Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Policy Management
Disaster Recovery

E85336-01

July 2017

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

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

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

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

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

EMAIL: support@oracle.com

Oracle Communications Policy Management Disaster Recovery

Table of Contents

List of Tables

1. INTRODUCTION

1.1 Purpose and Scope

This document is a guide to describe procedures used to run disaster recovery for Policy Management System, Release 12.3. This includes recovery of partial or a complete loss of one or more Policy Management servers and Policy Management components. This document provides step-by-step instructions to run disaster recovery for Policy Management Systems. Running this procedure also involves referring to and running procedures in existing support documents.

1.2 References

[1] E67765–Oracle Firmware Upgrade Release Notes, Release 3.1.5

[2] E67825–Oracle Firmware Upgrade Pack Upgrade Guide, Release 3.1.5

[3] E70315–Oracle Firmware Upgrade Release Notes, Release 3.1.6

[4] E70316–Oracle Firmware Upgrade Pack Upgrade Guide, Release 3.1.6

[5] E82950–HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.11

[6] E64917–HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.9

[7] E54387–PM&C Incremental Upgrade, Current Revision

[8] E56282–TVOE 3.2 Disaster Recovery Procedure, Release 7.2, Current Revision

[9] E53486–Tekelec Platform 7.0.x Configuration Procedure Reference, Current Revision

[10] E54388-02–PM&C Disaster Recovery, Release 6.0

[11] E67647–PM&C Disaster Recovery, Release 6.2

[11] E53487–PM&C 6.2 Incremental Upgrade Procedure, Current Revision

[12] E72270 Revision 01–Mediation Server User's Guide, Release 12.2

[13] E85333-01 Policy Management 12.3 Bare Metal Installation Guide

The documents listed are available on the Oracle Help Center.

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

1.3 Acronyms

Table 1: Acronyms

Acronym	Meaning
BIOS	Basic Input Output System
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
CMP	Configuration Management Platform
DR-CMP	Configuration Management Product for Disaster Recovery **NOTE:** It refers to the CMP on the secondary site
DVD	Digital Video Disc
GRUB	Grand Unified Boot loader

Acronym	Meaning
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 (for example, TPD)
PM&C	Platform Management & Configuration
RMM	Remote Management Module
RMS	Rack Mount Server
SOL	Serial Over LAN
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment
FRU	Field Replaceable Unit
USB	Universal Serial Bus

1.4 Logins and Passwords

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

1.5 Software Release Numbering

This guide applies to all Policy Management 12.3 versions. It is assumed that PM&C Version 6.0.3 or above has been previously installed, configured in this deployment and in working condition, i.e. PM&C is not affected. PM&C Disaster Recovery Release 6.0 (refer to document E54388-02 for c-Class hardware enclosure details). The Oracle X5-2, Netra X5-2 and HP RMS hardware systems do not use PM&C.

1.6 Terminology

Table 2: Terminology

Term	Description
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 operating system for the server: Tekelec Platform Distribution (TPD).
c-Class	HP marketing term for their enterprise server platform
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 Management server through the platcfg utility that brings the server's network interface online and allows management and configuration from the CMP

Disaster Recovery

Term	Description
Cluster mate	The clusters being in the same topology settings form the cluster mate relationships with each other.

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 Georedundant CMP (DR-CMP) servers)
  - 1 or more MPE/MRA/Mediation servers failed
- Recovery of the entire network from a total outage
  - The CMP servers are not available (neither primary, nor secondary) and other MPE/MRA/Mediation servers must be recovered

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

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

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

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

2.1 Scenarios

2.1.1 Single Node Outage MPE/MRA/Mediation/CMP with CMP Server Available

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

2.1.2 Recovery of Complete MPE/MRA/Mediation 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. The Perform Initial Configuration information must be restored either manually or from a server backup file to all of the replaced nodes, after which the cluster reforms. The CMP can then push application level configuration to the new cluster.

2.1.3 Recovery of the CMP Cluster When No Georedundant CMP Exists

The complete failure of the CMP requires re-installation using base recovery of hardware and software. The Perform Initial Configuration information must be restored either manually or from a server backup file. After the cluster is available, completion of the recovery requires the use of a stored system backup to recover application level configuration including policies and configuration of the MPE/MRA/Mediation clusters in the network.

2.1.4 Recovery of the CMP Cluster when georedundant CMP (DR-CMP) is available

The availability of a georedundant CMP (DR-CMP) simplifies restoration of a failed CMP. The georedundant CMP can be promoted to active primary, and the failed CMP requires re-installation using base recovery of hardware and software. The Perform Initial Configuration information must be restored either manually or from a server backup file. After the cluster is available, the primary running georedundant CMP replicates databases to the replaced CMP cluster.

2.1.5 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 georedundant 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 are taken from 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.

2.2 Perform Initial Configuration

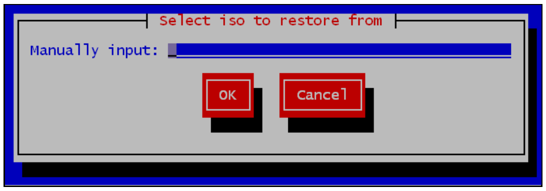
The information required for initial configuration is not extensive, and may be readily available from customer site documents, or from the topology configuration of the CMP. In some cases it can be easier to manually input the initial configuration in platcfg than to try to load a server backup file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

Needed initial configuration information:

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

2.3 Using the Server Backup File

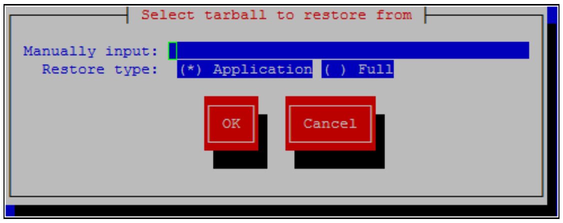
When asked to restore from a server backup, the platcfg utility looks in `/var/camiant/backup/local-archive/serverbackup` directory. If the directory is empty, the selection dialog opens.



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

2.4 Using the System Restore File

When asked to restore from system backup, the platcfg utility looks in the `/var/camiant/backup/local-archive/systembackup` directory. If the directory is empty, the selection dialog opens.



```
Select tarball to restore from

Manually input:
  Restore type:  (*) Application ( ) Full
```

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

2.5 PM&C Usage

When working with a c-Class enclosure, the PM&C establishes connectivity with DHCP to the server in the enclosure. This allows 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 servers over the internal 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 run.

3.1 Disaster Recovery Strategy

Disaster recovery procedures are 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 georedundant CMP (DR-CMP) is available
5. From the failure conditions, determine the recovery scenario and procedure to follow.
6. Run appropriate recovery procedures.

3.1.1 Required Materials

The following items are needed for disaster recovery:

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

3.2 Policy Server Backup

Backup of the Policy Management server can be done either manually from platcfg, or on a schedule as configured in platcfg. There are two types of backup operations available:

- 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 creates a Server Configuration Backup file, and must be run on each of the servers in the network.

- System Backup

There is one Application Configuration backup for the entire Policy Management system. The system backup gathers PCRF configuration information that is unique to this system. Information such as: Topology, Policies, Feature Configuration. The system backup is run only on the Active CMP at the primary site.

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

4. PROCEDURE PREPARATION

4.1 Purpose and Scope

Disaster recovery procedures are 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 procedures that are 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:

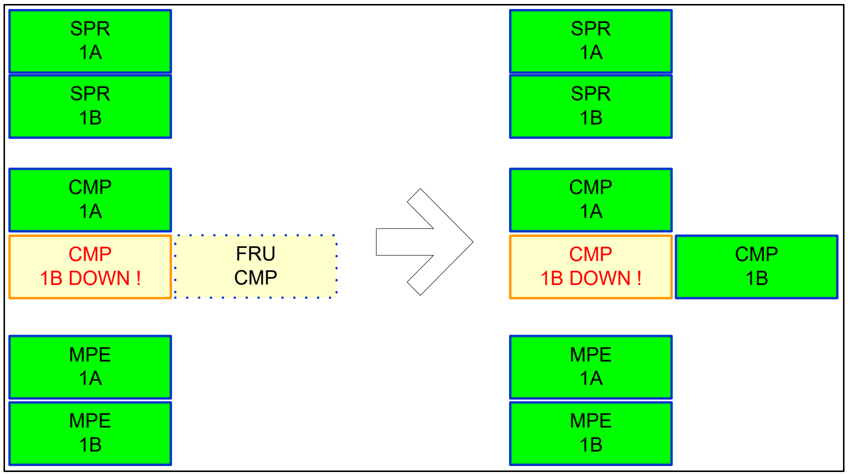
1. Verify BIOS time is correct on servers.
2. Verify Version of TPD installed.
3. Load application for corresponding server hardware types.
4. Check FW versions and upgraded if necessary.
5. Check NTP status after recovery.
6. Check Active Alarms from GUI and using both the `syscheck` command and `alarmMgr-alarmStatusfrom`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

4.2 Recovery Scenarios

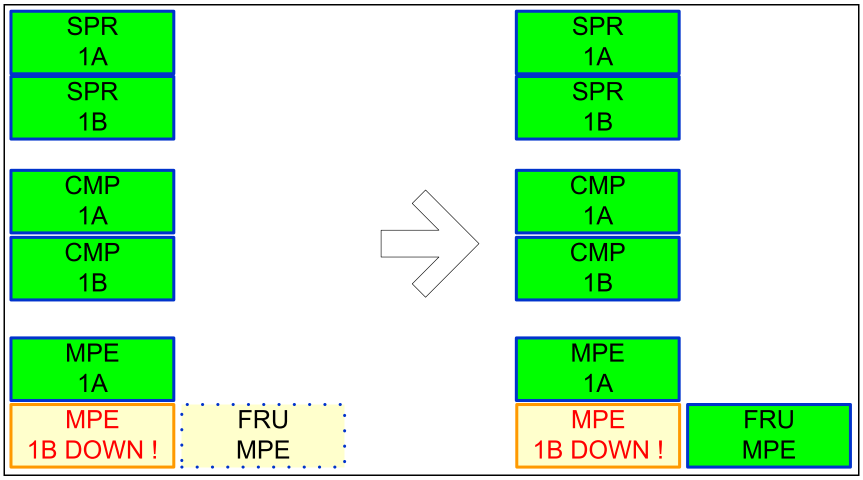
4.2.1 Recovery Scenario 1 (Partial Cluster Outage with Primary CMP Server Available)

For a partial outage with a CMP server available, only base recovery of hardware and software and initial Policy Management configuration is needed. A single CMP server is capable of restoring the configuration database via replication to all MPE/MRA/Mediation 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 run the procedure. The details for the procedure 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 Management configuration is re-installed, either through the platcfg utility, or from the server backup file
  - The database is intact at the active CMP server and is replicated to the standby CMP server.



- Recover any failed MPE/MRA/Mediation servers by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
  - Initial Policy Management configuration is re-installed, either through the platcfg utility 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/Mediation servers using the re-apply configuration function.



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/Mediation node without server backup file to recover MPE/MRA/Mediation nodes when one of the peers of the cluster is still available.

  Or Procedure 3: Restore single MPE/MRA/Mediation node with server backup file

- Use Procedure 5: Restoring complete cluster with the server backup files

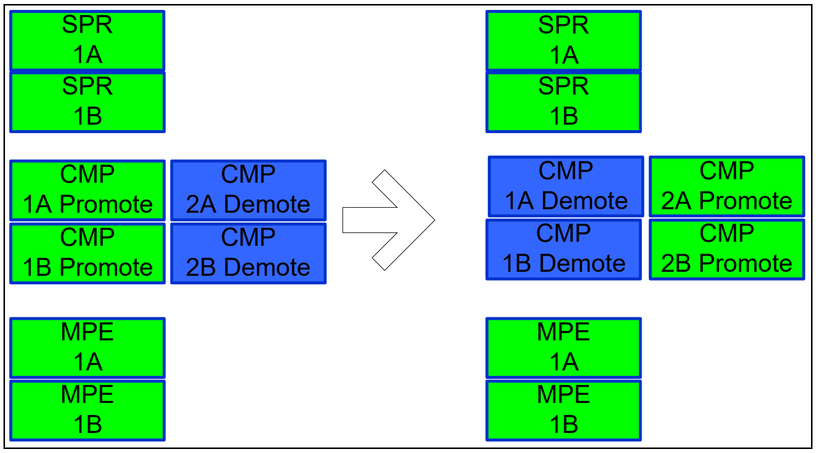
  Or Procedure 6: Restoring complete cluster without the server backup to recover complete MPE/MRA/Mediation clusters that have gone down.

- Use Procedure 7: Restoring CMP cluster with system backup available files to recover first of 2 nodes in CMP cluster
- Use Procedure 3: Restore single MPE/MRA/Mediation node with server backup file to recover the second node of MPE/MRA/Mediation cluster.

4.2.2 Recovery Scenario 2 (Partial Cluster Outage with Georedundant CMP Server Available)

For a partial outage with a georedundant CMP server available, the secondary site CMP must be manually promoted to Primary status as the controlling CMP for the Policy Management network. Then base recovery of hardware and software and initial Policy Management configuration is needed. The now active CMP server is capable of restoring the configuration database via replication to all MPE/MRA/Mediation 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 run the procedure. The detailed steps for the procedures are in Restore Procedures section. The major activities are summarized as follows:

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



This would only be done if the Primary CMP cluster needs to be restored. If it is an MRA, Mediation or MPE cluster that needs to be restored, you do not have to promote the georedundant CMP.

1. Recover any failed MPE/MRA/Mediation servers by recovering base hardware and software.
    a. Recover the base hardware.
    b. Recover the software.
    c. Initial Policy Management configuration is re-installed, either through the platcfg menu, or from the server backup file.
    d. 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/Mediation servers using the re-apply configuration function.
2. Recover other site CMP server by recovering base hardware and software.
    a. Recover the base hardware.

b. Recover the software.

c. Initial Policy Management configuration is re-installed, either through the platcfg utility or from the server backup file.

The database of the active georedundant CMP server is replicated to the new CMP server.

Refer to these procedures for detailed steps.

- Use Procedure 8: Promoting georedundant CMP cluster below to promote the georedundant CMP
- Use Procedure 4: Restore single MPE/MRA/Mediation node without server backup file to recover MPE/MRA/Mediation nodes when one of the peers of the cluster is still available.

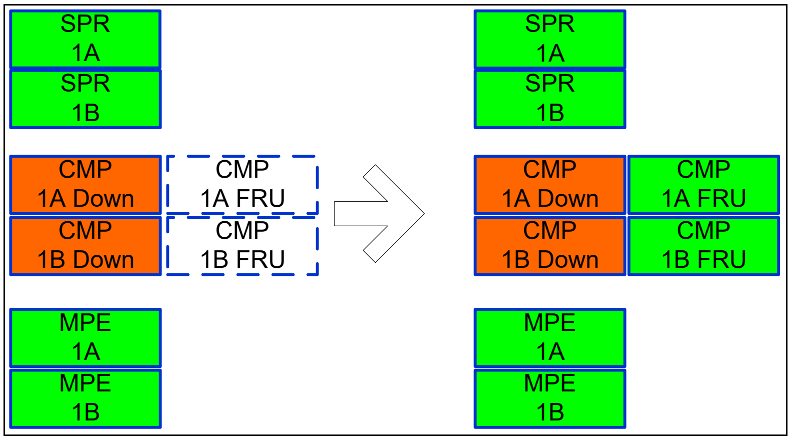
  Or Procedure 3: Restore single MPE/MRA/Mediation node with server backup file
- Use Procedure 5: Restoring complete cluster with the server backup files

  Or Procedure 6: Restoring complete cluster without the server backup to recover complete MPE/MRA/Mediation clusters that have gone down.
- Use Procedure 5: Restoring complete cluster with the server backup files

  Or Procedure 6: Restoring complete cluster without the server backup to recover the secondary site CMP. Recovery of the secondary site CMP can be left for late in the process because the now active CMP can handle all application level configuration as the network is brought back online.
- Use Procedure 7: Restoring CMP cluster with system backup available files to recover first of 2 nodes in CMP cluster
- Use Procedure 3: Restore single MPE/MRA/Mediation node with server backup file to recover the second node of MPE/MRA/Mediation cluster.

4.2.3 Recovery Scenario 3 (Full Cluster Outage of the CMP; Georedundancy 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 Management 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 forms 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 run the procedure. The details for the procedure are in the Restore Procedures section. The major activities are summarized as follows:



Disaster Recovery

1. Recover one Primary CMP server (if necessary) by recovering base hardware and software.
   a. Recover the base hardware.
   b. Recover the software.
   c. Initial Policy Management configuration is re-installed, either through the platcfg menu, or from the server backup file.
   d. The database of the CMP is restored from a system backup provided by the customer.
   e. 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.
2. Recover the second CMP server by recovering base hardware and software.
   a. Recover the base hardware.
   b. Recover the software.
   c. Initial Policy Management configuration is re-installed, either through the platcfg menu, or from the server backup file
   d. The configuration database is available at the now active CMP server and does not require restoration on the second CMP node. Configuration is replicated when the two new CMP nodes form a cluster.
3. Recover any failed MPE/MRA/Mediation servers by recovering base hardware and software.
   a. Recover the base hardware.
   b. Recover the software.
   c. Initial Policy Management configuration is re-installed, either through the platcfg menu, or from the server backup file
   d. 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/Mediation servers.

Refer to these procedures 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/Mediation node without server backup file to recover MPE/MRA/Mediation nodes when one of the peers of the cluster is still available.

  Or Procedure 3: Restore single MPE/MRA/Mediation node with server backup file
- Use Procedure 5: Restoring complete cluster with the server backup files

  Or Procedure 6: Restoring complete cluster without the server backup to recover complete MPE/MRA/Mediation clusters that have gone down.

Disaster Recovery

- Use Procedure 7: Restoring CMP cluster with system backup available files to recover first of 2 nodes in CMP cluster
- Use Procedure 3: Restore single MPE/MRA/Mediation node with server backup file to recover the second node of MPE/MRA/Mediation cluster.

5. RESTORE PROCEDURES

5.1 Procedure 1: Restore Standby CMP Node with Server Backup File

Use this procedure to replace one node of a CMP cluster. Restore the initial Policy Management 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, the initial Policy Management 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

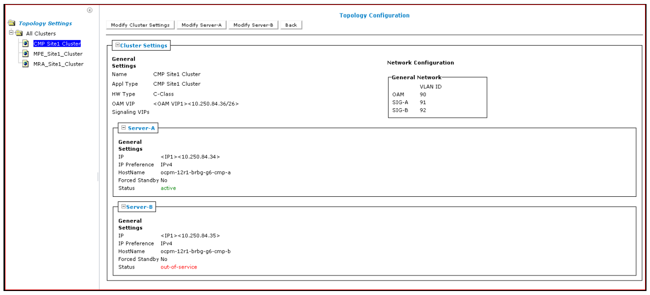
Prerequisites

1. Power down the failed server gracefully
   a. Access iLO with administrator privileges.
   b. Go to **Power Management Server Power**
   c. Click **Momentary Press**
2. Remove the failed server and replace.
3. Verify that the node has TPD installed. If TPD is not present, install TPD.
4. Install the CMP application software.

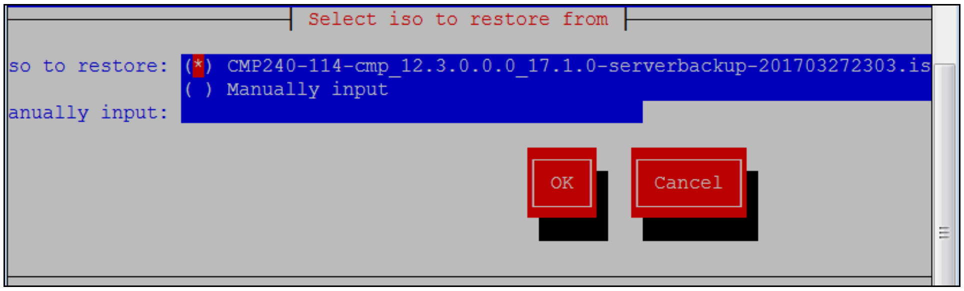
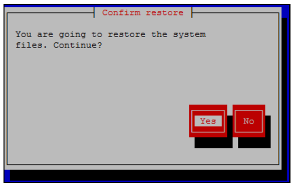
   NOTE: Refer to the Policy Management Bare Metal Installation Guide, Release 12.3. The documents are available on the Oracle Help Center

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

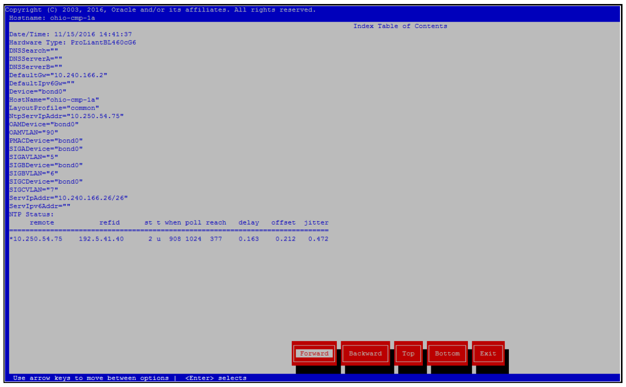
Should this procedure fail, contact My Oracle Support (MOS) Customer Care Center and ask for assistance.

