

**Oracle® Communications
Policy Management**

Disaster Recovery 12.1.x

**E70152-01
December 2015**

Copyright © 2010, 2015 Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government. This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

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

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

Table of Contents

1. INTRODUCTION	4
1.1. PURPOSE AND SCOPE.....	4
1.2. REFERENCES	4
1.3. ACRONYMS	4
1.4. LOGINS AND PASSWORDS.....	4
1.5. SOFTWARE RELEASE NUMBERING	5
1.6. TERMINOLOGY	5
2. GENERAL DESCRIPTION.....	7
3. PROCEDURE OVERVIEW	10
4. PROCEDURE PREPARATION.....	12
4.1. PURPOSE AND SCOPE.....	12
4.2. RECOVERY SCENARIOS	12
4.2.1. Recovery Scenario 1 (Partial Cluster Outage with Primary CMP Server available).....	12
4.2.2. Recovery Scenario 2 (Partial Cluster Outage with geo-redundant CMP Server available).....	14
4.2.3. Recovery Scenario 3 (Full cluster outage of the CMP; geo-redundancy not available; other servers as needed).....	15
5. RESTORE PROCEDURES.....	17
5.1. PROCEDURE 1: RESTORE STANDBY CMP NODE WITH SERVER BACKUP FILE	17
5.2. PROCEDURE 2: RESTORE STANDBY CMP NODE WITHOUT SERVER BACKUP FILE	24
5.3. PROCEDURE 3: RESTORE SINGLE MPE/MRA NODE WITH SERVER BACKUP FILE	30
5.4. PROCEDURE 4: RESTORE SINGLE MPE/MRA NODE WITHOUT SERVER BACKUP FILE	38
5.5. PROCEDURE 5: RESTORING COMPLETE CLUSTER WITH THE SERVER BACKUP FILES	45
5.6. PROCEDURE 6: RESTORING COMPLETE CLUSTER WITHOUT THE SERVER BACKUP	55
5.7. PROCEDURE 7: RESTORING CMP CLUSTER WITH SYSTEM BACKUP AVAILABLE	63
5.8. PROCEDURE 8: PROMOTING GEO-REDUNDANT CMP CLUSTER	70
5.8.1.1.1. CONTACTING ORACLE.....	74
5.8.1.1.2. RECOVERY OF THIRD PARTY COMPONENTS.....	75

List of Tables

Table 1: Acronyms	4
Table 2: Terminology	5

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 12.1.x. This includes recovery of partial or a complete loss of one or more Policy servers. 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] E65467 - Oracle Firmware Upgrade Pack 3.1.4, Release Notes
- [2] E65466 - Oracle Firmware Upgrade Pack Release 3.1.4 Upgrade Guide
- [3] E59722 - HP Solutions Firmware Upgrade Pack Release 2.2.8_Release Notes
- [4] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8
- [5] E59723 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.8
- [6] E54387 - PM&C Incremental Upgrade, Current Revision
- [7] E53019 - TVOE 3.0 Disaster Recovery Procedure, Current Revision
- [8] E53486 - Tekelec Platform 7.0.x Configuration Procedure Reference, Current Revision
- [9] E54388-02 - PM&C Disaster Recovery Release 6.0
- [10] E53487 - PM&C 6.2 Incremental Upgrade Procedure, Current Revision
- [11] E70153-01 - Oracle Communications Policy Management OCPM 12.1.x Installation Procedure

These documents can be accessed at the following link

<http://docs.oracle.com/en/industries/communications/>

1.3. Acronyms

Table 1: Acronyms

Acronym	Meaning
BIOS	Basic Input Output System
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
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
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
FRU	Field Replaceable Unit
USB	Universal Serial Bus

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 (refer to PR239591 for details), 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 12.1.x. It is assumed that PM&C Version 6.0 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, see document E54388-02 for c-Class hardware enclosure. The Oracle X-52 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

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.

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.

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 servers)
- 1 or more MPE/MRA servers failed

Recovery of the entire network from a total outage

- No CMP servers are available (neither primary, nor geo-redundant) and other MPE/MRA servers will need to be recovered

The existence of Geo-redundant system, including a geo-redundant 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 is critical when the CMP servers are all offline, or complete system, including CMP's must be restored.

Note that for Disaster Recovery of the PM&C Server Release 6.0, see document E54388-02, 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, CMP, MSR/SPR remotely with RMM/power connections. The FRU will be needed physically to replace the failed server, the cables for the new server have to be connected same as the failed one.

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

The simplest case of recovery is to recover a single node of a cluster when 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 cluster. This scenario can be used to recover one server of a MRA/MPE cluster or one server of a CMP cluster.

Recovery of complete MRA/MPE 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

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 clusters in the network.

Recovery of the CMP Cluster when geo-redundant CMP is available

The availability of a geo-redundant 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’:

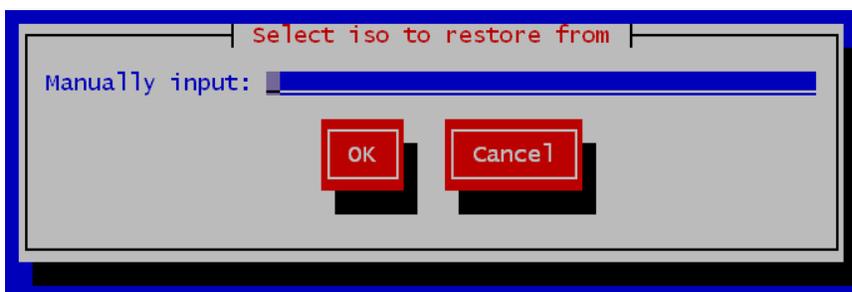
The information required for initial configuration is not extensive, and may be readily available from customer site documents, or from the CMP’s topology configuration. In some cases it can be easier to manually input the ‘initial configuration’ in platcfg than to try to load a server backup file into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

Using the server backup file

When asked to restore from ‘serverbackup’, 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.

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 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 (32 bits & 64 bits)*.
5. Platform Management & Configuration (PM&C) CD-ROM.
6. Policy Application installation .ISO for CMP, MPE, and MRA 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.

* The 32-bit TPD is used to IPM the PM&C Server, and the 64-bits TPD is used to IPM the application 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:

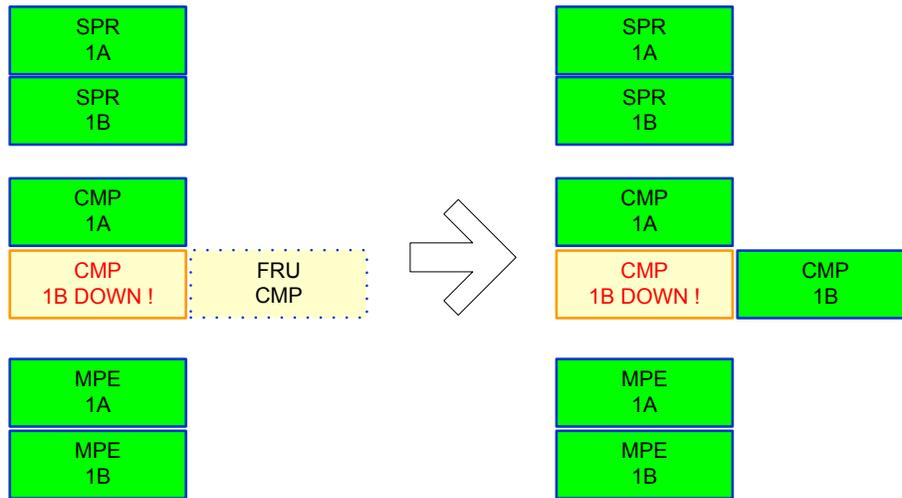
1. Verify BIOS time is correct on servers
2. Verify Version of TPD installed
3. Load application for corresponding Server HW types
4. Check FW versions and upgraded if necessary
5. Check NTP status after recovery
6. Check Active Alarms from GUI and both syscheck, alarmMgr–alarmStatusfrom CLI

4.2. Recovery Scenarios

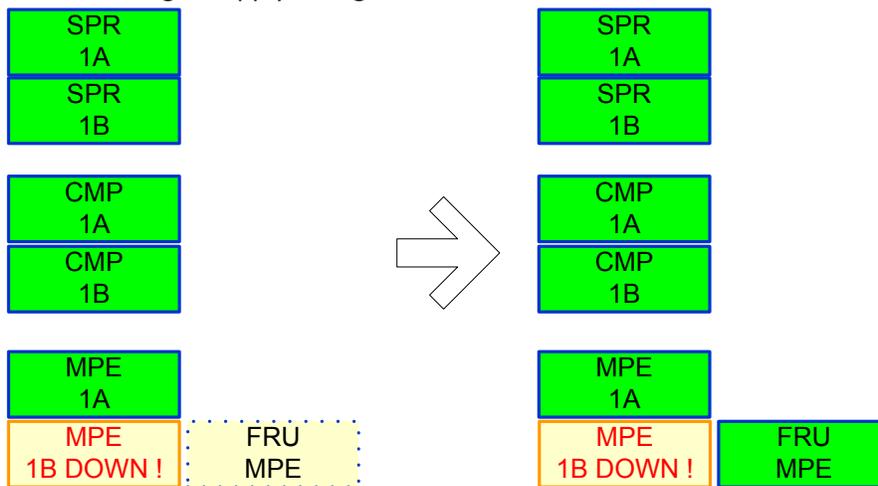
4.2.1. Recovery Scenario 1 (Partial Cluster Outage with Primary CMP Server available)

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 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 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 servers using 're-apply configuration'



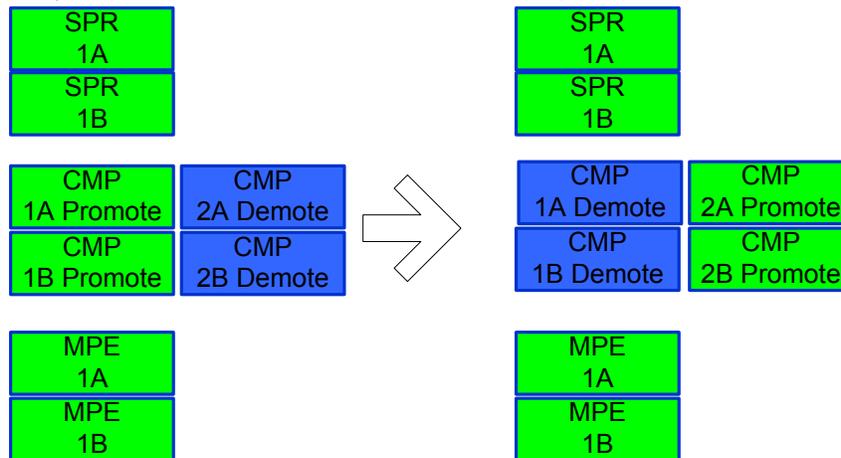
Follow the procedure below for detailed steps.

- 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 node without server backup file](#) to recover MPE / MRA nodes when one of the peers of the cluster is still available.
- 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 clusters that have gone down.

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 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 cluster that needs to be restored, there is no need to promote the Geo CMP.

- Recover any failed MPE/MRA 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 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.

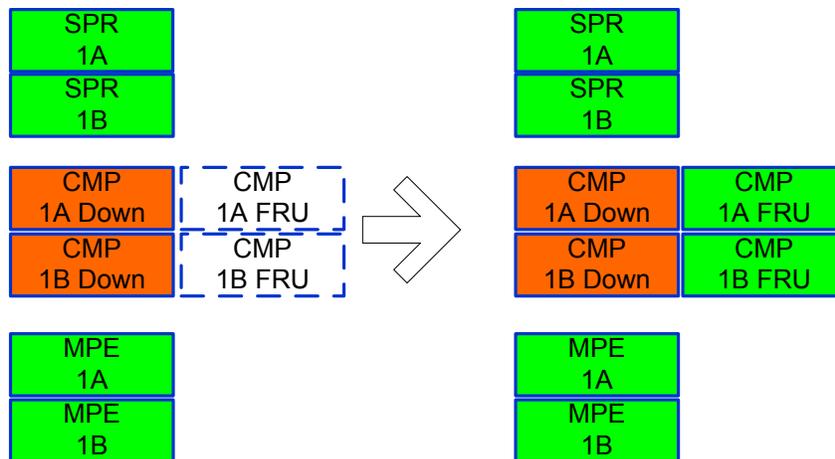
The database of the now active geo-redundant CMP server and will be replicated this new CMP server.

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 node without server backup](#) file to recover MPE / MRA nodes when one of the peers of the cluster is still available.
- 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 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.

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 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 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 servers.

Follow the procedure below for detailed steps.

- Use [Procedure 7: Restoring CMP 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 node without server backup file](#) to recover MPE / MRA nodes when one of the peers of the cluster is still available.
- 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 clusters that have gone down.

