Oracle® Communications Policy Management

Disaster Recovery Guide

Release 12.2

E82625 Revision 01

January 2017

CAUTION: In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

Contact Call the Oracle Customer Access Support Center at 1-800-223-1711 prior to executing this procedure to ensure that the proper recovery planning is performed.

Before disaster recovery, users must properly evaluate the outage scenario. This check ensures that the correct procedures are executed for the recovery.

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

NOTE: DISASTER Recovery is an exercise that requires collaboration of multiple groups and is expected to be coordinated by the TAC prime. Based on TAC's assessment of Disaster, it may be necessary to deviate from the documented process.
EMAIL: support@oracle.com

ORACLE

Oracle Communications Policy Management Disaster Recovery Guide, Release 12.2,

Part # E82625 -01

Table of Contents

List of Tables

1. Introduction

1.1. Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for Policy Management System, Release 12.2. This includes recovery of partial or a complete loss of one or more policy servers and policy components. This document provides step-by-step instructions to execute disaster recovery for Policy Management Systems. Executing this procedure also involves referring to and executing procedures in existing support documents.

1.2. References

[1] E67765 - Oracle Firmware Upgrade Release Notes, Release 3.1.5
[2] E67825 - Oracle Firmware Upgrade Pack Upgrade Guide, Release 3.1.5
[3] E70315 - Oracle Firmware Upgrade Release Notes, Release 3.1.6
[4] E70316 - Oracle Firmware Upgrade Pack Upgrade Guide, Release 3.1.6
[5] E76846 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.10
[6] E64917 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.9
[7] E54387 - PM&C Incremental Upgrade, Current Revision
[8] E56282 - TVOE 3.2 Disaster Recovery Procedure, Release 7.2, Current Revision
[9] E53486 - Tekelec Platform 7.0.x Configuration Procedure Reference, Current Revision
[10] E54388-02 - PM&C Disaster Recovery, Release 6.0
[11] E67647 – PM&C Disaster Recovery, Release 6.2
[11] E53487 - PM&C 6.2 Incremental Upgrade Procedure, Current Revision
[12] E72270 Revision 01 – Mediation Server User's Guide, Release 12.2
[13] E82615-01 - Oracle Communications Policy Management 12.2 Installation Procedure

The above documents are available at the Oracle Help Center.

Note: The HP Solutions Firmware Upgrade Pack (HP FUP) is provided for customers who bought their HP hardware through Oracle. If you need assistance, contact My Oracle Support.

1.3. Acronyms

Table 1: Acronyms

Acronym	Meaning
BIOS	Basic Input Output System
BOD	Bandwidth On Demand
CD	Compact Disk
ISO	The name *ISO* is taken from the ISO 9660 file system used with CD-ROM media, but an ISO image might also contain a UDF (ISO/IEC 13346) file system
c-Class	HP marketing term for their enterprise blade server platform
CMP	Configuration Management Platform
DR-CMP	Configuration Management Product for Disaster Recovery NOTE: It refers to the CMP on the secondary site
DVD	Digital Video Disc
GRUB	Grand Unified Boot loader
iLO	Integrated Lights-Out
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MPE	Multiprotocol Policy Engine
MRA	Multiprotocol Routing Agent
MA	Management Agent
OS	Operating System (e.g. TPD)
PM&C	Platform Management & Configuration
RMM	Remote Management Module
RMS	Rack Mount Server
SOL	Serial Over LAN
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment
FRU	Field Replaceable Unit

1.4. Logins and Passwords

The standard configuration steps will configure standard passwords for root, admusr, admin, and some other standard logins referenced in this procedure. Please note that SSH to Policy servers as root user is restricted, but allowed using 'admusr' user. These passwords are not included in this document.

1.5. Software Release Numbering

This guide applies to all Policy Management versions 12.2. It is assumed that PM&C Version 6.0.3 or above has been previously installed, configured in this deployment and in working condition, i.e. PM&C is not affected. PM&C Disaster Recovery Release 6.0 (refer to document E54388-02 for c-Class hardware enclosure details). The Oracle X5-2, Netra X5-2 and HP RMS hardware systems do not use PM&C.

1.6. Terminology

Table 2. Terminology

Base hardware	Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on and communicate on the network.
Base software	Base software includes installing the server's operating system: Tekelec Platform Distribution (TPD).
Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.
Perform initial configuration	The perform initial configuration put into the policy server through the platcfg utility that brings the server's network interface online and allows management and configuration from the CMP

2. General Description

The Policy Management disaster recovery procedure falls into two basic categories. It is primarily dependent on the state of the CMP servers:

- Recovery of one or more servers with at least one CMP server intact
  - 1 or more CMP servers intact (this can include Geo-Redundant CMP(DR-CMP) servers)
  - 1 or more MPE/MRA/BOD/MA servers failed
- Recovery of the entire network from a total outage
  - No CMP servers are available (neither primary, nor secondary) and other MPE/MRA/BOD/MA servers will need to be recovered

The existence of Geo-redundant system, including a geo-redundant CMP (DR-CMP) can mitigate massive outages by providing a running manager from which to synchronize new system as they are restored.

No matter the number of servers involved in the outage, the key to the severity is the status of the CMP. The availability of regular system backups of the CMP are critical when all CMP servers are offline and must be restored.

Note that for E54388-02 Disaster Recovery of the PM&C Server Release 6.0 *or* E67647 Disaster Recovery of the PM&C Server Release 6.2, see document, for Procedure 5: Post-Restoration Verification for Aggregate Switches, refer to Appendix A.

Note that the Field Replacement Unit (FRU server) can be deployed as type MPE, MRA, BOD, MA or CMP. The FRU will be needed to physically replace the failed server, the cables for the new server have to be connected same as the failed one.

Single node outage MRA/MPE/BOD/MA/CMP, with CMP Server available

The simplest case of recovery is to recover a single node of a cluster with one or both CMP servers intact. The node is recovered using base recovery of hardware and software. **Perform initial configuration** information needs to be restored either manually or from a server backup file, after which the cluster will reform, and database replication from the active server of the cluster will recover the server. This scenario can be used to recover one server of a MRA/MPE/BOD/MA cluster or one server of a CMP cluster. The SSH exchange keys with cluster mate from active CMP is also required.

Recovery of complete MRA/MPE/BOD/MA cluster, with CMP server available

The failure of a complete cluster can be recovered by replacing all nodes of the cluster. All nodes are recovered using base recovery of hardware and software '**Perform initial configuration'** information needs to be restored either manually or from a server backup file to all of the replaced nodes, after which the cluster will reform. The CMP can then push application level configuration to the new cluster.

Recovery of the CMP Cluster when no geo-redundant CMP exists

The complete failure of the CMP will require re-installation using base recovery of hardware and software. '**Perform initial configuration'** information needs to be restored either manually or from a server backup file. Once the cluster is available, completion of the recovery will require the use of a stored system backup in order to recover application level configuration including policies and configuration of the MPE/MRA/BOD/MA clusters in the network.

Recovery of the CMP Cluster when geo-redundant CMP (DR-CMP) is available

The availability of a geo-redundant CMP (DR-CMP) will simplify restoration of a failed CMP. The geo-redundant CMP can be promoted to active primary, and the failed CMP will then require re-installation using base recovery of hardware and software. **'Perform initial configuration'** information needs to be restored either manually or from a

server backup file. Once the cluster is available, the primary running geo-redundant CMP will replicate databases to the replaced CMP cluster.

Complete Server Outage (All servers)

This is the worst case scenario where all the servers in the network have suffered partial or complete software and/or hardware failure, and no geo-redundant CMP is available. The servers are recovered using base recovery of hardware and software and then restoring a system backup to the active CMP server. Database backups will be taken from customer offsite backup storage locations (assuming these were performed and stored offsite prior to the outage). If no backup file is available, the only option is to rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

A note on 'Perform initial configuration':

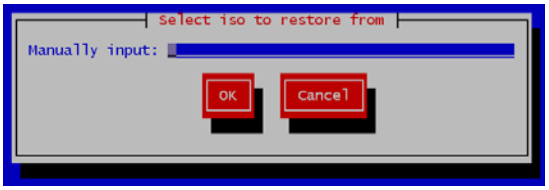
The information required for initial configuration is not extensive, and may be readily available from customer site documents, or from the CMP's topology configuration. In some cases it can be easier to manually input the 'initial configuration' in platcfg than to try to load a server backup file into the newly installed hardware.

Needed initial configuration information:

- Hostname
- OAM real IP address and network mask
- OAM default router address
- NTP server
- DNS server (optional)
- DNS search (optional)
- Interface device (usually bond0)
- VLAN configuration for c-Class and Sun Netra systems.

Using the server backup file

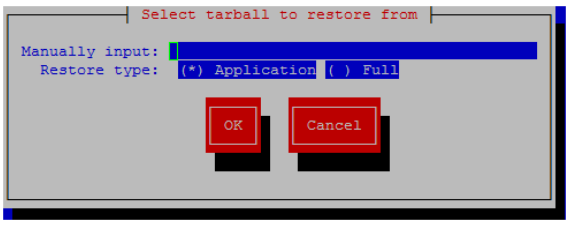
When asked to restore from 'server backup', the platcfg utility will look in /var/camiant/backup/local-archive/serverbackup directory. If no files are in that directory, the box below will be presented.



You will have to enter the complete path and filename in order to restore from a file that is not in the /var/camiant/backup/local-archive/serverbackup directory.

Using the system restore file

When asked to restore from 'system backup', the platcfg utility will look in /var/camiant/backup/local-archive/systembackup directory. If no files are in that directory, the box below will be presented.



You will have to enter the complete path and filename in order to restore from a file that is not in the /var/camiant/backup/local-archive/systembackup directory.

PM&C usage

When working with a c-Class enclosure, the PM&C will establish connectivity with DHCP to the blades in the enclosure. This will allow the PM&C to act as your central contact point in the work on a c-Class system. It can also be a staging point for restoration files to be sent to c-Class blades over the 192.168.1.0 network.

3. Procedure Overview

This section lists the materials required to perform disaster recovery procedures and a general overview (disaster recovery strategy) of the procedure executed.

Disaster Recovery Strategy

Disaster recovery procedure execution is performed as part of a disaster recovery strategy with the basic steps listed below:

1. Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedures. This means the failure conditions in the network match one of the failure scenarios described in Recovery Scenarios
2. Evaluate the availability of server and system backup files for the servers that are to be restored.
3. Read and review the content in this document.
4. Determine whether a geo-redundant CMP(DR-CMP) is available
5. From the failure conditions, determine the Recovery Scenario and procedure to follow.
6. Execute appropriate recovery procedures.

Required materials

The following items are needed for disaster recovery:

1. A hardcopy of this document and hardcopies of all documents in the reference list.
2. Hardcopy of all site surveys performed at the initial installation and network configuration of the customer's site. If the site surveys cannot be found, escalate this issue within Oracle CGBU Customer Service until the site survey documents can be located.
3. Policy 'System' backup file: electronic backup file (preferred) or hardcopy of all Policy system configuration and provisioning data.
4. Tekelec Platform Distribution (TPD) Media.
5. Platform Management & Configuration (PM&C) Media.
6. Policy Application installation .ISO for CMP, MPE, MRA, BoD and MA of the target release.
7. The switch configuration backup files used to configure the switches, available on the PM&C Server.
8. The Firmware Media for the corresponding builds and servers.

Policy server backup

Backup of the policy server can be done either manually from platcfg, or on a schedule as configured in platcfg. There are 2 types of backup operations available; '*server backup'* and '*system backup'*:

- **Server Backup:** There is one Server Configuration backup for each server in the system. The server backup is a Back-up of the OS information unique to the server. Information includes hostname, IP Addresses, NTP, DNS, Static Route configuration. This operation create a Server Configuration Backup file, and should be executed on each of the server in the customer's network.
- **System Backup**: There is one Application Configuration backup for the entire Policy system. The system backup will gather PCRF configuration information that is unique to this system. Information such as: Topology, Policy(s), Feature Configuration. The system backup is executed only on the Active CMP at the primary site.

The availability of a recent system backup is critical to the restoration of the policy network when the CMP is not available.

4. Procedure Preparation

4.1. Purpose and Scope

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. The first step is to evaluate the failure scenario and determine the procedure(s) that will be needed to restore operations. A series of procedures are included below that can be combined to recover one or more policy management nodes or clusters in the network.

Note: A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.