Step	Procedure	Details
1. □	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to **Platform Setting → Topology Settings → All Clusters** 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click **Modify Server-*X*** for the failed node 5. Select **Forced Standby** so that it is checked 6. Click **Save**.  Topology Settings All Clusters CMP Site1 Cluster MPE_Site1_Cluster MRA_Site1_Cluster Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings General Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type C-Class OAM VIP <OAM VIP1><10.250.84.36/26> Signaling VIPs Network Configuration General Network VLAN ID OAM 90 SIG-A 91 SIG-B 92 Server-A General Settings IP <IP1><10.250.84.34> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-cmp-a Forced Standby No Status active Server-B General Settings IP <IP1><10.250.84.35> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-cmp-b Forced Standby No Status out-of-service
2. □	Load the ISO for server restore	Obtain the **serverbackup**.iso for the node to be restored. When the replacement node is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE:** Later in this procedure, the platcfg utility restore function checks this directory and opens a menu. The platcfg utility also lets you manually enter any mounted path on the server.
3. □	Login into the node using SSH	For a c-Class System: 1. Start an SSH session from PM&C to the new server. 2. Using the PM&C GUI, select **Software → Software Inventory** to obtain the IP address for the server: For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System: 1. Use the iLO/iLOM (for Oracle hardware Oracle X5-2 and Netra X5-2) to login. 2. Start a remote console session to run commands.

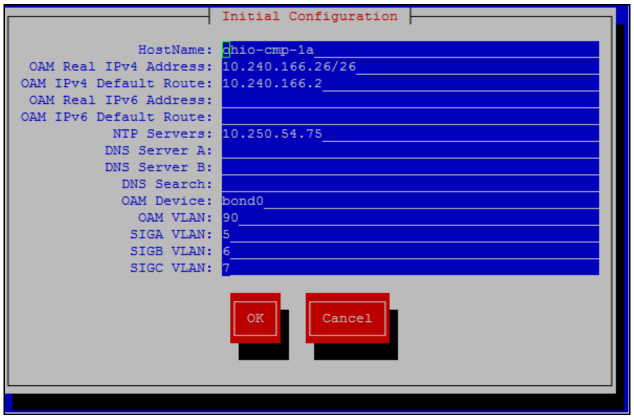
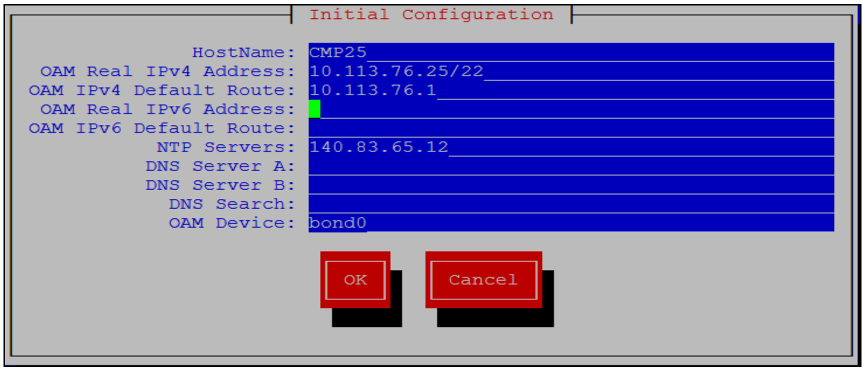
Step	Procedure	Details

☐	Perform platcfg restore from SSH session to replacement node	1. Start the platcfg utility.
		`# su – platcfg`
		2. From the platcfg utility, navigate to **Policy Configuration → Backup and Restore → Server Restore.**
		3. Select the **serverbackup**.ISO that you just copied to the system.
		4. Click **OK**.
		
		`Select iso to restore from`
		`so to restore: (*) CMP240-114-cmp_12.3.0.0.0_17.1.0-serverbackup-201703272303.is`
		`               ( ) Manually input`
		`anually input:`
		
		5. Click **Yes** to confirm.
		
		`Confirm restore`
		`You are going to restore the system files. Continue?`

☐	Verify the status	A dialog opens indicating that the restore operation was successful and instructing you to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

☐	Perform Initial configuration	1. Click **Exit** until you return to the Main Menu of the platcfg utility.
		2. Navigate to **Policy Configuration → Verify Initial Configuration**.
		
		`Copyright (C) 2003, 2016, Oracle and/or its affiliates. All rights reserved.`
		`Hostname: ohio-cmp-1a`
		`Index Table of Contents`
		`Date/Time: 11/15/2016 14:41:37`
		`Hardware Type: ProLiantBL460cG6`
		`DNSSearch=""`
		`DNSServerA=""`
		`DNSServerB=""`
		`DefaultGw="10.240.166.2"`
		`DefaultIpv6Gw=""`
		`Device="bond0"`
		`HostName="ohio-cmp-1a"`
		`LayoutProfile="common"`
		`NtpServIpAddr="10.250.54.75"`
		`OAMDevice="bond0"`
		`OAMVLAN="90"`
		`PMACDevice="bond0"`
		`SIGADevice="bond0"`
		`SIGAVLAN="5"`
		`SIGBDevice="bond0"`
		`SIGBVLAN="6"`
		`SIGCDevice="bond0"`
		`SIGCVLAN="7"`
		`ServIpAddr="10.240.166.26/26"`
		`ServIpv6Addr=""`
		`NTP Status:`
		`     remote           refid      st t when poll reach   delay   offset  jitter`
		`==============================================================================`
		`*10.250.54.75    192.5.41.40      2 u  908 1024  377    0.163    0.212   0.472`
		
		`Use arrow keys to move between options |  <Enter> selects`
		If the configuration does not exist, navigate to **Perform Initial Configuration** and enter:
		• Hostname
		• OAM IP
		• Configuration for your specific server

Step	Procedure	Details

		For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)
		
		Initial Configuration
		`HostName: chio-cmp-1a`
		`OAM Real IPv4 Address: 10.240.166.26/26`
		`OAM IPv4 Default Route: 10.240.166.2`
		`OAM Real IPv6 Address:`
		`OAM IPv6 Default Route:`
		`NTP Servers: 10.250.54.75`
		`DNS Server A:`
		`DNS Server B:`
		`DNS Search:`
		`OAM Device: bond0`
		`OAM VLAN: 90`
		`SIGA VLAN: 5`
		`SIGB VLAN: 6`
		`SIGC VLAN: 7`
		
		a. Ensure that your data is correct.
		b. Click **OK**.
		c. Click **Yes** to save and apply.
		d. Exit platcfg
		Exit the platcfg utility by clicking **Exit** until you are returned to the shell.
		For RMS (DL360/DL380)
		The platcfg utility for RMS does not use VLANs. For example: the SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.
		
		Initial Configuration
		`HostName: CMP25`
		`OAM Real IPv4 Address: 10.113.76.25/22`
		`OAM IPv4 Default Route: 10.113.76.1`
		`OAM Real IPv6 Address:`
		`OAM IPv6 Default Route:`
		`NTP Servers: 140.83.65.12`
		`DNS Server A:`
		`DNS Server B:`
		`DNS Search:`
		`OAM Device: bond0`

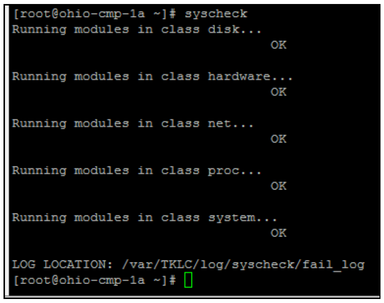
☞ ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System:** 1. Using SSH, reconnect the PM&C server to the node as admusr. 2. Switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C:** SSH directly to the node.

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>□</td><td>Verify basic network connectivity and server health.</td><td>

From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.

```
# ping <XMI or OAM gateway address>
```

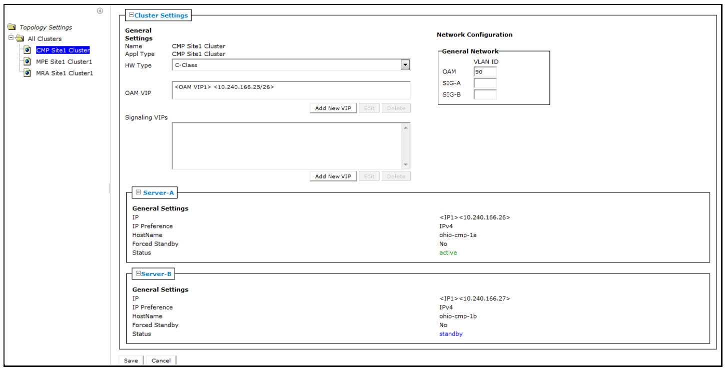
Run the **syscheck** command and ensure that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.



```
[root@ohio-cmp-1a ~]# 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@ohio-cmp-1a ~]#
```

</td></tr>
<tr><td>□</td><td>Remove Forced Standby designation on current node.</td><td>

1. In the CMP GUI, navigate to **Platform Setting → Topology Settings → All Clusters → <*current_cluster*>**
2. Click **Modify Server-*X*** for the server that has **Forced Standby**.
3. Clear the **Forced Standby** checkbox.
4. Click **Save**.



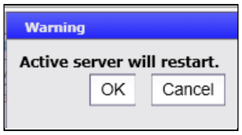
General Settings
Name CMP Site1 Cluster
Appl Type CMP Site1 Cluster
HW Type C-Class
OAM VIP <OAM VIP1> <10.240.166.25/26>
Signaling VIPs

Network Configuration
General Network
VLAN ID
OAM 90
SIG-A
SIG-B

Server-A General Settings
IP <IP1><10.240.166.26>
IP Preference IPv4
HostName ohio-cmp-1a
Forced Standby No
Status active

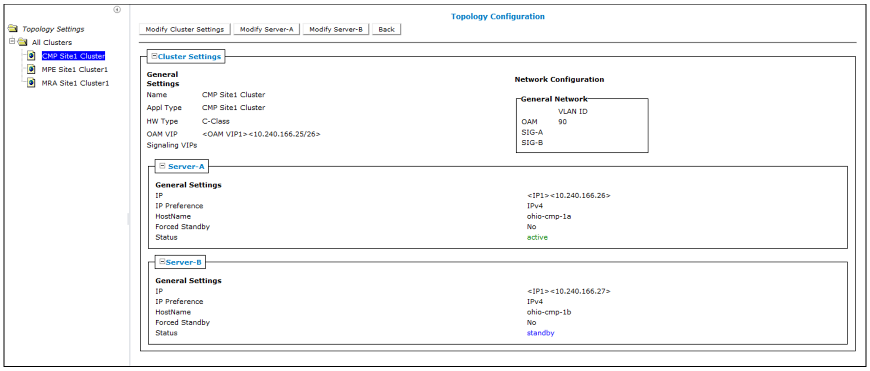
Server-B General Settings
IP <IP1><10.240.166.27>
IP Preference IPv4
HostName ohio-cmp-1b
Forced Standby No
Status standby

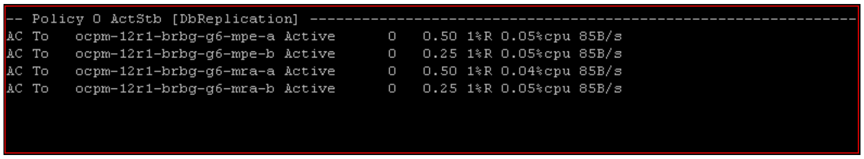
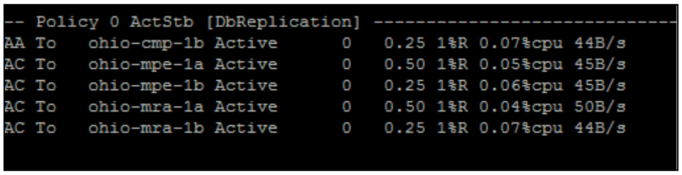
5. Clicking **OK** to restart the server.



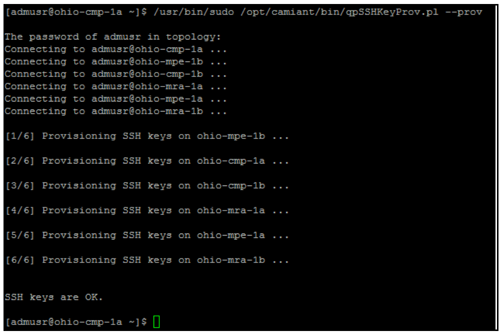
Active server will restart.

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

Step	Procedure	Details
10. □	Verify cluster status	In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters→** *<current_cmp_cluster>* Monitor clustering of the new node to its peer. Do not proceed until both nodes have a status of either active or standby, and all CMP related Active Alarms are cleared.  Topology Configuration Topology Settings All Clusters CMP Site1 Cluster MPE Site1 Cluster1 MRA Site1 Cluster1 Modify Cluster Settings | Modify Server-A | Modify Server-B | Back Cluster Settings General Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type C-Class OAM VIP <OAM VIP1><10.240.166.25/26> Signaling VIPs Network Configuration General Network VLAN ID OAM 90 SIG-A SIG-B Server-A General Settings IP <IP1><10.240.166.26> IP Preference IPv4 HostName ohio-cmp-1a Forced Standby No Status active Server-B General Settings IP <IP1><10.240.166.27> IP Preference IPv4 HostName ohio-cmp-1b Forced Standby No Status standby

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

Step		Procedure	Details

12.	□	Exchange keys with cluster mate (This step must be run from the active CMP server)	Exchanging SSH keys Utility
			1. As root, run:
			`/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root`
			2. As admusr, run:
			`/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov'`
			

---End of Procedure---			

```
[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov

The password of admusr in topology:
Connecting to admusr@ohio-cmp-1a ...
Connecting to admusr@ohio-mpe-1b ...
Connecting to admusr@ohio-cmp-1b ...
Connecting to admusr@ohio-mra-1a ...
Connecting to admusr@ohio-mpe-1a ...
Connecting to admusr@ohio-mra-1b ...

[1/6] Provisioning SSH keys on ohio-mpe-1b ...

[2/6] Provisioning SSH keys on ohio-cmp-1a ...

[3/6] Provisioning SSH keys on ohio-cmp-1b ...

[4/6] Provisioning SSH keys on ohio-mra-1a ...

[5/6] Provisioning SSH keys on ohio-mpe-1a ...

[6/6] Provisioning SSH keys on ohio-mra-1b ...


SSH keys are OK.

[admusr@ohio-cmp-1a ~]$ 
```

5.2 Procedure 2: Restore standby CMP Node without Server Backup File

The purpose of this procedure is to:

1. Replace one node of a CMP cluster.
2. Restore the initial Policy Management configuration using the Perform Initial Configuration page in the platcfg utility.
3. Allow the new node to re-sync to the existing node to form a complete CMP cluster.

In this example, the initial Policy Management configuration is restored to the new nodes using the Perform Initial Configuration page in the platcfg utility 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

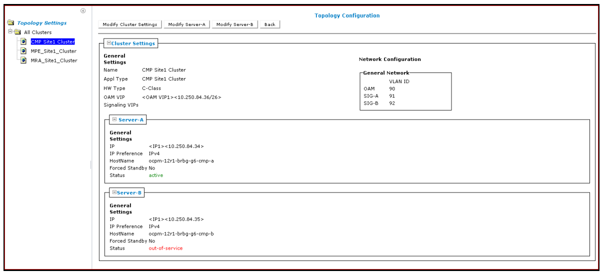
1. Power down the failed server gracefully
    a. Access iLO with administrator privileges.
    b. Go to **Power Management →Server Power**
    c. Click **Momentary Press**
2. Remove and replace the failed hardware.
3. Verify that the node has TPD installed. If TPD is not installed, install it on the node
4. Install the CMP application software.

NOTE: See the Policy Management Bare Metal Installation Guide Release 12.3 for more details. The documents are available on the Oracle Help Center

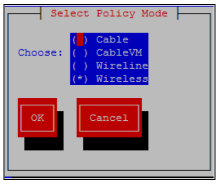
Use this procedure to restore the standby CMP node when a server level backup file is not available.

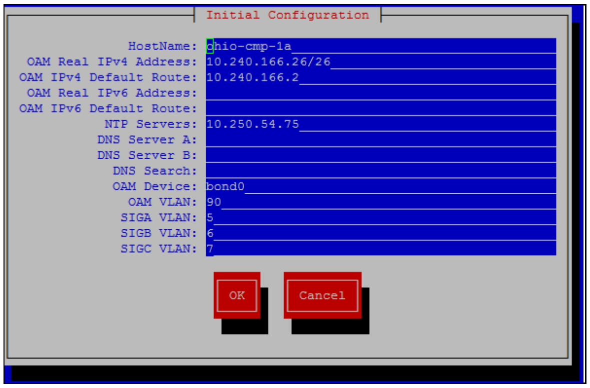
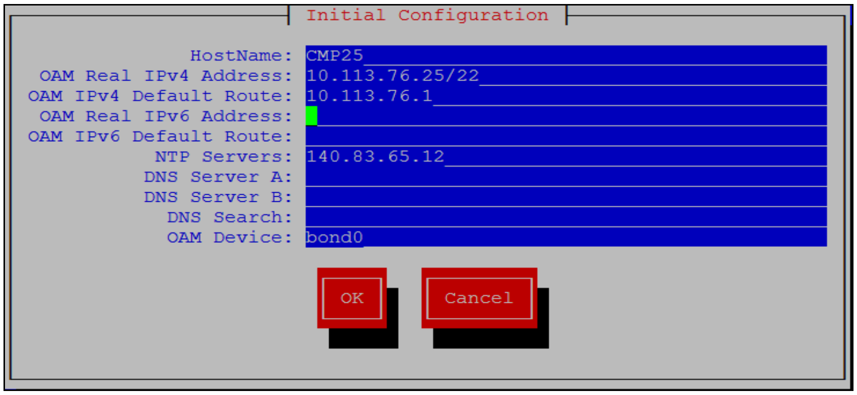
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Should this procedure fail, contact My Oracle Support (MOS) Customer Care Center and ask for assistance.

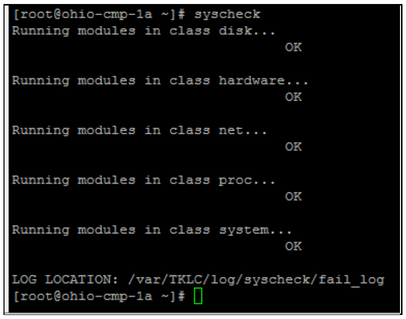
Step	Procedure	Details
1. □	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters** 2. Determine the cluster with the failed node. 3. Determine the failed node. 4. Click **Modify Server-*X*** for the failed node. 5. Select **Forced Standby** so that it is checked 6. Click **Save**.  Topology Configuration Topology Settings All Clusters CMP Site1 Cluster MPE_Site1_Cluster MRA_Site1_Cluster Modify Cluster Settings | Modify Server-A | Modify Server-B | Back Cluster Settings General Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type C-Class OAM VIP <OAM VIP1><10.250.84.36/26> Signaling VIPs Network Configuration General Network VLAN ID OAM 90 SIG-A 91 SIG-B 92 Server-A General Settings IP <IP1><10.250.84.34> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-cmp-a Forced Standby No Status active Server-B General Settings IP <IP1><10.250.84.35> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-cmp-b Forced Standby No Status out-of-service **NOTE:** From the figure, the Network Configuration/General Network (VLAN ID) is not available for RMS (DL360/DL380) Hardware

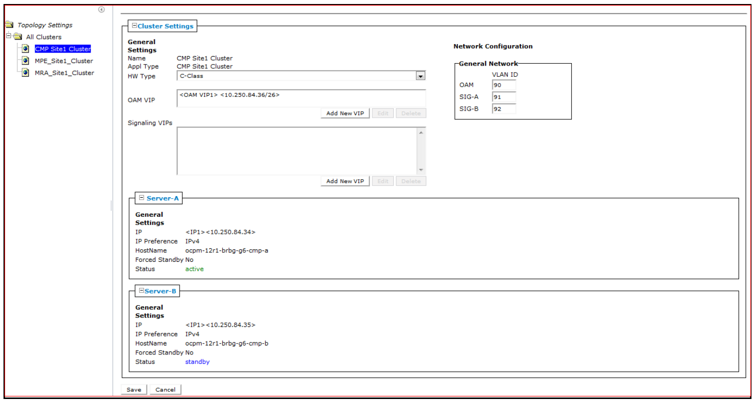
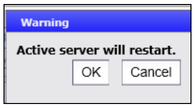
2. □	Login into the node using SSH	**For c-Class System**
		1. Start an SSH session from PM&C to new server.
		2. Go to the **PM&C GUI → Software → Software Inventory** to obtain the IP address for the server:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System
		Use the iLO/iLOM (for Oracle hardware Oracle X5-2 and Netra X5-2) to login, and start a remote console session to run commands.