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

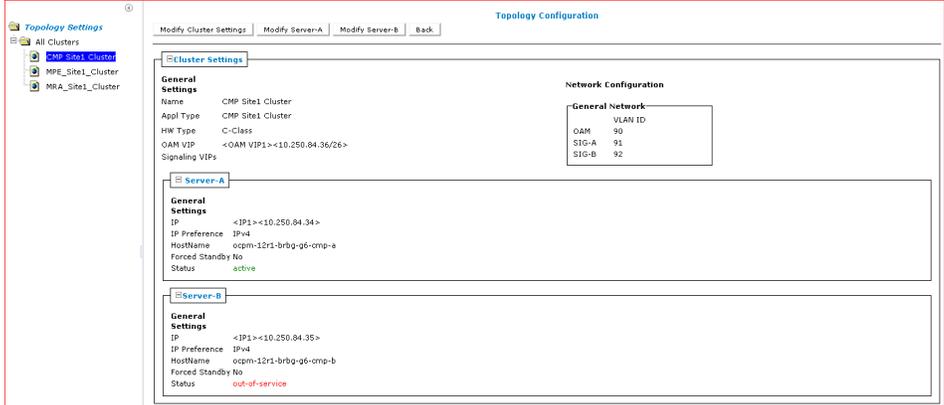
Prerequisites:

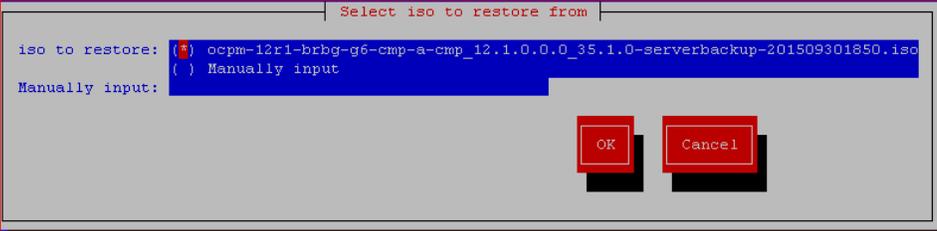
- Power down the failed server gracefully
Note: Access the iLO with Administrator privilege, then go to Power Management ->Server Power ->click on 'Momentary Press'
- Remove failed hardware and replace.
- Verify that the node has TPD on it, or install TPD
- Install application software – CMP

*Refer to the Policy Management Bare Metal Installation Guide Release 12.1.x

*These documents can be accessed at the following link

[\(http://docs.oracle.com/en/industries/communications/\)](http://docs.oracle.com/en/industries/communications/)

S T E P #	<p>This Procedure restores the standby CMP node when a server level backup is available.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.</p>	
1	<p>Set the failed node to 'Forced Standby'</p>	<p>In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters</p> <ol style="list-style-type: none"> 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	<p>Load the ISO for server restore</p>	<p>Obtain the <i>*serverbackup.iso*</i> 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:</p> <p><i>/var/camiant/backup/local_archive/serverbackup</i></p> <p>Note: Later in this procedure, the <i>plafcgr</i> restore function check this directory and offer the user a convenient menu to choose from. The <i>plafcgr</i> utility also allows the user to manually enter any mounted path on the server.</p>

3□.	Login via SSH to new node	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380/X-3-2/X5-2):</p> <p>Use the iLo to login, and a remote console session need to be started to execute commands</p>
4□	Perform platcfg restore from SSH session to replacement node	<p>Execute the following command:</p> <pre># su - platcfg</pre> <p>From within the platcfg utility, navigate to: Policy Configuration → Backup and Restore → Server Restore</p> <p>Select the *serverbackup*.ISO that you just put on the system and hit OK, then 'yes' to confirm.</p> 
5□	Verify the status	<p>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.</p>

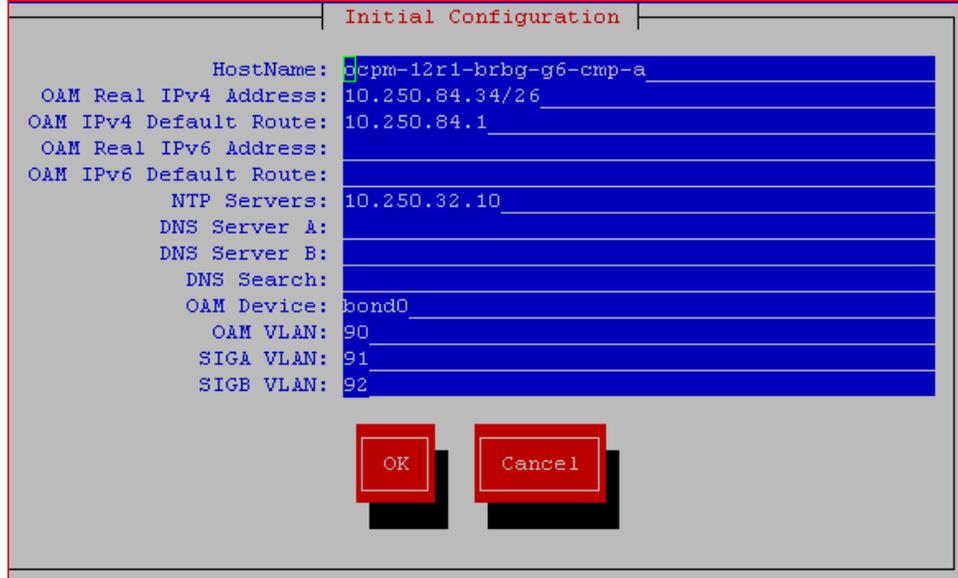
6□

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 configuration is not there, then navigate to 'Perform Initial Configuration' and fill in the hostname, OAM IP etc as shown below:



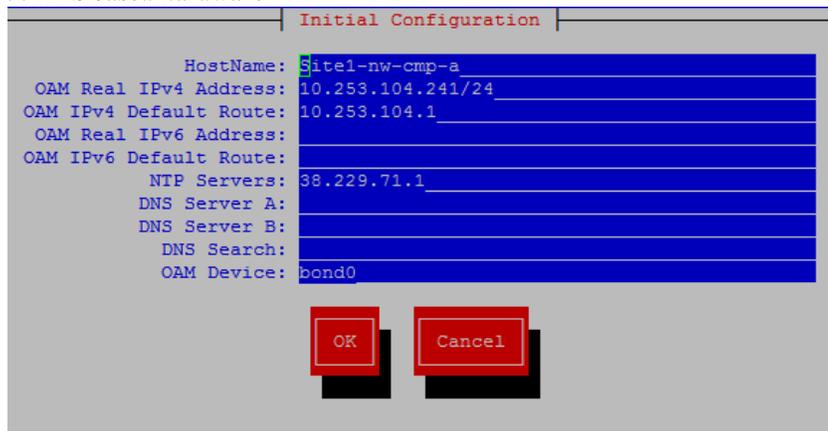
Note: The above screen shot example is for c-Class hardware

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/X-3-2/X5-2): The initial Configuration is different. For example: The 'SIGA VLAN' and 'SIGB VLAN' configuration parameters will not appear in RMS based hardware



Note: The above screen shot example is for RMS hardware

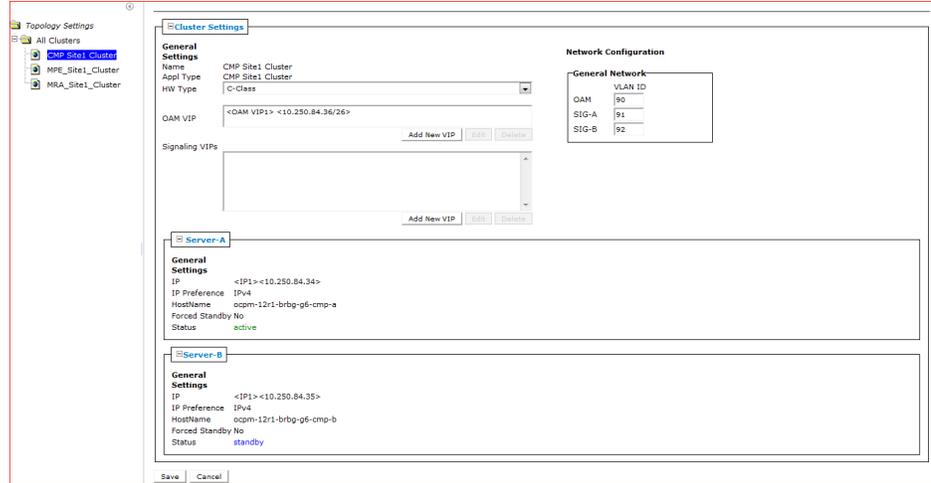
7□	Reboot the server	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as <i>admusr</i> first and then switch to <i>root</i> privileges.</p>
8□.	Verify basic network connectivity and server health.	<p>From the newly installed server, 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(MOS) before proceeding if network ping tests still fail.</p> <pre>#ping <XMI or OAM gateway address></pre> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support (MOS).</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ 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@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre>

9. Remove 'Forced Standby' designation on current node.

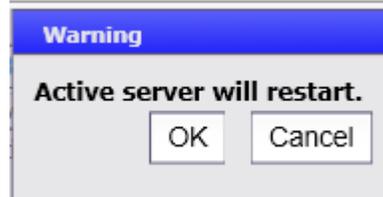
In the CMP GUI, navigate to:

Platform Setting → Topology Setting → Current Cluster

- Modify for the server that has 'forced standby'
- Clear the Forced Standby checkbox
- Click Save



Accept the resulting pop-up by clicking OK:

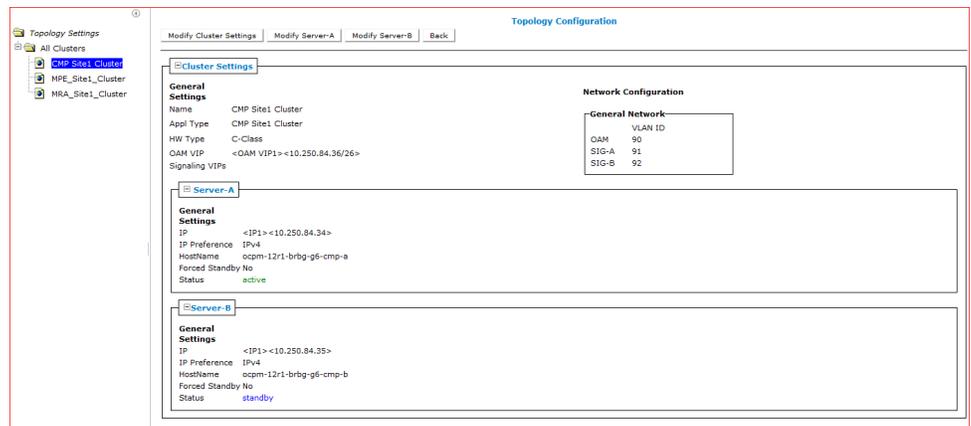


10. Verify cluster status

In the CMP GUI, navigate to:

Platform Setting → Topology Setting → All → 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	<p>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:</p> <pre># irepstat</pre> <p>Expected 'irepstat' output while waiting reconnection:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1R 0.05%cpu 85B/s AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.25 1R 0.05%cpu 85B/s AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.50 1R 0.04%cpu 85B/s AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.25 1R 0.05%cpu 85B/s</pre> <p>Expected 'irepstat' output after cluster has formed:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AA To ocpm-12r1-brbg-g6-cmp-b Active 0 0.00 1R 0.05%cpu 60B/s AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1R 0.04%cpu 78B/s AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.00 1R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.49 1R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.00 1R 0.05%cpu 78B/s</pre>
12□.	Exchange keys with cluster mate(This step need to run from active CMP)	<p>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'</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</pre> <p>The password of admusr in topology: Connecting to admusr@ocpm-12r1-brbg-g6-mpe-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-b ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-a ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-b ... Connecting to admusr@ocpm-12r1-brbg-g6-mpe-b ...</p> <pre>[1/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-b ... [2/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-a ... [3/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-a ... [4/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-b ... [5/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-a ... [6/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-b ...</pre> <p>SSH keys are OK.</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre> <p>This procedure is completed</p>

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

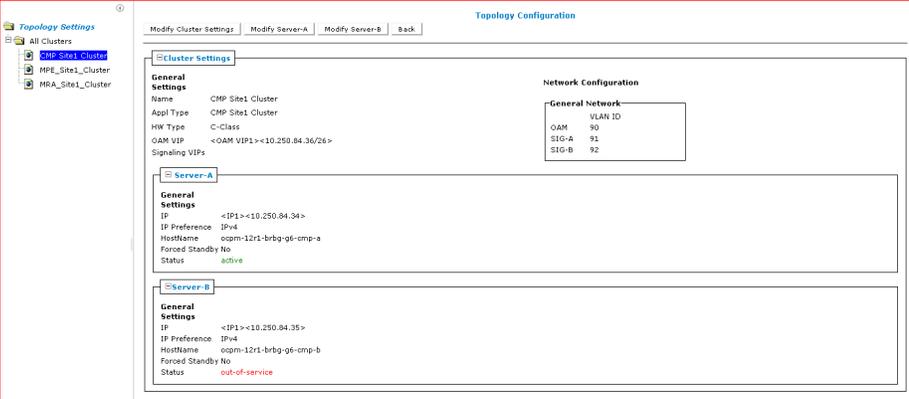
Prerequisites:

- Power down the failed server gracefully
 - o 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

*Refer to the Policy Management Bare Metal Installation Guide Release 12.1.x

*These documents can be accessed at the following link

[\(http://docs.oracle.com/en/industries/communications/\)](http://docs.oracle.com/en/industries/communications/)

S T E P #	<p>This Procedure restores the standby CMP node when a server level backup file is not available.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.</p>	
1	<p>Set the failed node to 'Forced Standby'</p>	<p>In the CMP GUI, navigate to:</p> <p>Platform Setting → Topology Setting → All Clusters</p> <ol style="list-style-type: none"> 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  <p><i>Note: From the above screenshot, the General Network(VLAN ID) will not appear for RMS (DL 360/DL380) Hardware</i></p>
2	<p>Login via SSH to new node</p>	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380/X3-2/X5-2):</p> <p>Use the iLo to login, and a remote console session need to be started to execute commands</p>

3

Perform platcfg restore from SSH session to replacement node

Perform Initial configuration

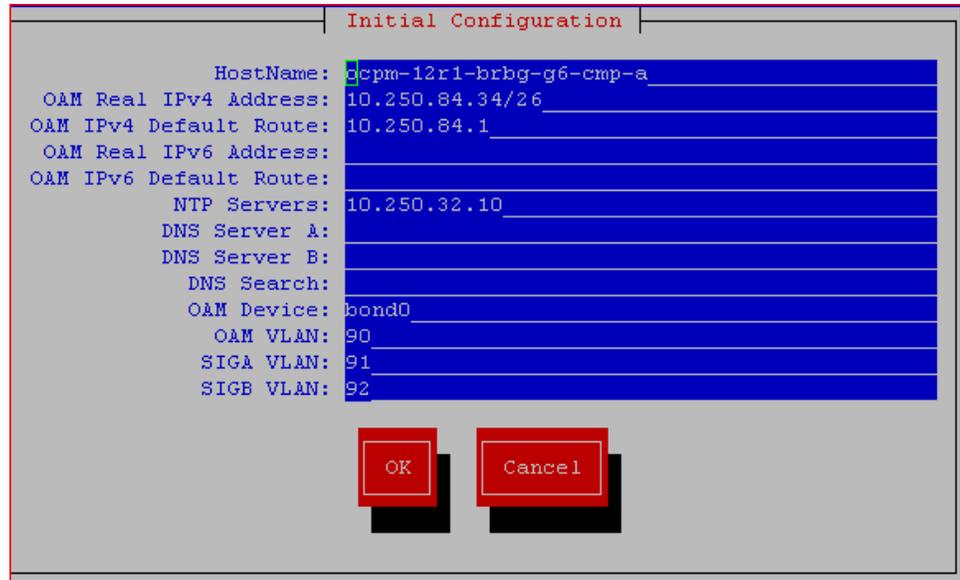
Execute the following command

```
# su - platcfg
```

From within the platcfg utility, navigate to:

Policy Configuration → Perform Initial Configuration

Enter the appropriate 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.