The general steps recovering servers are:

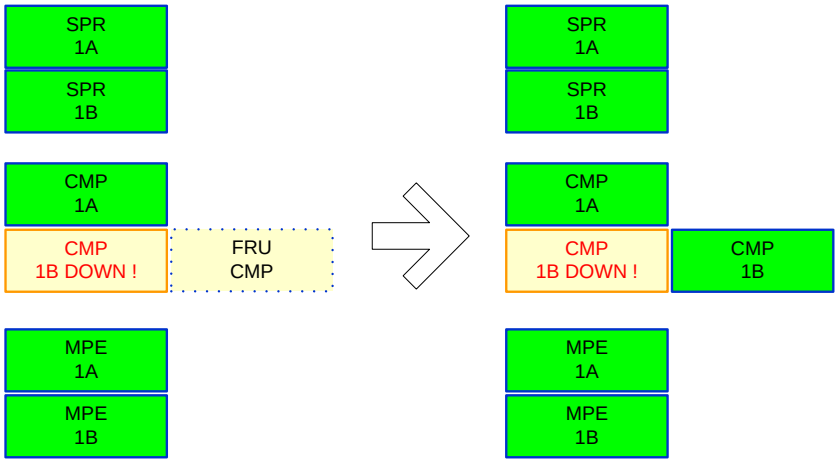
1. Verify BIOS time is correct on servers
2. Verify Version of TPD installed
3. Load application for corresponding server HW types
4. Check FW versions and upgraded if necessary
5. Check NTP status after recovery
6. Check Active Alarms from GUI and both syscheck, alarmMgr–alarmStatusfrom CLI

4.2. Recovery Scenarios

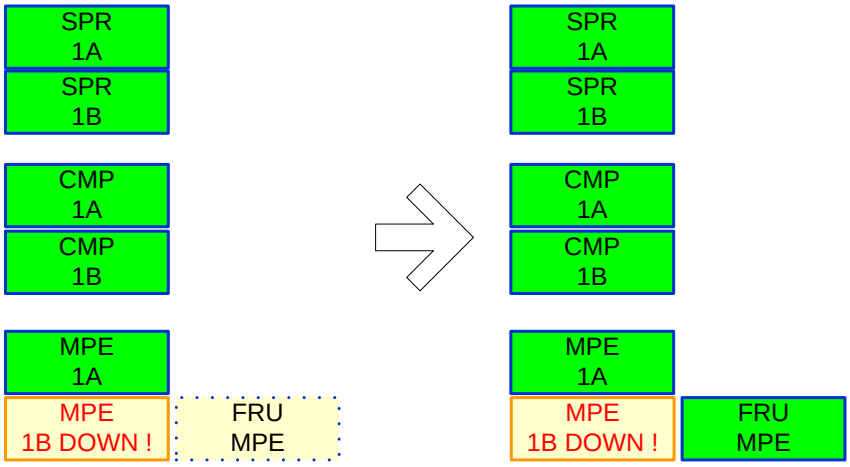
4.2.1. Recovery Scenario 1 (Partial Cluster Outage with Primary CMP Server available)

For a partial outage with a CMP server available, only base recovery of hardware and software and initial Policy configuration is needed. A single CMP server is capable of restoring the configuration database via replication to all MPE/MRA/BOD/MA servers, or to the other CMP node of a cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in the Restore Procedures section. The major activities are summarized as follows:

- Recover Standby CMP server (if necessary) by recovering base hardware and software.
    - Recover the base hardware.
    - Recover the software.
    - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
    - The database is intact at the active CMP server and will be replicated to the standby CMP server.



- Recover any failed MPE/MRA/BOD/MA servers by recovering base hardware and software.
    - Recover the base hardware.
    - Recover the software.
    - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
    - The configuration database is available at the active CMP server and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/MRA/BOD/MA servers using 're-apply configuration'



Follow the procedure below for detailed steps.

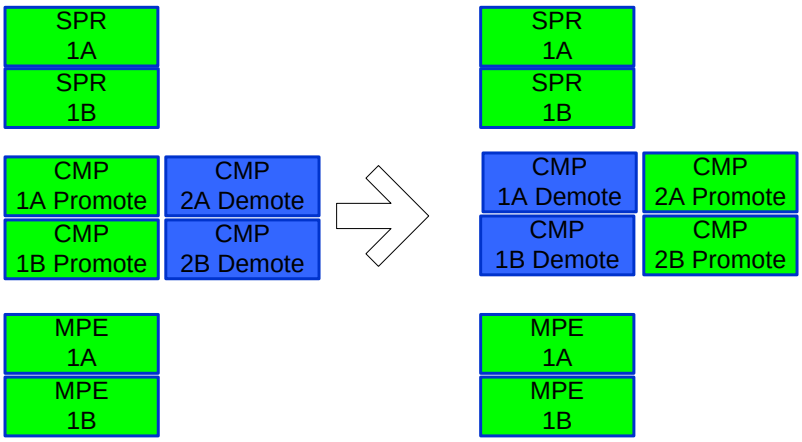
- Use Procedure 2: Restore standby CMP Node without server backup file
  Or Procedure 1: Restore standby CMP Node with server backup file to recover the second CMP node if necessary.
- Use Procedure 4: Restore single MPE/MRA/BOD/MA node without server backup file to recover MPE / MRA/BOD/MA nodes when one of the peers of the cluster is still available.
  Or Procedure 3: Restore single MPE/MRA/BOD/MA node with server backup file
- Use Procedure 5: Restoring complete cluster with the server backup files
  Or Procedure 6: Restoring complete cluster without the server backup to recover complete MPE / MRA/BOD clusters that have gone down.
- Use Procedure 7: Restoring CMP/MA cluster with system backup available files to recover first of 2 nodes in MA cluster
  Use Procedure 3: Restore single MPE/MRA/BOD/MA node with server backup file to recover the second node of MA cluster.

4.2.2. Recovery Scenario 2 (Partial Cluster Outage with geo-redundant CMP Server available)

For a partial outage with a geo-redundant CMP server available, the secondary site CMP must be manually promoted to Primary status as the controlling CMP for the policy network. Then base recovery of hardware and software and initial Policy configuration is needed. The now active CMP server is capable of restoring the configuration database via replication to all MPE/MRA/BOD/MA servers, and to the other CMP cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in the `Restore Procedures` section. The major activities are summarized as follows:

- Promote the geo-redundant CMP server.

- This step is done by logging into the OAM VIP address of the second site CMP cluster. Use procedure 7 below.



This would only need to be done if the Primary CMP cluster needs to be restored. If it's an MRA or MPE or BOD or MA cluster that needs to be restored, there is no need to promote the Geo CMP.

- Recover any failed MPE/MRA/BOD/MA servers by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - The configuration database is available at the active CMP server and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/MRA/BOD/MA servers using 're-apply configuration'
- Recover other site CMP server by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file.

The database of the active geo-redundant CMP server will be replicated to the new CMP server.

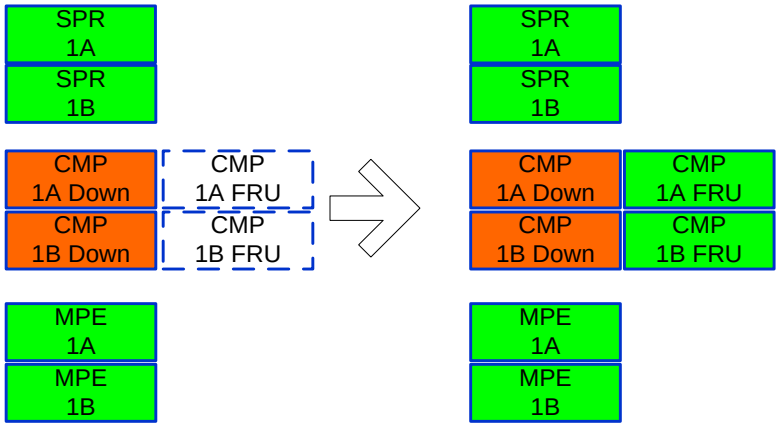
Follow the procedure below for detailed steps.

- Use Procedure 8: Promoting geo-redundant CMP cluster below to promote the geo-redundant CMP
- Use Procedure 4: Restore single MPE/MRA/BOD/MA node without server backup file to recover MPE / MRA / BOD / MA nodes when one of the peers of the cluster is still available.
  Or Procedure 3: Restore single MPE/MRA/BOD/MA node with server backup file
- Use Procedure 5: Restoring complete cluster with the server backup files
  Or Procedure 6: Restoring complete cluster without the server backup to recover complete MPE / MRA / BOD clusters that have gone down.
- Use Procedure 5: Restoring complete cluster with the server backup files
  Or Procedure 6: Restoring complete cluster without the server backup to recover the secondary site CMP. Recovery of the secondary site CMP can be left for late in the process because the now active CMP can handle all application level configuration as the network is brought back online.
- Use Procedure 7: Restoring CMP/MA cluster with system backup available files to recover first of 2 nodes in MA cluster

Use Procedure 3: Restore single MPE/MRA/BOD/MA node with server backup file to recover the second node of MA cluster.

4.2.3. Recovery Scenario 3 (Full cluster outage of the CMP; geo-redundancy not available; other servers as needed)

For a full outage with a CMP server unavailable, base recovery of hardware and software is needed, then the recovery from system backup of the application configuration for the policy network. The first CMP server is built and restored with the configuration database from a system backup. Replication of the restored database to a second rebuilt CMP node will form a CMP cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in the `Restore Procedures section`. The major activities are summarized as follows:



- Recover one Primary CMP server (if necessary) by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file.
  - The database of the CMP will be restored from a system backup provided by the customer.
  - If a system backup is not available, use customer site survey, and site installation documentation to restore application level configuration to the CMP. It is possible to use the data at the MPEs (that should still be good) to verify that the re-entered data on the CMPs matches the previous configuration that was in-use. Also, check with engineering team for possible approach to verify if the data at the operational MPEs matches the data that has been re-entered at the CMP after re-entering the Policies and other application level data to the CMP.
- Recover the second CMP server by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - The configuration database is available at the now active CMP server and does not require restoration on the second CMP node. Configuration will be replicated when the two new CMP nodes form a cluster.
- Recover any failed MPE/MRA/BOD/MA servers by recovering base hardware and software.
  - Recover the base hardware.

- Recover the software.
- Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
- The configuration database is available at the now active CMP server and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/MRA/BOD/MA servers.

Follow the procedure below for detailed steps.

- Use Procedure 7: Restoring CMP/MA cluster with system backup available below to recover the first of 2 nodes in the CMP cluster.
- Use Procedure 2: Restore standby CMP Node below to recover the second node of the CMP cluster
- Use Procedure 4: Restore single MPE/MRA/BOD/MA node without server backup file to recover MPE/MRA/BOD/MA nodes when one of the peers of the cluster is still available.
  Or Procedure 3: Restore single MPE/MRA/BOD/MA node with server backup file
- Use Procedure 5: Restoring complete cluster with the server backup files
  Or Procedure 6: Restoring complete cluster without the server backup to recover complete MPE/MRA/BOD clusters that have gone down.
- Use Procedure 7: Restoring CMP/MA cluster with system backup available files to recover first of 2 nodes in MA cluster
  Use Procedure 3: Restore single MPE/MRA/BOD/MA node with server backup file to recover the second node of MA cluster.

5. Restore Procedures

5.1. Procedure 1: Restore standby CMP Node with server backup file

The purpose of this procedure is to replace one node of a CMP cluster. Restore initial Policy configuration from a server backup file, and then allow the new node to re-sync to the existing node to form a complete CMP cluster. In this example, initial Policy configuration is restored to the new nodes through the use of server backup files for each server to be restored.

Required resources:

- Replacement node hardware
- TPD installation ISO
- Policy APP installation ISO.
- *serverbackup*.ISO of the node to be replaced

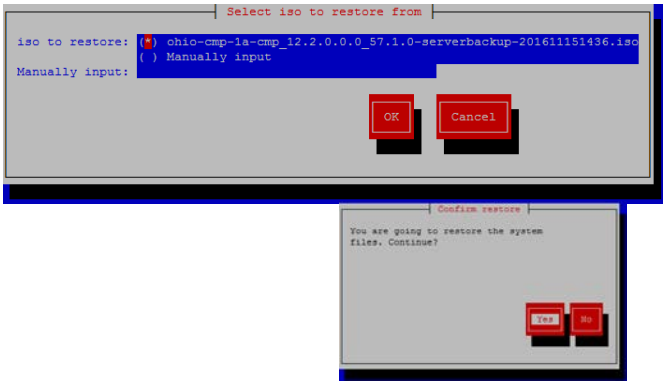
Prerequisites:

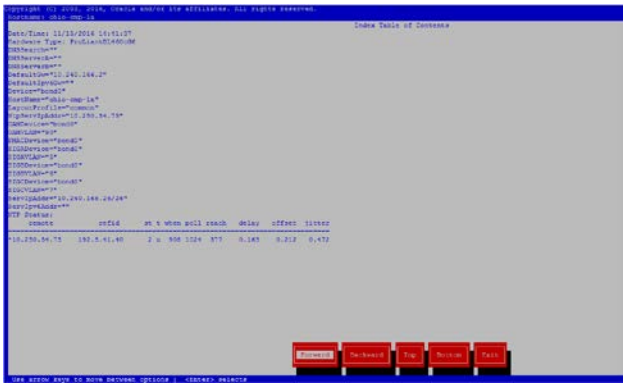
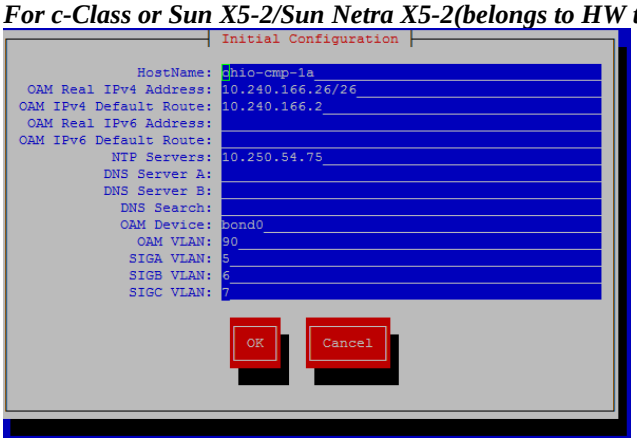
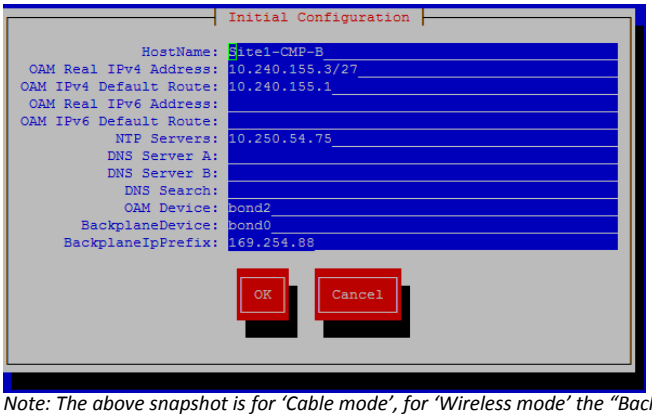
- Power down the failed server gracefully
  - Note: Access the iLO with Administrator privilege, then go to Power Management →Server Power →click on 'Momentary Press'
- Remove failed hardware and replace.
- Verify that the node has TPD on it, or install TPD
- Install application software – CMP
  - Note: Refer to the Policy Management Bare Metal Installation Guide Release 12.2, the documents are available at the Oracle Help Center

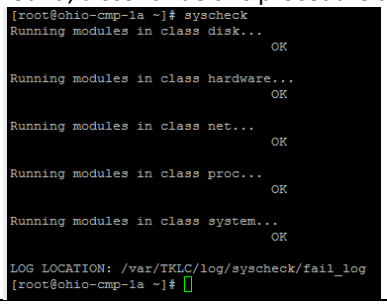
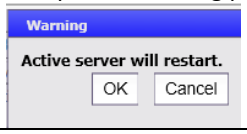
S T E P #	This Procedure restores the standby CMP node when a server level backup is available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	
1. ☐	Set the failed node to 'Forced Standby'	In the CMP GUI, navigate to: **Platform Setting → Topology Settings → All Clusters** 1. Determine the cluster with the failed node 2. Determine the failed node 3. Click the Modify Server-X for the failed node 4. Click the Forced Standby checkbox so that it is checked, then click Save 

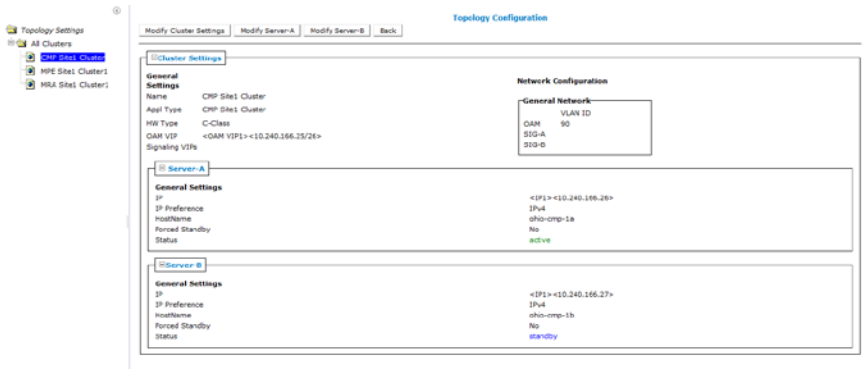
2. ☐	Load the ISO for server restore	Obtain the **serverbackup.iso** for the node to be restored. When the replacement node is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: **`/var/camiant/backup/local_archive/serverbackup`** ***Note:*** *Later in this procedure, the platcfg restore function check this directory and offer the user a convenient menu to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.*

3. ☐	Login via SSH to new node	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

4. ☐	Perform platcfg restore from SSH session to replacement node	Execute the following command: `# su - platcfg` From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.ISO that you just put on the system and hit OK, then 'Yes' to confirm. 
5. ☐	Verify the status	A window will pop-up, indicating restore operation was successful and will ask the user to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

6. ☐	Perform Initial configuration	Choose Exit repeatedly until back to the Main Menu of the *platcfg* utility. While still within the *platcfg* utility, navigate to: **Policy Configuration → Verify Initial Configuration**  If the configuration does not exists, then navigate to '**Perform Initial Configuration'** and fill in the hostname, OAM IP and configuration as shown below: ***For c-Class or Sun X5-2/Sun Netra X5-2(belongs to HW type 'Oracle RMS'):***  Ensure that your data is correct, and select 'Ok', then 'yes' to save and apply **`Exit platcfg`** Exit platcfg by selecting **Exit** from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380):*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*

7. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.
8. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the `syscheck` command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
9. ☐	Remove 'Forced Standby' designation on current node.	In the CMP GUI, navigate to: **Platform Setting → Topology Settings → All Clusters → Current Cluster** 1. Modify for the server that has 'Forced Standby' 2. Clear the Forced Standby checkbox 3. Click Save  Accept the resulting pop-up by clicking OK: 

10. ☐	Verify cluster status	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters→ Current CMP Cluster** Monitor clustering of the new node to its peer, do not proceed until both nodes have a status of either 'active' or 'standby', and that there are no CMP related 'Active Alarms' as shown below. 

11. ☐	Alternative method to check replication status	You can also monitor the clustering of the new node from within the shell on the primary node with 'irepstat'. To do so, SSH to the Active node of the current cluster and execute the irepstat command:
		
		`# irepstat`
		
		Expected 'irepstat' output while waiting reconnection:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1%R 0.05%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.25 1%R 0.05%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.50 1%R 0.04%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.25 1%R 0.05%cpu 85B/s`
		
		Expected 'irepstat' output after cluster has formed:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To ohio-cmp-1b Active 0 0.25 1%R 0.07%cpu 44B/s`
		`AC To ohio-mpe-1a Active 0 0.50 1%R 0.05%cpu 45B/s`
		`AC To ohio-mpe-1b Active 0 0.25 1%R 0.06%cpu 45B/s`
		`AC To ohio-mra-1a Active 0 0.50 1%R 0.04%cpu 50B/s`
		`AC To ohio-mra-1b Active 0 0.25 1%R 0.07%cpu 44B/s`

12. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility as root, please run '`/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root`'; as admusr, please run '`/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`'  This procedure is completed

5.2. Procedure 2: Restore standby CMP Node without server backup file

The purpose of this procedure is to replace one node of a CMP cluster. Restore initial Policy configuration using platcfg's 'Perform Initial Configuration', and then allow the new node to re-sync to the existing node to form a complete CMP cluster. In this example, initial Policy configuration is restored to the new nodes through the use of platcfg's 'Perform Initial Configuration' menu for each server to be restored.

Required resources:

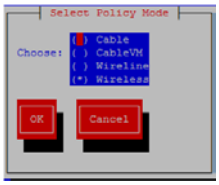
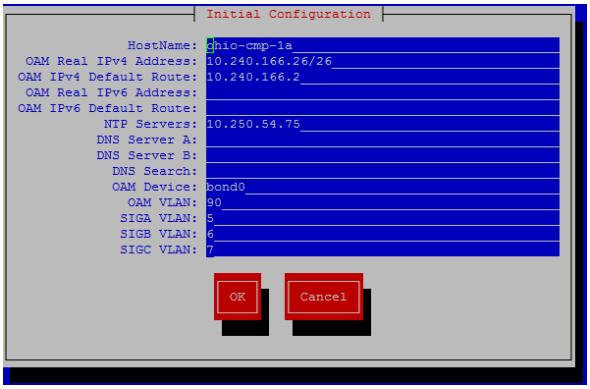
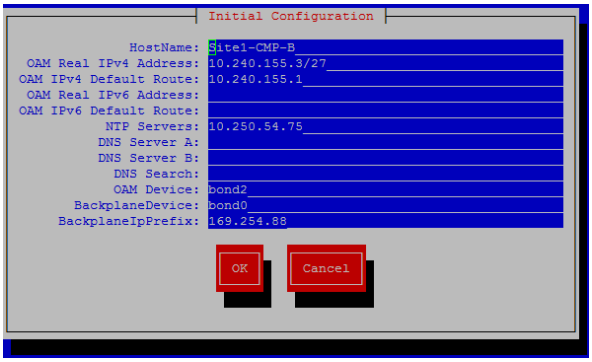
- Replacement node hardware
- TPD installation ISO
- Policy APP installation ISO.
- Node IP addresses, VLANs, NTP IP address, and hostname from CMP GUI

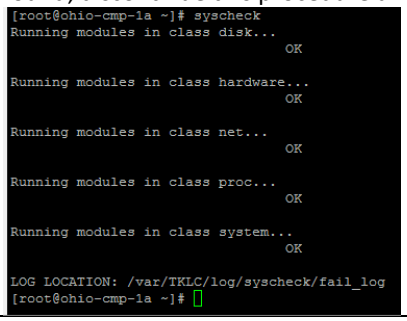
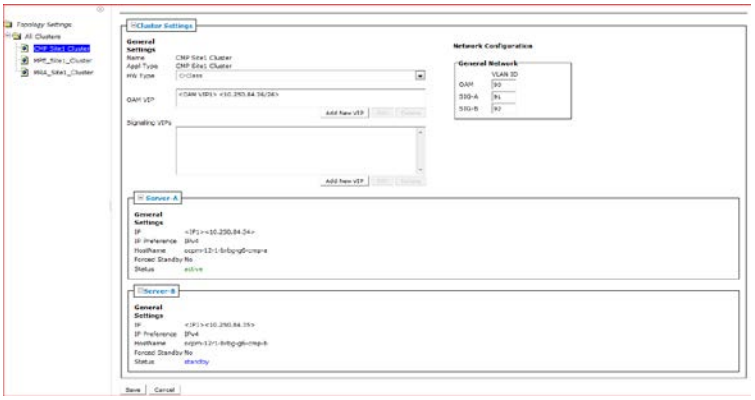
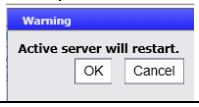
Prerequisites:

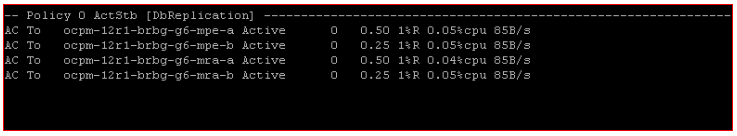
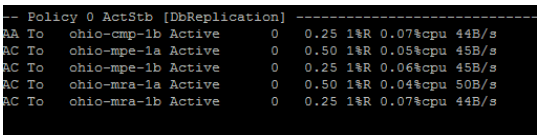
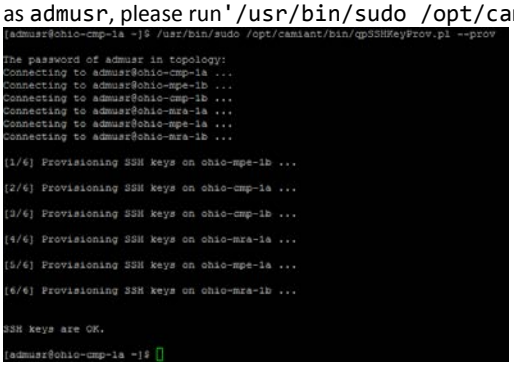
- Power down the failed server gracefully
  - Note: Access the iLO with Administrator privilege, then go to Power Management →Server Power →click on 'Momentary Press'
- Remove failed hardware and replace.
- Verify that the node has TPD on it, or install TPD
- Install application software – CMP
  - Note: Refer to the Policy Management Bare Metal Installation Guide Release 12.2, the documents are available at the Oracle Help Center

S T E P #	This Procedure restores the standby CMP node when a server level backup file is not available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	
1. ☐	Set the failed node to 'Forced Standby'	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 1. Determine the cluster with the failed node 2. Determine the failed node 3. Click the Modify Server-X for the failed node 4. Click the Forced Standby checkbox so that it is checked, then click Save  *Note: From the above screenshot, the Network Configuration/General Network(VLAN ID) will not appear for RMS (DL 360/ DL380) Hardware*

2. ☐	Login via SSH to new node	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

3. ☐	Perform platcfg restore from SSH session to replacement node Perform Initial configuration	Execute the following command `# su - platcfg` a) From within the platcfg utility, navigate to: **Policy Configuration → Set Policy Mode**  Choose 'Cable' if solution is for cable mode or leave it as default 'Wireless' if it will be wireless mode and select OK to continue. b)From within the platcfg utility, navigate to: **Policy Configuration → Perform Initial Configuration** Enter the appropriate configuration details for this node, verify that entries are correct, and select 'OK' to continue. Accept the resulting popup that appears asking to apply the configuration. Once the operation is complete, select 'Exit' on the platcfg menu until you are dropped back to the shell. ***For c-Class or Sun X5-2/Sun Netra X5-2(belongs to HW type 'Oracle RMS'):***  Ensure that configured data is correct, and select 'OK', then 'yes' to save and apply **Exit platcfg** Exit platcfg by selecting **Exit** from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380):*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*

4. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.
5. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
6. ☐	Remove 'Forced Standby' designation on current node.	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → Current Cluster** 1. Modify for the server that has 'Forced standby' 2. Clear the Forced Standby checkbox 3. Click Save  Accept the resulting pop-up by clicking OK: 

7. ☐	Verify cluster status	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All → Current CMP Cluster** Monitor clustering of the new node to its peer, do not proceed until both nodes have a status of either '*active*' or '*standby*', and that there are no CMP related 'Active Alarms' as shown below. 
8. ☐	Alternative method to check replication status	You can also monitor the clustering of the new node from within the shell on the primary node with 'irepstat'. To do so, SSH to the Active node of the current cluster and execute the irepstat command: `# irepstat` Expected 'irepstat' output while waiting reconnection:  Expected 'irepstat' output after cluster has formed: 
9. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility as `root`, please run `'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root'`; as `admusr`, please run `'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'`;  This procedure is completed.