3. □	Perform platcfg restore from SSH session to replacement node Perform Initial configuration	1. Start the platcfg utility. `# su – platcfg` 2. From the platcfg utility, navigate to **Policy Configuration → Set Policy Mode**  Select Policy Mode Choose: ( ) Cable ( ) CableVM ( ) Wireline (*) Wireless OK Cancel 3. Verify that Wireless is selected. Click **OK** to continue or you can skip this step.

Step	Procedure	Details
		4. From the platcfg utility, navigate to **Policy Configuration → Perform Initial Configuration** 5. Enter the configuration details for the node. 6. Verify that entries are correct and click **OK** to continue. 7. Accept the resulting dialog that opens asking you to apply the configuration. 8. After the operation is complete, click **Exit** on the platcfg utility menu until you are returned to the shell. **For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS):**  Initial Configuration HostName: ohio-cmp-1a OAM Real IPv4 Address: 10.240.166.26/26 OAM IPv4 Default Route: 10.240.166.2 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 10.250.54.75 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0 OAM VLAN: 90 SIGA VLAN: 5 SIGB VLAN: 6 SIGC VLAN: 7 a. Ensure that configured data is correct, and click **OK**. b. Click **Yes** to save and apply. c. Exit the platcfg utility by clicking **Exit** until you are returned to the shell. **For RMS (DL360/DL380)** The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.  Initial Configuration HostName: CMP25 OAM Real IPv4 Address: 10.113.76.25/22 OAM IPv4 Default Route: 10.113.76.1 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 140.83.65.12 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0

Step	Procedure	Details
4. □	Reboot the server	Reboot: `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System** Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C** SSH directly to the node.

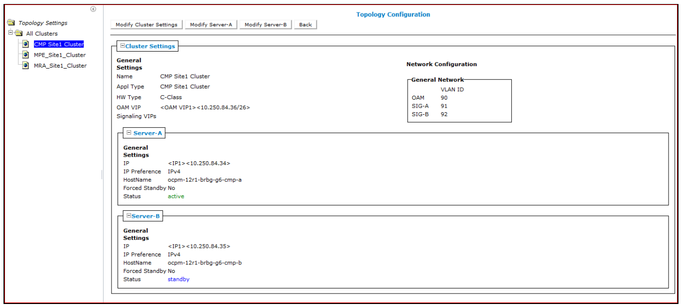
5. □	Verify basic network connectivity and server health.	From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.
		`# ping <XMI or OAM gateway address>`
		Run the **`syscheck`** command. Verify that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.
		
		`[root@ohio-cmp-1a ~]# 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@ohio-cmp-1a ~]#`

6. □	Remove Forced Standby designation on current node.	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting →** <*current_cluster*> 2. Click **Modify Server-*X*** for the server that is in **Forced Standby**. 3. Clear the **Forced Standby** checkbox 4. Click **Save**.  Topology Settings All Clusters CMP Site1 Cluster MPE_Site1_Cluster MRA_Site1_Cluster Cluster Settings General Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type C-Class OAM VIP <OAM VIP1> <10.250.84.36/26> Add New VIP Edit Delete Signaling VIPs Add New VIP Edit Delete Network Configuration General Network VLAN ID OAM 90 SIG-A 91 SIG-B 92 Server-A General Settings IP <IP1><10.250.84.34> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-cmp-a Forced Standby No Status active Server-B General Settings IP <IP1><10.250.84.35> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-cmp-b Forced Standby No Status standby Save Cancel 5. Accept the dialog by clicking **OK**.  Warning Active server will restart. OK Cancel

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>7. □</td><td>Verify cluster status</td><td>

1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All →** ***<current_cmp_cluster>***

2. Monitor clustering of the node to its peer, do not proceed until both nodes have a status of either active or standby, and all CMP related Active Alarms are cleared.



General Settings
Name CMP Site1 Cluster
Appl Type CMP Site1 Cluster
HW Type C-Class
OAM VIP <OAM VIP1><10.250.84.36/26>
Signaling VIPs

Network Configuration

General Network

	VLAN ID
OAM	90
SIG-A	91
SIG-B	92

Server-A
General Settings
IP <IP1><10.250.84.34>
IP Preference IPv4
HostName ocpm-12r1-brbg-g6-cmp-a
Forced Standby No
Status active

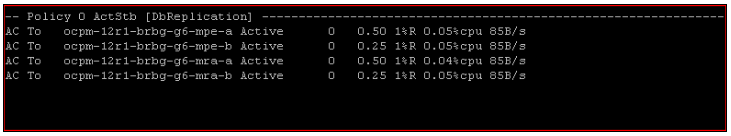
Server-B
General Settings
IP <IP1><10.250.84.35>
IP Preference IPv4
HostName ocpm-12r1-brbg-g6-cmp-b
Forced Standby No
Status standby

</td></tr>
<tr><td>8. □</td><td>Alternative method to check replication status</td><td>

You can also monitor the clustering of the node from the shell on the primary node with the **`irepstat`** command. SSH to the Active node of the current cluster and run the **`irepstat`** command:

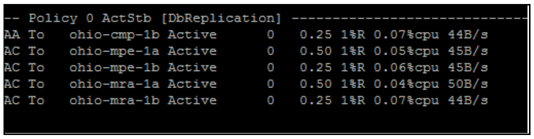
```
# irepstat
```

Expected **`irepstat`** command output while waiting reconnection:



```
-- Policy 0 ActStb [DbReplication] -----------------------------------------------------------
AC To   ocpm-12r1-brbg-g6-mpe-a Active      0   0.50 1%R 0.05%cpu 85B/s
AC To   ocpm-12r1-brbg-g6-mpe-b Active      0   0.25 1%R 0.05%cpu 85B/s
AC To   ocpm-12r1-brbg-g6-mra-a Active      0   0.50 1%R 0.04%cpu 85B/s
AC To   ocpm-12r1-brbg-g6-mra-b Active      0   0.25 1%R 0.05%cpu 85B/s
```

Expected **`irepstat`** command output after cluster has formed:



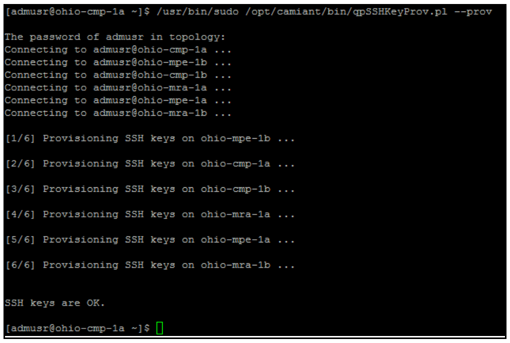
```
-- Policy 0 ActStb [DbReplication] ----------------------------
AA To   ohio-cmp-1b Active      0   0.25 1%R 0.07%cpu 44B/s
AC To   ohio-mpe-1a Active      0   0.50 1%R 0.05%cpu 45B/s
AC To   ohio-mpe-1b Active      0   0.25 1%R 0.06%cpu 45B/s
AC To   ohio-mra-1a Active      0   0.50 1%R 0.04%cpu 50B/s
AC To   ohio-mra-1b Active      0   0.25 1%R 0.07%cpu 44B/s
```

</td></tr>
<tr><td>9. □</td><td>Exchange keys with cluster mate (This step must be run from the active CMP server)</td><td>

Exchanging SSH keys Utility

1. As root, run:
   `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root`

2. As admusr, run:
   `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`



```
[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov

The password of admusr in topology:
Connecting to admusr@ohio-cmp-1a ...
Connecting to admusr@ohio-mpe-1b ...
Connecting to admusr@ohio-cmp-1b ...
Connecting to admusr@ohio-mra-1a ...
Connecting to admusr@ohio-mpe-1a ...
Connecting to admusr@ohio-mra-1b ...

[1/6] Provisioning SSH keys on ohio-mpe-1b ...

[2/6] Provisioning SSH keys on ohio-cmp-1a ...

[3/6] Provisioning SSH keys on ohio-cmp-1b ...

[4/6] Provisioning SSH keys on ohio-mra-1a ...

[5/6] Provisioning SSH keys on ohio-mpe-1a ...

[6/6] Provisioning SSH keys on ohio-mra-1b ...


SSH keys are OK.

[admusr@ohio-cmp-1a ~]$
```

</td></tr>
<tr><td colspan="3"><b>---End of Procedure---</b></td></tr>
</table>

5.3 Procedure 3: Restore single MPE/MRA/Mediation node with server backup file

The purpose of this procedure is to replace one node of a Policy Management cluster. Restore initial Policy Management 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, the initial Policy Management 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 file.
- Policy APP installation ISO file.
- **serverbackup**.ISO of the node to be replaced.

Prerequisites

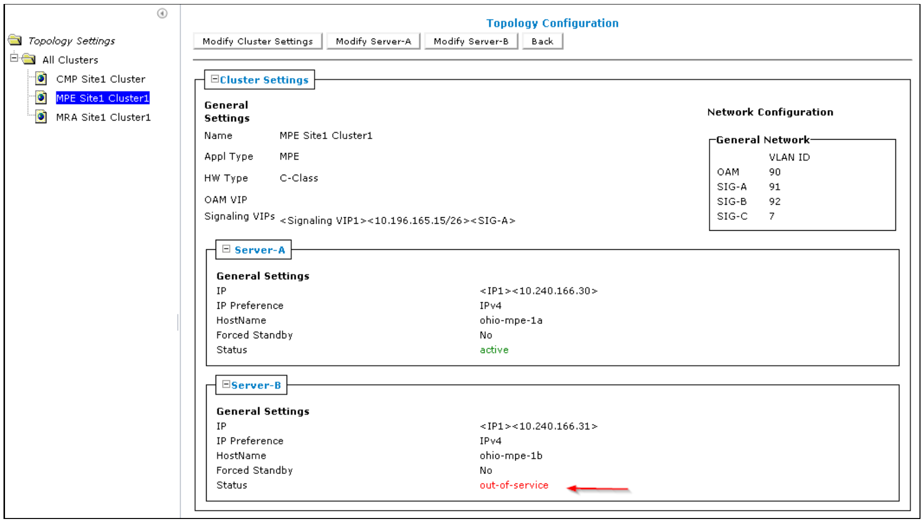
1. Power down the failed server gracefully
   a. Access iLO with administrator privileges.
   b. Go to **Power Management →Server Power**
   c. Click **Momentary Press**.
2. Remove and replace the failed hardware.
3. Verify that the hardware has TPD installed. If TPD is not installed, install it on the server
4. Install application software–MPE or MRA or Mediation

   See the Policy Management Bare Metal Installation Guide Release 12.3 for more details. The documents are available on the Oracle Help Center

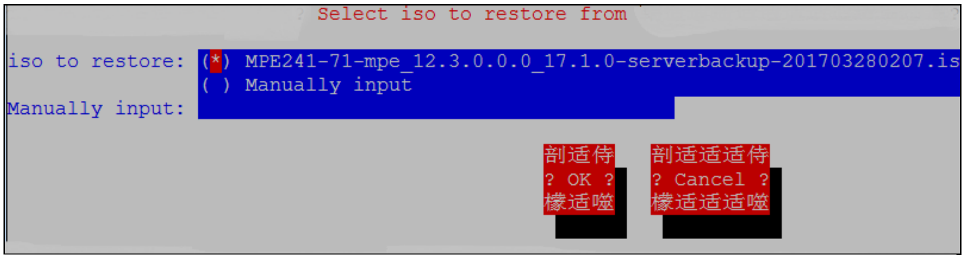
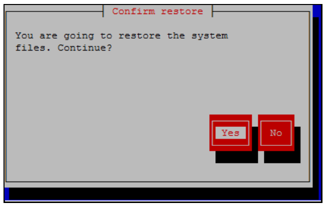
Use this procedure to perform restore on a single MPE/MRA/Mediation node with server backup file.

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

Should this procedure fail, contact My Oracle Support (MOS) Customer Care Center and ask for assistance.

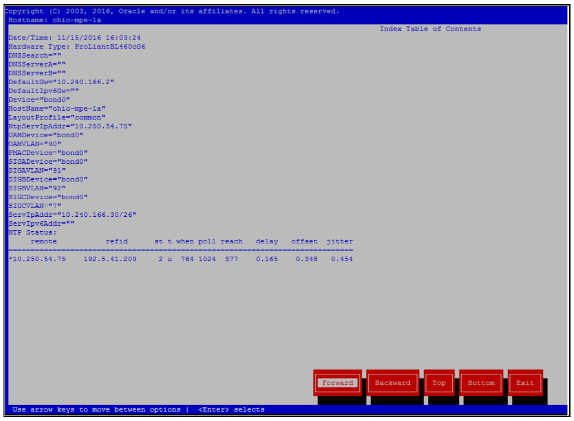
<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>1. □</td><td>Set the failed node to Forced Standby</td><td>
1. In the CMP GUI, navigate to <b>Platform Setting → Topology Setting → All Clusters</b>
2. Determine the cluster with the failed node.
3. Determine the failed node.
4. Click the <b>Modify Server-<i>X</i></b> for the failed node.
5. Click <b>Forced Standby</b> so that it is checked.
6. Click <b>Save</b>.


Cluster Settings
General Settings
Name MPE Site1 Cluster1
Appl Type MPE
HW Type C-Class
OAM VIP
Signaling VIPs &lt;Signaling VIP1&gt;&lt;10.196.165.15/26&gt;&lt;SIG-A&gt;
Network Configuration
General Network
VLAN ID
OAM 90
SIG-A 91
SIG-B 92
SIG-C 7
Server-A
General Settings
IP &lt;IP1&gt;&lt;10.240.166.30&gt;
IP Preference IPv4
HostName ohio-mpe-1a
Forced Standby No
Status active
Server-B
General Settings
IP &lt;IP1&gt;&lt;10.240.166.31&gt;
IP Preference IPv4
HostName ohio-mpe-1b
Forced Standby No
Status out-of-service
</td></tr>
<tr><td>2. □</td><td>Load the ISO for server backup</td><td>
Obtain the <i>*serverbackup*</i>.iso for the node to be restored. When the replacement node is available (IPM/App installation complete), copy the server backup file using secure copy (pscp,scp, or WinSCP) to the following directory:
<code>/var/camiant/backup/local_archive/serverbackup</code>
<b>NOTE:</b> Later in this procedure, the platcfg utility restore function checks this directory and opens a menu. The platcfg utility also lets you manually enter any mounted path on the server.
</td></tr>
<tr><td>3. □</td><td>Login into the node using SSH</td><td>
<b>For c-Class System</b>
SSH session from PM&C to new server, navigate to <b>PM&amp;C GUI → Software → Software Inventory</b> to obtain the IP address for the server:
<code># ssh admusr@<node_IP_Address&gt;</code>
<code>$ sudo su -</code>
<b>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System</b>
Use the iLO/iLOM (for Oracle hardware Oracle X5-2 and Netra X5-2) to login, and start a remote console session to run commands.
</td></tr>
</table>

Step		Procedure	Details
4.	□	Perform platcfg restore from SSH session to replacement hardware	1. Start the platcfg utility. `# su - platcfg` 2. From the platcfg utility, navigate to **Policy Configuration → Backup and Restore → Server Restore** 3. Select the **serverbackup**.ISO that you just put on the system and click **OK**. 4. Click **Yes** to confirm.  Select iso to restore from iso to restore: (*) MPE241-71-mpe_12.3.0.0.0_17.1.0-serverbackup-201703280207.is ( ) Manually input Manually input:  Confirm restore You are going to restore the system files. Continue?
5.	□	Verify the status	A dialog opens indicating the restore operation was successful and asks you to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>6. □</td><td>Perform Initial configuration</td><td>

1. Click **Exit** until you return to the Main Menu of the platcfg utility.
2. Navigate to **Policy Configuration → Verify Initial Configuration**

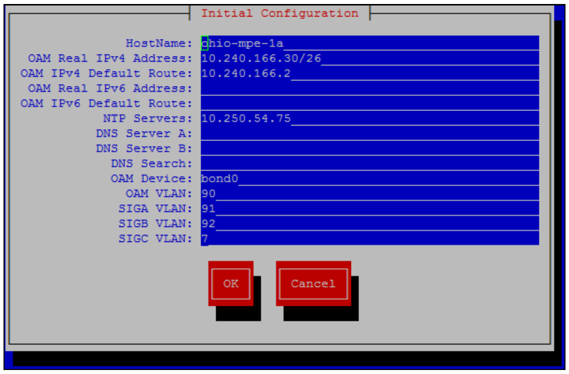


```
Copyright (C) 2003, 2016, Oracle and/or its affiliates. All rights reserved.
 Hostname: ohio-mpe-1a
                                                                    Index Table of Contents
 Date/Time: 11/15/2016 16:03:24
 Hardware Type: ProLiantBL460cG6
 DNSSearch=""
 DNSServerA=""
 DNSServerB=""
 DefaultGw="10.240.166.2"
 DefaultIpv6Gw=""
 Device="bond0"
 HostName="ohio-mpe-1a"
 LayoutProfile="common"
 NtpServIpAddr="10.250.54.75"
 OAMDevice="bond0"
 OAMVLAN="90"
 PMACDevice="bond0"
 SIGADevice="bond0"
 SIGAVLAN="91"
 SIGBDevice="bond0"
 SIGBVLAN="92"
 SIGCDevice="bond0"
 SIGCVLAN="7"
 ServIpAddr="10.240.166.30/26"
 ServIpv6Addr=""
 NTP Status:
      remote           refid      st t when poll reach   delay   offset  jitter
 ==============================================================================
 *10.250.54.75    192.5.41.209     2 u  764 1024  377    0.165    0.348   0.454

  Use arrow keys to move between options |  <Enter> selects
```

3. If the configuration does not exist, navigate to **Perform Initial Configuration** and enter initial configuration:

   - Hostname
   - OAM IP
   - NTP servers configurations

For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS):



```
              Initial Configuration
           HostName: ohio-mpe-1a
  OAM Real IPv4 Address: 10.240.166.30/26
 OAM IPv4 Default Route: 10.240.166.2
  OAM Real IPv6 Address:
 OAM IPv6 Default Route:
            NTP Servers: 10.250.54.75
           DNS Server A:
           DNS Server B:
             DNS Search:
             OAM Device: bond0
               OAM VLAN: 90
              SIGA VLAN: 91
              SIGB VLAN: 92
              SIGC VLAN: 7
```

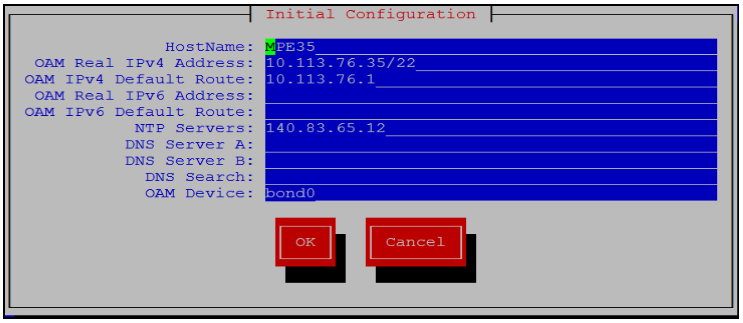
a. Ensure the configured data is correct, and click OK Click Yes to save and apply.

b. Exit platcfg.

c. Exit the platcfg utility by clicking **Exit** until you are returned to the shell.

For RMS (DL360/DL380) System

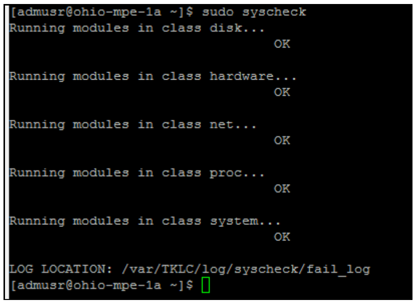
The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.