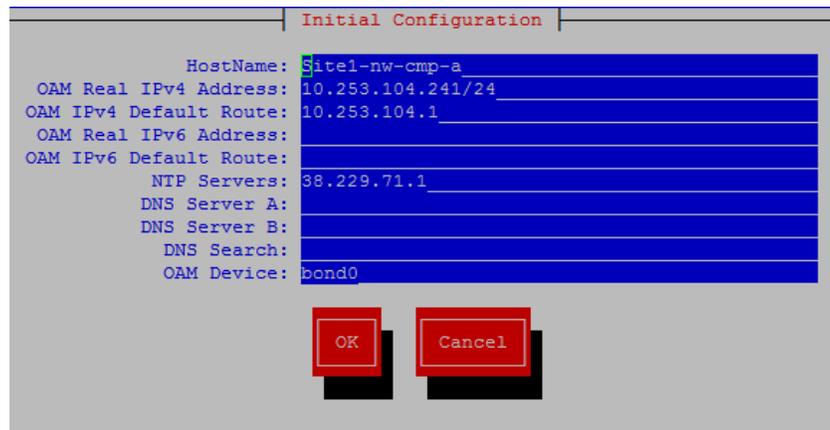
Note: The above screen shot example is for c-Class hardware

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/X-3-2/X5-2): The initial Configuration is different. For example: The 'SIGA VLAN' and 'SIGB VLAN' configuration parameters will not appear in RMS based hardware



Note: The above screen shot example is for RMS hardware

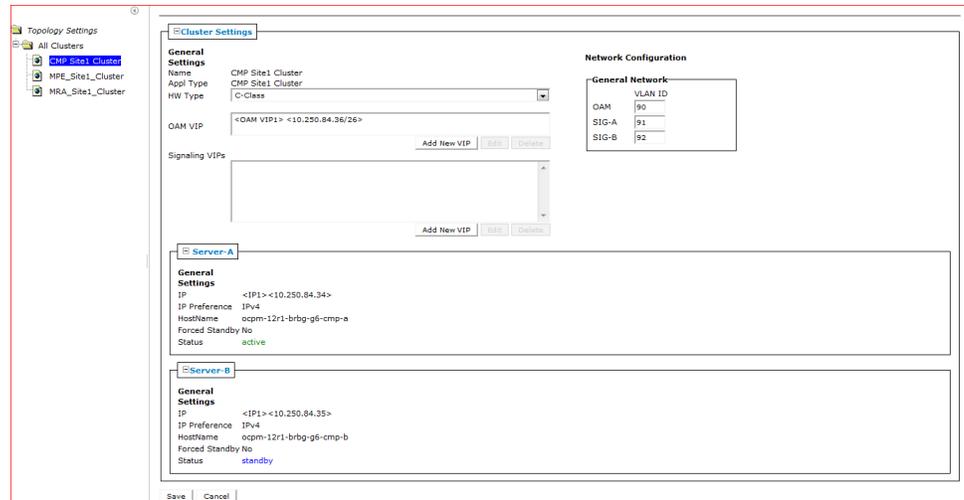
4□	Reboot the server	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as <i>admusr</i> first and then switch to <i>root</i> privileges.</p>
5□	Verify basic network connectivity and server health.	<p>From the newly installed server, 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(MOS) before proceeding if network ping tests still fail.</p> <pre>#ping <XMI or OAM gateway address></pre> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support(MOS).</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ 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@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre>

6. Remove 'Forced Standby' designation on current node.

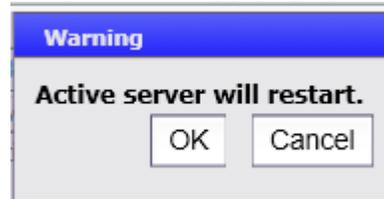
In the CMP GUI, navigate to:

Platform Setting → Topology Setting → Current Cluster

- Modify for the server that has 'forced standby'
- Clear the Forced Standby checkbox
- Click Save



Accept the resulting pop-up by clicking OK:

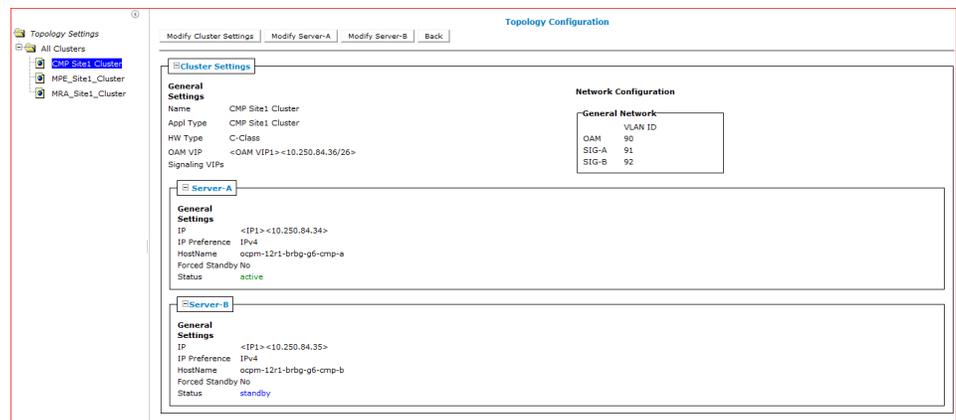


7. Verify cluster status

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	<p>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:</p> <pre># irepstat</pre> <p>Expected 'irepstat' output while waiting reconnection:</p> <pre> -- Policy 0 ActStb [DbReplication] ----- AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1R 0.05%cpu 85B/s AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.25 1R 0.05%cpu 85B/s AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.50 1R 0.04%cpu 85B/s AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.25 1R 0.05%cpu 85B/s </pre> <p>Expected 'irepstat' output after cluster has formed:</p> <pre> -- Policy 0 ActStb [DbReplication] ----- AA To ocpm-12r1-brbg-g6-cmp-b Active 0 0.00 1R 0.05%cpu 60B/s AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1R 0.04%cpu 78B/s AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.00 1R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.49 1R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.00 1R 0.05%cpu 78B/s </pre>
9□	Exchange keys with cluster mate(This step need to run from active CMP)	<p>Exchanging SSH keys Utility</p> <p>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'</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@ocpm-12r1-brbg-g6-mpe-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-b ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-a ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-b ... Connecting to admusr@ocpm-12r1-brbg-g6-mpe-b ... [1/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-b ... [2/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-a ... [3/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-a ... [4/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-b ... [5/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-a ... [6/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-b ... SSH keys are OK. [admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre> <p>This procedure is completed.</p>

5.3. Procedure 3: Restore single MPE/MRA 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:

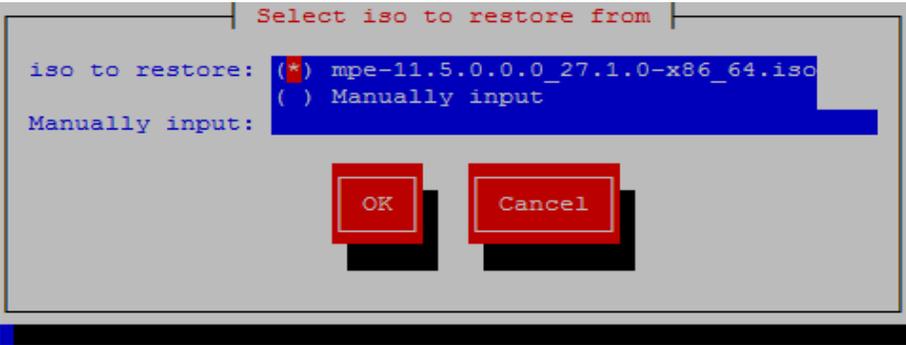
- Power down the failed server gracefully
 - o Note: Access the iLO with Administrator privilege, then go to Power Management ->Server Power ->click on 'Momentary Press'
- Remove failed hardware and replace.
- Verify that the hardware had TPD on it, or install TPD
- Install application software – MPE or MRA

*Refer to the Policy Management Bare Metal Installation Guide Release 12.1.x

*These documents can be accessed at the following link

[\(http://docs.oracle.com/en/industries/communications/\)](http://docs.oracle.com/en/industries/communications/)

S T E P #	<p>This procedure performs Restore single MPE/MRA node with server backup file.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.</p>											
1	<p>Set the failed node to 'Forced Standby'</p>	<p>In the CMP GUI, navigate to:</p> <p>Platform Setting → Topology Setting → All Clusters</p> <ol style="list-style-type: none"> 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  <table border="1" data-bbox="1193 779 1372 869"> <thead> <tr> <th colspan="2">General Network</th> </tr> <tr> <th></th> <th>VLAN ID</th> </tr> </thead> <tbody> <tr> <td>OAM</td> <td>90</td> </tr> <tr> <td>SIG-A</td> <td>91</td> </tr> <tr> <td>SIG-B</td> <td>92</td> </tr> </tbody> </table>	General Network			VLAN ID	OAM	90	SIG-A	91	SIG-B	92
General Network												
	VLAN ID											
OAM	90											
SIG-A	91											
SIG-B	92											
2	<p>Load the ISO for server backup</p>	<p>Obtain the <i>*serverbackup.iso*</i> 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:</p> <p><i>/var/camiant/backup/local_archive/serverbackup</i></p> <p>Note: <i>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.</i></p>										

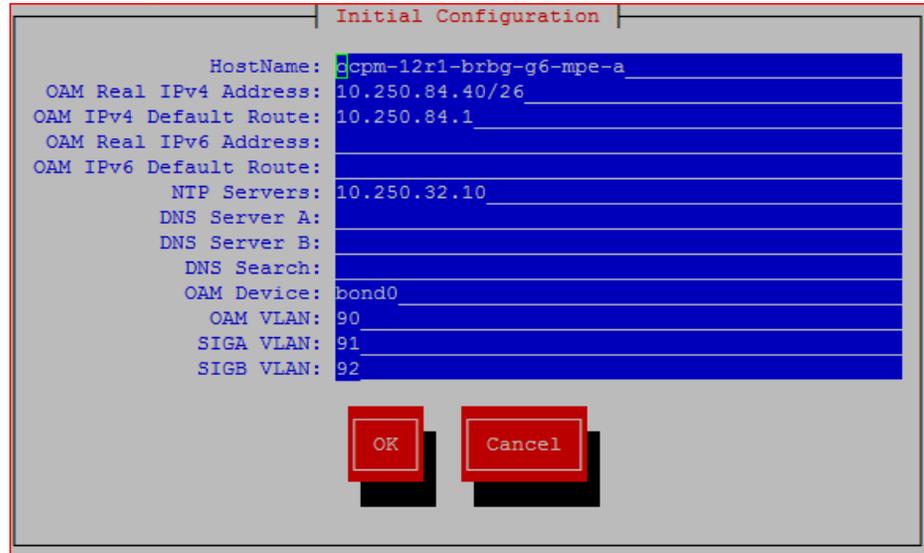
3	Login via SSH to new node	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380/X3-2/X5-2): Use the iLo to login, and a remote console session need to be started to execute commands</p>
4	Perform platcfg restore from SSH session to replacement hardware	<p>Execute the following command:</p> <pre># su - platcfg</pre> <p>From within the platcfg utility, navigate to:</p> <p>Policy Configuration → Backup and Restore → Server Restore</p> <p>Select the *serverbackup*.ISO that you just put on the system and hit ok – then ‘yes’ to confirm.</p> 
5	Verify the status	<p>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.</p>

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 configuration is not there, then navigate to ‘Perform Initial Configuration’ and fill in the hostname, OAM IP etc as shown below:



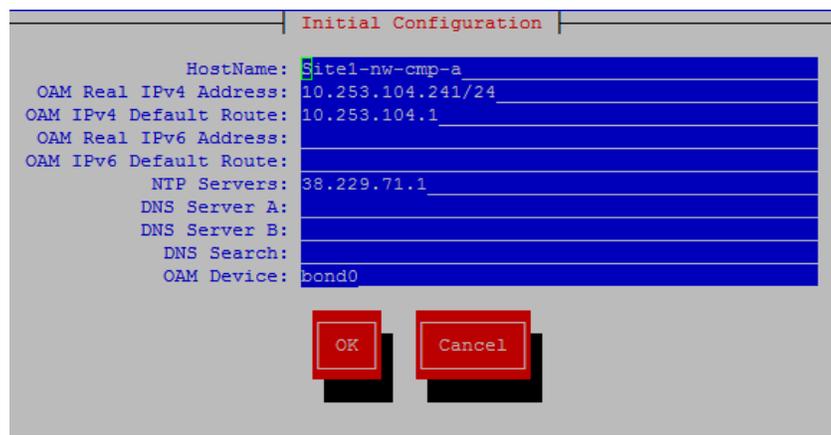
Note: The above screen shot example is for c-Class hardware

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/X-3-2/X5-2): The initial Configuration is different. For example: The ‘SIGA VLAN’ and ‘SIGB VLAN’ configuration parameters will not appear in RMS based hardware