5.3. Procedure 3: Restore single MPE/MRA/BOD/MA node with server backup file

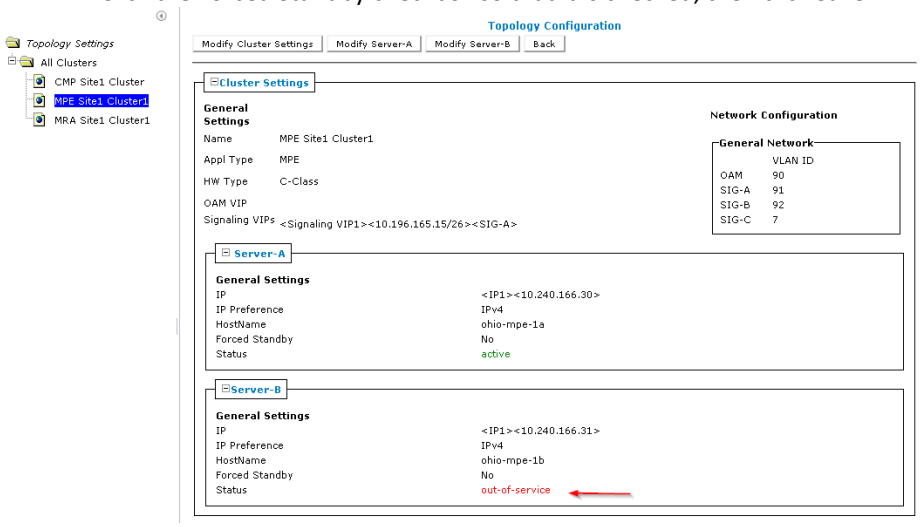
The purpose of this procedure is to replace one node of a policy cluster. Restore initial Policy configuration from a server backup file, and then allow the new node to re-sync to the existing node to form a complete cluster. In this example, initial Policy configuration is restored to the new nodes through the use of server backup files for each server to be restored.

Required resources:

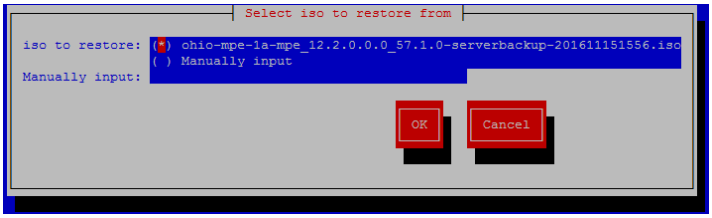
- Replacement node hardware
- TPD installation ISO
- Policy APP installation ISO.
- *serverbackup*.ISO of the node to be replaced

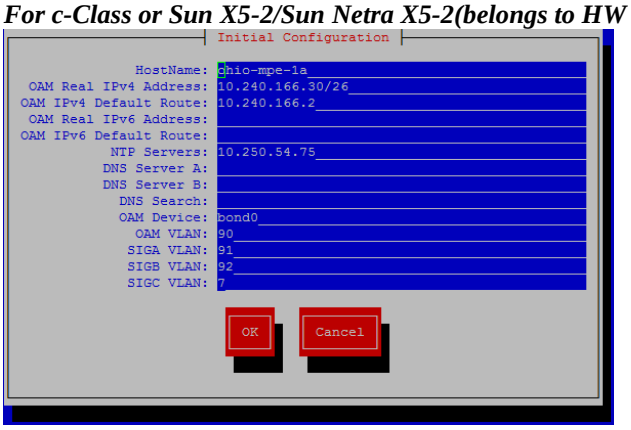
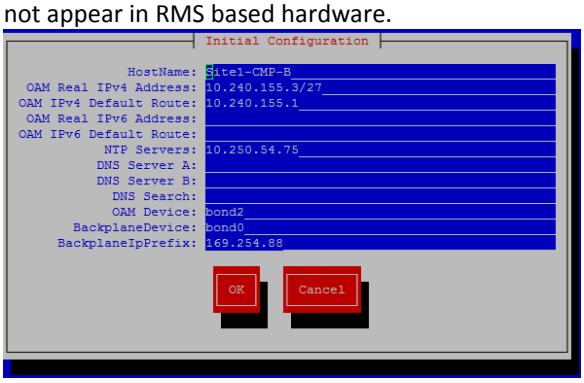
Prerequisites:

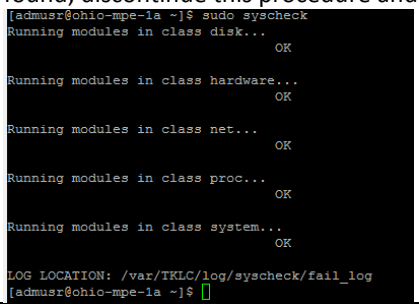
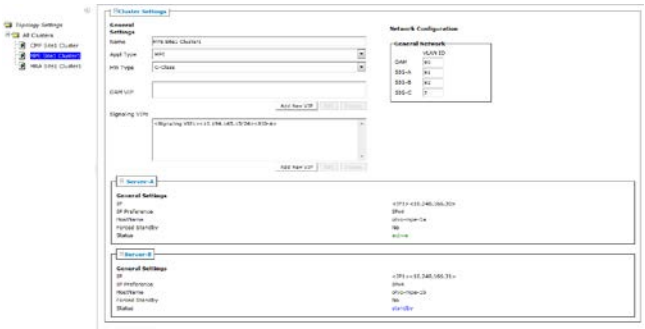
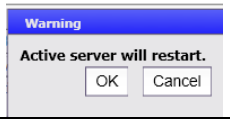
- Power down the failed server gracefully
    - Note: Access the iLO with Administrator privilege, then go to Power Management →Server Power →click on 'Momentary Press'
- Remove failed hardware and replace.
- Verify that the hardware had TPD on it, or install TPD
- Install application software – MPE or MRA or BOD or MA
    - Note: Refer to the Policy Management Bare Metal Installation Guide Release 12.2, the documents are available at the Oracle Help Center

S T E P #	This procedure performs Restore single MPE/MRA/BOD/MA node with server backup file. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	
1. ☐	Set the failed node to 'Forced Standby'	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 1. Determine the cluster with the failed node 2. Determine the failed node 3. Click the Modify Server-X for the failed node 4. Click the Forced Standby checkbox so that it is checked, then click Save 
2. ☐	Load the ISO for server backup	Obtain the *serverbackup.iso* for the node to be restored. When the replacement node is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: **`/var/camiant/backup/local_archive/serverbackup`** ***Note:*** *Later in this procedure, the platcfg restore function check this directory and offer the user a convenient menu to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.*

3. ☐	Login via SSH to new node	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

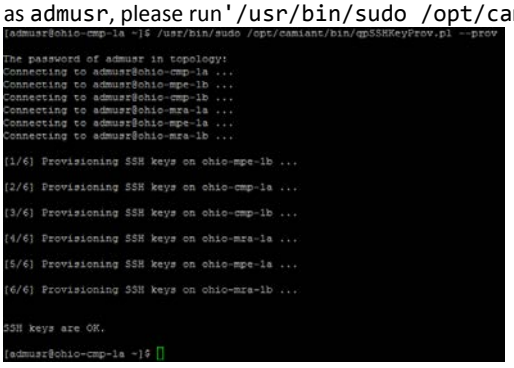
4. ☐	Perform platcfg restore from SSH session to replacement hardware	Execute the following command: `# su - platcfg` From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.ISO that you just put on the system and hit 'ok' – then 'yes' to confirm.  
5. ☐	Verify the status	A window will pop-up, indicating restore operation was successful and will ask the user to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

6. ☐	Perform Initial configuration	Choose Exit repeatedly until back to the Main Menu of the platcfg utility. While still within the platcfg utility, navigate to:**Policy Configuration → Verify Initial Configuration**  If the configuration does not exists, then navigate to **'Perform Initial Configuration'** and fill in initial configuration: hostname, OAM IP and NTP servers configurations as shown below: ***For c-Class or Sun X5-2/Sun Netra X5-2(belongs to HW type 'Oracle RMS'):***  Ensure the configured data is correct, and select 'OK', then 'yes' to save and apply **Exit platcfg**. Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*	

7. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.
8. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the `syscheck` command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
9. ☐	Remove 'Forced Standby' designation on current node.	In the CMP GUI, navigate to: **Platform Setting → Topology Settings → All Clusters → Current Cluster** 1. Modify for the server that has 'Forced Standby' 2. Clear the 'Forced Standby' checkbox 3. Click Save  Accept the resulting pop-up by clicking OK: 

10. ☐	Check status	In the CMP GUI, depending on the type of the node, perform the following: If this is an MPE node, navigate to: **Policy Server → Configuration → All→*<Recovered MPE Cluster>*→ Reports Tab** If this is an MRA node, navigate to: **MRA → Configuration → All →*<Recovered MRA Cluster>*→ Reports Tab** If this is an BOD node, navigate to: **BOD → Configuration → All →*<Recovered BOD Cluster>*→ Reports Tab** If this is an MA node, navigate to: **MA →*<Recovered MA Cluster>*→Reports Tab** Monitor clustering of the new node to its peer, do not proceed until the Cluster Status returns from '*Degraded*' to '*On-line'* 

11. ☐	Alternative method to check replication status	You can also monitor the clustering of the new node from within the shell on the primary node with 'irepstat'. To do so, SSH to the Active node of the current cluster and execute the irepstat command:
		
		`# irepstat`
		Expected 'irepstat' output while waiting reconnection:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC From ocpm-12r1-brbg-g6-cmp-a Active 0 0.25 ^0.04%cpu 45B/s A=me`
		
		Expected 'irepstat' output after cluster has formed:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC From ocpm-12r1-brbg-g6-cmp-a Active 0 0.25 ^0.04%cpu 52B/s A=C2488.184`
		`CC From ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 ^0.06 2.45%cpu 35B/s A=C2488.184`

12. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility
		as `root`, please run `'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root';`
		as `admusr`, please run`'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov';`
		 
		`[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:`
		`Connecting to admusr@ohio-cmp-1a ...`
		`Connecting to admusr@ohio-mpe-1b ...`
		`Connecting to admusr@ohio-cmp-1b ...`
		`Connecting to admusr@ohio-mra-1a ...`
		`Connecting to admusr@ohio-mpe-1a ...`
		`Connecting to admusr@ohio-mra-1b ...`
		`[1/6] Provisioning SSH keys on ohio-mpe-1b ...`
		`[2/6] Provisioning SSH keys on ohio-cmp-1a ...`
		`[3/6] Provisioning SSH keys on ohio-cmp-1b ...`
		`[4/6] Provisioning SSH keys on ohio-mra-1a ...`
		`[5/6] Provisioning SSH keys on ohio-mpe-1a ...`
		`[6/6] Provisioning SSH keys on ohio-mra-1b ...`
		`SSH keys are OK.`
		`[admusr@ohio-cmp-1a ~]$`
		
		This procedure is completed.

5.4. Procedure 4: Restore single MPE/MRA/BOD/MA node without server backup file

The purpose of this procedure is to create a policy cluster from the replacement of one node of the cluster. The active primary node will then synchronize the newly installed node to complete the cluster. In this example, initial policy configuration is restored to the new node by manual entry.