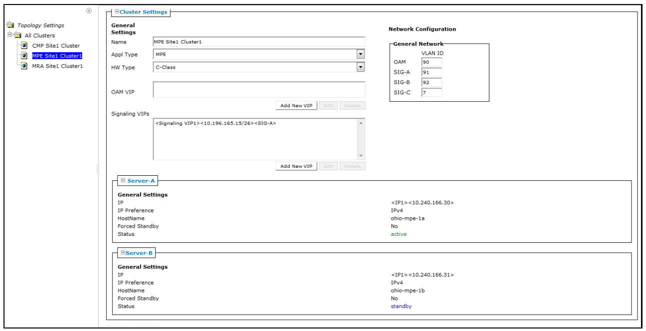
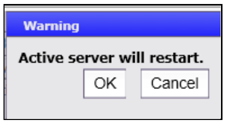


```
              Initial Configuration
           HostName: MPE35
  OAM Real IPv4 Address: 10.113.76.35/22
 OAM IPv4 Default Route: 10.113.76.1
  OAM Real IPv6 Address:
 OAM IPv6 Default Route:
            NTP Servers: 140.83.65.12
           DNS Server A:
           DNS Server B:
             DNS Search:
             OAM Device: bond0
```

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

Step	Procedure	Details
7. □	Reboot the server	Reboot: `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System** Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C** SSH directly to the node.

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

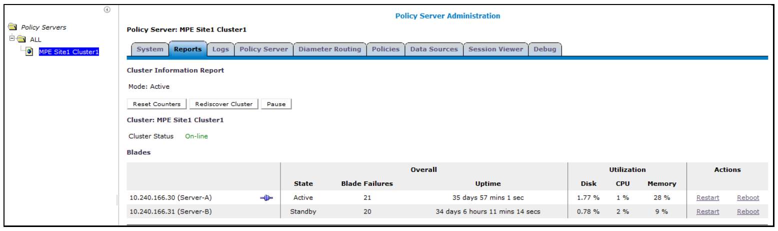
9. □	Remove Forced Standby designation on current node.	1. In the CMP GUI, navigate to **Platform Setting → Topology Settings → All Clusters → <*current_cluster*>** 2. Click **Modify Server-***X* for the server that has Forced Standby 3. Clear the Forced Standby checkbox 4. Click Save  Topology Settings All Clusters CMP Site1 Cluster MPE Site1 Cluster1 MRA Site1 Cluster1 Cluster Settings Add New VIP Edit Delete Network Configuration Server-A Server-B General Settings Name: MPE Site1 Cluster1 Appl Type: MPE HW Type: C-Class OAM VIP: Signaling VIPs: <Signaling VIP1><10.196.165.15/26><SIG-A> General Network VLAN ID OAM: 90 SIG-A: 91 SIG-B: 92 SIG-C: 7 Server-A General Settings IP: <IP1><10.240.166.30> IP Preference: IPv4 HostName: ohio-mpe-1a Forced Standby: No Status: active Server-B General Settings IP: <IP1><10.240.166.31> IP Preference: IPv4 HostName: ohio-mpe-1b Forced Standby: No Status: standby 5. Click **OK** to restart the server.  Active server will restart.

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>10. □</td><td>Check status</td><td>

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

- If this is an MPE node, navigate to:
  Policy Server → Configuration → All → <*recovered_mpe_cluster*> **→ Reports**
- If this is an MRA node, navigate to:
  MRA → Configuration → All → <*recovered_mra_cluster*> **→ Reports**
- If this is an Mediation node, navigate to:
  Mediation → Configuration → All → <recovered_mediation_cluster> → Reports

Monitor clustering of the new node to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.



Policy Server Administration

Policy Server: MPE Site1 Cluster1

Cluster Information Report

Mode: Active

Cluster: MPE Site1 Cluster1

Cluster Status On-line

Blades

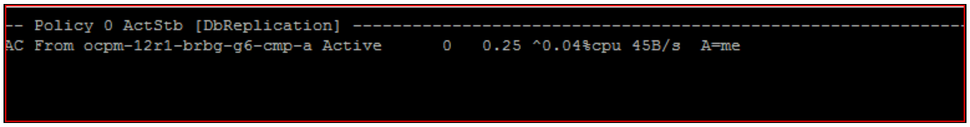
<table>
<tr><th></th><th colspan="3">Overall</th><th colspan="3">Utilization</th><th colspan="2">Actions</th></tr>
<tr><th></th><th>State</th><th>Blade Failures</th><th>Uptime</th><th>Disk</th><th>CPU</th><th>Memory</th><th></th><th></th></tr>
<tr><td>10.240.166.30 (Server-A)</td><td>Active</td><td>21</td><td>35 days 57 mins 1 sec</td><td>1.77 %</td><td>1 %</td><td>28 %</td><td>Restart</td><td>Reboot</td></tr>
<tr><td>10.240.166.31 (Server-B)</td><td>Standby</td><td>20</td><td>34 days 6 hours 11 mins 14 secs</td><td>0.78 %</td><td>2 %</td><td>9 %</td><td>Restart</td><td>Reboot</td></tr>
</table>

</td></tr>
<tr><td>11. □</td><td>Alternative method to check replication status</td><td>

You can also monitor the clustering of the new node from the shell on the primary node with the **`irepstat`** command. SSH to the active node of the current cluster and run the **`irepstat`** command:

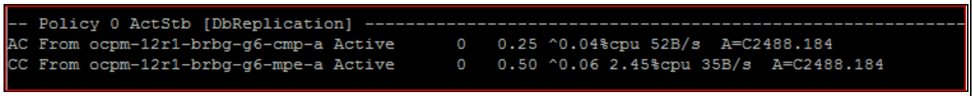
```
# irepstat
```

Expected **`irepstat`** command output while waiting reconnection:



```
-- Policy 0 ActStb [DbReplication] -------------------------------------------------------------
AC From ocpm-12r1-brbg-g6-cmp-a Active      0    0.25 ^0.04%cpu 45B/s   A=me
```

Expected **`irepstat`** command output after cluster has formed:

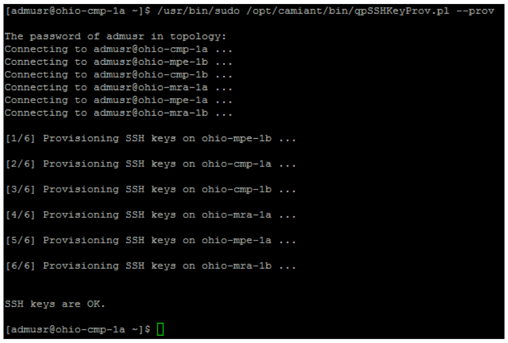


```
-- Policy 0 ActStb [DbReplication] -------------------------------------------------------------
AC From ocpm-12r1-brbg-g6-cmp-a Active      0    0.25 ^0.04%cpu 52B/s   A=C2488.184
CC From ocpm-12r1-brbg-g6-mpe-a Active      0    0.50 ^0.06 2.45%cpu 35B/s   A=C2488.184
```

</td></tr>
<tr><td>12. □</td><td>Exchange keys with cluster mate (This step must be run from the active CMP server)</td><td>

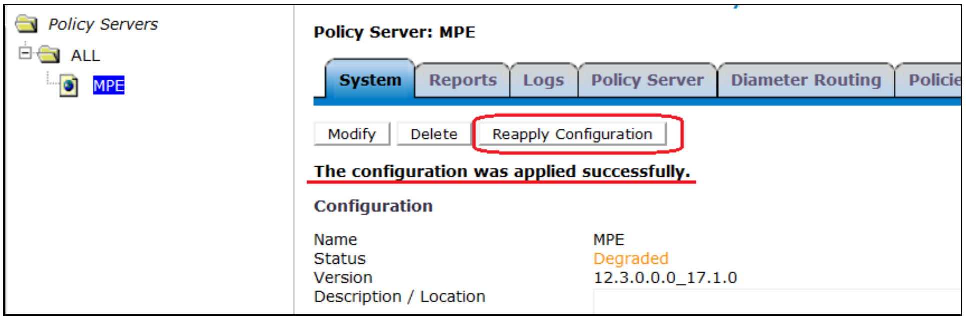
Exchanging SSH keys Utility

1. As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root`
2. As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`



```
[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov

The password of admusr in topology:
Connecting to admusr@ohio-cmp-1a ...
Connecting to admusr@ohio-mpe-1b ...
Connecting to admusr@ohio-cmp-1b ...
Connecting to admusr@ohio-mra-1a ...
Connecting to admusr@ohio-mpe-1a ...
Connecting to admusr@ohio-mra-1b ...

[1/6] Provisioning SSH keys on ohio-mpe-1b ...

[2/6] Provisioning SSH keys on ohio-cmp-1a ...

[3/6] Provisioning SSH keys on ohio-cmp-1b ...

[4/6] Provisioning SSH keys on ohio-mra-1a ...

[5/6] Provisioning SSH keys on ohio-mpe-1a ...

[6/6] Provisioning SSH keys on ohio-mra-1b ...


SSH keys are OK.

[admusr@ohio-cmp-1a ~]$
```

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

Step		Procedure	Details
13.	□	Reapply Configuration	In the CMP GUI, click **Reapply Configuration** for the MPE/MRA/Mediation cluster. The message `The configuration was applied successfully` displays.  Policy Servers ALL MPE Policy Server: MPE System Reports Logs Policy Server Diameter Routing Policie Modify Delete Reapply Configuration The configuration was applied successfully. Configuration Name MPE Status Degraded Version 12.3.0.0.0_17.1.0 Description / Location
---End of Procedure---			

5.4 Procedure 4: Restore single MPE/MRA/Mediation node without server backup file

The purpose of this procedure is to create a Policy Management cluster from the replacement of one node of the cluster. The active primary node synchronizes the installed node to complete the cluster. In this example, the initial Policy Management configuration is restored to the new node by manual entry.

Required Resources

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

Hostname, OAM IP address, and VLAN configuration can be gathered from:

Platform Setting → Topology Setting → <*cluster_name*>

NTP server configuration (and optionally DNS configuration can be gathered from platcfg of the running node)

Verify that routing is configured correctly. Verify that XSI is the default and any associated OAM routes are added.

Prerequisites

1. Power down the failed server gracefully
   a. Access iLO with administrator privileges.
   b. Go to **Power Management → Server Power**
   c. Click **Momentary Press**
2. Remove and replace the failed hardware.
3. Verify that the node has TPD installed. If TPD is not installed, install it on the node

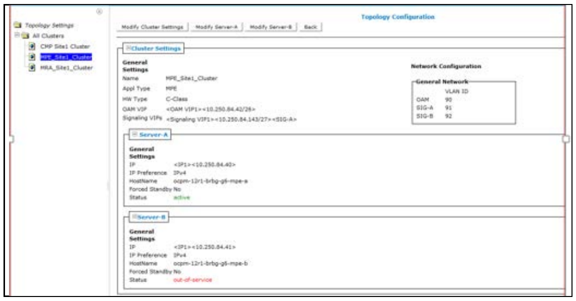
4. Install application software–MPE or MRA or Mediation

NOTE: See the Policy Management Bare Metal Installation Guide Release 12.3 for more details. The documents are available on the Oracle Help Center

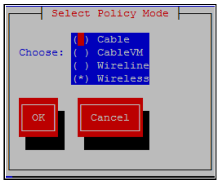
Use this procedure to perform a restore on a single MPE/MRA/Mediation node without server backup file

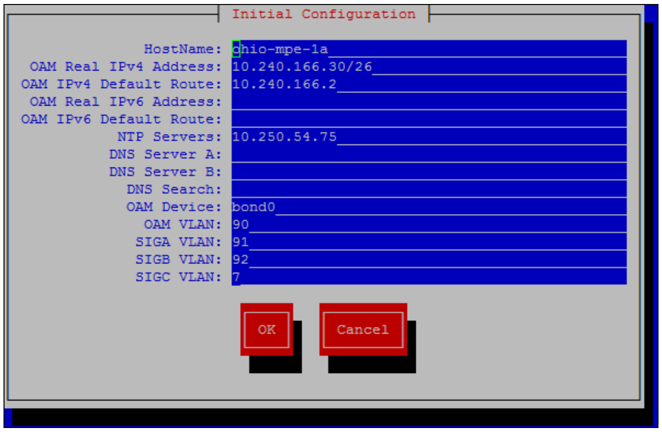
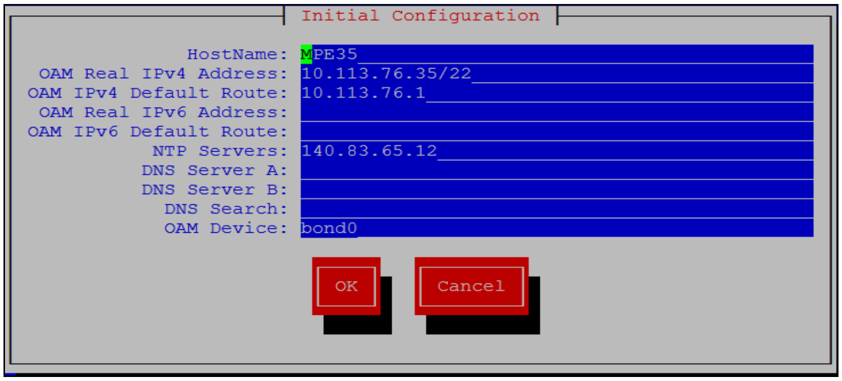
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Should this procedure fail, contact My Oracle Support (MOS) Customer Care Center and ask for assistance.

Step	Procedure	Details
1. □	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters** 2. Determine the cluster with the failed node. 3. Determine the failed node. 4. Click **Modify Server-*X*** for the failed node. 5. Click **Forced Standby** so that it is checked. 6. Click **Save**.  Topology Settings All Clusters CMP Site1 Cluster MPE_Site1_Cluster MRA_Site1_Cluster Modify Cluster Settings Modify Server-A Modify Server-B Back Topology Configuration Cluster Settings General Settings Name MPE_Site1_Cluster Appl Type MPE HW Type C-Class OAM VIP <OAM VIP1><10.250.84.42/26> Signaling VIPs <Signaling VIP1><10.250.84.143/27><SIG-A> Network Configuration General Network VLAN ID OAM 90 SIG-A 91 SIG-B 92 Server-A General Settings IP <IP1><10.250.84.40> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-mpe-a Forced Standby No Status active Server-B General Settings IP <IP1><10.250.84.41> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-mpe-b Forced Standby No Status out-of-service

2. □	Login into the node using SSH	**For c-Class System**
		SSH session from PM&C to new server. Use the **PM&C GUI → Software → Software Inventory** page to obtain the IP address for the server.
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System
		Use the iLO/iLOM (for Oracle hardware Oracle X5-2 and Netra X5-2) to login, and start a remote console session to run commands.

3. □	From the platcfg utility, run the Initial Policy Configuration for the installed node	1. Open the platcfg utility: `# su – platcfg` 2. Navigate to **Policy Configuration → Set Policy Mode**  Select Policy Mode Choose: ( ) Cable ( ) CableVM ( ) Wireline (*) Wireless 3. Verify that Wireless is selected. Click **OK** to continue or you can skip this step.

Step	Procedure	Details
		4. Navigate to **Policy Configuration → Perform Initial Configuration** 5. Enter the configuration details for the node being replaced. **For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)** Initial Configuration HostName: chio-mpe-1a OAM Real IPv4 Address: 10.240.166.30/26 OAM IPv4 Default Route: 10.240.166.2 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 10.250.54.75 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0 OAM VLAN: 90 SIGA VLAN: 91 SIGB VLAN: 92 SIGC VLAN: 7 a. After the server details are entered and verified, click **OK**. b. A menu displays asking if the settings should be applied, click **Yes** and wait for the operation to complete. A message is not displayed when the operation is successful, but an error displays if it does not complete. In this case, review the settings from the Perform Initial Configuration page. If the information is correct, contact My Oracle Support before proceeding. c. Exit the platcfg utility by clicking **Exit** until you are returned to the shell. **For RMS (DL360/DL380) System** The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration. Initial Configuration HostName: MPE35 OAM Real IPv4 Address: 10.113.76.35/22 OAM IPv4 Default Route: 10.113.76.1 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 140.83.65.12 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>4. □</td><td>Reboot the server</td><td>

Reboot:

```
# init 6
```

Allow the server time to reboot.

For c-Class or Netra X5-2(Oracle RMS)System

Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges.

For RMS (DL360/DL380/Oracle X5-2)System without PM&C

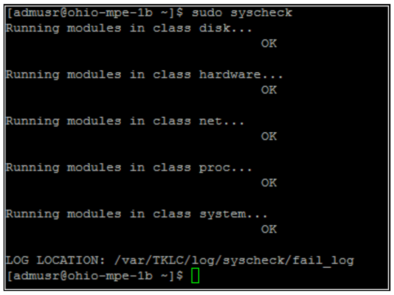
SSH directly to the node.

</td></tr>
<tr><td>5. □</td><td>Verify basic network connectivity and server health.</td><td>

From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old server configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.

```
# ping <XMI or OAM gateway address>
```

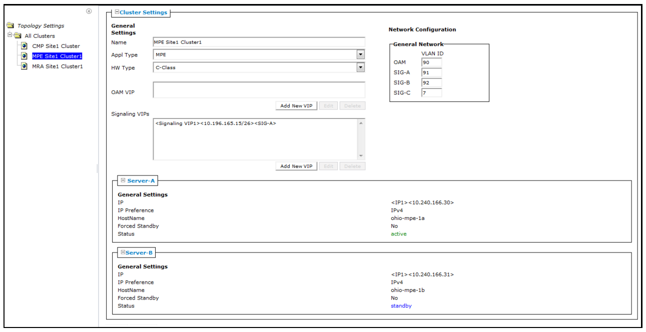
Run the `syscheck` command. Verify that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.



```
[admusr@ohio-mpe-1b ~]$ sudo syscheck
Running modules in class disk...
                                    OK

Running modules in class hardware...
                                    OK

Running modules in class net...
                                    OK

Running modules in class proc...
                                    OK

Running modules in class system...
                                    OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
[admusr@ohio-mpe-1b ~]$
```

</td></tr>
<tr><td>6. □</td><td>Remove Forced Standby designation on current server.</td><td>

1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → <*current_cluster*>**
2. Click **Modify Server-*X*** for the server that has Forced Standby selected.
3. Clear **Forced Standby**.
4. Click **Save**.



General Settings

Name: MPE Site1 Cluster1

Appl Type: MPE

HW Type: C-Class

OAM VIP:

Signaling VIPs: <Signaling VIP1><10.196.165.15/26><SIG-A>

Network Configuration

General Network

	VLAN ID
OAM	90
SIG-A	91
SIG-B	92
SIG-C	7

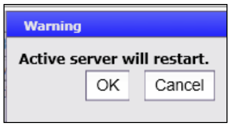
Server-A General Settings

IP	<IP1><10.240.166.30>
IP Preference	IPv4
HostName	ohio-mpe-1a
Forced Standby	No
Status	active

Server-B General Settings

IP	<IP1><10.240.166.31>
IP Preference	IPv4
HostName	ohio-mpe-1b
Forced Standby	No
Status	standby

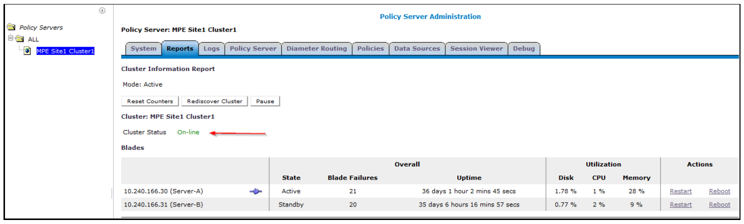
5. Click **OK** to restart the server.

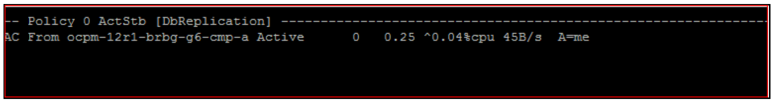
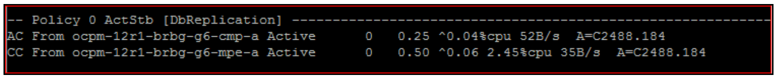


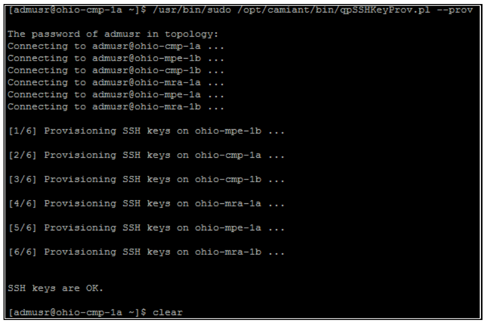
Warning

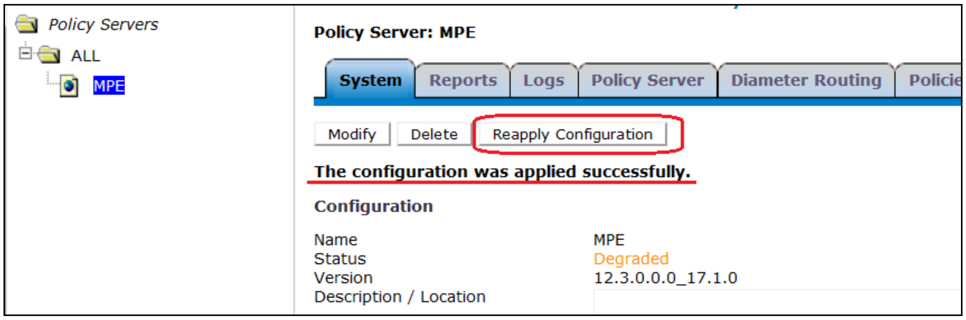
Active server will restart.