Note: The above screen shot example is for RMS hardware

7	Reboot the server	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as <i>admusr</i> first and then switch to <i>root</i> privileges.</p>
8	Verify basic network connectivity and server health.	<p>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(MOS) before proceeding if network ping tests still fail.</p> <pre>#ping <XMI or OAM gateway address></pre> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support(MOS).</p> <pre>[admusr@ocpm-12r1-brbg-g6-mpe-b ~]\$ 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@ocpm-12r1-brbg-g6-mpe-b ~]\$</pre>

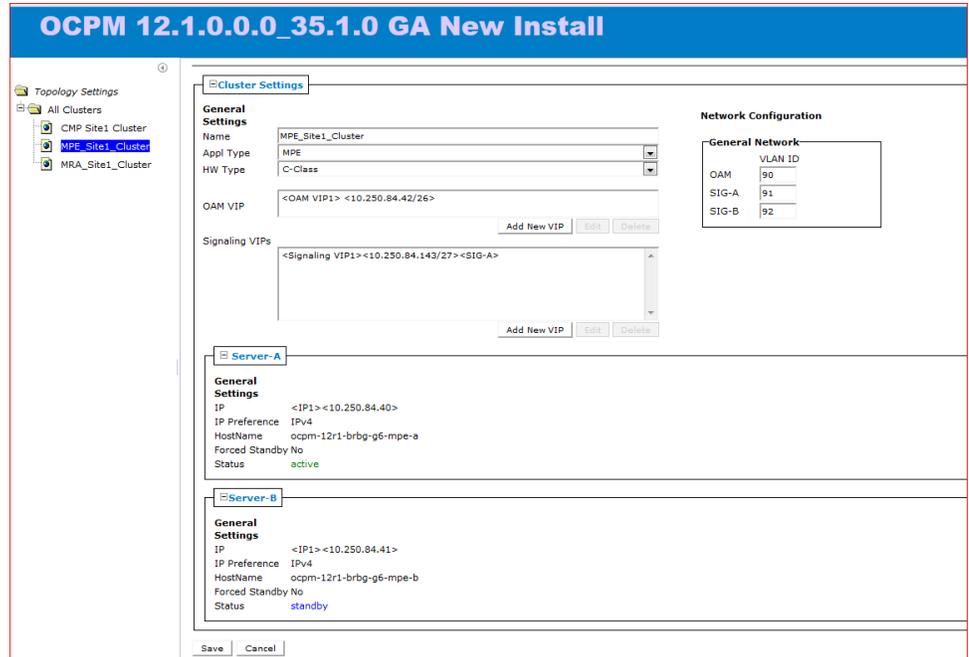
9. Remove 'Forced Standby' designation on current node.

In the CMP GUI, navigate to:

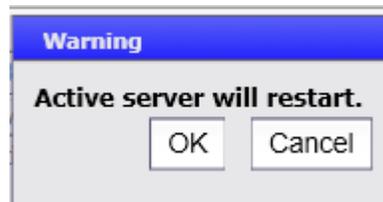
Platform Setting → Topology Setting → Current Cluster

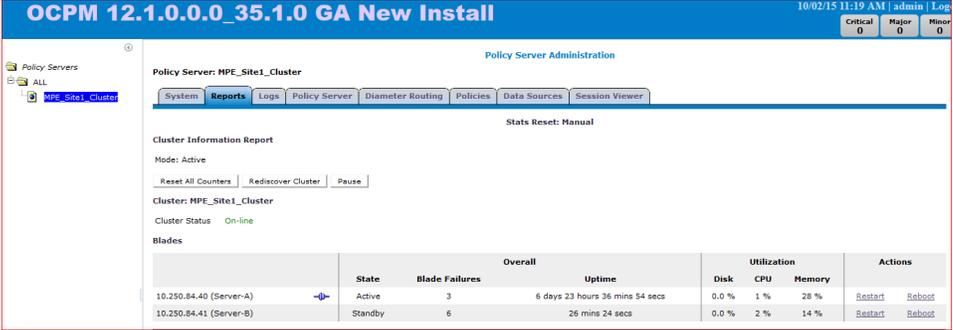
Modify for the server that has 'forced standby'

- Clear the Forced Standby checkbox
- Click Save



Accept the resulting pop-up by clicking OK:



10	Check status	<p>In the CMP GUI, depending on the type of the node, perform the following:</p> <ul style="list-style-type: none"> - If this is an MPE node, navigate to: <ul style="list-style-type: none"> ○ Policy Server → Configuration → All → Reports Tab - If this is an MRA node, navigate to: <ul style="list-style-type: none"> ○ MRA → Configuration → All → Reports Tab <p>Monitor clustering of the new node to its peer, do not proceed until the Cluster Status returns from 'Degraded' to 'On-line'</p> 
11	Alternative method to check replication status	<p>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:</p> <p># irepstat</p> <p>Expected 'irepstat' output while waiting reconnection:</p> <pre> -- Policy 0 ActStb [DbReplication] ----- AC From ocpm-12r1-brbg-g6-cmp-a Active 0 0.25 ^0.04%cpu 45B/s A=me </pre> <p>Expected 'irepstat' output after cluster has formed:</p> <pre> -- 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 </pre>

12□	Exchange keys with cluster mate(This step need to run from active CMP)	<p>Exchanging SSH keys Utility as root, please run <code>'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root'</code>; as admusr, please run <code>'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'</code></p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@ocpm-12r1-brbg-g6-mpe-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-b ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-a ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-b ... Connecting to admusr@ocpm-12r1-brbg-g6-mpe-b ... [1/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-b ... [2/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-a ... [3/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-a ... [4/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-b ... [5/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-a ... [6/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-b ... SSH keys are OK. [admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ █</pre> <p>This procedure is completed.</p>
-----	--	---

5.4. Procedure 4: Restore single MPE/MRA 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:
 - o OAM IP address, default gateway, NTP & SNMP server IP addresses
 - o 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

*Refer to the Policy Management Bare Metal Installation Guide Release 12.1.x

*These documents can be accessed at the following link
(<http://docs.oracle.com/en/industries/communications/>)

S
T
E
P
#

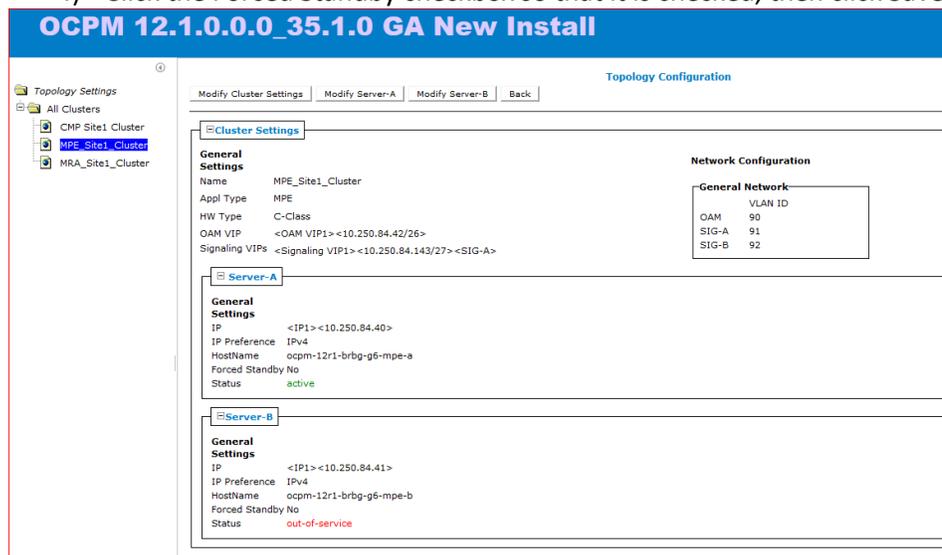
This Procedure performs Restore single MPE/MRA node without server backup file
 Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.
 Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

1□ Set the failed node to 'Forced Standby'

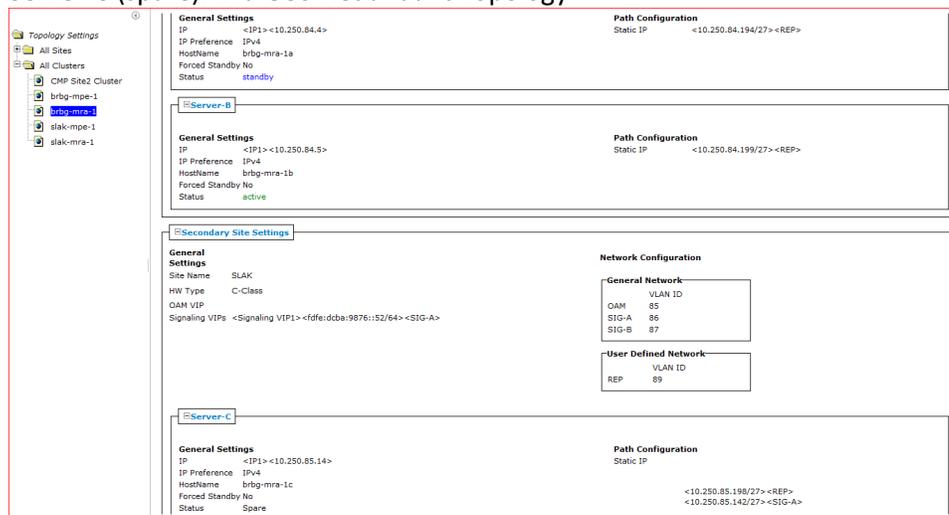
In the CMP GUI, navigate to:

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-Redundant 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	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380/X3-2/X5-2): Use the iLo to login, and a remote console session need to be started to execute commands</p>
----	---------------------------	---

3. Perform 'Initial Policy Configuration' from within platcfg utility on newly installed node

Execute the following command

```
# su - platcfg
```

From within the platcfg utility, navigate to:

Policy Configuration → Perform Initial Configuration

Enter the relevant details from the node being replaced:

```
Initial Configuration

HostName: dcpm-12r1-brbg-g6-mpe-a
OAM Real IPv4 Address: 10.250.84.40/26
OAM IPv4 Default Route: 10.250.84.1
OAM Real IPv6 Address:
OAM IPv6 Default Route:
NTP Servers: 10.250.32.10
DNS Server A:
DNS Server B:
DNS Search:
OAM Device: bond0
OAM VLAN: 90
SIGA VLAN: 91
SIGB VLAN: 92

OK Cancel
```

Note: The above screen shot example is for c-Class hardware

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 MOS support before proceeding.

Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell.

For RMS (DL360/DL380/X-3-2/X5-2): The initial Configuration is different. For example: The 'SIGA VLAN' and 'SIGB VLAN' configuration parameters will not appear in RMS based hardware

```
Initial Configuration

HostName: Site1-nw-cmp-a
OAM Real IPv4 Address: 10.253.104.241/24
OAM IPv4 Default Route: 10.253.104.1
OAM Real IPv6 Address:
OAM IPv6 Default Route:
NTP Servers: 38.229.71.1
DNS Server A:
DNS Server B:
DNS Search:
OAM Device: bond0

OK Cancel
```

Note: The above screen shot example is for RMS hardware

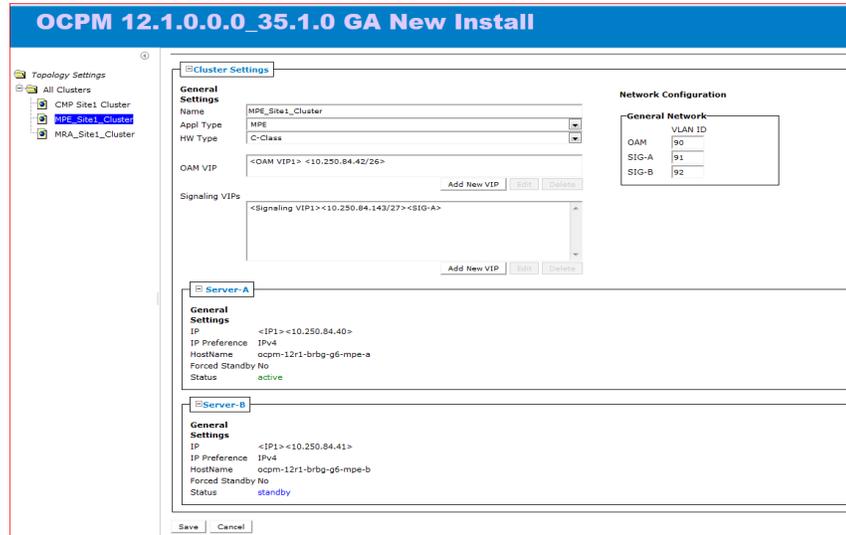
4	Reboot the server	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as <i>admusr</i> first and then switch to <i>root</i> privileges.</p>
5	Verify basic network connectivity and server health.	<p>From the newly installed server, 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(MOS) before proceeding if network ping tests still fail.</p> <pre>#ping <XMI or OAM gateway address></pre> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support(MOS).</p> <pre>[admusr@ocpm-12r1-brbg-g6-mpe-b ~]\$ 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@ocpm-12r1-brbg-g6-mpe-b ~]\$</pre>

6. Remove 'Forced Standby' designation on current blade.

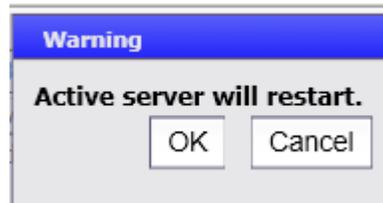
In the CMP GUI, navigate to:

Platform Setting → Topology Setting → Current Cluster

- Modify for the server that has 'forced standby'
- Clear the Forced Standby checkbox
- Click Save



Accept the resulting pop-up by clicking OK:

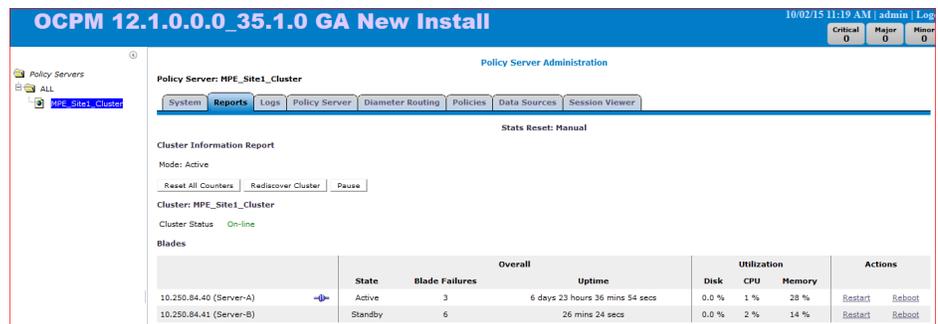


7. Check status

In the CMP GUI, depending on the type of the blade, perform the following:

- If this is an MPE/MPE-LI blade, navigate to:
 - o **Policy Server → Configuration → All → Reports Tab**
- If this is an MRA blade, navigate to:
 - o **MRA → Configuration → All → Reports Tab**

Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from 'Degraded' to 'On-line'



<p>8□</p>	<p>Alternative method to check replication status</p>	<p>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:</p> <pre># irepstat</pre> <p>Expected 'irepstat' output while waiting reconnection:</p> <pre> -- Policy 0 ActStb [DbReplication] ----- AC From ocpm-12r1-brbg-g6-cmp-a Active 0 0.25 ^0.04%cpu 45B/s A=me </pre> <p>Expected 'irepstat' output after cluster has formed:</p> <pre> -- 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 </pre>
<p>9□</p>	<p>Exchange keys with cluster mate(This step need to run from active CMP)</p>	<p>Exchanging SSH keys Utility</p> <p>as root, please run <code>'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root'</code>;</p> <p>as admusr, please run <code>'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'</code></p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@ocpm-12r1-brbg-g6-mpe-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-b ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-a ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-b ... Connecting to admusr@ocpm-12r1-brbg-g6-mpe-b ... [1/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-b ... [2/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-a ... [3/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-a ... [4/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-b ... [5/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-a ... [6/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-b ... SSH keys are OK. [admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre> <p>This procedure is completed.</p>

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)

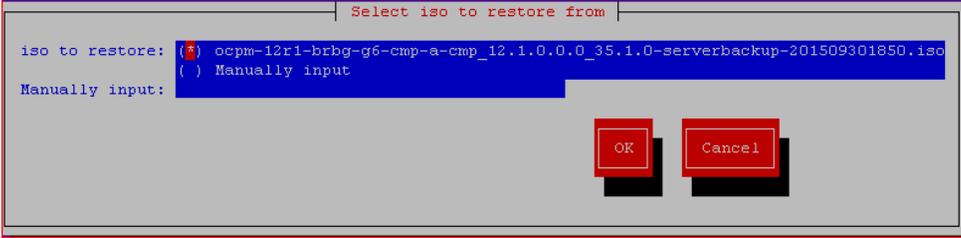
Note: In case it is a CMP Cluster that is being rebuilt, restore application data either from system backup or manually if no backup available.

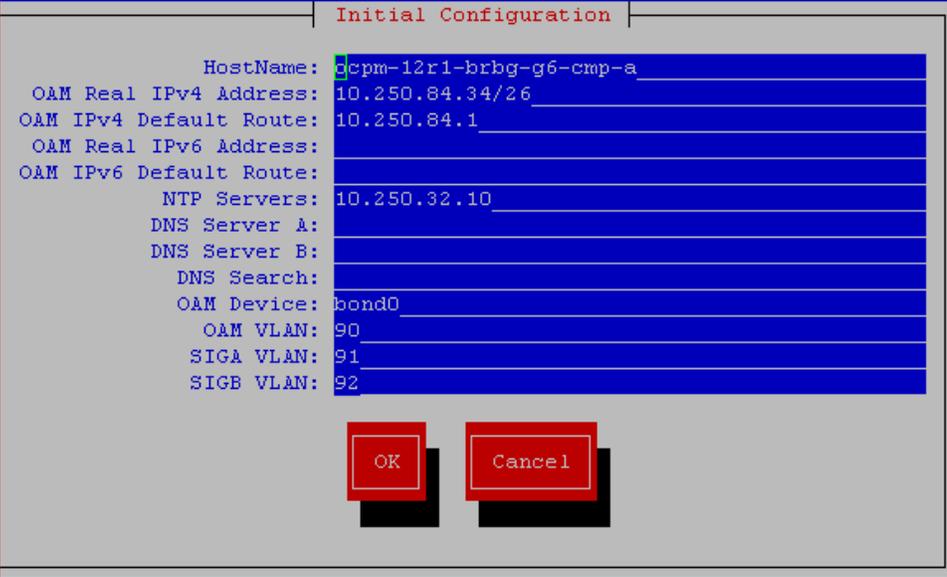
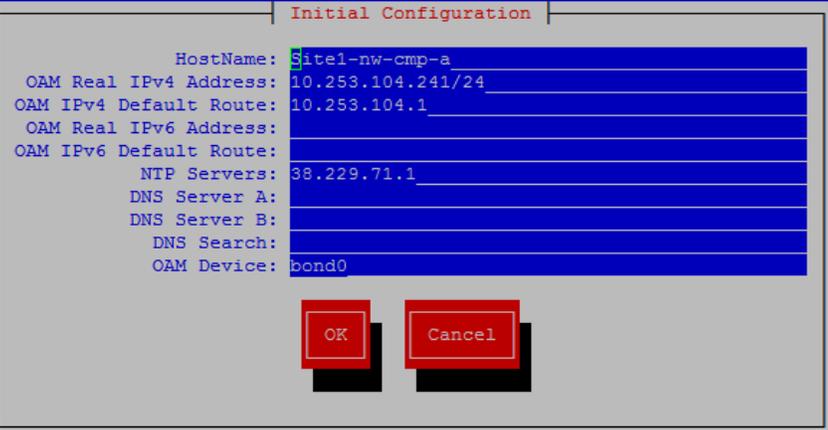
*Refer to the Policy Management Bare Metal Installation Guide Release 12.1.x

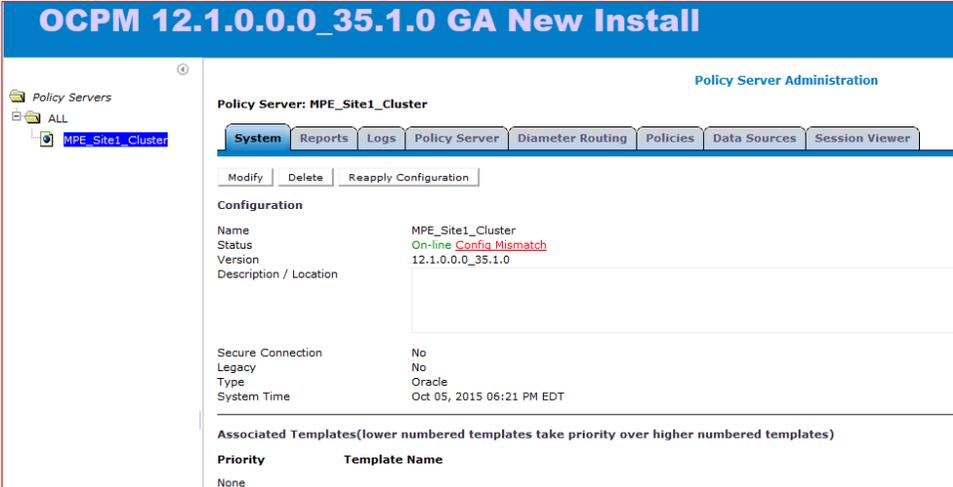
*These documents can be accessed at the following link

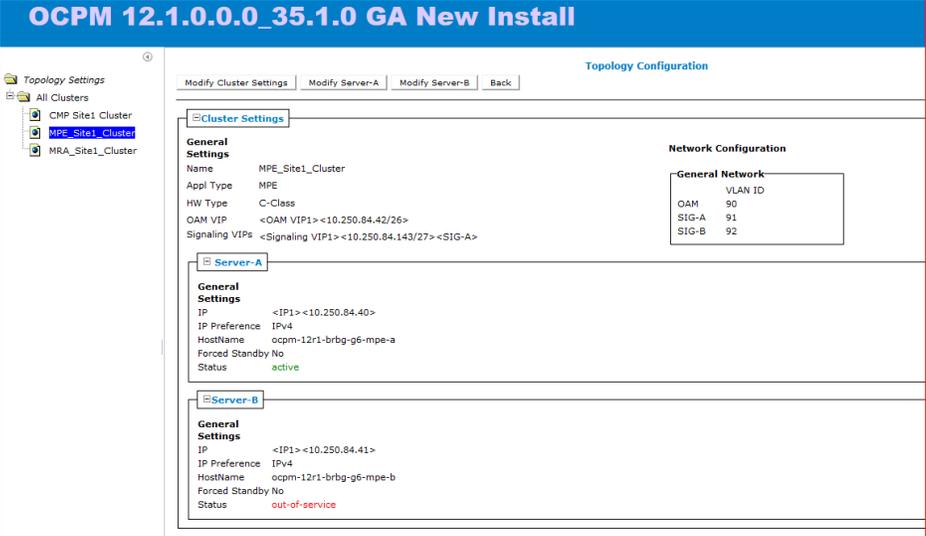
[\(http://docs.oracle.com/en/industries/communications/\)](http://docs.oracle.com/en/industries/communications/)

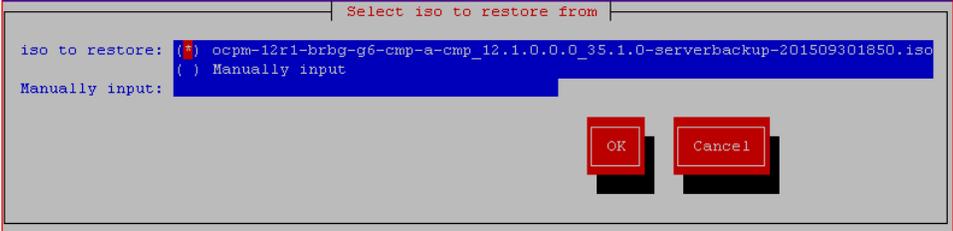
S T E P #	This Procedure performs Restoring complete cluster with the server backup files Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	
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: <pre style="color: red;"># ssh admusr@<node_IP_Address> \$ su - root</pre> For RMS (DL360/DL380): Use the iLo to login, and a remote console session need to be started to execute commands

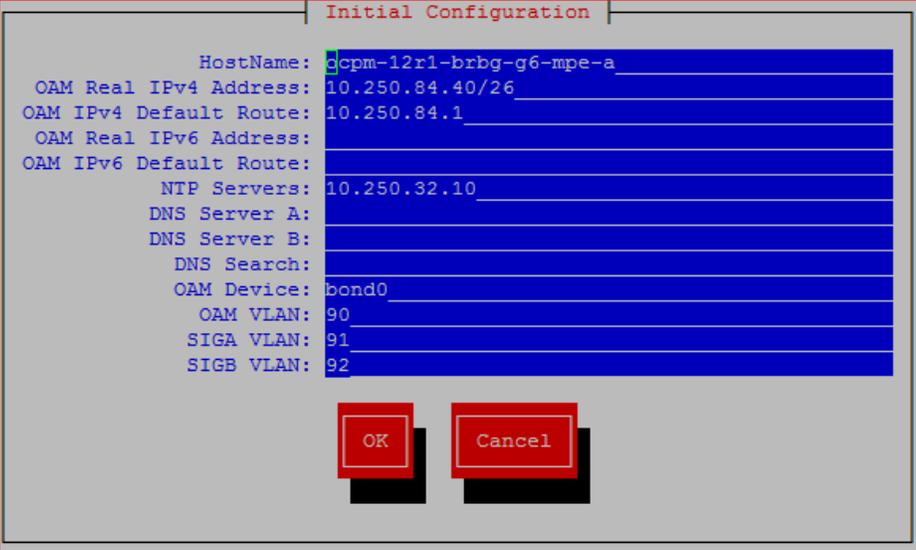
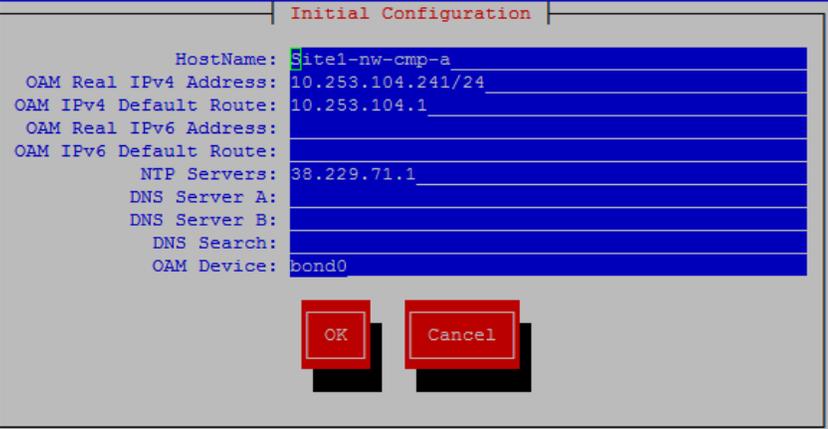
2☐	Load the ISO to restore 1 st server of the cluster	<p>Obtain the *serverbackup.iso* for the blade to be restored. When the replacement blade is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory:</p> <p>/var/camiant/backup/local_archive/serverbackup.</p> <p><i>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.</i></p>
3☐	Perform platcfg restore from SSH session to replacement blade	<p>Execute the following command</p> <pre># su - platcfg</pre> <p>From within the platcfg utility, navigate to:</p> <p>Policy Configuration → Backup and Restore → Server Restore</p> <p>Select the *serverbackup*.iso that you just put on the system and hit ok – then ‘yes’ to confirm.</p> 
4☐	Verify the status	<p>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.</p>