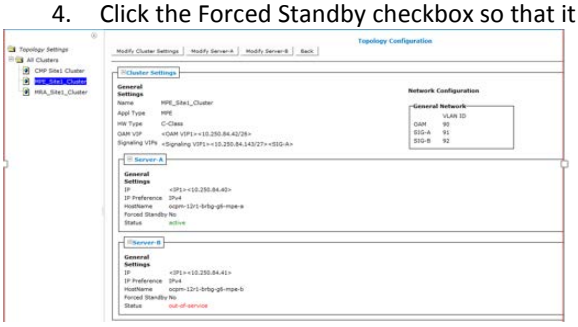
Required resources:

- Replacement node hardware.
- TPD installation ISO.
- Policy APP installation ISO.
- Initial configuration information about the node to be restored:
  - OAM IP address, default gateway, NTP & SNMP server IP addresses
  - VLAN configuration information.

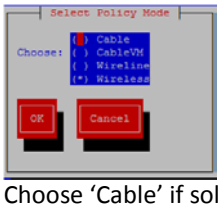
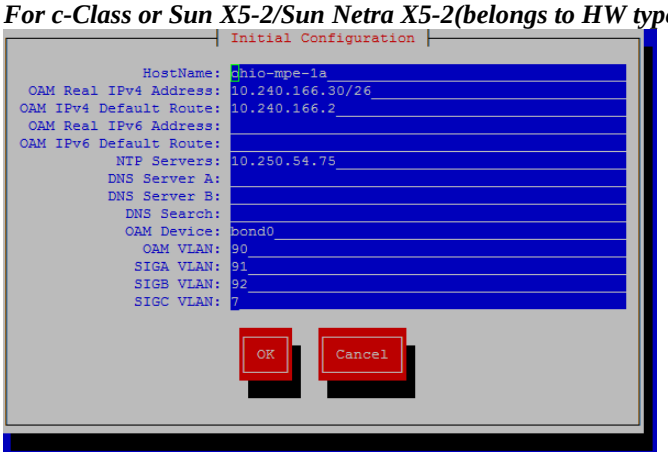
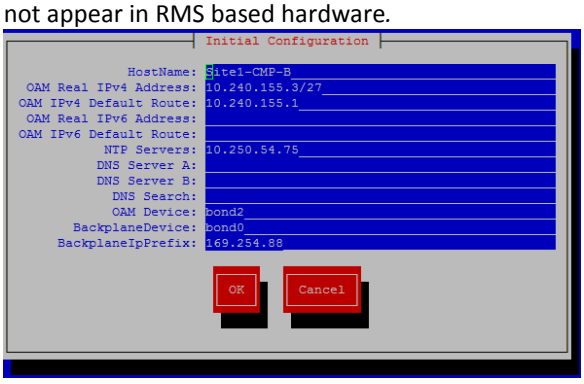
Hostname, OAM IP address, and VLAN configuration can be gleaned from:
Platform Setting → Topology Setting → <Cluster_Name>
NTP server configuration (and optionally DNS configuration can be gotten from platcfg of the running node)
Verify that routing is configured correctly i.e. XSI is default and any associated OAM routes are added.

Prerequisites:

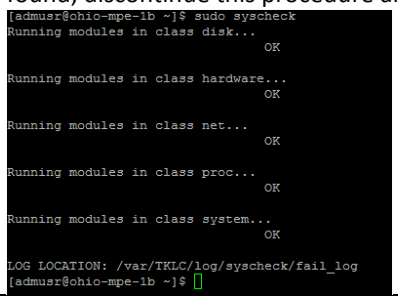
- Power down the failed server gracefully
  - Note: Access the iLO with Administrator privilege, then go to Power Management →Server Power →click on 'Momentary Press'
- Remove failed hardware and replace.
- Verify that the node has TPD on it, or install TPD
- Install application software – MPE or MRA or BOD or MA
  - Note: Refer to the Policy Management Bare Metal Installation Guide Release 12.2, the documents are available at the Oracle Help Center

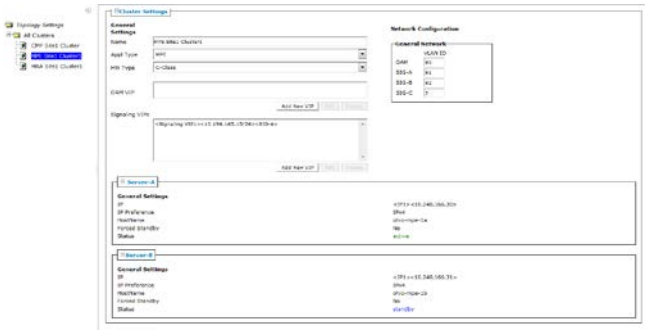
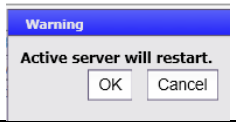
S T E P #	This Procedure performs Restore single MPE/MRA/BOD/MA node without server backup file Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	
1. ☐	Set the failed node to 'Forced Standby'	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 1. Determine the cluster with the failed node 2. Determine the failed node Note: It is possible that for a Geo-Redudant Topology, the server C will be a failed node could be spare Server-C (as per below screen shot) 3. Click the Modify Server-X for the failed node 4. Click the Forced Standby checkbox so that it is checked, then click Save  *Server-C (spare): In a Geo-Redundant Topology* 

2. ☐	Login via SSH to new node	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

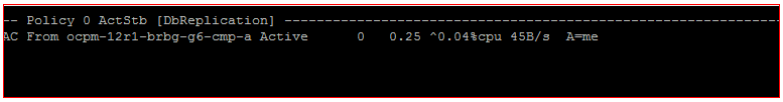
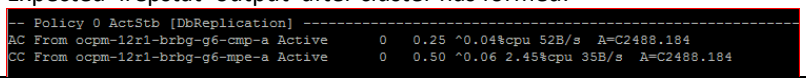
3. ☐	Perform 'Initial Policy Configuration' from within platcfg utility on newly installed node	Execute the following command `# su - platcfg` a) From within the platcfg utility, navigate to: **Policy Configuration → Set Policy Mode**  Choose 'Cable' if solution is for cable mode or leave it as default 'Wireless' if it will be wireless mode and select OK to continue. b)From within the platcfg utility, navigate to: **Policy Configuration → Perform Initial Configuration**. Enter the configuration details from the node being replaced: ***For c-Class or Sun X5-2/Sun Netra X5-2(belongs to HW type 'Oracle RMS'):***  Once the server details are entered and verified for correctness select 'Ok'. A menu will appear asking if the new settings should be applied, select 'YES' and allow the operation to complete. No specific message is given when the operation is successful, but an error will appear if it was not completed. In this case, review the settings from the 'Perform Initial Configuration screen again, if all appears as expected, contact My Oracle Support before proceeding. Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist*.

4. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.

5. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.
		`# ping <XMI or OAM gateway address>`
		
		Execute the `syscheck` command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.
		 
		`[admusr@ohio-mpe-1b ~]$ sudo syscheck`
		`Running modules in class disk...`
		`OK`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`Running modules in class system...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		`[admusr@ohio-mpe-1b ~]$`

6. ☐	Remove 'Forced Standby' designation on current blade.	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → Current Cluster** 1. Modify for the server that has 'Forced Standby' 2. Clear the 'Forced Standby' checkbox 3. Click Save  Accept the resulting pop-up by clicking OK: 

7. ☐	Check status	In the CMP GUI, depending on the type of the blade, perform the following: If this is an MPE node, navigate to: **Policy Server → Configuration → All→*<Recovered MPE Cluster>*→ Reports Tab** If this is an MRA node, navigate to: **MRA → Configuration → All →*<Recovered MRA Cluster>*→ Reports Tab** If this is an BOD node, navigate to: **BOD → Configuration → All →*<Recovered BOD Cluster>*→ Reports Tab** If this is an MA node, navigate to: **MA →*<Recovered MA Cluster>*→Reports Tab** Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from '*Degraded*' to '*On-line'* 

8. ☐	Alternative method to check replication status	You can also monitor the clustering of the new blade from within the shell on the primary node with 'irepstat'. To do so, SSH to the Active node of the current cluster and execute the irepstat command:
		`# irepstat`
		Expected 'irepstat' output while waiting reconnection:
		 
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC From ocpm-12r1-brbg-g6-cmp-a Active 0 0.25 ^0.04%cpu 45B/s A=me`
		
		Expected 'irepstat' output after cluster has formed:
		 
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC From ocpm-12r1-brbg-g6-cmp-a Active 0 0.25 ^0.04%cpu 52B/s A=C2488.184`
		`CC From ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 ^0.06 2.45%cpu 35B/s A=C2488.184`

9. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility
		as `root`, please run `'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root';`
		as `admusr`, please run`'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'`
		 
		`[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:`
		`Connecting to admusr@ohio-cmp-1a ...`
		`Connecting to admusr@ohio-mpe-1b ...`
		`Connecting to admusr@ohio-cmp-1b ...`
		`Connecting to admusr@ohio-mra-1a ...`
		`Connecting to admusr@ohio-mpe-1a ...`
		`Connecting to admusr@ohio-mra-1b ...`
		`[1/6] Provisioning SSH keys on ohio-mpe-1b ...`
		`[2/6] Provisioning SSH keys on ohio-cmp-1a ...`
		`[3/6] Provisioning SSH keys on ohio-cmp-1b ...`
		`[4/6] Provisioning SSH keys on ohio-mra-1a ...`
		`[5/6] Provisioning SSH keys on ohio-mpe-1a ...`
		`[6/6] Provisioning SSH keys on ohio-mra-1b ...`
		`SSH keys are OK.`
		`[admusr@ohio-cmp-1a ~]$ clear`
		
		This procedure is completed.

5.5. Procedure 5: Restoring complete cluster with the server backup files

The purpose of this procedure is to create a policy cluster from replacement hardware and software, then restore application level configuration by push that configuration from the active CMP. In this example, initial Policy configuration is restored to the new blades through the use of server backup files for each server to be restored.

Required resources:

- Replacement blade
- TPD installation ISO
- Policy APP installation ISO.
- *serverbackup*.iso of the blade to be replaced

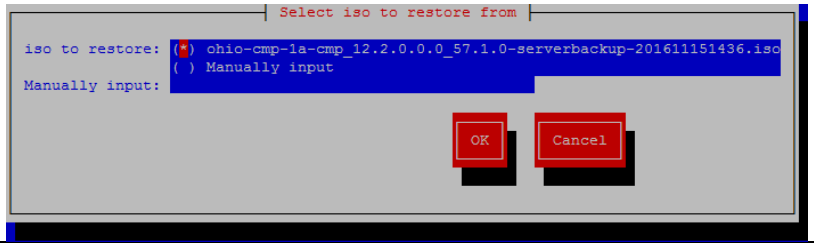
Prerequisites:

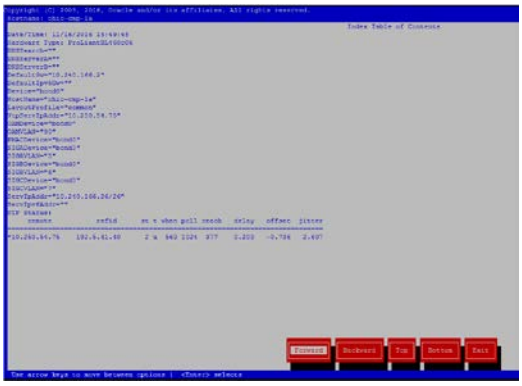
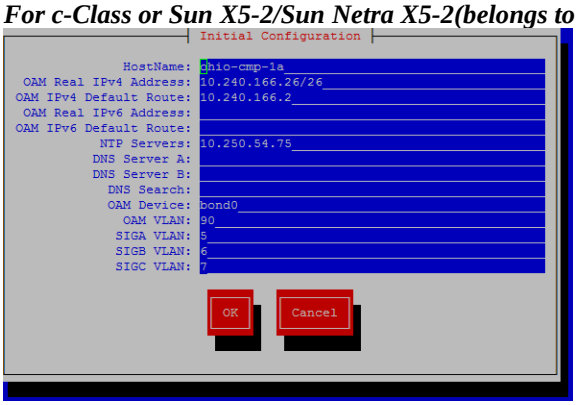
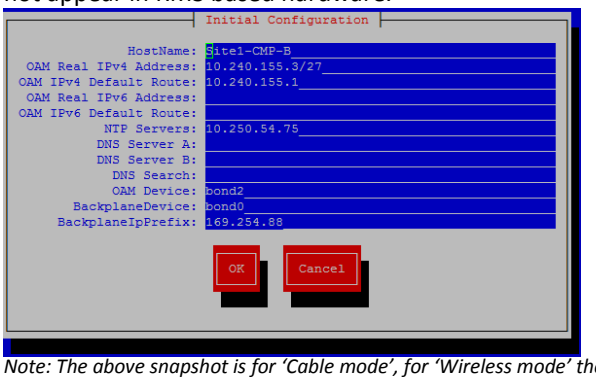
- Power down the failed server gracefully
  - Note: Access the iLO with Administrator privilege, then go to Power Management →Server Power →click on 'Momentary Press'
- Remove and replace both blades
- IPM both blades
- Install application on both blades(either CMP, MPE, MRA, BOD, MA)
  - Note: In case it is a CMP Cluster that is being rebuilt, restore application data either from system backup or manually if no backup available.
  - Note: Refer to the Policy Management Bare Metal Installation Guide Release 12.2, the documents are available at the Oracle Help Center