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

Step	Procedure	Details
7. □	Check status	In the CMP GUI, depending on the type of the server, perform the following: - If this is an MPE node, navigate to: **Policy Server → Configuration → All →** *<recovered_mpe_cluster>* **→ Reports** - If this is an MRA node, navigate to: **MRA → Configuration → All →** *<recovered_mra_cluster>* **→ Reports** - If this is an Mediation node, navigate to: **Mediation → Configuration → All → <recovered_mediation_cluster> → Reports** Monitor clustering of the new server to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.  Policy Server Administration Policy Server: MPE Site1 Cluster1 Cluster Information Report Mode: Active Cluster: MPE Site1 Cluster1 Cluster Status On-line Blades Overall / Utilization / Actions State, Blade Failures, Uptime, Disk, CPU, Memory 10.240.166.30 (Server-A) Active 21 36 days 1 hour 2 mins 45 secs 1.78 % 1 % 28 % Restart Reboot 10.240.166.31 (Server-B) Standby 20 35 days 6 hours 16 mins 57 secs 0.77 % 2 % 9 % Restart Reboot Policy Servers ALL MPE Site1 Cluster1 System Reports Logs Policy Server Diameter Routing Policies Data Sources Session Viewer Debug Reset Counters Rediscover Cluster Pause

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

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

Step	Procedure	Details
10. □	Reapply Configuration	In the CMP GUI, click **Reapply Configuration** for the MPE/MRA/Mediation cluster. The message `The configuration was applied successfully` displays.  Policy Servers ALL MPE System Reports Logs Policy Server Diameter Routing Policie Modify Delete Reapply Configuration Policy Server: MPE The configuration was applied successfully. Configuration Name MPE Status Degraded Version 12.3.0.0.0_17.1.0 Description / Location
---End of Procedure---		

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

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

Required Resources

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

Prerequisites

1. Power down the failed server gracefully
   a. Access iLO with administrator privileges.
   b. Go to **Power Management →Server Power**
   c. Click **Momentary Press**
2. Remove and replace both servers
3. IPM both servers
4. Install the application on both servers (either CMP, MPE, MRA, Mediation)

   NOTES:

   o If it is a CMP Cluster being rebuilt, restore the application data either by using the system backup or manually if no backup is available.

   o See the Policy Management Bare Metal Installation Guide Release 12.3 for more details. The documents are available on the Oracle Help Center

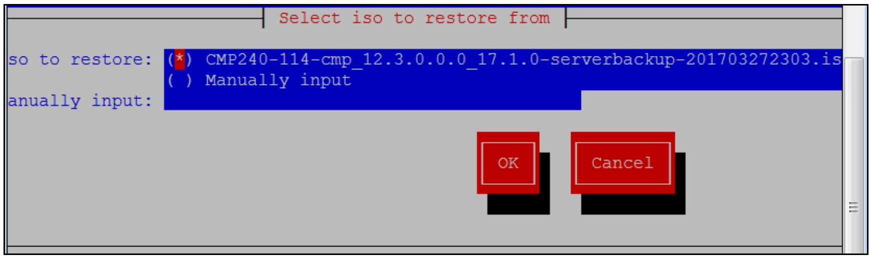
Use this procedure to restore a complete cluster with the server backup files

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

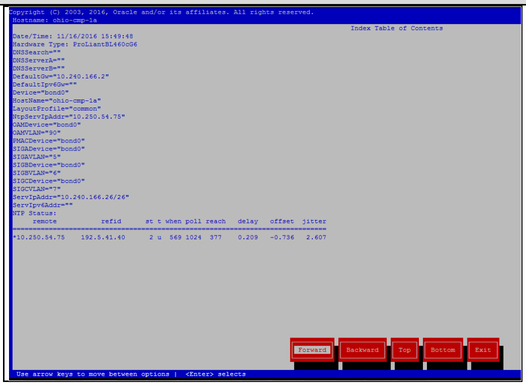
Should this procedure fail, contact My Oracle Support (MOS) Customer Care Center and ask for assistance.

Step	Procedure	Details

1. □	SSH to replacement server	**For c-Class System**
		SSH session from PM&C to new server, navigate to **PM&C GUI→Software → Software** Inventory to obtain the IP address for the server:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System
		Use the iLO/iLOM (for Oracle hardware Oracle X5-2 and Netra X5-2) to login, and start a remote console session to run commands.

2. □	Load the ISO to restore the first server of the cluster	Obtain the **serverbackup**.iso for the server to be restored. When the replacement server is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE:** Later in this procedure, the platcfg utility restore function checks this directory and opens a menu. The platcfg utility also lets you manually enter any mounted path on the server.
3. □	Using platcfg, restore the backup from SSH session to replacement server	1. Start the platcfg utility. `# su - platcfg` **2.** From the platcfg utility, navigate to **Policy Configuration → Backup and Restore → Server Restore** 3. Select the **serverbackup**.iso that you just put on the system. 4. Click **OK**. 5. Click **Yes** to confirm.  Select iso to restore from so to restore: (*) CMP240-114-cmp_12.3.0.0.0_17.1.0-serverbackup-201703272303.is ( ) Manually input anually input:
4. □	Verify the status	A dialog opens indicating that the restore operation was successful and instructing you to press any key to exit. If the restore is not successful, retry the restore operation. If the second restore is not successful, stop and contact the support or engineering team for assistance.
5. □	Verify Initial configuration	1. Click Exit until you return to the Main Menu of the platcfg utility. 2. Navigate to **Policy Configuration → Verify Initial Configuration**

Step	Procedure	Details

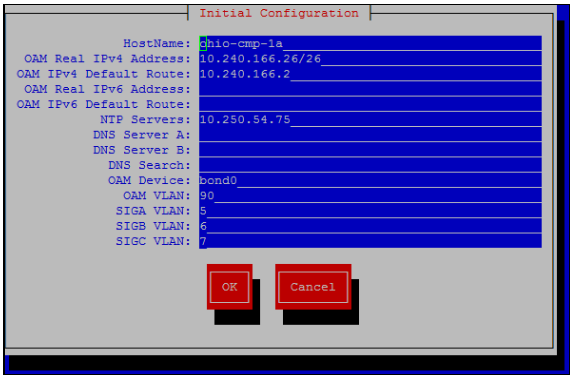


```
Copyright (C) 2003, 2016, Oracle and/or its affiliates. All rights reserved.
 Hostname: ohio-cmp-1a
                                                                   Index Table of Contents
Date/Time: 11/16/2016 15:49:48
Hardware Type: ProLiantBL460cG6
DNSSearch=""
DNSServerA=""
DNSServerB=""
DefaultGw="10.240.166.2"
DefaultIpv6Gw=""
Device="bond0"
HostName="ohio-cmp-1a"
LayoutProfile="common"
NtpServIpAddr="10.250.54.75"
OAMDevice="bond0"
OAMVLAN="90"
PMACDevice="bond0"
SIGADevice="bond0"
SIGAVLAN="5"
SIGBDevice="bond0"
SIGBVLAN="6"
SIGCDevice="bond0"
SIGCVLAN="7"
ServIpAddr="10.240.166.26/26"
ServIpv6Addr=""
NTP Status:
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.250.54.75    192.5.41.40      2 u  569 1024  377    0.209   -0.736   2.607

 Use arrow keys to move between options |  <Enter> selects
```

If the configuration does not exist, then navigate to **Perform Initial Configuration** and enter initial configuration information:

- Hostname
- OAM IP
- NTP servers configurations.

For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)

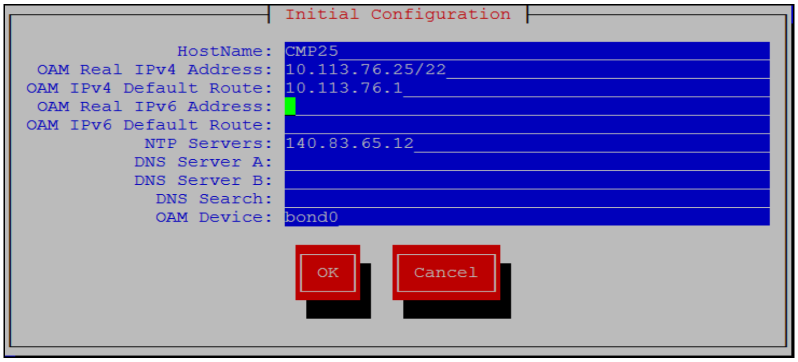


```
                    Initial Configuration
             HostName: ohio-cmp-1a
   OAM Real IPv4 Address: 10.240.166.26/26
  OAM IPv4 Default Route: 10.240.166.2
   OAM Real IPv6 Address:
  OAM IPv6 Default Route:
             NTP Servers: 10.250.54.75
            DNS Server A:
            DNS Server B:
              DNS Search:
              OAM Device: bond0
                OAM VLAN: 90
               SIGA VLAN: 5
               SIGB VLAN: 6
               SIGC VLAN: 7
```

1. Verify that your data is correct.
2. Click **OK**.
3. Click **Yes** to save and apply.
4. Exit platcfg by clicking **Exit** until you are returned to the shell.

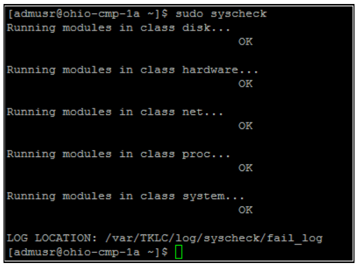
For RMS (DL360/DL380) System

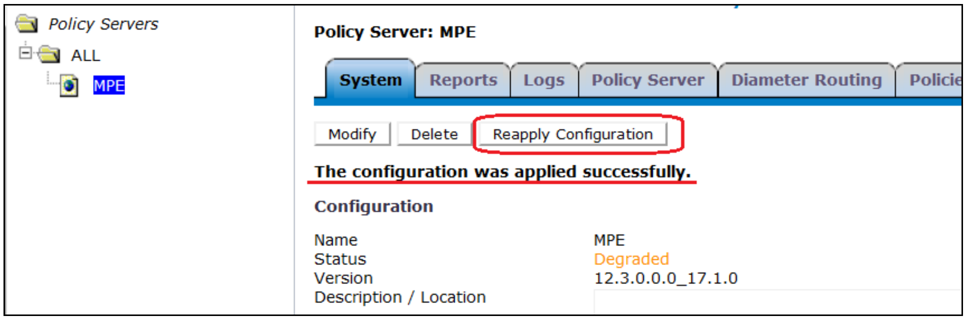
The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.

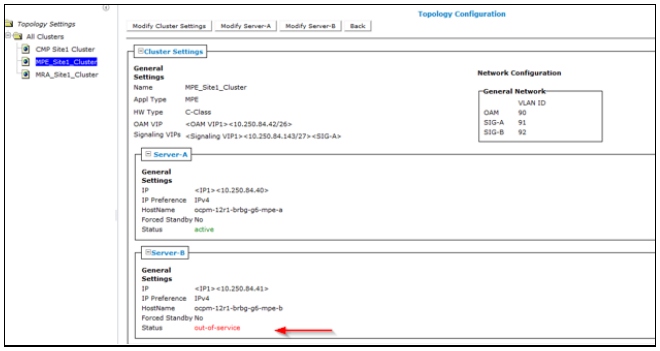
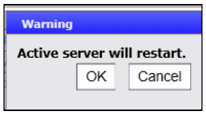


```
                    Initial Configuration
               HostName: CMP25
   OAM Real IPv4 Address: 10.113.76.25/22
  OAM IPv4 Default Route: 10.113.76.1
   OAM Real IPv6 Address:
  OAM IPv6 Default Route:
             NTP Servers: 140.83.65.12
            DNS Server A:
            DNS Server B:
              DNS Search:
              OAM Device: bond0
```

Step		Procedure	Details
6.	□	Reboot the server	Reboot: `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System** Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C** SSH directly to the node.

7.	□	Verify basic network connectivity and server health.	From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old server configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.
			`# ping <XMI or OAM gateway address>`
			Run the **`syscheck`** command. Verify that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.
			
			`[admusr@ohio-cmp-1a ~]$ sudo syscheck`
			`Running modules in class disk...`
			`                                 OK`
			
			`Running modules in class hardware...`
			`                                 OK`
			
			`Running modules in class net...`
			`                                 OK`
			
			`Running modules in class proc...`
			`                                 OK`
			
			`Running modules in class system...`
			`                                 OK`
			
			`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
			`[admusr@ohio-cmp-1a ~]$`
			NOTE: If you are restoring a CMP cluster, you must perform a system restoration for this server after this step. Then you must also perform a server restoration for the standby CMP server.

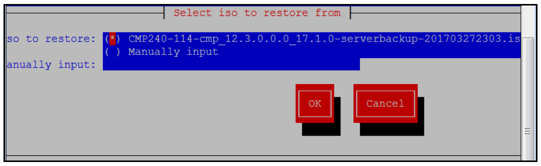
8.	□	Check status	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters** 2. Check system tab for the cluster. If the Status field indicates Config Mismatch, click **Reapply Configuration** and wait for the Config Mismatch designation to change. If it does not, contact My Oracle Support before proceeding.  Policy Servers ALL MPE System Reports Logs Policy Server Diameter Routing Policie Modify Delete Reapply Configuration **Policy Server: MPE** **The configuration was applied successfully.** **Configuration** Name MPE Status Degraded Version 12.3.0.0.0_17.1.0 Description / Location

Step		Procedure	Details
9.	□	Set Forced Standby designation on cluster node that is still out-of-service.	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting →** *<current_cluster>* 2. Click **Modify Server-***X* for the server that has a status of out-of-service. 3. Select **Forced Standby**. 4. Click **Save**.  Topology Settings All Clusters CMP Site1 Cluster MPE_Site1_Cluster MRA_Site1_Cluster Modify Cluster Settings Modify Server-A Modify Server-B Back Topology Configuration Cluster Settings General Settings Name MPE_Site1_Cluster Appl Type MPE HW Type C-Class OAM VIP <OAM VIP1><10.250.84.42/26> Signaling VIPs <Signaling VIP1><10.250.84.143/27><SIG-A> Network Configuration General Network VLAN ID OAM 90 SIG-A 91 SIG-B 92 Server-A General Settings IP <IP1><10.250.84.40> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-mpe-a Forced Standby No Status active Server-B General Settings IP <IP1><10.250.84.41> IP Preference IPv4 HostName ocpm-12r1-brbg-g6-mpe-b Forced Standby No Status out-of-service 5. Click **OK** to restart the server.  Warning Active server will restart.

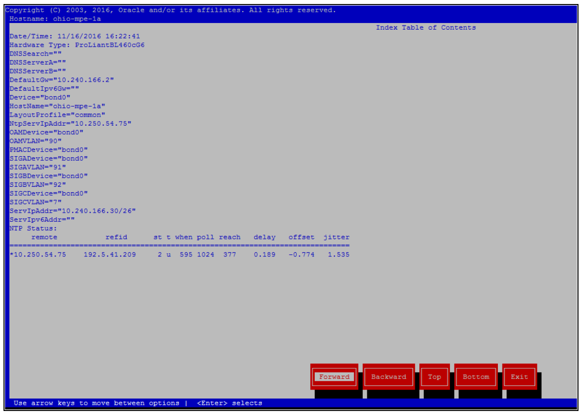
10.	□	SSH from the PM&C server to replacement server	**For c-Class System**
			SSH session from PM&C to new server, using the **PM&C GUI → Software → Software Inventory** to obtain the IP address for the server:
			`# ssh admusr@<node_IP_Address>`
			`$ sudo su -`
			For RMS (DL360/DL380/Oracle X5-2/Netra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

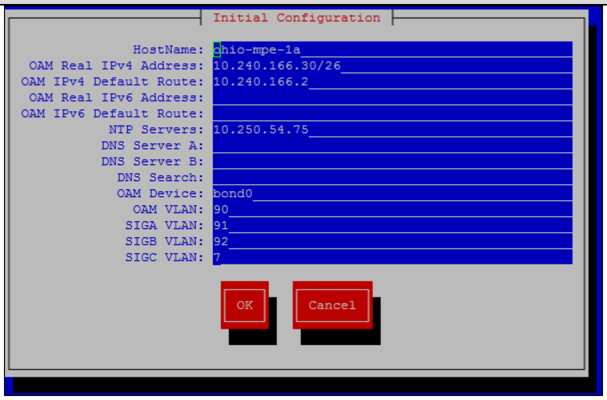
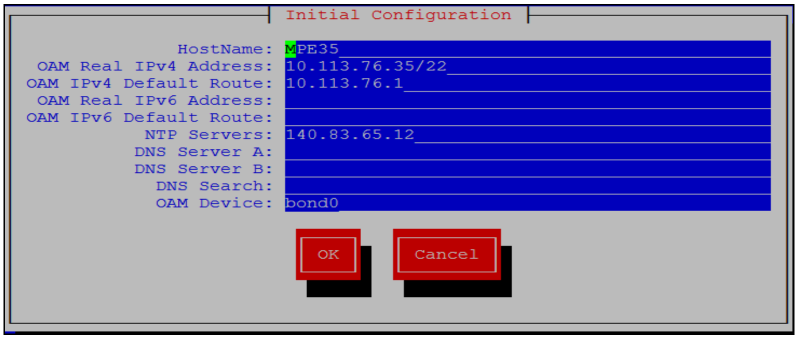
11.	□	Load the ISO to restore second server of the cluster	Obtain the **serverbackup**.iso for the server to be restored. When the replacement server is available (IPM/App installation complete), the server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE:** Later in this procedure, the platcfg utility restore function checks this directory and opens a menu. The platcfg utility also lets you manually enter any mounted path on the server.

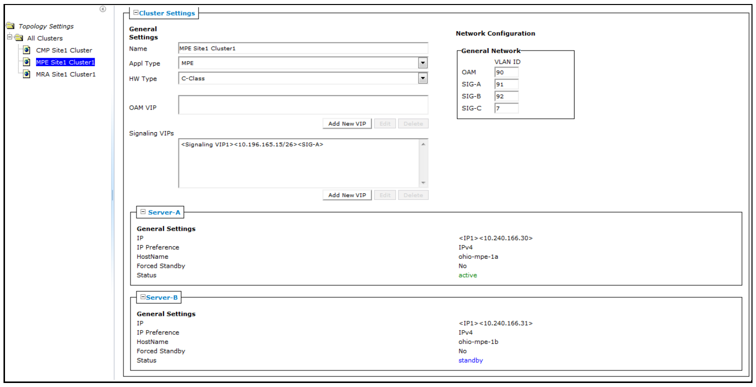
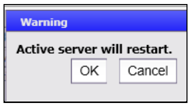
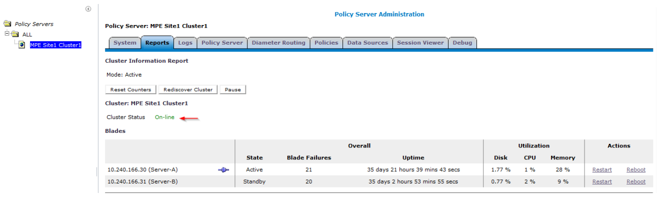
Step	Procedure	Details

12. □	Perform platcfg restore from SSH session to replacement server	1. Start the platcfg utility.
		`# su – platcfg`
		2. From the platcfg utility, navigate to **Policy Configuration → Backup and Restore → Server Restore**
		3. Select the **serverbackup**.iso that you just put on the system.
		4. Click **OK**.
		5. Click **Yes** to confirm.
		
		
		`so to restore: (*) CMP240-114-cmp_12.3.0.0.0_17.1.0-serverbackup-201703272303.is`
		`               ( ) Manually input`
		`anually input:`

13. □	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding.

