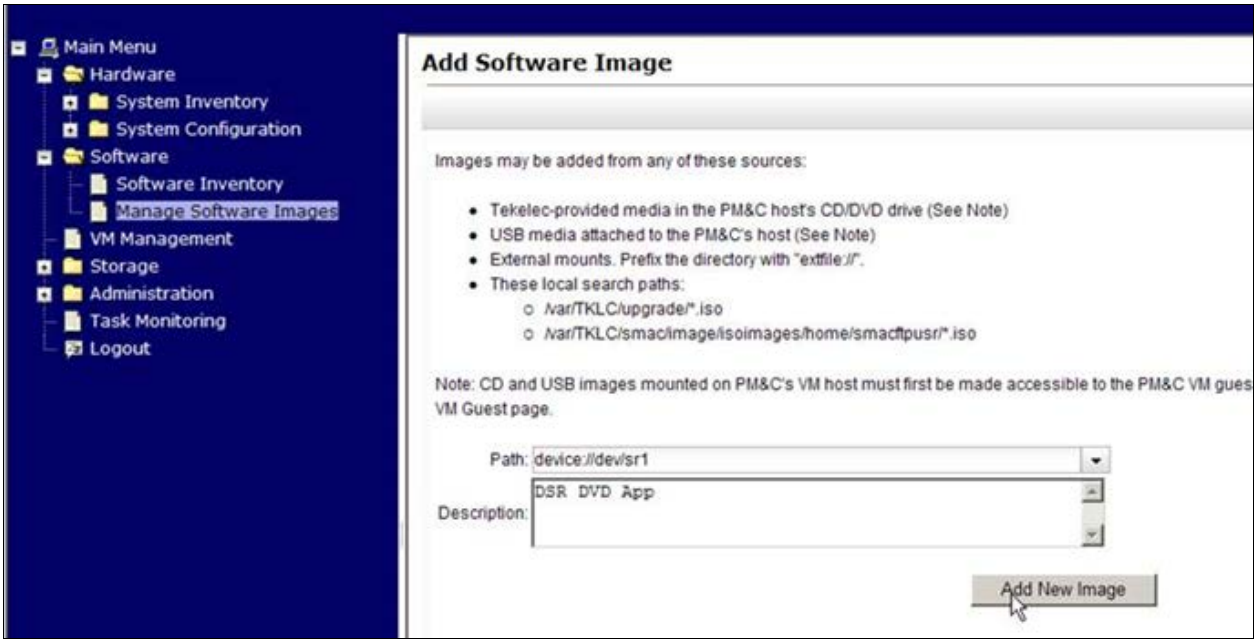


You will notice the DVD is mounted as /dev/sr0



When adding the Image select /dev/sr1 (even though it was mounted above as `/dev/sr0`) as shown below:





Task reported as successful:

Image is shown correctly in the PMAC GUI:

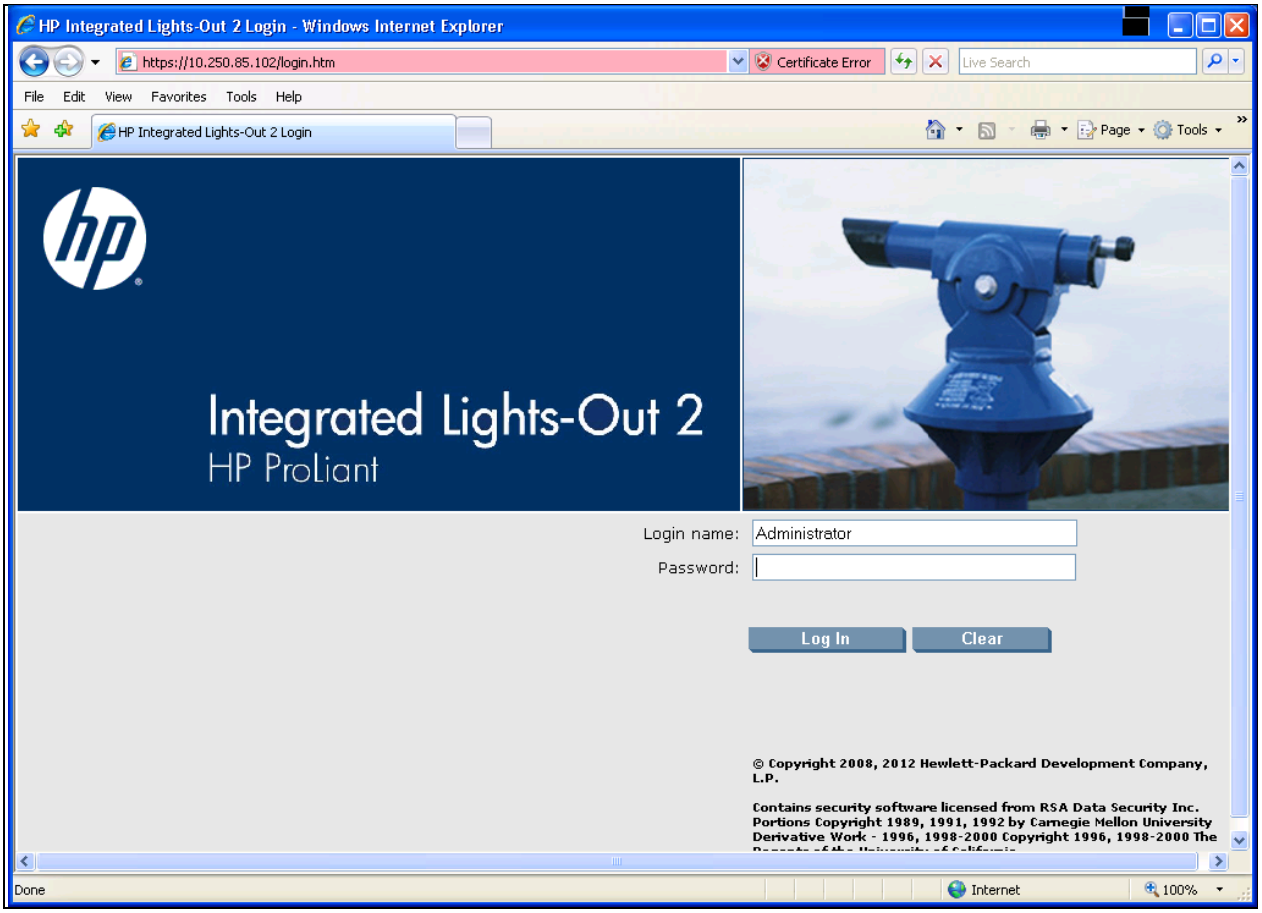
APPENDIX H. USING ILO (OR RMM) TO REMOTELY ACCESS A SERVER