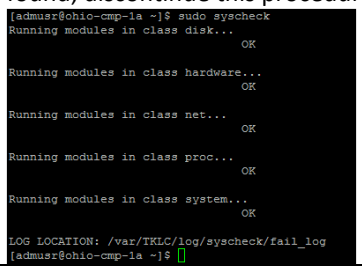
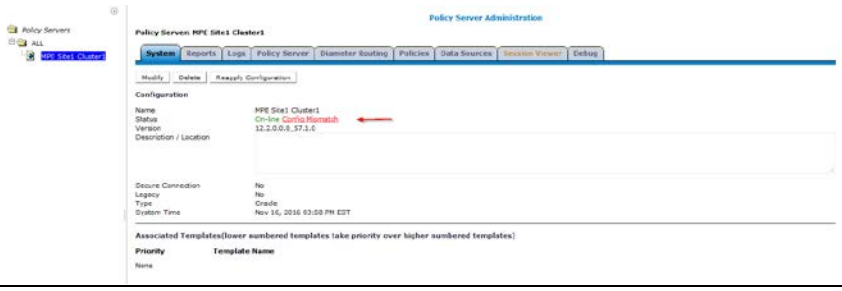
S T E P #	This Procedure performs Restoring complete cluster with the server backup files Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	

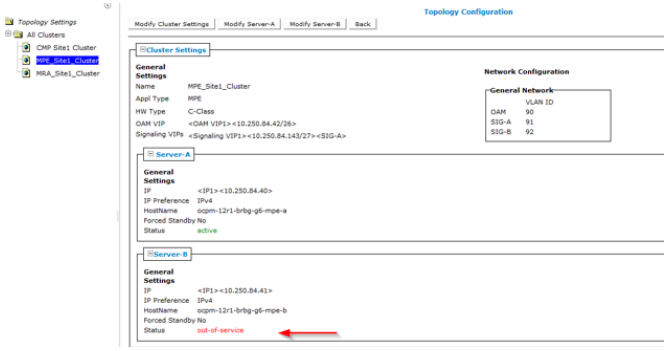
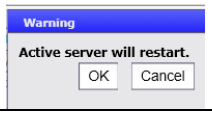
1. ☐	SSH to replacement blade	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

2. ☐	Load the ISO to restore 1st server of the cluster	Obtain the *serverbackup.iso* for the blade to be restored. When the replacement blade is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: **`/var/camiant/backup/local_archive/serverbackup`** ***Note:*** *Later in this procedure, the platcfg restore function check this directory and offer the user a convenient menu to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.*

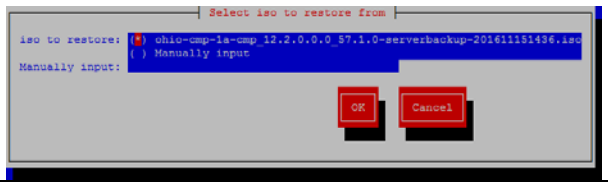
3. ☐	Perform platcfg restore from SSH session to replacement blade	Execute the following command `# su - platcfg` From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.iso that you just put on the system and hit ok – then 'yes' to confirm. 
4. ☐	Verify the status	A window will pop-up, indicating restore operation was successful and will ask the user to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance.

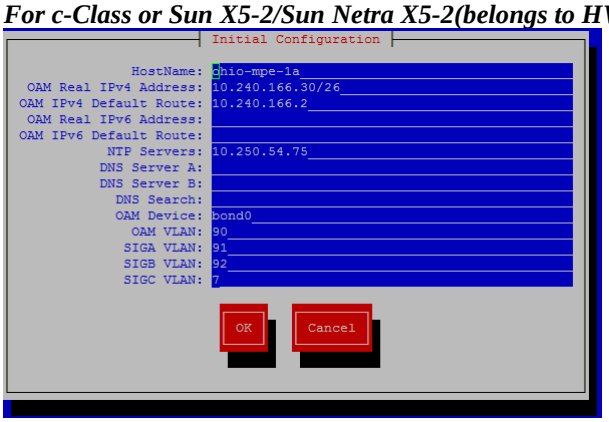
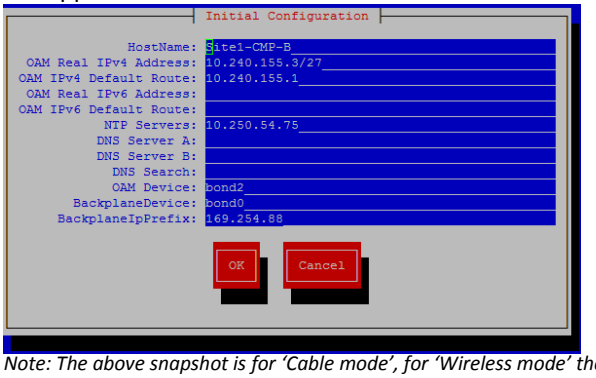
5. ☐	Verify Initial configuration	Choose Exit repeatedly until back to the Main Menu of the platcfg utility. While still within the platcfg utility, navigate to:**Policy Configuration → Verify Initial Configuration**  If the configuration does not exists, then navigate to **'Perform Initial Configuration'** and fill in initial configuration: hostname, OAM IP and NTP servers configurations as shown below: ***For c-Class or Sun X5-2/Sun Netra X5-2(belongs to HW type 'Oracle RMS'):***  Ensure that your data is correct, and select 'Ok', then 'yes' to save and apply **Exit platcfg**: Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*

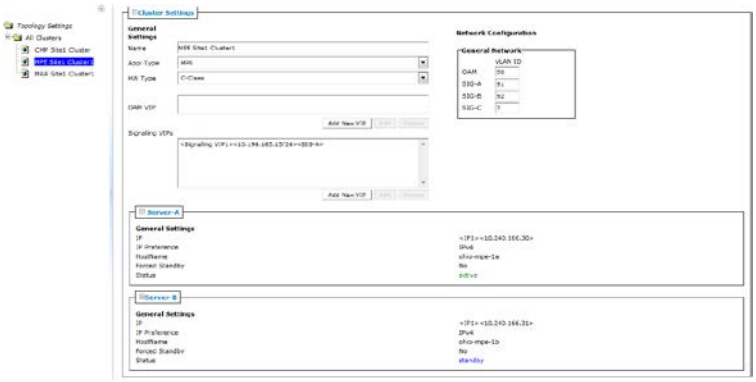
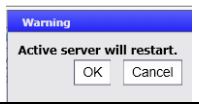
6. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.	
7. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the `syscheck` command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  	
8. ☐	Check status	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** Check system tab for the cluster. If the Status field indicates '*Config Mismatch*', click the '***Reapply Configuration***' button and wait for the '*Config Mismatch*' designation to disappear. If it does not, contact My Oracle Support before proceeding.  	

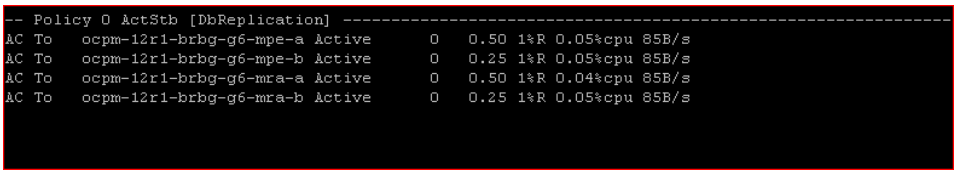
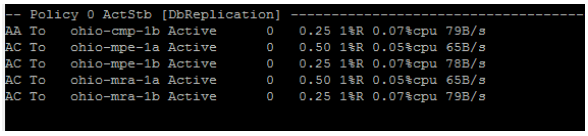
9. ☐	Set 'Forced Standby' designation on cluster node that is still 'out-of-service'.	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → Current Cluster** 1. Modify for the server that has a status of '*out-of-service*' 2. Check the Forced Standby checkbox 3. Click Save  Accept the resulting pop-up by clicking OK: 

10. ☐	SSH from the PM&C server to replacement blade	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System: Use the iLo to login, and a remote console session need to be started to execute commands

11. ☐	Load the ISO to restore 2nd server of the cluster	Obtain the *serverbackup.iso* for the blade to be restored. When the replacement blade is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: **`/var/camiant/backup/local_archive/serverbackup`** ***Note:*** *Later in this procedure, the platcfg restore function check this directory and offer the user a convenient menu to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.*
12. ☐	Perform platcfg restore from SSH session to replacement blade	Execute the following command `# su – platcfg` From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.iso that you just put on the system and hit ok – then 'yes' to confirm. 
13. ☐	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding.

14. ☐	Verify Initial configuration	Choose Exit repeatedly until back to the Main Menu of the platcfg utility. While still within the platcfg utility, navigate to:**Policy Configuration → Verify Initial Configuration**  If the configuration does not exists, then navigate to **'Perform Initial Configuration'** and fill in initial configuration: hostname, OAM IP and NTP servers configurations as shown below: ***For c-Class or Sun X5-2/Sun Netra X5-2(belongs to HW type 'Oracle RMS'):***  Ensure that your data is correct, and select 'Ok', then 'yes' to save and apply **Exit platcfg** Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*

15. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.
16. ☐	Remove 'Forced Standby' designation on current blade.	In the CMP GUI, navigate to: **Platform Setting → Topology Settings → Current Cluster** 1. Modify for the server that has 'Forced Standby' 2. Clear the 'Forced Standby' checkbox 3. Click Save  Accept the resulting pop-up by clicking OK: 
17. ☐	Check status	In the CMP GUI, depending on the type of the blade, perform the following: If this is an MPE node, navigate to: **Policy Server → Configuration → All→*<Recovered MPE Cluster>*→ Reports Tab** If this is an MRA node, navigate to: **MRA → Configuration → All →*<Recovered MRA Cluster>*→ Reports Tab** If this is an BOD node, navigate to: **BOD → Configuration → All →*<Recovered BOD Cluster>*→ Reports Tab** If this is an MA node, navigate to: **MA →*<Recovered MA Cluster>*→Reports Tab** Check CMP cluster status (as indicated in the previous step), navigate to: **Platform Setting → Topology Setting → Current CMP Cluster** Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from *'Degraded'* to *'On-Line'* 

18. ☐	Alternative method to check replication status	You can also monitor the clustering of the new blade from within the shell on the primary node with 'irepstat'. To do so, SSH to the Active node of the current cluster and execute the irepstat command: `# irepstat` Expected 'irepstat' output while waiting reconnection:  Expected 'irepstat' output after cluster has formed: 
19. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility as `root`, please run `'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root';` as `admusr`, please run `'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'`  This procedure is completed.

5.6. Procedure 6: Restoring complete cluster without the server backup

The purpose of this procedure is to restore a policy cluster without the server backup file. The active primary blade will then synchronize the newly installed blade to complete the cluster. In this example, initial Policy configuration is restored to the new blade by manual entry.

Required resources:

- Replacement blade.
- TPD installation ISO.
- Policy APP installation ISO.
- Initial configuration information about the blade to be restored:
  - OAM blade Ip address, default gateway, ntp server ip address
  - Vlan configuration information.

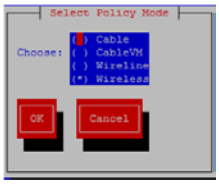
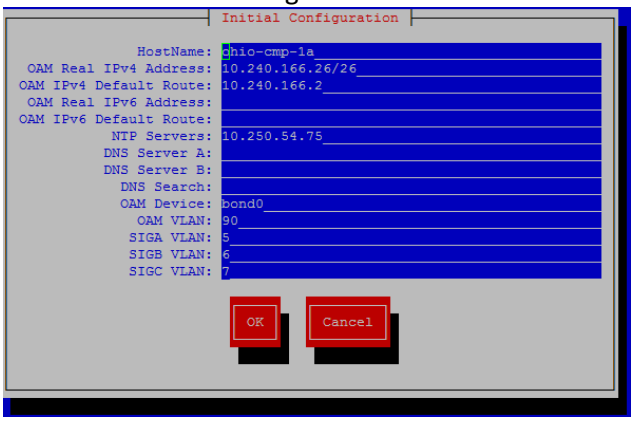
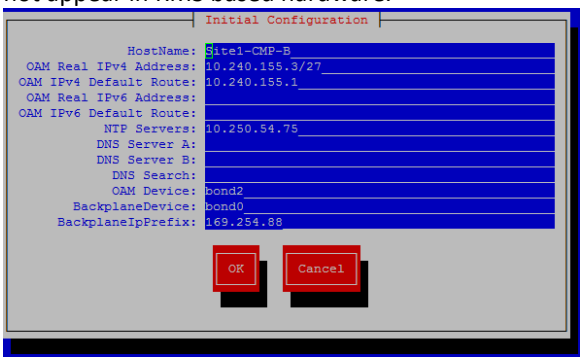
Hostname, OAM IP address, and VLAN configuration can be gleaned from:
Platform Setting → Topology Setting → <Cluster_Name>
NTP server configuration (and optionally DNS configuration can be gotten from platcfg of the running blade)
Verify that routing is configured correctly i.e. XSI is default and any associated OAM routes are added.