5	<p>Verify Initial configuration</p>	<p>Choose Exit repeatedly until back to the Main Menu of the platcfg utility. While still within the platcfg utility, navigate to:</p> <p>Policy Configuration → Verify Initial Configuration</p> <p>If configuration is not there, then navigate to ‘Perform Initial Configuration’ and fill in the hostname, OAM IP etc as shown below:</p>  <p>Note: The above screen shot example is for c-Class hardware</p> <p>Ensure that your data is correct, and select ‘OK’, then ‘yes’ to save and apply</p> <p>Exit platcfg.</p> <p>Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell.</p> <p><i>For RMS (DL360/DL380/X-3-2/X5-2): The initial Configuration is different. For example: The ‘SIGA VLAN’ and ‘SIGB VLAN’ configuration parameters will not appear in RMS based hardware</i></p>  <p>Note: The above screen shot example is for RMS hardware</p>
6	<p>Reboot the server</p>	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as <i>admusr</i> first and then switch to <i>root</i> privileges.</p>

7	Verify basic network connectivity and server health.	<p>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(MOS) before proceeding if network ping tests still fail.</p> <p>#ping <XMI or OAM gateway address></p> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle support(MOS).</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ 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@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre>																
8	Check status	<p>In the CMP GUI, navigate to:</p> <p>Platform Setting → Topology Setting → All Clusters</p> <p>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 (MOS) before proceeding.</p>  <p>The screenshot shows the OCPM 12.1.0.0_35.1.0 GA New Install GUI. The main heading is 'OCPM 12.1.0.0_35.1.0 GA New Install'. Below this, there is a navigation menu with 'Policy Servers' selected. Under 'Policy Servers', 'MPE_Site1_Cluster' is selected. The main content area shows 'Policy Server Administration' for 'Policy Server: MPE_Site1_Cluster'. There are tabs for 'System', 'Reports', 'Logs', 'Policy Server', 'Diameter Routing', 'Policies', 'Data Sources', and 'Session Viewer'. The 'System' tab is active, showing buttons for 'Modify', 'Delete', and 'Reapply Configuration'. The 'Configuration' section displays the following details:</p> <table border="1"> <tr> <td>Name</td> <td>MPE_Site1_Cluster</td> </tr> <tr> <td>Status</td> <td>On-line Config Mismatch</td> </tr> <tr> <td>Version</td> <td>12.1.0.0_35.1.0</td> </tr> <tr> <td>Description / Location</td> <td></td> </tr> <tr> <td>Secure Connection</td> <td>No</td> </tr> <tr> <td>Legacy</td> <td>No</td> </tr> <tr> <td>Type</td> <td>Oracle</td> </tr> <tr> <td>System Time</td> <td>Oct 05, 2015 06:21 PM EDT</td> </tr> </table> <p>Below the configuration details, there is a section for 'Associated Templates(lower numbered templates take priority over higher numbered templates)'. It shows a table with columns for 'Priority' and 'Template Name', with 'None' listed under 'Priority'.</p>	Name	MPE_Site1_Cluster	Status	On-line Config Mismatch	Version	12.1.0.0_35.1.0	Description / Location		Secure Connection	No	Legacy	No	Type	Oracle	System Time	Oct 05, 2015 06:21 PM EDT
Name	MPE_Site1_Cluster																	
Status	On-line Config Mismatch																	
Version	12.1.0.0_35.1.0																	
Description / Location																		
Secure Connection	No																	
Legacy	No																	
Type	Oracle																	
System Time	Oct 05, 2015 06:21 PM EDT																	

<p>9□</p>	<p>Set 'Forced Standby' designation on cluster node that is still 'out-of-service'.</p>	<p>In the CMP GUI, navigate to:</p> <p>Platform Setting → Topology Setting → Current Cluster</p> <ul style="list-style-type: none"> - Modify for the server that has a status of 'out-of-service' - Check the Forced Standby checkbox - Click Save  <p>Accept the resulting pop-up by clicking OK:</p> 
<p>10□</p>	<p>SSH from the PM&C server to replacement blade</p>	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380): Use the iLo to login, and a remote console session need to be started to execute commands</p>

11□	Load the ISO to restore 2 nd server of the cluster	<p>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:</p> <p>/var/camiant/backup/local_archive/serverbackup.</p> <p><i>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.</i></p>
12□	Perform platcfg restore from SSH session to replacement blade	<p>Execute the following command</p> <pre># su - platcfg</pre> <p>From within the platcfg utility, navigate to:</p> <p>Policy Configuration → Backup and Restore → Server Restore</p> <p>Select the *serverbackup*.iso that you just put on the system and hit ok – then ‘yes’ to confirm.</p> 
13□	Verify the status	<p>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:</p>

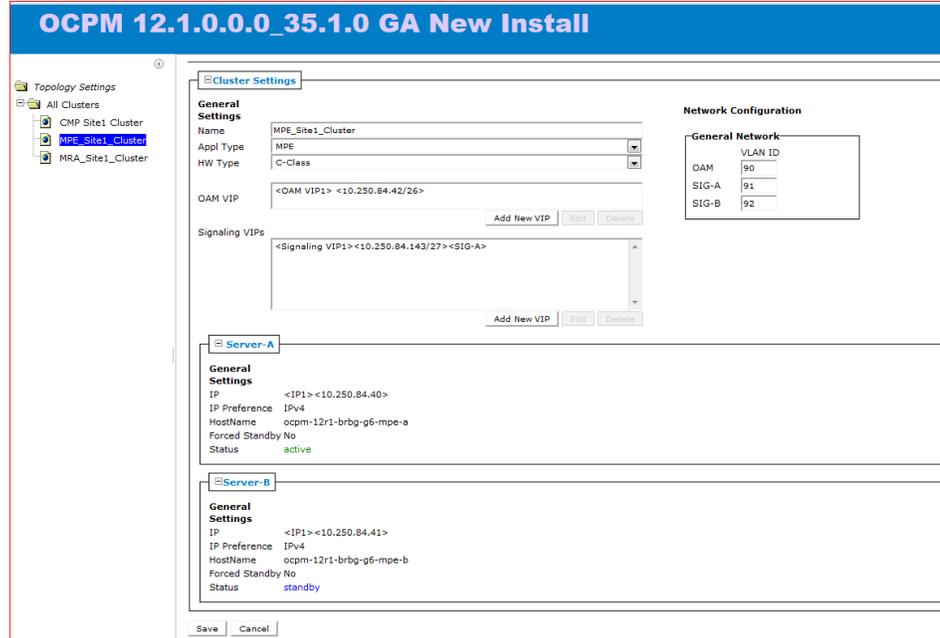
<p>14□</p>	<p>Verify Initial configuration</p>	<p>Choose Exit repeatedly until back to the Main Menu of the platcfg utility. While still within the platcfg utility, navigate to:</p> <p>Policy Configuration → Verify Initial Configuration</p> <p>If configuration is not there, then navigate to ‘Perform Initial Configuration’ and fill in the hostname, OAM IP etc as shown below:</p>  <p>Note: The above screen shot example is for c-Class hardware</p> <p>Ensure that your data is correct, and select ‘OK’, then ‘yes’ to save and apply</p> <p>Exit platcfg</p> <p>Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell.</p> <p><i>For RMS (DL360/DL380/X-3-2/X5-2): The initial Configuration is different. For example: The ‘SIGA VLAN’ and ‘SIGB VLAN’ configuration parameters will not appear in RMS based hardware</i></p>  <p>Note: The above screen shot example is for RMS hardware</p>
<p>15□</p>	<p>Reboot the server</p>	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as admusr first and then switch to root privileges.</p>

16 Remove 'Forced Standby' designation on current blade.

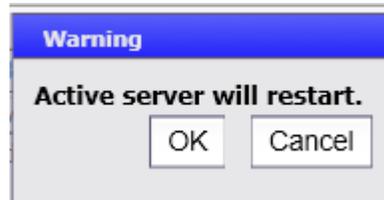
In the CMP GUI, navigate to:

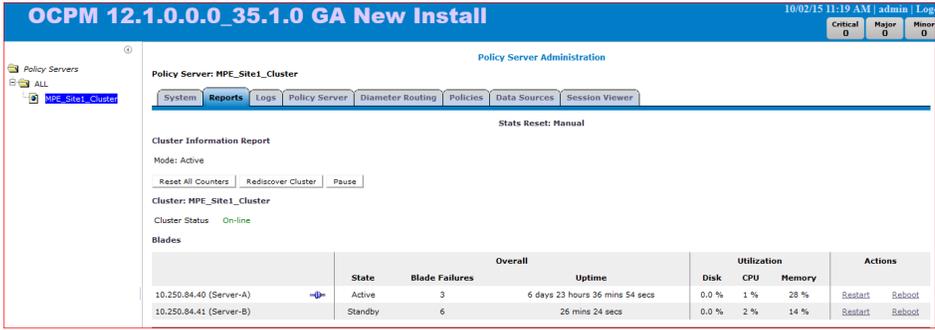
Platform Setting → Topology Setting → Current Cluster

- Modify for the server that has 'forced standby'
- Clear the Forced Standby checkbox
- Click Save



Accept the resulting pop-up by clicking OK:



17	<p>Check status</p>	<p>In the CMP GUI, depending on the type of the blade, perform the following:</p> <ul style="list-style-type: none"> - If this is an MPE/MPE-LI blade, navigate to: <ul style="list-style-type: none"> o Policy Server → Configuration → All → Reports Tab - If this is an MRA blade, navigate to: <ul style="list-style-type: none"> o MRA → Configuration → All → Reports Tab - Check CMP cluster status (as indicated in the previous step), navigate to: <ul style="list-style-type: none"> o Platform Setting → Topology Setting → Current CMP Cluster <p>Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from 'Degraded' to 'On-line'</p> 
18	<p>Alternative method to check replication status</p>	<p>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:</p> <p># irepstat</p> <p>Expected 'irepstat' output while waiting reconnection:</p> <pre data-bbox="511 1270 1458 1432"> -- 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 </pre> <p>Expected 'irepstat' output after cluster has formed:</p> <pre data-bbox="511 1549 1458 1726"> -- Policy 0 ActStb [DbReplication] ----- AA To ocpm-12r1-brbg-g6-cmp-b Active 0 0.00 1%R 0.05%cpu 60B/s AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1%R 0.04%cpu 78B/s AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.00 1%R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.49 1%R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.00 1%R 0.05%cpu 78B/s </pre>

<p>19□</p>	<p>Exchange keys with cluster mate(This step need to run from active CMP)</p>	<p>Exchanging SSH keys Utility as root, please run <code>'/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root'</code>; as admusr, please run <code>'/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'</code></p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@ocpm-12r1-brbg-g6-mpe-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-b ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-a ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-b ... Connecting to admusr@ocpm-12r1-brbg-g6-mpe-b ... [1/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-b ... [2/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-a ... [3/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-a ... [4/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-b ... [5/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-a ... [6/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-b ... SSH keys are OK. [admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ █</pre> <p>This procedure is completed.</p>
------------	---	---

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:
 - o OAM blade Ip address, default gateway, ntp server ip address
 - o 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, or MRA

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.

*Refer to the Policy Management Bare Metal Installation Guide Release 12.1.x

*These documents can be accessed at the following link

[\(http://docs.oracle.com/en/industries/communications/\)](http://docs.oracle.com/en/industries/communications/)

S T E P #	<p>This Procedure performs Restoring complete cluster without the server backup</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>Should this procedure fail, contact the My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Login via SSH to new blade	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380): Use the iLo to login, and a remote console session need to be started to execute commands</p>

2❑ Perform 'Initial Policy Configuration' from within platcfg utility on newly installed blade

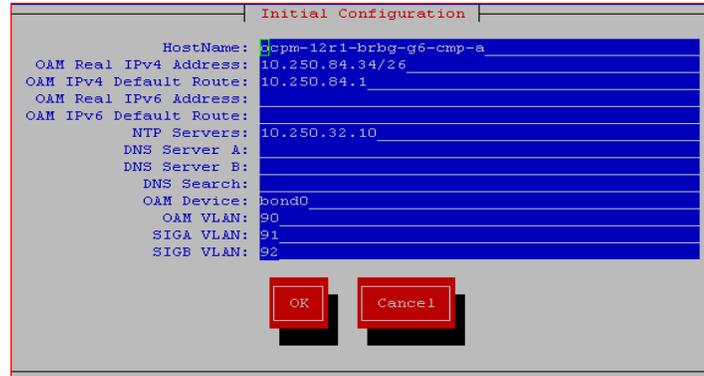
Execute the following command

```
# su - platcfg
```

From within the platcfg utility, navigate to:

Policy Configuration → Perform Initial Configuration

Enter the relevant details from the blade being replaced:

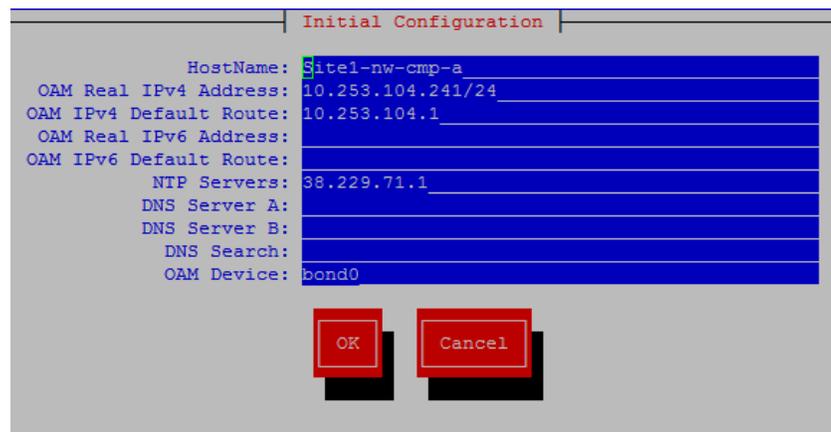


Note: The above screen shot example is for c-Class hardware

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 (MOS) before proceeding.