14. □	Verify Initial configuration	1. Click **Exit** until you return to the Main Menu of the platcfg utility.
		2. Navigate to **Policy Configuration → Verify Initial Configuration**
		
		 Index Table of Contents
		Forward
		Backward
		Top
		Bottom
		Exit
		`Copyright (C) 2003, 2016, Oracle and/or its affiliates. All rights reserved.`
		` Hostname: ohio-mpe-1a`
		`Date/Time: 11/16/2016 16:22:41`
		`Hardware Type: ProLiantBL460cG6`
		`DNSSearch=""`
		`DNSServerA=""`
		`DNSServerB=""`
		`DefaultGw="10.240.166.2"`
		`DefaultIpv6Gw=""`
		`Device="bond0"`
		`HostName="ohio-mpe-1a"`
		`LayoutProfile="common"`
		`NtpServIpAddr="10.250.54.75"`
		`OAMDevice="bond0"`
		`OAMVLAN="90"`
		`PMACDevice="bond0"`
		`SIGADevice="bond0"`
		`SIGAVLAN="91"`
		`SIGBDevice="bond0"`
		`SIGBVLAN="92"`
		`SIGCDevice="bond0"`
		`SIGCVLAN="7"`
		`ServIpAddr="10.240.166.30/26"`
		`ServIpv6Addr=""`
		`NTP Status:`
		`     remote           refid      st t when poll reach   delay   offset  jitter`
		`==============================================================================`
		`*10.250.54.75    192.5.41.209     2 u  595 1024  377    0.189   -0.774   1.535`
		`Use arrow keys to move between options |  <Enter> selects`
		3. If the configuration does not exist, then navigate to **Perform Initial Configuration** and enter the initial configuration:
		- hostname
		- OAM IP
		- NTP servers configurations
		For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS):

Step	Procedure	Details
		 Initial Configuration HostName: ohio-mpe-1a OAM Real IPv4 Address: 10.240.166.30/26 OAM IPv4 Default Route: 10.240.166.2 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 10.250.54.75 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0 OAM VLAN: 90 SIGA VLAN: 91 SIGB VLAN: 92 SIGC VLAN: 7 1. Verify that your data is correct, and click **OK**. 2. Click **Yes** to save and apply. 3. Exit the platcfg utility by clicking **Exit** until you are returned to the shell. **For RMS (DL360/DL380) System** The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.  Initial Configuration HostName: MPE35 OAM Real IPv4 Address: 10.113.76.35/22 OAM IPv4 Default Route: 10.113.76.1 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 140.83.65.12 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0
15. □	Reboot the server	Reboot `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System** Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C** SSH directly to the node.

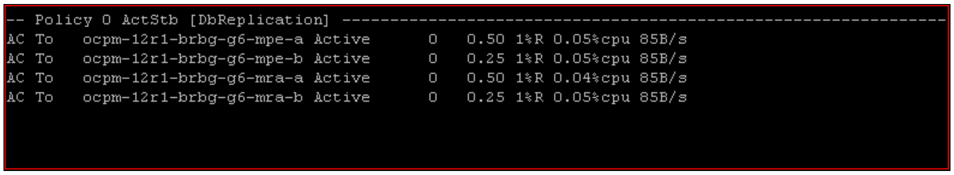
Step	Procedure	Details
16. ☐	Remove Forced Standby designation on current server.	1. In the CMP GUI, navigate to **Platform Setting → Topology Settings →** <*current_cluster*> 2. Click **Modify Server-***X* for the server that has Forced Standby 3. Clear **Forced Standby** option. 4. Click **Save**.  Topology Settings All Clusters CMP Site1 Cluster MPE Site1 Cluster1 MRA Site1 Cluster1 Cluster Settings General Settings Name: MPE Site1 Cluster1 Appl Type: MPE HW Type: C-Class OAM VIP: Add New VIP | Edit | Delete Signaling VIPs: <Signaling VIP1><10.196.165.15/26><SIG-A> Add New VIP | Edit | Delete Network Configuration General Network VLAN ID OAM: 90 SIG-A: 91 SIG-B: 92 SIG-C: 7 Server-A General Settings IP: <IP1><10.240.166.30> IP Preference: IPv4 HostName: ohio-mpe-1a Forced Standby: No Status: active Server-B General Settings IP: <IP1><10.240.166.31> IP Preference: IPv4 HostName: ohio-mpe-1b Forced Standby: No Status: standby 5. Click **OK** to restart the server.  Warning Active server will restart. OK | Cancel
17. ☐	Check status	In the CMP GUI, depending on the type of the server, perform the following: • If this is an MPE node, navigate to: **Policy Server → Configuration → All →** <*recovered_mpe_cluster*> **→ Reports** • If this is an MRA node, navigate to: **MRA → Configuration → All →** <*recovered_mra_cluster*> **→ Reports** • If this is an Mediation node, navigate to: **Mediation → Configuration → All →** <*recovered_mediation_cluster*> **→ Reports** Check CMP cluster status (as indicated in the previous step), navigate to **Platform Setting → Topology Setting →** <*current_cmp_cluster*> Monitor clustering of the new server to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.  Policy Servers ALL MPE Site1 Cluster1 Policy Server Administration Policy Server: MPE Site1 Cluster1 System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sources | Session Viewer | Debug Cluster Information Report Mode: Active Reset Counters | Rediscover Cluster | Pause Cluster: MPE Site1 Cluster1 Cluster Status: On-line Blades Overall: State | Blade Failures | Uptime; Utilization: Disk | CPU | Memory; Actions 10.240.166.30 (Server-A) | Active | 21 | 35 days 21 hours 39 mins 43 secs | 1.77 % | 1 % | 28 % | Restart | Reboot 10.240.166.31 (Server-B) | Standby | 20 | 35 days 2 hours 53 mins 55 secs | 0.77 % | 2 % | 9 % | Restart | Reboot

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>18. □</td><td>Alternative method to check replication status</td><td>

You can also monitor the clustering of the new server from the shell on the primary node with the **irepstat** command. SSH to the Active node of the current cluster and run the **irepstat** command:

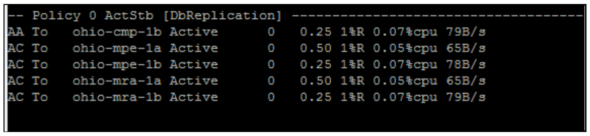
```
# irepstat
```

Expected **irepstat** command output while waiting reconnection:



```
-- Policy 0 ActStb [DbReplication] -----------------------------------------------------------------
AC To   ocpm-12r1-brbg-g6-mpe-a Active      0   0.50 1%R 0.05%cpu 85B/s
AC To   ocpm-12r1-brbg-g6-mpe-b Active      0   0.25 1%R 0.05%cpu 85B/s
AC To   ocpm-12r1-brbg-g6-mra-a Active      0   0.50 1%R 0.04%cpu 85B/s
AC To   ocpm-12r1-brbg-g6-mra-b Active      0   0.25 1%R 0.05%cpu 85B/s
```

Expected **irepstat** command output after cluster has formed:

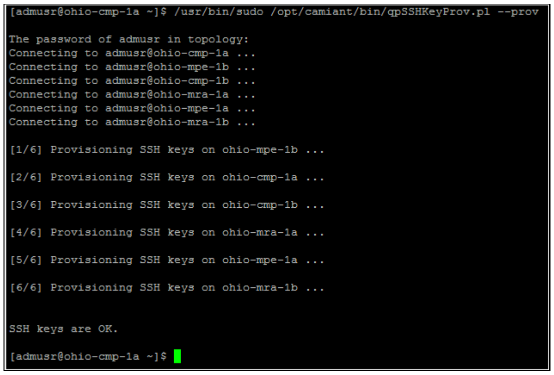


```
-- Policy 0 ActStb [DbReplication] ------------------------------------
AA To   ohio-cmp-1b Active      0   0.25 1%R 0.07%cpu 79B/s
AC To   ohio-mpe-1a Active      0   0.50 1%R 0.05%cpu 65B/s
AC To   ohio-mpe-1b Active      0   0.25 1%R 0.07%cpu 78B/s
AC To   ohio-mra-1a Active      0   0.50 1%R 0.05%cpu 65B/s
AC To   ohio-mra-1b Active      0   0.25 1%R 0.07%cpu 79B/s
```

</td></tr>
<tr><td>19. □</td><td>Exchange keys with cluster mate (This step must be run from the active CMP server)</td><td>

Exchanging SSH keys Utility

1. As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root`
2. As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`



```
[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov

The password of admusr in topology:
Connecting to admusr@ohio-cmp-1a ...
Connecting to admusr@ohio-mpe-1b ...
Connecting to admusr@ohio-cmp-1b ...
Connecting to admusr@ohio-mra-1a ...
Connecting to admusr@ohio-mpe-1a ...
Connecting to admusr@ohio-mra-1b ...

[1/6] Provisioning SSH keys on ohio-mpe-1b ...

[2/6] Provisioning SSH keys on ohio-cmp-1a ...

[3/6] Provisioning SSH keys on ohio-cmp-1b ...

[4/6] Provisioning SSH keys on ohio-mra-1a ...

[5/6] Provisioning SSH keys on ohio-mpe-1a ...

[6/6] Provisioning SSH keys on ohio-mra-1b ...


SSH keys are OK.

[admusr@ohio-cmp-1a ~]$
```

</td></tr>
<tr><td>20. □</td><td>Reapply Configuration</td><td>In the CMP GUI, click <b>Reapply Configuration</b> for the MPE/MRA/Mediation cluster. The message <code>The configuration was applied successfully</code> displays.</td></tr>
<tr><td colspan="3"><b>---End of Procedure---</b></td></tr>
</table>

5.6 Procedure 6: Restoring complete cluster without the server backup

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

Required Resources

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

- o Vlan configuration information, hostname, OAM IP address, and VLAN configuration can be gathered from:

  Platform Setting → Topology Setting → <*cluster_name*>

- NTP server configuration (and optionally DNS configuration can be gotten from platcfg of the running server)
- Verify that routing is configured correctly i.e. XSI is default and any associated OAM routes are added.

Prerequisites

1. Power down the failed server gracefully
   a. Access the iLO with administrator privileges.
   b. Go to **Power Management →Server Power**
   c. Click **Momentary Press**
2. Remove failed server and replace.
3. Verify that the server has TPD installed. If it is not installed, install TPD on the server.
4. Install the CMP application software, MPE, MRA, or Mediation
   - o In case it is a CMP Cluster that is being rebuilt, restore application data either from system backup or manually if no backup available.
   - o See the Policy Management Bare Metal Installation Guide Release 12.3 for more details. The documents are available on the Oracle Help Center

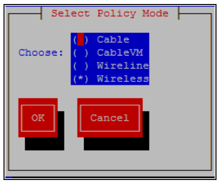
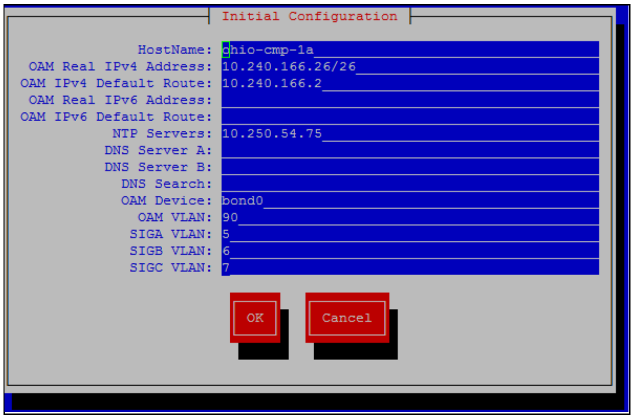
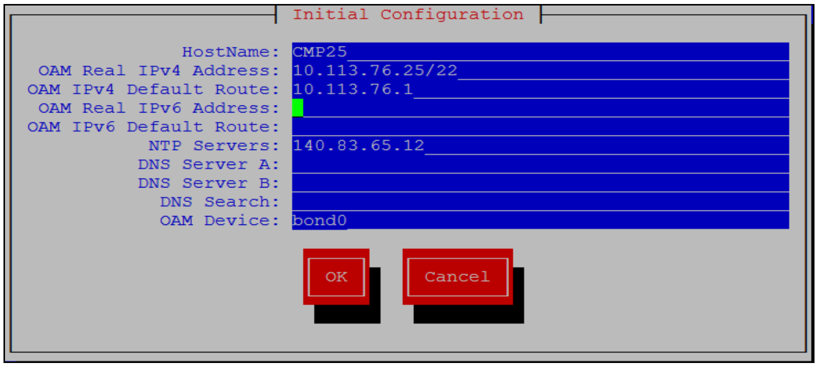
Use this procedure to restore a complete cluster without the server backup

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

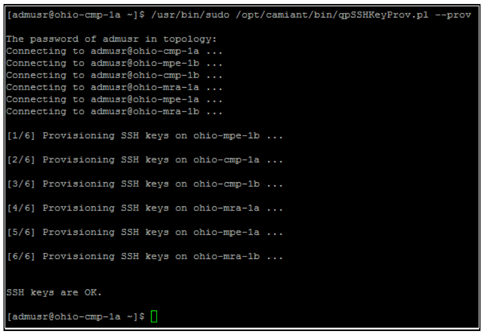
Should this procedure fail, contact My Oracle Support (MOS) and ask for assistance.

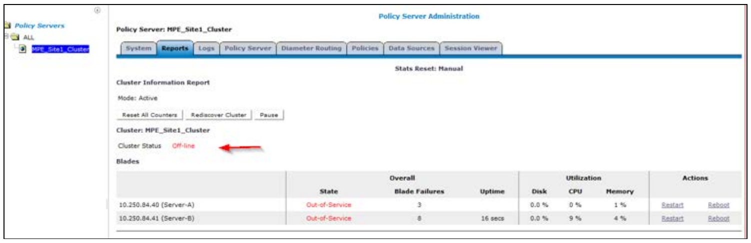
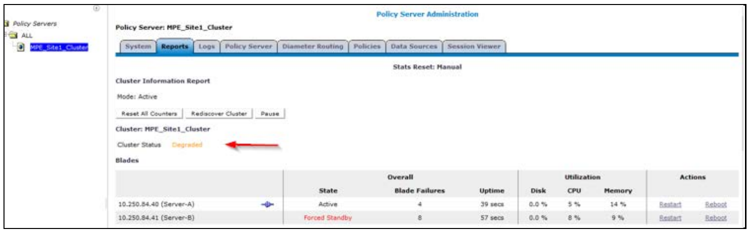
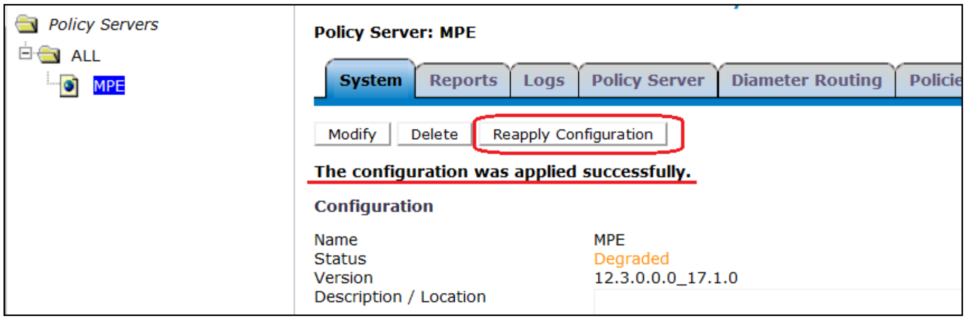
Step	Procedure	Details

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

Step	Procedure	Details
2. □	Form the platcfg utility, run the Initial Policy Configuration on installed server	1. Start the platcfg utility. `# su - platcfg` 2. From the platcfg utility, navigate to: **Policy Configuration → Set Policy Mode**  Choose: ( ) Cable ( ) CableVM ( ) Wireline (*) Wireless 3. Verify that Wireless is selected. Click **OK** to continue or you can skip this step. 4. From the platcfg utility, navigate to **Policy Configuration → Perform Initial Configuration** 5. Enter the configuration details for the server being replaced.  HostName: ohio-cmp-1a OAM Real IPv4 Address: 10.240.166.26/26 OAM IPv4 Default Route: 10.240.166.2 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 10.250.54.75 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0 OAM VLAN: 90 SIGA VLAN: 5 SIGB VLAN: 6 SIGC VLAN: 7 6. After the server details are entered and verified for correctness, click **OK**. 7. A menu displays asking if the settings should be applied, click **Yes** and wait for the operation to complete. A message is not displayed when the operation is successful, but an error displays if it does not complete. In this case, review the settings from the Perform Initial Configuration page. If all the information is correct, contact My Oracle Support before proceeding. 8. Exit the platcfg utility by clicking **Exit** until you are returned to the shell. **For RMS (DL360/DL380) System** The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.  HostName: CMP25 OAM Real IPv4 Address: 10.113.76.25/22 OAM IPv4 Default Route: 10.113.76.1 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 140.83.65.12 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0

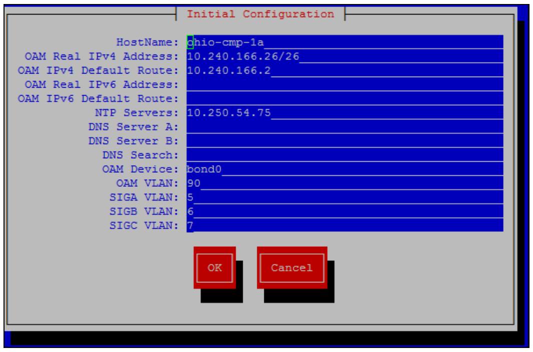
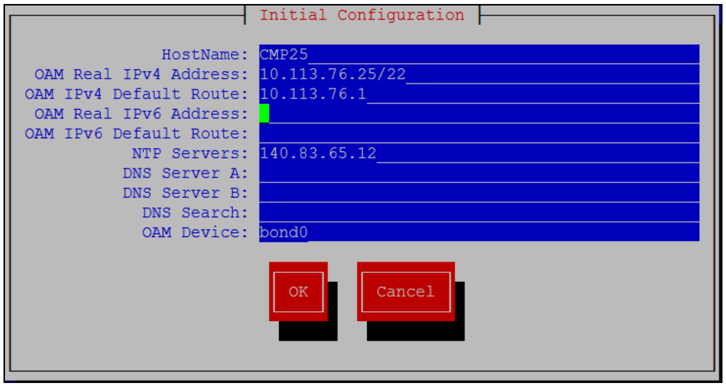
Step	Procedure	Details
3. □	Reboot the server	Reboot: `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System:** Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C:** SSH directly to the node.

4. □	Verify basic network connectivity and server health.	From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old server configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.
		`# ping <XMI or OAM gateway address>`
		Run the **`syscheck`** command. Verify that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.
		