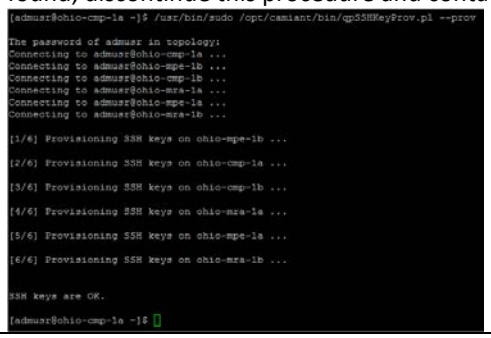
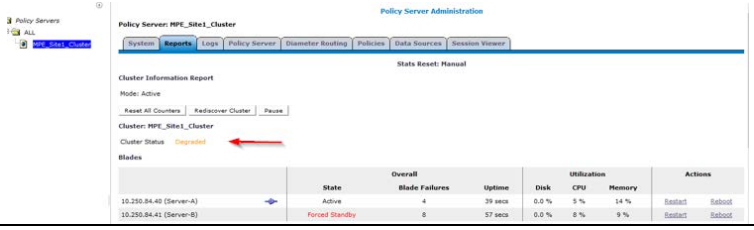
Prerequisites:

- Power down the failed server gracefully
  - Note: Access the iLO with Administrator privilege, then go to Power Management →Server Power →click on 'Momentary Press'
- Remove failed blade and replace.
- Verify that the blade had TPD on it, or install TPD
- Install application software – CMP, MPE, MRA, BOD or MA
  - Note: In case it is a CMP Cluster that is being rebuilt, restore application data either from system backup or manually if no backup available.
  - Note: Refer to the Policy Management Bare Metal Installation Guide Release 12.2, the documents are available at the Oracle Help Center

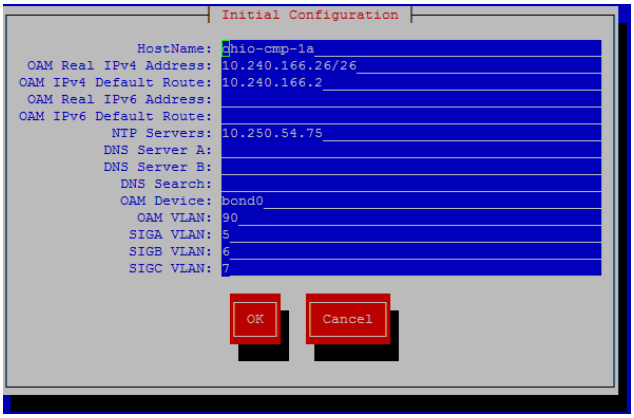
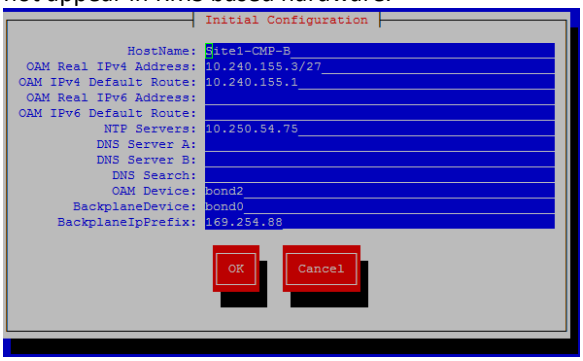
S T E P #	This Procedure performs Restoring complete cluster without the server backup Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) and ask for assistance.	

1. ☐	Login via SSH to new blade	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

2. ☐	Perform 'Initial Policy Configuration' from within platcfg utility on newly installed blade	Execute the following command `# su - platcfg` a) From within the platcfg utility, navigate to: **Policy Configuration → Set Policy Mode**  Choose 'Cable' if solution is for cable mode or leave it as default 'Wireless' if it will be wireless mode and select OK to continue. b)From within the platcfg utility, navigate to: **Policy Configuration → Perform Initial Configuration** Enter the relevant configuration details from the blade being replaced:  Once the server details are entered and verified for correctness select 'Ok'. A menu will appear asking if the new settings should be applied, select 'YES' and allow the operation to complete. No specific message is given when the operation is successful, but an error will appear if it was not completed. In this case, review the settings from the 'Perform Initial Configuration screen again, if all appears as expected, contact My Oracle Support before proceeding. Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*

3. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.
4. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
5. ☐	Check status	In the CMP GUI, depending on the type of the blade, perform the following: If this is an MPE node, navigate to: **Policy Server → Configuration → All→*<Recovered MPE Cluster>*→ Reports Tab** If this is an MRA node, navigate to: **MRA → Configuration → All →*<Recovered MRA Cluster>*→ Reports Tab** If this is an BOD node, navigate to: **BOD → Configuration → All →*<Recovered BOD Cluster>*→ Reports Tab** If this is an MA node, navigate to: **MA →*<Recovered MA Cluster>*→Reports Tab** Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from `'Off-line' to 'Degraded'.` *Off-line*  *Degraded* 

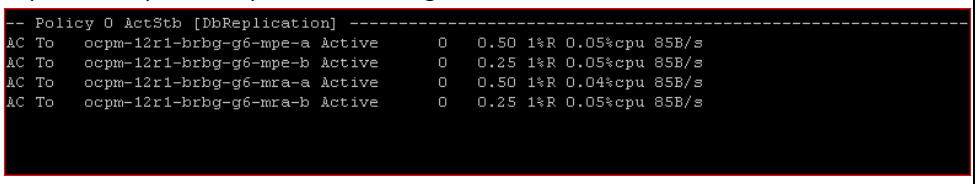
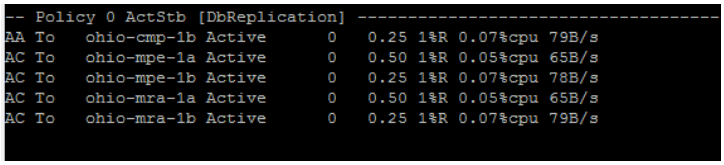
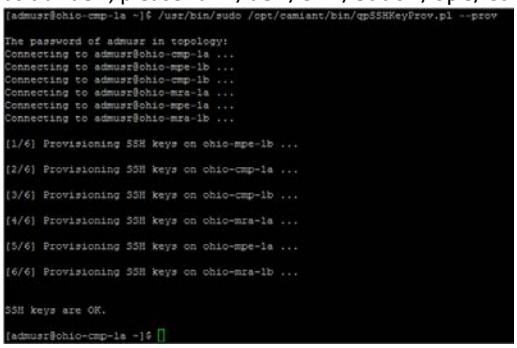
6. ☐	Login via SSH to second node of the current cluster	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.	

7. ☐	Perform 'Initial Policy Configuration' from within platcfg utility on second node of cluster	Execute the following command `# su – platcfg` From within the platcfg utility, navigate to: **Policy Configuration → Initial Configuration** Enter the relevant details from the blade being replaced:  Once the server details are entered and verified for correctness select 'Ok'. A menu will appear asking if the new settings should be applied, select 'YES' and allow the operation to complete. No specific message is given when the operation is successful, but an error will appear if it was not completed. In this case, review the settings from the 'Perform Initial Configuration screen again, if all appears as expected, contact My Oracle Support before proceeding. **Exit platcfg** by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist*.	

8. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.

9. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.
		`# ping <XMI or OAM gateway address>`
		
		Execute the `syscheck` command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.
		`[admusr@ohio-cmp-1a ~]$ sudo syscheck`
		`Running modules in class disk...`
		`OK`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`Running modules in class system...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		`[admusr@ohio-cmp-1a ~]$`

10. ☐	Check status	In the CMP GUI, depending on the type of the blade, perform the following: If this is an MPE node, navigate to: **Policy Server → Configuration → All→*<Recovered MPE Cluster>*→ Reports Tab** If this is an MRA node, navigate to: **MRA → Configuration → All →*<Recovered MRA Cluster>*→ Reports Tab** If this is an BOD node, navigate to: **BOD → Configuration → All →*<Recovered BOD Cluster>*→ Reports Tab** If this is an MA node, navigate to: **MA →*<Recovered MA Cluster>*→Reports Tab** Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from `'Degraded' to 'On-line'` *MPE:*  *MRA:* 

11. ☐	Alternative method to check replication status	You can also monitor the clustering of the new blade from within the shell on the primary node with 'irepstat'. To do so, SSH to the Active node of the current cluster and execute the irepstat command: `# irepstat` Expected 'irepstat' output while waiting reconnection:  Expected 'irepstat' output after cluster has formed: 
12. ☐	Exchange keys with cluster mate (This step need to run from active CMP)	Exchanging SSH keys Utility as `root`, please run `'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root';` as `admusr`, please run `'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'`  This procedure is completed.

5.7. Procedure 7: Restoring CMP/MA cluster with system backup available

The purpose of this procedure is to re-create a CMP with the application level configuration of the policy network that can be used to re-create the policy network that is to be recovered. Once a CMP is online, all other servers of the policy network can be re-created using the above procedures and then their application level configuration restored from this CMP. In the case of a massive outage that includes the CMP, at least one of the CMP blades should be restored first.

Required resources:

- Replacement blade.
- TPD installation ISO.
- Policy APP installation ISO.
- Recent System backup file.
- Initial configuration information about the blade to be restored:
  - OAM IP address, default gateway, NTP & SNMP server IP addresses
  - VLAN configuration information.

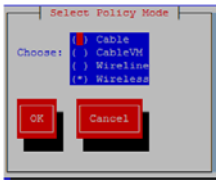
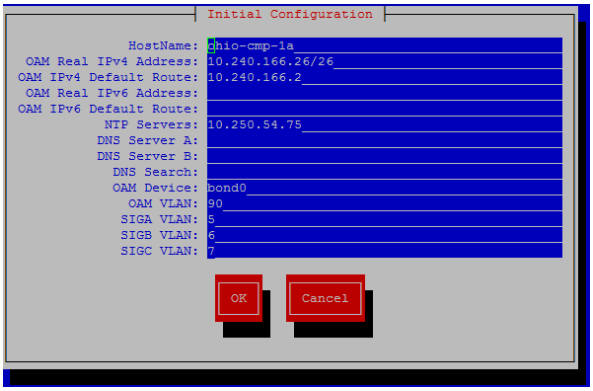
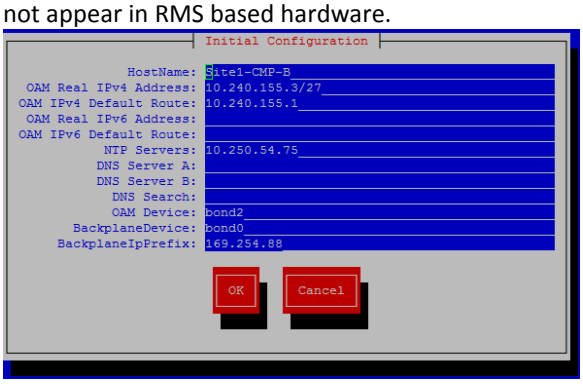
Hostname, OAM IP address, and VLAN configuration can be gleaned from:
Platform Setting → Topology Setting → <Cluster_Name>
NTP server configuration (and optionally DNS configuration can be gotten from platcfg of the running blade)
Verify that routing is configured correctly i.e. XSI is default and any associated OAM routes are added.