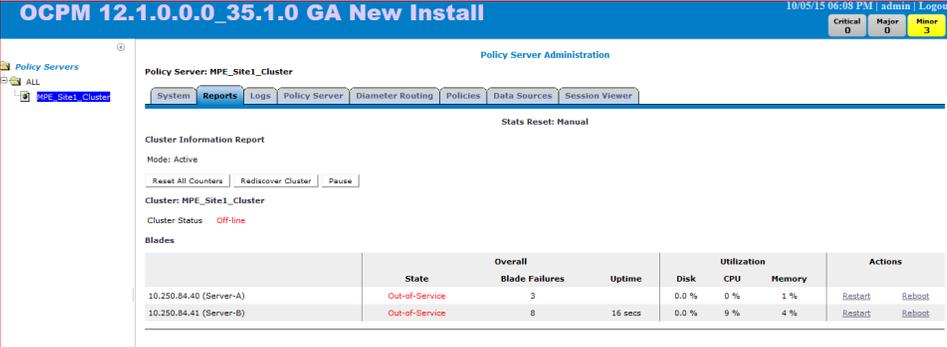
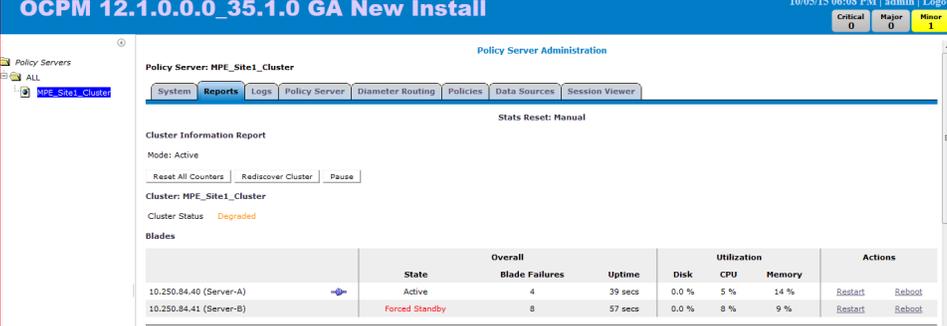
Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell.

For RMS (DL360/DL380/X-3-2/X5-2): The initial Configuration is different. For example: The 'SIGA VLAN' and 'SIGB VLAN' configuration parameters will not appear in RMS based hardware.



Note: The above screen shot example is for RMS hardware

3	Reboot the server	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as <i>admusr</i> first and then switch to <i>root</i> privileges.</p>
4	Verify basic network connectivity and server health.	<p>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(MOS) before proceeding if network ping tests still fail.</p> <pre>#ping <XMI or OAM gateway address></pre> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support(MOS).</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</pre> <pre>The password of admusr in topology: Connecting to admusr@ocpm-12r1-brbg-g6-mpe-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-b ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-a ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-b ... Connecting to admusr@ocpm-12r1-brbg-g6-mpe-b ... [1/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-b ... [2/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-a ... [3/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-a ... [4/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-b ... [5/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-a ... [6/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-b ... SSH keys are OK. [admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre>

<p>5</p>	<p>Check status</p>	<p>In the CMP GUI, depending on the type of the blade, perform the following:</p> <ul style="list-style-type: none"> - If this is an MPE/MPE-LI blade, navigate to: <ul style="list-style-type: none"> o Policy Server → Configuration → All → Reports Tab - If this is an MRA blade, navigate to: <ul style="list-style-type: none"> o MRA → Configuration → All → Reports Tab <p>Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from 'Off-line' to 'Degraded'.</p> <p>Off-line</p>  <p>Degraded</p> 
<p>6</p>	<p>Login via SSH to second node of the current cluster</p>	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380):</p> <p>Use the iLo to login, and a remote console session need to be started to execute commands</p>

70 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:

The screenshot shows the 'Initial Configuration' utility interface. The title bar reads 'Initial Configuration'. The main area contains the following configuration fields:

- HostName: ccpm-12r1-brbg-g6-cmp-a
- OAM Real IPv4 Address: 10.250.84.34/26
- OAM IPv4 Default Route: 10.250.84.1
- OAM Real IPv6 Address: _____
- OAM IPv6 Default Route: _____
- NTP Servers: 10.250.32.10
- DNS Server A: _____
- DNS Server B: _____
- DNS Search: _____
- OAM Device: bond0
- OAM VLAN: 90
- SIGA VLAN: 91
- SIGB VLAN: 92

At the bottom of the utility, there are two red buttons: 'OK' and 'Cancel'.

Note: The above screen shot example is for c-Class hardware

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 (MOS) before proceeding.

Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell.

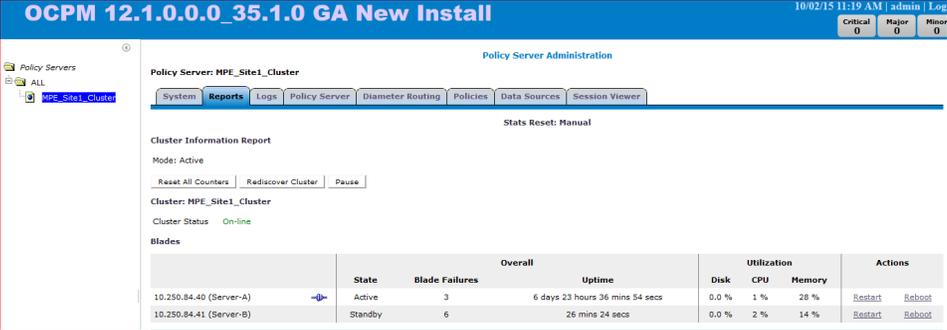
For RMS (DL360/DL380/X-3-2/X5-2): The initial Configuration is different. For example: The 'SIGA VLAN' and 'SIGB VLAN' configuration parameters will not appear in RMS based hardware.

The screenshot shows the 'Initial Configuration' utility interface for RMS hardware. The title bar reads 'Initial Configuration'. The main area contains the following configuration fields:

- HostName: Site1-nw-cmp-a
- OAM Real IPv4 Address: 10.253.104.241/24
- OAM IPv4 Default Route: 10.253.104.1
- OAM Real IPv6 Address: _____
- OAM IPv6 Default Route: _____
- NTP Servers: 38.229.71.1
- DNS Server A: _____
- DNS Server B: _____
- DNS Search: _____
- OAM Device: bond0

At the bottom of the utility, there are two red buttons: 'OK' and 'Cancel'.

Note: The above screen shot example is for RMS hardware

8	Reboot the server	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as <i>admusr</i> first and then switch to <i>root</i> privileges.</p>																													
9	Verify basic network connectivity and server health.	<p>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(MOS) before proceeding if network ping tests still fail.</p> <pre>#ping <XMI or OAM gateway address></pre> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support(MOS) support.</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ 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@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre>																													
10	Check status	<p>In the CMP GUI, depending on the type of the blade, perform the following:</p> <ul style="list-style-type: none"> - If this is an MPE/MPE-LI blade, navigate to: <ul style="list-style-type: none"> o Policy Server → Configuration → All → Reports Tab - If this is an MRA blade, navigate to: <ul style="list-style-type: none"> o MRA → Configuration → All → Reports Tab <p>Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from 'Degraded' to 'On-line'</p>  <table border="1" data-bbox="662 1583 1458 1661"> <thead> <tr> <th rowspan="2"></th> <th rowspan="2">State</th> <th rowspan="2">Blade Failures</th> <th colspan="2">Overall</th> <th colspan="3">Utilization</th> <th rowspan="2">Actions</th> </tr> <tr> <th>Uptime</th> <th>Disk</th> <th>CPU</th> <th>Memory</th> </tr> </thead> <tbody> <tr> <td>10.250.84.40 (Server-A)</td> <td>Active</td> <td>3</td> <td>6 days 23 hours 36 mins 54 secs</td> <td>0.0 %</td> <td>1 %</td> <td>28 %</td> <td>Restart Reboot</td> </tr> <tr> <td>10.250.84.41 (Server-B)</td> <td>Standby</td> <td>6</td> <td>26 mins 24 secs</td> <td>0.0 %</td> <td>2 %</td> <td>14 %</td> <td>Restart Reboot</td> </tr> </tbody> </table>		State	Blade Failures	Overall		Utilization			Actions	Uptime	Disk	CPU	Memory	10.250.84.40 (Server-A)	Active	3	6 days 23 hours 36 mins 54 secs	0.0 %	1 %	28 %	Restart Reboot	10.250.84.41 (Server-B)	Standby	6	26 mins 24 secs	0.0 %	2 %	14 %	Restart Reboot
	State	Blade Failures				Overall		Utilization				Actions																			
			Uptime	Disk	CPU	Memory																									
10.250.84.40 (Server-A)	Active	3	6 days 23 hours 36 mins 54 secs	0.0 %	1 %	28 %	Restart Reboot																								
10.250.84.41 (Server-B)	Standby	6	26 mins 24 secs	0.0 %	2 %	14 %	Restart Reboot																								

11□	Alternative method to check replication status	<p>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:</p> <pre># irepstat</pre> <p>Expected 'irepstat' output while waiting reconnection:</p> <pre> -- 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 </pre> <p>Expected 'irepstat' output after cluster has formed:</p> <pre> -- Policy 0 ActStb [DbReplication] ----- AA To ocpm-12r1-brbg-g6-cmp-b Active 0 0.00 1%R 0.05%cpu 60B/s AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1%R 0.04%cpu 78B/s AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.00 1%R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.49 1%R 0.05%cpu 78B/s AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.00 1%R 0.05%cpu 78B/s </pre>
12□	Exchange keys with cluster mate (This step need to run from active CMP)	<p>Exchanging SSH keys Utility</p> <p>as root, please run '<code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code>';</p> <p>as admusr, please run '<code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code>'</p> <pre> [admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@ocpm-12r1-brbg-g6-mpe-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-a ... Connecting to admusr@ocpm-12r1-brbg-g6-mra-b ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-a ... Connecting to admusr@ocpm-12r1-brbg-g6-cmp-b ... Connecting to admusr@ocpm-12r1-brbg-g6-mpe-b ... [1/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-b ... [2/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mra-a ... [3/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-a ... [4/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-b ... [5/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-cmp-a ... [6/6] Provisioning SSH keys on ocpm-12r1-brbg-g6-mpe-b ... SSH keys are OK. [admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ █ </pre> <p>This procedure is completed.</p>

5.7. Procedure 7: Restoring CMP 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.
- Initial configuration information about the blade to be restored:
 - o OAM IP address, default gateway, NTP & SNMP server IP addresses
 - o 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

*Refer to the Policy Management Bare Metal Installation Guide Release 12.1.x

*These documents can be accessed at the following link
[\(http://docs.oracle.com/en/industries/communications/\)](http://docs.oracle.com/en/industries/communications/)

S T E P #	<p>This Procedure performs Restoring CMP cluster with system backup available</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.</p>	
1 <input type="checkbox"/>	Login via SSH to new blade	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre style="color: red;"># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380): Use the iLo to login, and a remote console session need to be started to execute commands.</p>

2❑ Perform 'Initial Policy Configuration' from within platcfg utility on newly installed blade

Execute the following command

```
# su - platcfg
```

From within the platcfg utility, navigate to:

Policy Configuration → Perform Initial Configuration

Enter the relevant details from the blade being replaced:

```
Initial Configuration
HostName: ccpm-12r1-brbg-g6-cmp-a
OAM Real IPv4 Address: 10.250.84.34/26
OAM IPv4 Default Route: 10.250.84.1
OAM Real IPv6 Address:
OAM IPv6 Default Route:
NTP Servers: 10.250.32.10
DNS Server A:
DNS Server B:
DNS Search:
OAM Device: bond0
OAM VLAN: 90
SIGA VLAN: 91
SIGB VLAN: 92
OK Cancel
```

Note: The above screen shot example is for c-Class hardware

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 (MOS) support before proceeding.

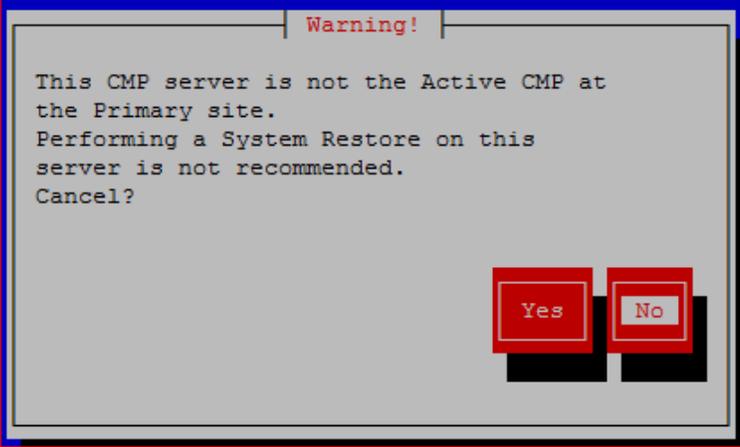
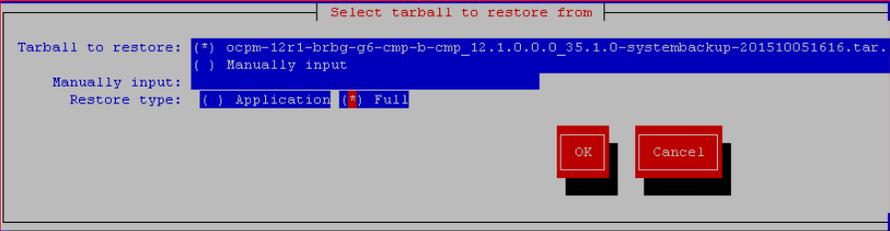
Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell.