		`[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`
		
		`The password of admusr in topology:`
		`Connecting to admusr@ohio-cmp-1a ...`
		`Connecting to admusr@ohio-mpe-1b ...`
		`Connecting to admusr@ohio-cmp-1b ...`
		`Connecting to admusr@ohio-mra-1a ...`
		`Connecting to admusr@ohio-mpe-1a ...`
		`Connecting to admusr@ohio-mra-1b ...`
		
		`[1/6] Provisioning SSH keys on ohio-mpe-1b ...`
		
		`[2/6] Provisioning SSH keys on ohio-cmp-1a ...`
		
		`[3/6] Provisioning SSH keys on ohio-cmp-1b ...`
		
		`[4/6] Provisioning SSH keys on ohio-mra-1a ...`
		
		`[5/6] Provisioning SSH keys on ohio-mpe-1a ...`
		
		`[6/6] Provisioning SSH keys on ohio-mra-1b ...`
		
		`SSH keys are OK.`
		
		`[admusr@ohio-cmp-1a ~]$`

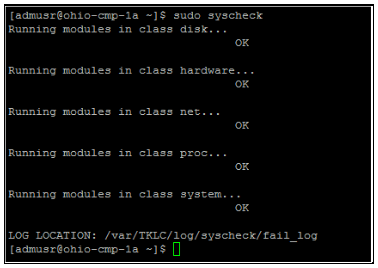
Step	Procedure	Details
5. □	Check status	In the CMP GUI, depending on the type of the server, perform the following: • If this is an MPE node, navigate to: **Policy Server → Configuration → All →** <*recovered_mpe_cluster*> **→ Reports** • If this is an MRA node, navigate to: **MRA → Configuration → All →** <*recovered_mra_cluster*> **→ Reports** • If this is an Mediation node, navigate to: **Mediation → Configuration → All →** <*recovered_mediation_cluster*> **→ Reports** Monitor clustering of the new server to its peer, do not proceed until the Cluster Status changes from Off-line to Degraded. **Off-line**  Policy Servers ALL MPE_Site1_Cluster Policy Server Administration System Reports Logs Policy Server Diameter Routing Policies Data Sources Session Viewer Reset All Counters Rediscover Cluster Pause Policy Server: MPE_Site1_Cluster Stats Reset: Manual Cluster Information Report Mode: Active Cluster: MPE_Site1_Cluster Cluster Status Off-line Blades Overall: State / Blade Failures / Uptime; Utilization: Disk / CPU / Memory; Actions 10.250.84.40 (Server-A) Out-of-Service 3 0.0 % 0 % 1 % Restart Reboot 10.250.84.41 (Server-B) Out-of-Service 8 16 secs 0.0 % 9 % 4 % Restart Reboot **Degraded**  Policy Servers ALL MPE_Site1_Cluster Policy Server Administration System Reports Logs Policy Server Diameter Routing Policies Data Sources Session Viewer Reset All Counters Rediscover Cluster Pause Policy Server: MPE_Site1_Cluster Stats Reset: Manual Cluster Information Report Mode: Active Cluster: MPE_Site1_Cluster Cluster Status Degraded Blades Overall: State / Blade Failures / Uptime; Utilization: Disk / CPU / Memory; Actions 10.250.84.40 (Server-A) Active 4 39 secs 0.0 % 5 % 14 % Restart Reboot 10.250.84.41 (Server-B) Forced Standby 8 57 secs 0.0 % 8 % 9 % Restart Reboot
6. □	Check status	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters** 2. Check the **System** tab for the cluster. If the Status field indicates Config Mismatch, click **Reapply Configuration** and wait for the Config Mismatch designation to change. If it does not, contact My Oracle Support before proceeding.  Policy Servers ALL MPE System Reports Logs Policy Server Diameter Routing Policie Modify Delete Reapply Configuration Policy Server: MPE The configuration was applied successfully. Configuration Name MPE Status Degraded Version 12.3.0.0.0_17.1.0 Description / Location

Step	Procedure	Details

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

8. □	From the platcfg utility, Perform the Initial Policy Configuration operation on the second node of cluster	1. Start the platcfg utility.
		`# su - platcfg`
		2. Navigate to **Policy Configuration → Initial Configuration**
		3. Enter the details for the server being replaced.
		
		Initial Configuration
		`HostName: ohio-cmp-1a`
		`OAM Real IPv4 Address: 10.240.166.26/26`
		`OAM IPv4 Default Route: 10.240.166.2`
		`OAM Real IPv6 Address:`
		`OAM IPv6 Default Route:`
		`NTP Servers: 10.250.54.75`
		`DNS Server A:`
		`DNS Server B:`
		`DNS Search:`
		`OAM Device: bond0`
		`OAM VLAN: 90`
		`SIGA VLAN: 5`
		`SIGB VLAN: 6`
		`SIGC VLAN: 7`
		
		4. After the server details are entered and verified for correctness, click **OK**.
		5. A menu displays asking if the settings should be applied, click **Yes**. Wait for the operation to complete. A message is not displayed when the operation is successful, but an error displays if it does not complete. In this case, review the settings on the Perform Initial Configuration page. If the information is correct, contact My Oracle Support before proceeding.
		6. Exit the platcfg utility by clicking **Exit** until you are returned to the shell.
		For RMS (DL360/DL380) System
		The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.
		
		Initial Configuration
		`HostName: CMP25`
		`OAM Real IPv4 Address: 10.113.76.25/22`
		`OAM IPv4 Default Route: 10.113.76.1`
		`OAM Real IPv6 Address:`
		`OAM IPv6 Default Route:`
		`NTP Servers: 140.83.65.12`
		`DNS Server A:`
		`DNS Server B:`
		`DNS Search:`
		`OAM Device: bond0`

Step	Procedure	Details
9. □	Reboot the server	Reboot: `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System:** Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C** SSH directly to the node.

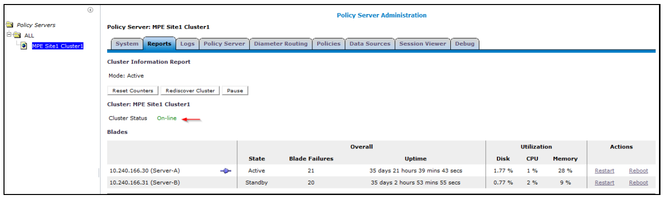
10. □	Verify basic network connectivity and server health.	From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old server configuration and reconfigure if needed. If the network ping tests still fails, contact My Oracle Support before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

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr>
<td>11. □</td>
<td>Check status</td>
<td>
In the CMP GUI, depending on the type of the server, perform the following:

- If this is an MPE node, navigate to:
  Policy Server → Configuration → All → <*recovered_mpe_cluster*> **→ Reports**
- If this is an MRA node, navigate to:
  MRA → Configuration → All → <*recovered_mra_cluster*> **→ Reports**
- If this is an Mediation node, navigate to:
  Mediation → Configuration → All → <*recovered_mediation_cluster*> **→ Reports**

Monitor clustering of the new server to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.

MPE



Policy Server Administration

Policy Server: MPE Site1 Cluster1

Cluster Information Report

Mode: Active

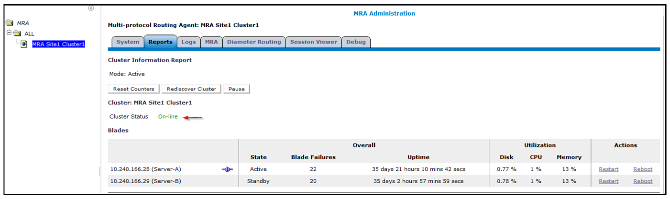
Cluster: MPE Site1 Cluster1

Cluster Status On-line

Blades

<table>
<tr><th></th><th>Overall</th><th></th><th></th><th>Utilization</th><th></th><th></th><th>Actions</th><th></th></tr>
<tr><th></th><th>State</th><th>Blade Failures</th><th>Uptime</th><th>Disk</th><th>CPU</th><th>Memory</th><th></th><th></th></tr>
<tr><td>10.240.166.30 (Server-A)</td><td>Active</td><td>21</td><td>35 days 21 hours 39 mins 43 secs</td><td>1.77 %</td><td>1 %</td><td>28 %</td><td>Restart</td><td>Reboot</td></tr>
<tr><td>10.240.166.31 (Server-B)</td><td>Standby</td><td>20</td><td>35 days 2 hours 53 mins 55 secs</td><td>0.77 %</td><td>2 %</td><td>9 %</td><td>Restart</td><td>Reboot</td></tr>
</table>

MRA



MRA Administration

Multi-protocol Routing Agent: MRA Site1 Cluster1

Cluster Information Report

Mode: Active

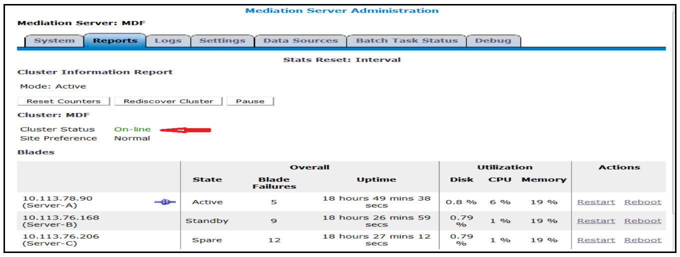
Cluster: MRA Site1 Cluster1

Cluster Status On-line

Blades

<table>
<tr><th></th><th>Overall</th><th></th><th></th><th>Utilization</th><th></th><th></th><th>Actions</th><th></th></tr>
<tr><th></th><th>State</th><th>Blade Failures</th><th>Uptime</th><th>Disk</th><th>CPU</th><th>Memory</th><th></th><th></th></tr>
<tr><td>10.240.166.28 (Server-A)</td><td>Active</td><td>22</td><td>35 days 21 hours 10 mins 42 secs</td><td>0.77 %</td><td>1 %</td><td>13 %</td><td>Restart</td><td>Reboot</td></tr>
<tr><td>10.240.166.29 (Server-B)</td><td>Standby</td><td>20</td><td>35 days 2 hours 57 mins 59 secs</td><td>0.78 %</td><td>1 %</td><td>13 %</td><td>Restart</td><td>Reboot</td></tr>
</table>

Mediation



Mediation Server Administration

Mediation Server: MDF

Stats Reset: Interval

Cluster Information Report

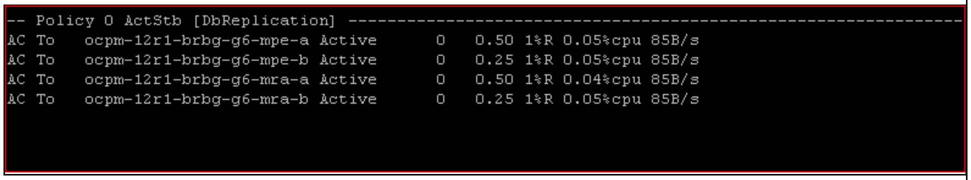
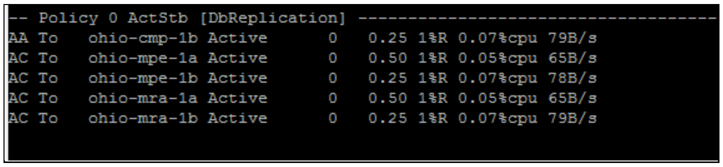
Mode: Active

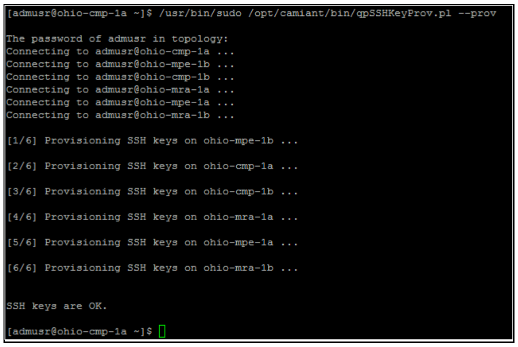
Cluster: MDF

Cluster Status On-line
Site Preference Normal

Blades

<table>
<tr><th></th><th>Overall</th><th></th><th></th><th>Utilization</th><th></th><th></th><th>Actions</th><th></th></tr>
<tr><th></th><th>State</th><th>Blade Failures</th><th>Uptime</th><th>Disk</th><th>CPU</th><th>Memory</th><th></th><th></th></tr>
<tr><td>10.113.78.90 (Server-A)</td><td>Active</td><td>5</td><td>18 hours 49 mins 38 secs</td><td>0.8 %</td><td>6 %</td><td>19 %</td><td>Restart</td><td>Reboot</td></tr>
<tr><td>10.113.76.168 (Server-B)</td><td>Standby</td><td>9</td><td>18 hours 26 mins 59 secs</td><td>0.79 %</td><td>1 %</td><td>19 %</td><td>Restart</td><td>Reboot</td></tr>
<tr><td>10.113.76.206 (Server-C)</td><td>Spare</td><td>12</td><td>18 hours 27 mins 12 secs</td><td>0.79 %</td><td>1 %</td><td>19 %</td><td>Restart</td><td>Reboot</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>12. □</td><td>Alternative method to check replication status</td><td>You can also monitor the clustering of the new server from the shell on the primary node with the <b>irepstat</b> command. SSH to the Active node of the current cluster and run the <b>irepstat</b> command:
<pre>
# irepstat
</pre>
Expected <b>irepstat</b> command output while waiting reconnection:

<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>
Expected <b>irepstat</b> command output after cluster has formed:

<pre>
-- Policy 0 ActStb [DbReplication] ------------------------------------
AA To   ohio-cmp-1b Active   0   0.25 1%R 0.07%cpu 79B/s
AC To   ohio-mpe-1a Active   0   0.50 1%R 0.05%cpu 65B/s
AC To   ohio-mpe-1b Active   0   0.25 1%R 0.07%cpu 78B/s
AC To   ohio-mra-1a Active   0   0.50 1%R 0.05%cpu 65B/s
AC To   ohio-mra-1b Active   0   0.25 1%R 0.07%cpu 79B/s
</pre></td></tr>
<tr><td>13. □</td><td>Exchange keys with cluster mate (This step need to run from active CMP)</td><td>Exchanging SSH keys Utility
<pre>
As root, run /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root

As admusr, run /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov
</pre>

<pre>
[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov

The password of admusr in topology:
Connecting to admusr@ohio-cmp-1a ...
Connecting to admusr@ohio-mpe-1b ...
Connecting to admusr@ohio-cmp-1b ...
Connecting to admusr@ohio-mra-1a ...
Connecting to admusr@ohio-mpe-1a ...
Connecting to admusr@ohio-mra-1b ...

[1/6] Provisioning SSH keys on ohio-mpe-1b ...

[2/6] Provisioning SSH keys on ohio-cmp-1a ...

[3/6] Provisioning SSH keys on ohio-cmp-1b ...

[4/6] Provisioning SSH keys on ohio-mra-1a ...

[5/6] Provisioning SSH keys on ohio-mpe-1a ...

[6/6] Provisioning SSH keys on ohio-mra-1b ...

SSH keys are OK.

[admusr@ohio-cmp-1a ~]$
</pre></td></tr>
<tr><td>14. □</td><td>Reapply Configuration</td><td>In the CMP GUI, click <b>Reapply Configuration</b> for the MPE/MRA/Mediation cluster. The message <code>The configuration was applied successfully</code> displays.</td></tr>
<tr><td colspan="3"><b>---End of Procedure---</b></td></tr>
</table>

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 Management network that can be used to re-create the Policy Management network that is to be recovered. After a CMP is online, all other servers of the Policy Management 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 servers should be restored first.

Required Resources

- Replacement server.
- TPD installation ISO.
- Policy APP installation ISO.
- Recent System backup file.

- Initial configuration information about the server to be restored:
  - OAM IP address, default gateway, NTP & SNMP server IP addresses
  - VLAN configuration information.

Hostname, OAM IP address, and VLAN configuration can be gathered from:

Platform Setting → Topology Setting → <*Cluster_Name*>

NTP server configuration (and optionally DNS configuration can be gotten from platcfg of the running server)

Verify that routing is configured correctly i.e. XSI is default and any associated OAM routes are added.

Prerequisites

1. Power down the failed server gracefully
   a. Access the iLO with administrator privileges.
   b. Go to **Power Management →Server Power**
   c. Click on **Momentary Press**
2. Remove failed servers and replace.
3. Verify that the server has TPD installed. If it is not installed, install TPD on the server.
4. Install the CMP application software

   NOTE: See the Policy Management Bare Metal Installation Guide Release 12.3 for more details. The documents are available on the Oracle Help Center.

Use this procedure to restore a CMP cluster with system backup available

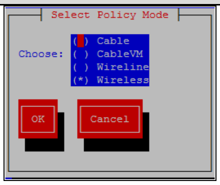
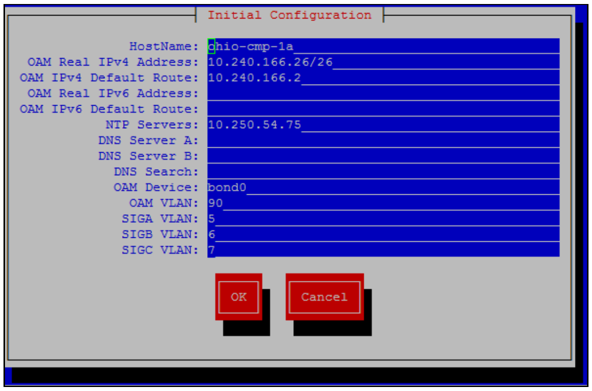
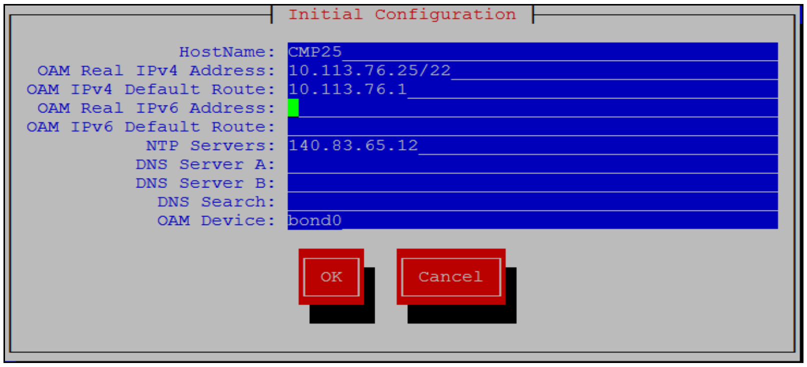
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Should this procedure fail, contact My Oracle Support (MOS) Customer Care Center and ask for assistance.

Step	Procedure	Details

1. □	Login via SSH to new server	**For c-Class System**
		SSH session from PM&C to new server. Use the **PM&C GUI → Software → Software Inventory** page to obtain the IP address for the server.
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`
		For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:
		Use the iLO/iLOM (for Oracle hardware Oracle X5-2 and Netra X5-2) to login, and start a remote console session to run commands.

2. □	From the platcfg utility, perform Initial Policy Configuration on the installed server	1. Start the platcfg utility. `# su – platcfg` **2.** Navigate to **Policy Configuration → Set Policy Mode**

Step	Procedure	Details
		 Select Policy Mode Choose: ( ) Cable ( ) CableVM ( ) Wireline (*) Wireless 3. Verify that Wireless is selected. Click **OK** to continue or you can skip this step. 4. Navigate to **Policy Configuration → Perform Initial Configuration.** 5. Enter the details for the server being replaced:  Initial Configuration HostName: ohio-cmp-1a OAM Real IPv4 Address: 10.240.166.26/26 OAM IPv4 Default Route: 10.240.166.2 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 10.250.54.75 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0 OAM VLAN: 90 SIGA VLAN: 5 SIGB VLAN: 6 SIGC VLAN: 7 6. After the server details are entered and verified for correctness, click **OK**. 7. A menu displays asking if the settings should be applied, click **Yes** and wait for the operation to complete. A message is not displayed when the operation is successful, but an error displays if it does not complete. In this case, review the settings from the Perform Initial Configuration page. If the values are correct, contact My Oracle Support before proceeding. 8. Exit the platcfg utility by clicking Exit until you are returned to the shell. **For RMS (DL360/DL380) System** The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.  Initial Configuration HostName: CMP25 OAM Real IPv4 Address: 10.113.76.25/22 OAM IPv4 Default Route: 10.113.76.1 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 140.83.65.12 DNS Server A: DNS Server B: DNS Search: OAM Device: bond0

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>3. □</td><td>Reboot the server</td><td>

Reboot:

```
# init 6
```

Allow the server time to reboot.

For c-Class or Netra X5-2(Oracle RMS)System

Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges.

For RMS (DL360/DL380/Oracle X5-2)System without PM&C:

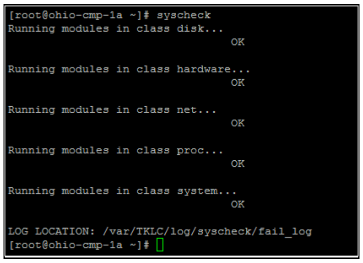
SSH directly to the node.

</td></tr>
<tr><td>4. □</td><td>Verify basic network connectivity and server health.</td><td>

From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old server configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.

```
# ping <XMI or OAM gateway address>
```

Run the **`syscheck`** command. Verify that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.