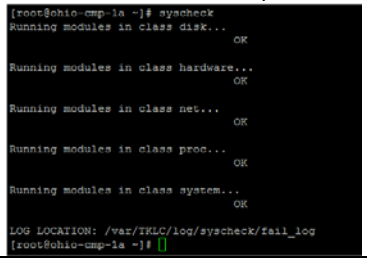
Prerequisites:

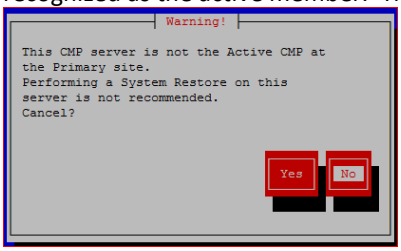
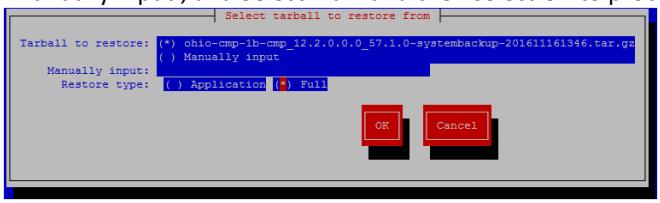
- Power down the failed server gracefully
  - Note: Access the iLO with Administrator privilege, then go to Power Management →Server Power →click on 'Momentary Press'
- Remove failed blades and replace.
- Verify that the blade had TPD on it, or install TPD
- Install application software – CMP
  - Note: Refer to the Policy Management Bare Metal Installation Guide Release 12.2, the documents are available at the Oracle Help Center

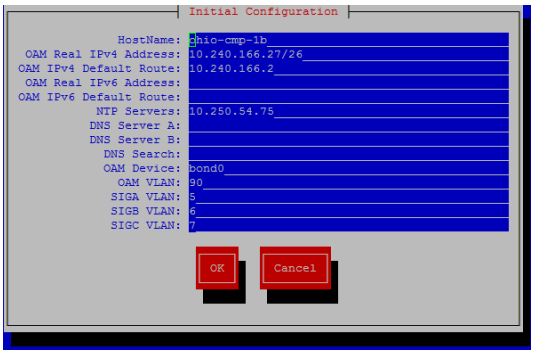
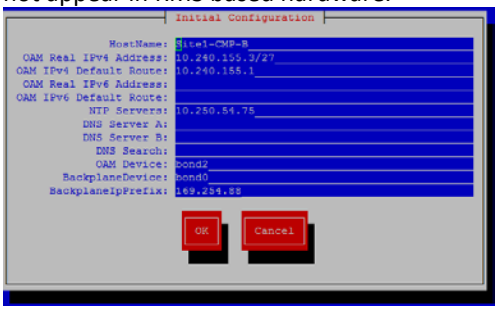
S T E P #	This Procedure performs Restoring CMP cluster with system backup available Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	

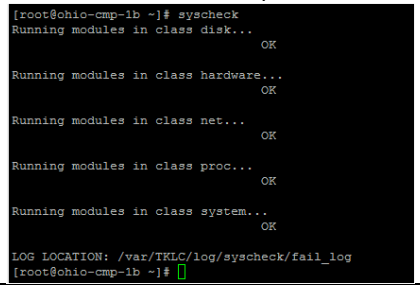
1. ☐	Login via SSH to new blade	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

2. ☐	Perform 'Initial Policy Configuration' from within platcfg utility on newly installed blade	Execute the following command `# su - platcfg` a) From within the platcfg utility, navigate to: **Policy Configuration → Set Policy Mode**  Choose 'Cable' if solution is for cable mode or leave it as default 'Wireless' if it will be wireless mode and select OK to continue. b)From within the platcfg utility, navigate to: **Policy Configuration → Perform Initial Configuration** Enter the relevant details from the blade being replaced:  Once the server details are entered and verified for correctness select 'Ok'. A menu will appear asking if the new settings should be applied, select 'YES' and allow the operation to complete. No specific message is given when the operation is successful, but an error will appear if it was not completed. In this case, review the settings from the 'Perform Initial Configuration screen again, if all appears as expected, contact My Oracle Support before proceeding. Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*

3. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.
4. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the `syscheck` command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
5. ☐	Load the system backup(ISO) file for server restore	The system backup file contains the database information that makes up the application level configuration of the policy network. Without that backup, the application configuration will have to be restored either through the platcfg menu, or from the server backup file from site documentation. If the system backup file is available, put a copy of the file on the newly constructed CMP blade into the: via secure copy (pscp scp, or WinSCP). **/var/camiant/backup/local_archive/systembackup/**

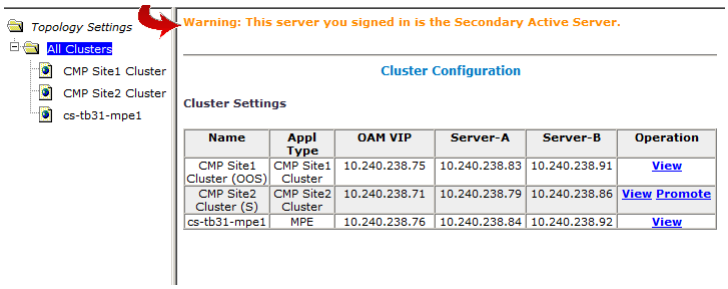
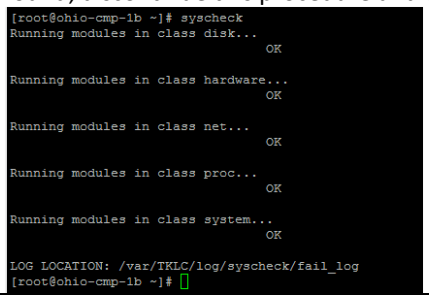
6. ☐	Perform platcfg restore from SSH session to replacement blade	Execute the following command `# su - platcfg` From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → System Restore** A message will appear prompting confirmation to restore even though this node is not recognized as the active member. This behavior is expected, continue by selecting 'NO'.  Then a screen will appear asking to select the file to restore from. If the file was copied correctly in the previous step, it will be shown here as an option, otherwise select 'Manually Input', and Select 'Full' and then select OK to proceed.  ***Note**: "Full" will also restore Comcol data, But "Application" will exclude Comcol.*	
7. ☐	Verify the status	A window will pop-up, indicating restore operation was successful and will ask the user to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.	

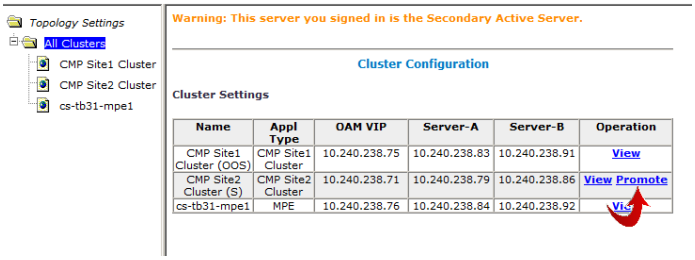
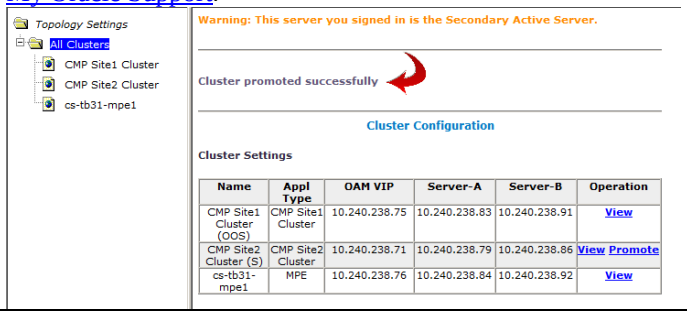
8. ☐	Verify Initial configuration	Choose Exit repeatedly until back to the Main Menu of the platcfg utility. While still within the platcfg utility, navigate to: **Policy Configuration → Verify Initial Configuration**  Ensure that your data is correct, if configuration is not there, then navigate to '**Perform Initial Configuration**' and fill in the hostname, OAM IP etc as shown below:  Select 'OK', then 'YES' to save and apply Once the server details are entered and verified for correctness select 'OK'. A menu will appear asking if the new settings should be applied, select 'YES' and allow the operation to complete. No specific message is given when the operation is successful, but an error will appear if it was not completed. In this case, review the settings from the 'Perform Initial Configuration screen again, if all appears as expected, contact My Oracle Support before proceeding. Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. ***For RMS (DL360/DL380) System:*** The platcfg for RMS doesn't natively use vlans. For example: The 'SIGA VLAN', 'SIGB VLAN' and 'SIGC VLAN' configuration parameters will not appear in RMS based hardware.  *Note: The above snapshot is for 'Cable mode', for 'Wireless mode' the "Backplane Device" and "Backplane IP Prefix" parameters will not exist.*

9. ☐	Reboot the server	Reboot. `# init 6` Allow the server time to reboot; ***For c-Class or Netra X5-2(Oracle RMS)System:*** Reconnect via SSH from the PM&C server to the node as ***admusr*** first and then switch to ***root*** privileges. ***For RMS (DL360/DL380/Oracle X5-2)System with no PM&C:*** SSH directly to the node.
10. ☐	Verify basic network connectivity and server health.	From the newly installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
11. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility as root, please run `'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root';` as admusr, please run `'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov';` 
12. ☐	Check status	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** When the server has returned to online status, log into the GUI on the OAM virtual IP address • Verify to the best of your abilities that the new manager has configuration for the MPE clusters in the network (whether those clusters are online or not) • Verify other application configuration properties as you are able. Once one CMP is in place, the other node of the CMP cluster can replaced with the procedures above, and any other clusters or individual nodes that need replacement can be handled with the above procedures. This procedure is completed.

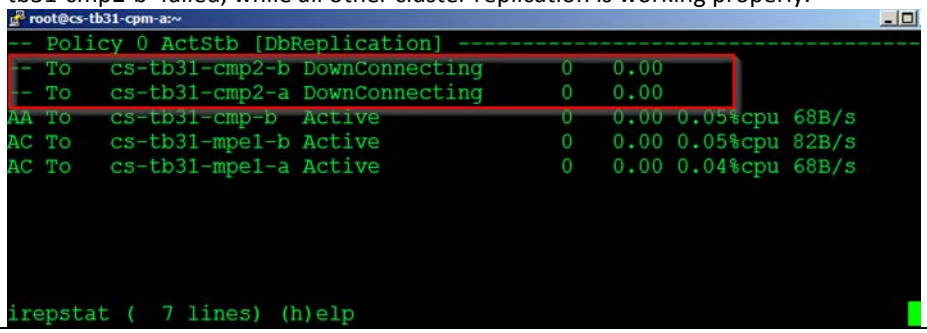
5.8 Procedure 8: Promoting geo-redundant CMP cluster

This procedure is used to bring a geo-redundant secondary active CMP online before beginning restoration of other policy clusters in the network. Once a CMP is online, all other servers of the policy network can be re-created using the above procedures and then their application level configuration restored from this CMP.

S T E P #	This Procedure performs Promoting geo-redundant CMP cluster Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	
1. ☐	Access to the system	Log into the GUI on the OAM VIP of the geo-redundant CMP.
2. ☐	Check status	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** You will be warned that you are not on the primary cluster of the policy network. The secondary server has limited functionality. 
3. ☐	Verify basic network connectivity and server health.	From the active server of site 2 CMP('Promote' server), ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Execute the `syscheck` command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 

4. ☐	Promote secondary CMP cluster	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** Select 'Promote' on the secondary server. Accept the resulting pop-up by clicking 'OK'.  You should see a message appear above the 'Cluster Configuration' header indicating successful promotion (see example below). If not, retry the operation and/or contact My Oracle Support. 
5. ☐	Logout of the CMP GUI	Logout of the CMP GUI by clicking the 'Logout' link or closing the browser window.
6. ☐	Verify operation via CMP GUI	Relogin to the CMP GUI using the VIP of CMP Site2 In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** Ensure all clusters are performing as expected. Follow procedures listed in this document to bring other failed servers/clusters back online.

7. ☐	SSH to active node of newly promoted cluster	***For c-Class System:***
		SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:
		Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and a remote console session need to be started to execute commands.

8. ☐	Verify irepstat output shows expected status	From the SSH session from PM&C to the active node of newly promoted CMP cluster, execute the irepstat command to verify that cluster replication is 'Active'. If not 'Active' after 5 minutes, check the CMP GUI for any active alarms. # irepstat -- Policy 0 ActStb [DbReplication] ---------- AA To Site1-nw-cmp-a Active 0 0.25 1%R 0.04%cpu 65B/s AA To Site2-nw-cmp-a Active 0 0.50 1%R 0.04%cpu 65B/s The status of all clusters except known failed servers should have a status of 'Active' as in the above snapshot. Otherwise if any of the replication paths show 'DownConnecting' as in the snapshot below contact My Oracle Support. The example shown below shows our installation with servers 'cs-tb31-cmp2-a' and 'cs-tb31-cmp2-b' failed, while all other cluster replication is working properly. 
9. ☐	Rebuild failed CMP cluster	Refer to Procedure 6: Restoring complete cluster without the server backup to rebuild failed CMP cluster. This procedure is completed

APPENDIX A. Contacting Oracle

Disaster recovery activity may require real-time assessment by Oracle Engineering in order to determine the best course of action. Customers are instructed to contact the Oracle Customer Access Support for assistance if an enclosure FRU is requested.

Accessing the Oracle Customer Support Site and Hotlines:

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

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html.* The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

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

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

APPENDIX B. Recovery of third party components

Refer **[9] E53486 - Tekelec Platform 7.0.x Configuration Procedure Reference, Current Revision** for supported recovery procedures for 3rd party network and enclosure components:

3.1.2.3 Replace a Failed 4948/4948E/4948E-F Switch (PM&C Installed) (netConfig)
3.1.3.2 Replace a Failed 3020 Switch (netConfig)
3.1.3.4 Replace a Failed HP (6120XG, 6125G) Switch (netConfig)
3.5.6 Restore OA Configuration from Management Server

APPENDIX C. Recovery of Mediation Server (MDF) for CMCC deployment

Note that for Disaster Recovery of the Mediation Server (MDF), (if necessary) re-install the MDF server.
Refer [**12] E72270 Revision 01 – Mediation Server User's Guide, Release 12.2** for supported procedures:

Chapter 3: Managing Mediation Servers
Chapter 4: Configuring a Mediation Server
Chapter 6: Configuring FTP Settings