For RMS (DL360/DL380/X-3-2/X5-2): The initial Configuration is different. For example: The 'SIGA VLAN' and 'SIGB VLAN' configuration parameters will not appear in RMS based hardware.

```
Initial Configuration
HostName: Site1-nw-cmp-a
OAM Real IPv4 Address: 10.253.104.241/24
OAM IPv4 Default Route: 10.253.104.1
OAM Real IPv6 Address:
OAM IPv6 Default Route:
NTP Servers: 38.229.71.1
DNS Server A:
DNS Server B:
DNS Search:
OAM Device: bond0
OK Cancel
```

Note: The above screen shot example is for RMS hardware

3	Reboot the server	<p>Reboot:</p> <pre>#init 6</pre> <p>Allow the server time to reboot; reconnect via SSH from the PM&C server to the node as admusr first and then switch to root privileges.</p>
4	Verify basic network connectivity and server health.	<p>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(MOS) support before proceeding if network ping tests still fail.</p> <pre>#ping <XMI or OAM gateway address></pre> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support(MOS) support.</p> <pre>[admusr@ocpm-12r1-brbg-g6-cmp-a ~]\$ 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@ocpm-12r1-brbg-g6-cmp-a ~]\$</pre>
5	Load the system backup(ISO) file for server restore	<p>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.</p> <p>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).</p> <p>/var/camiant/backup/local_archive/systembackup/</p>

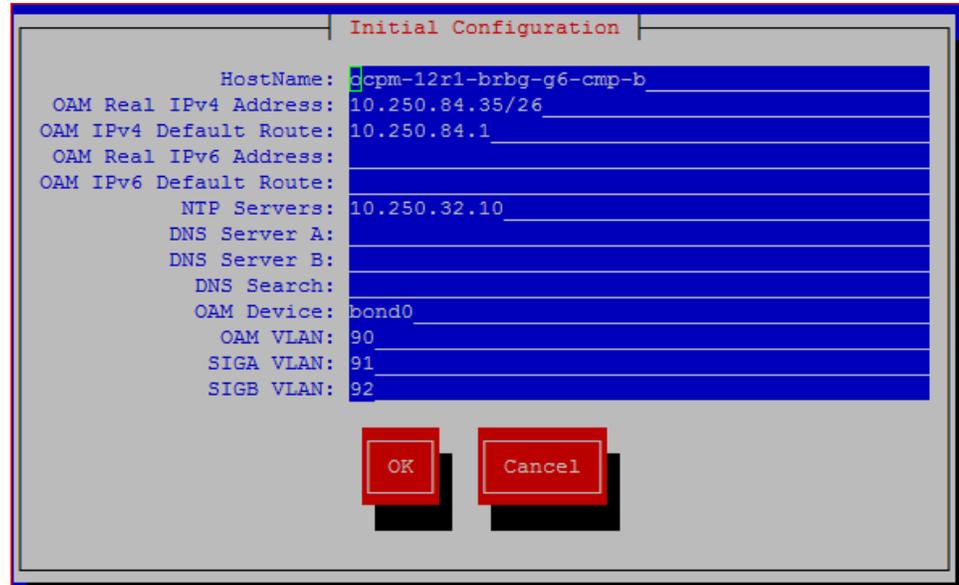
<p>6□</p>	<p>Perform platcfg restore from SSH session to replacement blade</p>	<p>Execute the following command</p> <pre># su - platcfg</pre> <p>From within the platcfg utility, navigate to:</p> <p>Policy Configuration → Backup and Restore → System Restore</p> <p>A message will appear prompting confirmation to restore even though this node is not recognized as the active member. This behavior is expected, continue by selecting 'NO'.</p>  <p>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.</p>  <p>Note: "Full" will also restore Comcol data, But "Application" will exclude Comcol.</p>
<p>7□</p>	<p>Verify the status</p>	<p>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 (MOS) support team or engineering team for assistance.</p>

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:

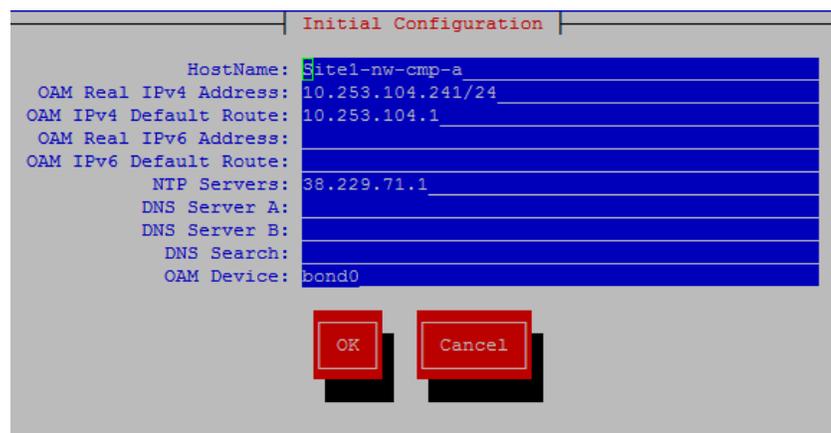


Select ‘Ok’, then ‘yes’ to save and apply

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 (MOS) before proceeding.

Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell.

Note: The above screen shot example is for c-Class hardware
For RMS (DL360/DL380/X-3-2/X5-2): The initial Configuration is different. For example: The ‘OAM VLAN’, ‘SIGA VLAN’ and ‘SIGB VLAN’ configuration parameters will not appear in RMS based hardware , **Note:** The below is a screenshot for RMS hardware



9□	Reboot the server	<p>Reboot. Allow the server time to reboot, then reconnect via SSH from the PM&C server.</p> <pre>#init 6</pre>
10□	Verify basic network connectivity and server health.	<p>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(MOS) support before proceeding if network ping tests still fail.</p> <p>#ping <XMI or OAM gateway address></p> <p>Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support(MOS) support.</p> <pre>Using username "admusr". Last login: Mon Oct 5 16:15:10 2015 from 10.154.169.3 [admusr@ocpm-12r1-brbg-g6-cmp-b ~]\$ su - root Password: [root@ocpm-12r1-brbg-g6-cmp-b ~]# 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 [root@ocpm-12r1-brbg-g6-cmp-b ~]#</pre>
11□	Check status	<p>In the CMP GUI, navigate to:</p> <p>Platform Setting → Topology Setting → All Clusters</p> <p>When the server has returned to online status, log into the GUI on the OAM virtual IP address</p> <p>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)</p> <p>Verify other application configuration properties as you are able.</p> <p>Once one CMP is in place, the other node of the CMP cluster can be replaced with the procedures above, and any other clusters or individual nodes that need replacement can be handled with the above procedures.</p> <p>This procedure is completed.</p>

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.

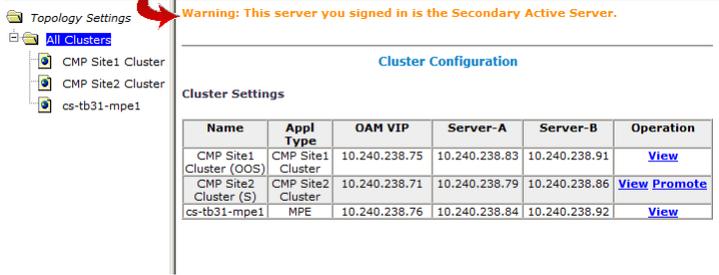
S	This Procedure performs Promoting geo-redundant CMP cluster	
T	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
E	Should this procedure fail, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.	
P		
#		
1	<input type="checkbox"/> 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.



The screenshot shows a warning: "Warning: This server you signed in is the Secondary Active Server." Below this is a "Cluster Configuration" section with a table of "Cluster Settings".

Name	Appl Type	OAM VIP	Server-A	Server-B	Operation
CMP Site1 Cluster (OOS)	CMP Site1 Cluster	10.240.238.75	10.240.238.83	10.240.238.91	View
CMP Site2 Cluster (S)	CMP Site2 Cluster	10.240.238.71	10.240.238.79	10.240.238.86	View Promote
cs-tb31-mpe1	MPE	10.240.238.76	10.240.238.84	10.240.238.92	View

3☐ Verify basic network connectivity and server health.

From the newly Promoted server(active server of site 2 CMP), 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(MOS) 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(MOS) support.

```
[root@ocpm-12r1-brbg-g6-cmp-b ~]# syscheck
Running modules in class disk...
                                OK

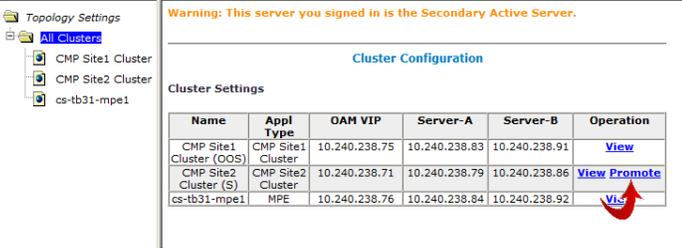
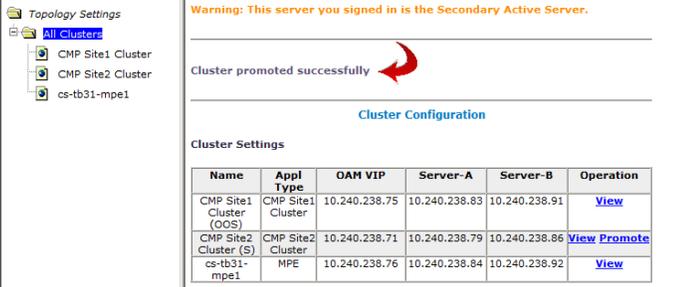
Running modules in class hardware...
                                OK

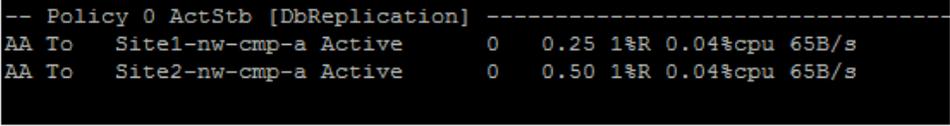
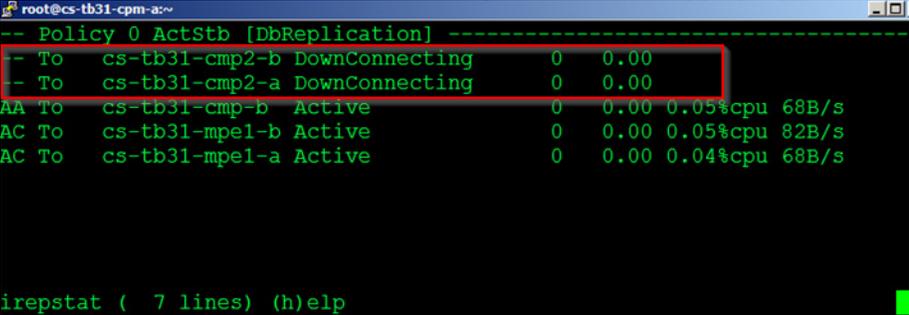
Running modules in class net...
                                OK

Running modules in class proc...
                                OK

Running modules in class system...
                                OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
[root@ocpm-12r1-brbg-g6-cmp-b ~]#
```

4	Promote secondary CMP cluster	<p>In the CMP GUI, navigate to:</p> <p>Platform Setting → Topology Setting → All Clusters</p> <p>Select 'Promote' on the secondary server. Accept the resulting pop-up by clicking 'OK'.</p>  <p>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 (MOS) support.</p> 
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	<p>Relogin to the CMP GUI using the VIP of CMP Site2</p> <p>In the CMP GUI, navigate to:</p> <p>Platform Setting → Topology Setting → All Clusters</p> <p>Ensure all clusters are performing as expected. Follow procedures listed in this document to bring other failed servers/clusters back online.</p>
7	SSH to active node of newly promoted cluster	<p>For c-Class System:</p> <p>SSH session from PM&C to new server, using the PM&C GUI > Software > Software Inventory screen to obtain the blade IP address:</p> <pre># ssh admusr@<node_IP_Address> \$ su - root</pre> <p>For RMS (DL360/DL380): Use the iLo to login, and a remote console session need to be started to execute commands.</p>

8□	Verify irepstat output shows expected status	<p>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.</p> <pre># irepstat</pre>  <pre>-- 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</pre> <p>The status of all clusters except known failed servers should have a status of 'Active' as in the above snapshot.</p> <p>Otherwise if any of the replication paths show 'DownConnecting' as in the snapshot below contact My Oracle Support (MOS) support.</p> <p>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.</p>  <pre>root@cs-tb31-cmp-a:~ -- Policy 0 ActStb [DbReplication] ----- -- To cs-tb31-cmp2-b DownConnecting 0 0.00 -- To cs-tb31-cmp2-a DownConnecting 0 0.00 AA To cs-tb31-cmp-b Active 0 0.00 0.05%cpu 68B/s AC To cs-tb31-mpel-b Active 0 0.00 0.05%cpu 82B/s AC To cs-tb31-mpel-a Active 0 0.00 0.04%cpu 68B/s irepstat (7 lines) (h)elp</pre>
9□	Rebuild failed CMP cluster	<p>Refer to Procedure 6: Restoring complete cluster without the server backup to rebuild failed CMP cluster.</p> <p>This procedure is completed.</p>

5.8.1.1.1. 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.

My Oracle Support (MOS)

MOS is available 24 hours a day, 7 days a week, 365 days a year:

Web portal (preferred option): [My Oracle Support \(MOS\)](https://support.oracle.com/) at <https://support.oracle.com/>

Phone: +1.800.223.1711 (toll-free in the US),

Or retrieve your local hotline from [Oracle Global Customer Support Center](http://www.oracle.com/support/contact.html) at <http://www.oracle.com/support/contact.html>

Make the following selections on the Support telephone menu:

Select **2** for New Service Request

Then select **3** for Hardware, Networking, and Solaris Operating System Support

Then: either

4.2.3. select **1** for **Technical Issues**,

When talking to the agent, please indicate that you are an existing Tekelec customer.

Note: Oracle support personnel performing installations or upgrades on a customer site must obtain the customer Support Identification (SI) number prior to seeking assistance.

OR

4.2.4. Select **2** for **Non-Technical Issues**, for example, for My Oracle Support (MOS) registration.

When talking to the agent, mention that you are a Tekelec Customer new to MOS.

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.

5.8.1.1.2. Recovery of third party components

Refer [8] 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**