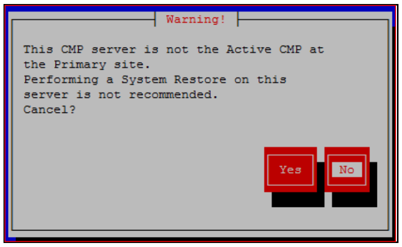
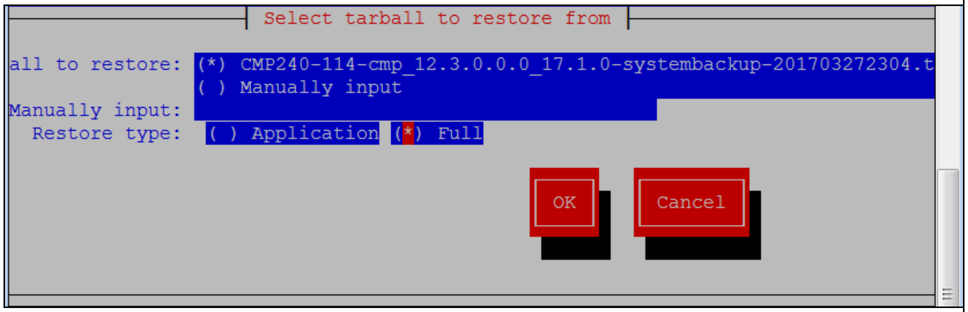
```
[root@ohio-cmp-1a ~]# syscheck
Running modules in class disk...
                                 OK

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@ohio-cmp-1a ~]# 
```

</td></tr>
<tr><td>5. □</td><td>Load the system backup(ISO) file for server restore</td><td>

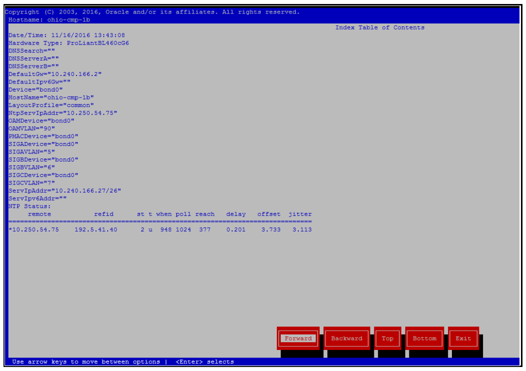
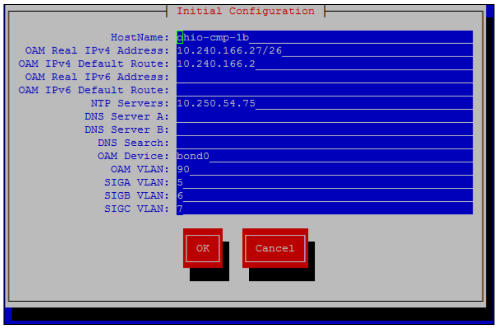
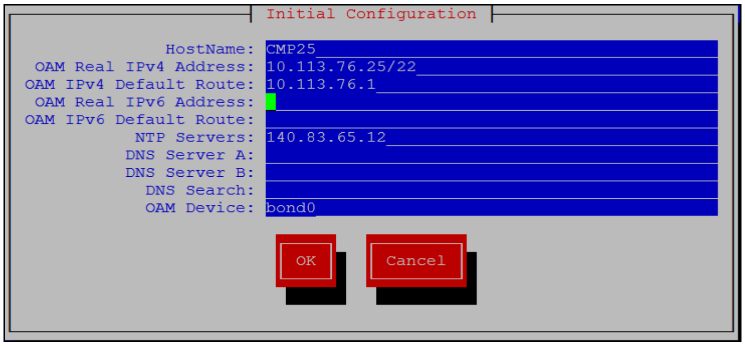
The system backup file contains the database information that makes up the application level configuration of the Policy Management network. Without that backup, the application configuration must be restored either through the platcfg menu, or from the server backup file from site documentation.

If the system backup file is available, put a copy of the file on the constructed CMP server into the `/var/camiant/backup/local_archive/systembackup` directory using secure copy (pscp scp, or WinSCP).

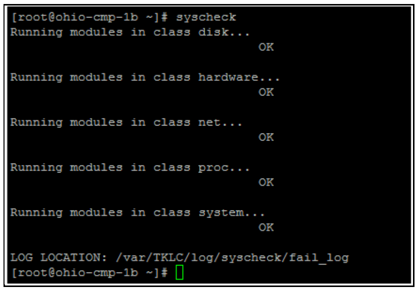
</td></tr>
</table>

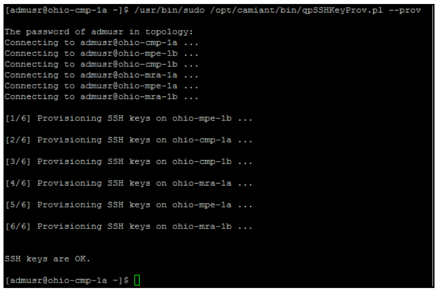
Step	Procedure	Details
6. □	Perform platcfg restore from SSH session to replacement server	1. Start the platcfg utility. `# su - platcfg` **2.** From the platcfg utility, navigate to **Policy Configuration → Backup and Restore → System Restore** 3. A message displays asking for confirmation to restore even though this node is not recognized as the active member. This behavior is expected, continue by clicking **NO**.  Warning! This CMP server is not the Active CMP at the Primary site. Performing a System Restore on this server is not recommended. Cancel? 4. A page opens asking you to select the file to use for the restore. If the file was copied correctly in the previous step, it is shown here as an option, otherwise select **Manually Input**, and select **Full**. 5. Select **OK** to proceed.  Select tarball to restore from all to restore: (*) CMP240-114-cmp_12.3.0.0.0_17.1.0-systembackup-201703272304.t ( ) Manually input Manually input: Restore type: ( ) Application (*) Full **NOTE: Full** restores COMCOL data, **Application** does not restore COMCOL data.
7. □	Verify the status	A dialog opens indicating that the restore operation was successful and instructing you to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

Step	Procedure	Details

8. □	Verify Initial configuration	1. Click **Exit** until you return to the Main Menu of the platcfg utility.
		2. Navigate to **Policy Configuration → Verify Initial Configuration**
		
		`Copyright (C) 2003, 2016, Oracle and/or its affiliates. All rights reserved.`
		`Hostname: ohio-cmp-1b`
		`Index Table of Contents`
		`Date/Time: 11/16/2016 13:43:08`
		`Hardware Type: ProLiantBL460cG6`
		`DNSSearch=""`
		`DNSServerA=""`
		`DNSServerB=""`
		`DefaultGw="10.240.166.2"`
		`DefaultIpv6Gw=""`
		`Device="bond0"`
		`HostName="ohio-cmp-1b"`
		`LayoutProfile="common"`
		`NtpServIpAddr="10.250.54.75"`
		`OAMDevice="bond0"`
		`OAMVLAN="90"`
		`PMACDevice="bond0"`
		`SIGADevice="bond0"`
		`SIGAVLAN="5"`
		`SIGBDevice="bond0"`
		`SIGBVLAN="6"`
		`SIGCDevice="bond0"`
		`SIGCVLAN="7"`
		`ServIpAddr="10.240.166.27/26"`
		`ServIpv6Addr=""`
		`NTP Status:`
		`     remote           refid      st t when poll reach   delay   offset  jitter`
		`==============================================================================`
		`*10.250.54.75    192.5.41.40      2 u  948 1024  377    0.201    3.733   3.113`
		
		`Use arrow keys to move between options |  <Enter> selects`
		3. Verify that your data is correct. If configuration is not there, then navigate to **Perform Initial Configuration** and enter the configuration information.
		
		`Initial Configuration`
		`HostName: ohio-cmp-1b`
		`OAM Real IPv4 Address: 10.240.166.27/26`
		`OAM IPv4 Default Route: 10.240.166.2`
		`OAM Real IPv6 Address:`
		`OAM IPv6 Default Route:`
		`NTP Servers: 10.250.54.75`
		`DNS Server A:`
		`DNS Server B:`
		`DNS Search:`
		`OAM Device: bond0`
		`OAM VLAN: 90`
		`SIGA VLAN: 5`
		`SIGB VLAN: 6`
		`SIGC VLAN: 7`
		
		4. Click **OK**.
		5. Click **Yes** to save and apply
		6. After the server details are entered and verified for correctness click **OK**.
		7. A menu displays asking if the settings should be applied, click **Yes** and wait for the operation to complete. A message is not displayed when the operation is successful, but an error displays if it does not complete. In this case, review the settings from the **Perform Initial Configuration** page. If the information is correct, contact My Oracle Support before proceeding.
		8. Exit the platcfg utility by clicking Exit until you are returned to the shell.
		For RMS (DL360/DL380) System
		The platcfg utility for RMS does not use VLANs. The SIGA VLAN, SIGB VLAN and SIGC VLAN configuration parameters are not available for the RMS configuration.
		
		`Initial Configuration`
		`HostName: CMP25`
		`OAM Real IPv4 Address: 10.113.76.25/22`
		`OAM IPv4 Default Route: 10.113.76.1`
		`OAM Real IPv6 Address:`
		`OAM IPv6 Default Route:`
		`NTP Servers: 140.83.65.12`
		`DNS Server A:`
		`DNS Server B:`
		`DNS Search:`
		`OAM Device: bond0`

Step	Procedure	Details
9. □	Reboot the server	Reboot. `# init 6` Allow the server time to reboot. **For c-Class or Netra X5-2(Oracle RMS)System** Using SSH, reconnect the PM&C server to the node as admusr and then switch to root privileges. **For RMS (DL360/DL380/Oracle X5-2)System without PM&C** SSH directly to the node.

10. □	Verify basic network connectivity and server health.	From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.
		`# ping <XMI or OAM gateway address>`
		Run the **`syscheck`** command. Verify that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.
		
		`[root@ohio-cmp-1b ~]# 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@ohio-cmp-1b ~]#`

11. □	Exchange keys with cluster mate (This step must be run from the active CMP server)	Exchanging SSH keys Utility
		1. As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root`
		2. As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`
		
		`[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`
		
		`The password of admusr in topology:`
		`Connecting to admusr@ohio-cmp-1a ...`
		`Connecting to admusr@ohio-mpe-1b ...`
		`Connecting to admusr@ohio-cmp-1b ...`
		`Connecting to admusr@ohio-mra-1a ...`
		`Connecting to admusr@ohio-mpe-1a ...`
		`Connecting to admusr@ohio-mra-1b ...`
		
		`[1/6] Provisioning SSH keys on ohio-mpe-1b ...`
		
		`[2/6] Provisioning SSH keys on ohio-cmp-1a ...`
		
		`[3/6] Provisioning SSH keys on ohio-cmp-1b ...`
		
		`[4/6] Provisioning SSH keys on ohio-mra-1a ...`
		
		`[5/6] Provisioning SSH keys on ohio-mpe-1a ...`
		
		`[6/6] Provisioning SSH keys on ohio-mra-1b ...`
		
		`SSH keys are OK.`
		
		`[admusr@ohio-cmp-1a ~]$`

12. □	Check status	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters.** 2. When the server has returned to online status, log into the GUI on the OAM virtual IP address - Verify that the new manager has the configuration for the MPE clusters in the network (whether those clusters are online or not) - Verify other application configuration properties. After one CMP is in place, the other node of the CMP cluster can be replaced using the procedures above, and any other clusters or individual nodes that need replacement can be handled with the above procedures.
---End of Procedure---		

5.8 Procedure 8: Promoting georedundant CMP cluster

The purpose of this procedure is to bring a georedundant secondary active CMP online before beginning restoration of other Policy Management clusters in the network. After a CMP is online, all other servers of the Policy Management network can be re-created using the above procedures and then their application level configuration restored from this CMP.

Use this procedure to promote a georedundant CMP cluster

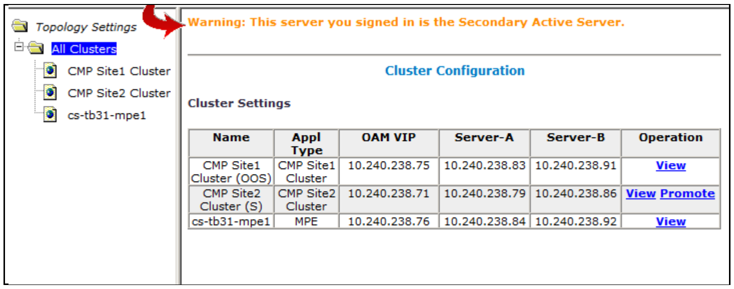
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Should this procedure fail, contact My Oracle Support (MOS) Customer Care Center and ask for assistance.

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>1. □</td><td>Access to the system</td><td>Log into the GUI on the OAM VIP of the georedundant CMP.</td></tr>
<tr><td>2. □</td><td>Check status</td><td>

In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters**

You are warned that you are not on the primary cluster of the Policy Management network. The secondary server has limited functionality.



Warning: This server you signed in is the Secondary Active Server.

Cluster Configuration

Cluster Settings

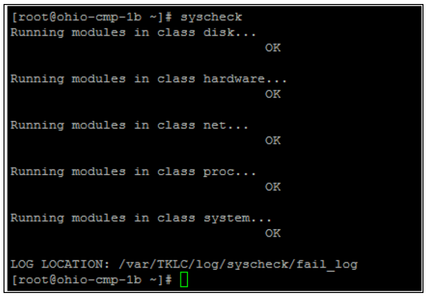
<table>
<tr><th>Name</th><th>Appl Type</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Operation</th></tr>
<tr><td>CMP Site1 Cluster (OOS)</td><td>CMP Site1 Cluster</td><td>10.240.238.75</td><td>10.240.238.83</td><td>10.240.238.91</td><td>View</td></tr>
<tr><td>CMP Site2 Cluster (S)</td><td>CMP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

</td></tr>
<tr><td>3. □</td><td>Verify basic network connectivity and server health.</td><td>

1. From the active server of site 2 CMP (Promote server), ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.

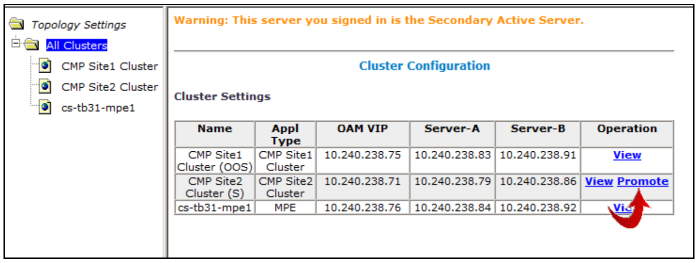
```
# ping <XMI or OAM gateway address>
```

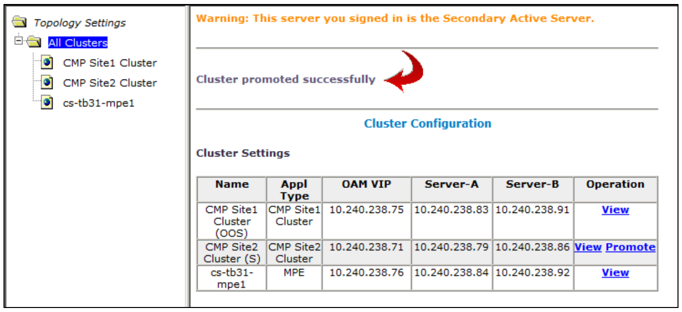
2. Run the **syscheck** command. Verify that all tests return successfully. If errors occur, discontinue this procedure and contact My Oracle Support.



```
[root@ohio-cmp-1b ~]# 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@ohio-cmp-1b ~]#
```

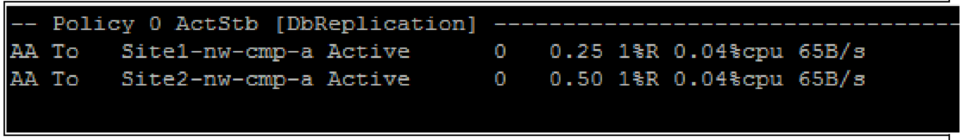
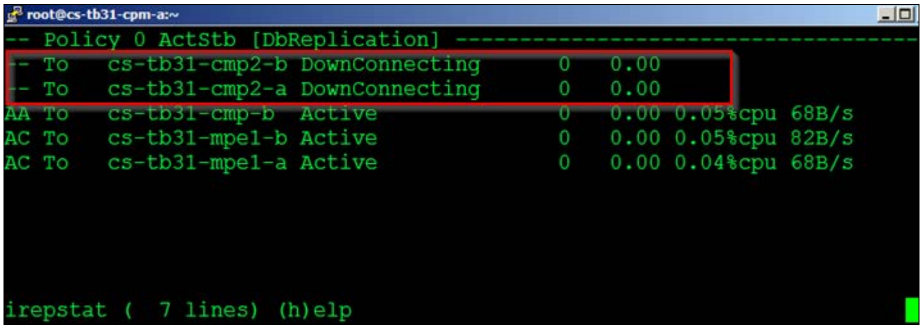
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>4. □</td><td>Promote secondary CMP cluster</td><td>1. In the CMP GUI, navigate to <b>Platform Setting → Topology Setting → All Clusters</b>
2. Click <b>Promote</b> for the secondary server.
3. Clicking <b>OK</b>.


Warning: This server you signed in is the Secondary Active Server.
Cluster Configuration
Cluster Settings
<table>
<tr><th>Name</th><th>Appl Type</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Operation</th></tr>
<tr><td>CMP Site1 Cluster (OOS)</td><td>CMP Site1 Cluster</td><td>10.240.238.75</td><td>10.240.238.83</td><td>10.240.238.91</td><td>View</td></tr>
<tr><td>CMP Site2 Cluster (S)</td><td>CMP Site2 Cluster</td><td>10.240.238.71</td><td>10.240.238.79</td><td>10.240.238.86</td><td>View Promote</td></tr>
<tr><td>cs-tb31-mpe1</td><td>MPE</td><td>10.240.238.76</td><td>10.240.238.84</td><td>10.240.238.92</td><td>Vie</td></tr>
</table>
You should see a message appear above the Cluster Configuration heading that indicates the successful promotion (see example below). If not, retry the operation and/or contact My Oracle Support.


Warning: This server you signed in is the Secondary Active Server.
Cluster promoted successfully
Cluster Configuration
Cluster Settings
<table>
<tr><th>Name</th><th>Appl Type</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Operation</th></tr>
<tr><td>CMP Site1 Cluster (OOS)</td><td>CMP Site1 Cluster</td><td>10.240.238.75</td><td>10.240.238.83</td><td>10.240.238.91</td><td>View</td></tr>
<tr><td>CMP Site2 Cluster (S)</td><td>CMP Site2 Cluster</td><td>10.240.238.71</td><td>10.240.238.79</td><td>10.240.238.86</td><td>View Promote</td></tr>
<tr><td>cs-tb31-mpe1</td><td>MPE</td><td>10.240.238.76</td><td>10.240.238.84</td><td>10.240.238.92</td><td>View</td></tr>
</table></td></tr>
<tr><td>5. □</td><td>Logout of the CMP GUI</td><td>Logout of the CMP GUI by clicking the <b>Logout</b> link or closing the browser window.</td></tr>
<tr><td>6. □</td><td>Verify operation via CMP GUI</td><td>1. Login to the CMP GUI using the VIP of CMP Site2.
2. In the CMP GUI, navigate to <b>Platform Setting → Topology Setting → All Clusters</b>
3. Verify that all clusters are performing as expected.
4. Follow the procedures in this document to bring the other failed servers/clusters back online.</td></tr>
<tr><td>7. □</td><td>SSH to active node of the promoted cluster</td><td><b>For c-Class System</b>
SSH session from PM&C to new server, using the <b>PM&C GUI → Software → Software Inventory</b> to obtain the IP address for the server:
ssh admusr@<node_IP_Address>
$ sudo su -
<b>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System</b>
Use the iLO/iLOM (for Oracle hardware Oracle X5-2 and Netra X5-2) to login, and start a remote console session to run commands.</td></tr>
</table>

Step	Procedure	Details

8. □	Verify **irepstat** output shows expected status	From the SSH session from PM&C to the active node of the promoted CMP cluster, run the **irepstat** command to verify that cluster replication is Active. If not Active after 5 minutes, check the CMP GUI for any active alarms.
		`# irepstat`
		
		`-- Policy 0 ActStb [DbReplication] -----------------------------------`
		`AA To   Site1-nw-cmp-a Active      0   0.25 1%R 0.04%cpu 65B/s`
		`AA To   Site2-nw-cmp-a Active      0   0.50 1%R 0.04%cpu 65B/s`
		The status of all clusters except known failed servers should have a status of Active as in the above figure.
		Otherwise if any of the replication paths show `DownConnecting`, as shown in the figure, contact My Oracle Support.
		The example shown below shows our installation with servers cs-tb31-cmp2-a and cs-tb31-cmp2-b failed, while all other cluster replication is working properly.
		
		root@cs-tb31-cpm-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-mpe1-b Active              0   0.00 0.05%cpu 82B/s`
		`AC To   cs-tb31-mpe1-a Active              0   0.00 0.04%cpu 68B/s`
		`irepstat (  7 lines)  (h)elp`

9. □	Rebuild failed CMP cluster	Refer to Procedure 6: Restoring complete cluster without the server backup to rebuild failed CMP cluster.
		---End of Procedure---

APPENDIX A. CONTACTING ORACLE

Disaster recovery activities may require real-time assessment by Oracle Engineering to determine the best course of action. You can contact the Oracle Customer Access Support for assistance if an enclosure FRU is requested.

A.1 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) at https://support.oracle.com/
- Phone: +1.800.223.1711 (toll-free in the US), or retrieve your local hotline number from Oracle Global Customer Support Center at http://www.oracle.com/support/contact.html

  Make the following selections on the Support telephone menu:

  a. Select **2** for New Service Request.

  d. Select **3** for Hardware, Networking, and Solaris Operating System Support.

  - If you are an existing customer, select **1** for Technical Issues. When speaking to the agent, indicate that you are an existing customer.

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

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

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

A.2 Emergency Response

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

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

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

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

APPENDIX B. RECOVERY OF THIRD PARTY COMPONENTS

Refer *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