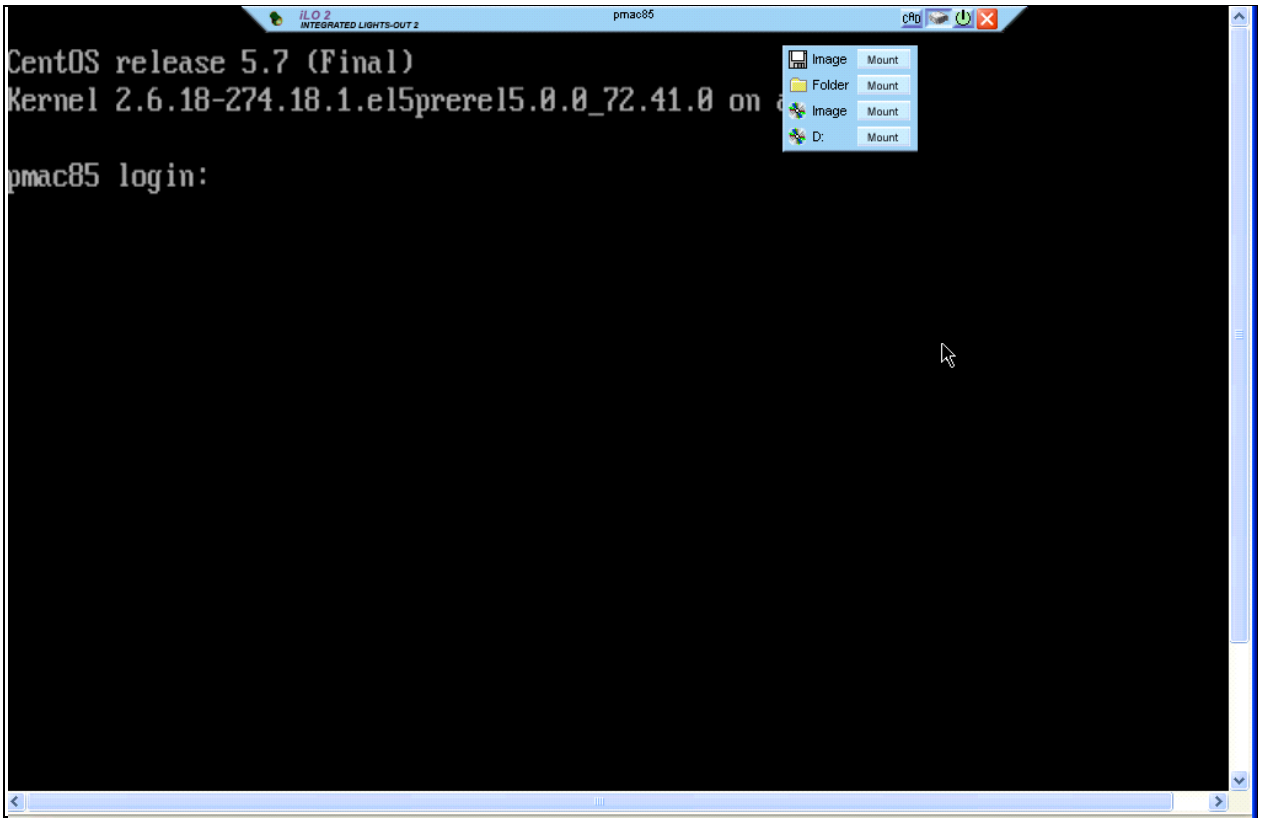
The iLo (or RMM for PP5160) interface of the server is a method to get access to the server, even if it won't boot.

The remote console access option of the iLo (or RMM) can be used to get console access to the server. This has the benefit that the user will see the console output while the server is re-booting.

The remote console access can also be used in case the server IP interfaces are down, and the server state is unknown.

From this interface, it is also possible to mount an ISO located on your computer to the server, using the iLo (or RMM) Virtual Mount utility. You can also remotely force a boot of the server.




iLO 2
INTEGRATED LIGHTS-OUT 2
pmac85
CentOS release 5.7 (Final)
Kernel 2.6.18-274.18.1.el5prerel5.0.0_72.41.0 on
pmac85 login:
Image
Mount
Folder
Mount
Image
Mount
D:
Mount

APPENDIX I. ACCESSING THE ORACLE CUSTOMER SUPPORT SITE

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

1. Log into Oracle Customer Support site at 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

APPENDIX J. USING THE SCREEN SHELL TOOL

The Linux screen tool is provided on the Policy servers, to establish an ssh session that will not be lost during a remote access disconnect. It also provides a method to log user activities and responses into a file.

To execute an action that should not be interrupted, ssh to the server, and start a screen session.

After the session is started, all the same privileges and commands are available but the session will be maintained even if the user connection to the server is broken.

J.1 Start Screen Session

1. SSH to server, login as root

```
# screen
# <user commands for upgrade>
```

2. Terminate a previously started session

```
# exit
```

3. Detach from session

   To leave the session, but keep the session running (detach):

```
# screen -d
# exit
```

4. Re-Attach to a previously started session

   SSH to server, login as root

```
# screen -ls
```

   There is a screen on:

```
        31808.pts-0.<hostname> (Detached)
```

5. 1 Socket in /var/run/screen/S-root.

```
# screen -x 31808
```

Uuser is now back in the same session started before the detach or disconnect.

J.2 Screen Logging

Using Ctrl-A then H, creates a running log of the session. Screen will keep appending data to the file through multiple sessions. Using the log function is very useful for capturing what you have done, especially if you are making a lot of changes.

J.3 Screen Help

Ctrl-A then ?

J.4 Other capabilities

The screen tool has multiple capabilities.

Further information is available on the Web.