

# Oracle® Communications

---

## Disaster Recovery

# Policy Management Disaster Recovery Guide Release 12.6.1

F47282-02

April 2022



**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 before 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 performed for the recovery.

**\*\*\* WARNING \*\*\***

**Note:** Disaster Recovery is an exercise that requires collaboration of multiple groups and is expected to be coordinated by the Technical Assistance Center (TAC) prime. Based on the assessment of the disaster by TAC, it may be necessary to deviate from the documented process.

EMAIL: [support@oracle.com](mailto:support@oracle.com)



Oracle Communications Policy Management Disaster Recovery for Release 12.6.1  
Copyright © 2013, 2022 Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

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

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



## Table of Contents

|   |           |
|---|-----------|
| <b>1. INTRODUCTION.....</b>   | <b>7</b>  |
| 1.1 Purpose and Scope .....   | 7         |
| 1.2 References .....  | 7         |
| 1.3 Acronyms .....  | 7         |
| 1.4 Logins and Passwords .....  | 8         |
| 1.5 Software Release Numbering .....  | 8         |
| 1.6 Terminology.....  | 8         |
| <b>2. GENERAL DESCRIPTION .....</b>   | <b>9</b>  |
| 2.1 Single Node Outage MRA/MPE/Mediation/CMP, with CMP Server Available .....   | 9         |
| 2.2 Recovery of Complete MRA/MPE/Mediation Cluster, with CMP Server Available .....                                   | 9         |
| 2.3 Recovery of the CMP Cluster when a Georedundant CMP Does Not Exist .....  | 9         |
| 2.4 Recovery of the CMP Cluster when a Georedundant CMP (DR-CMP) is Available .....                                   | 10        |
| 2.5 Complete Server Outage (All servers) .....  | 10        |
| 2.6 Performing Initial Configuration.....   | 10        |
| 2.7 Using the Server Backup File .....  | 10        |
| 2.8 Using the System Restore File .....   | 11        |
| 2.9 PM&C Usage.....   | 11        |
| <b>3. PROCEDURE OVERVIEW .....</b>  | <b>12</b> |
| <b>4. PROCEDURE PREPARATION.....</b>  | <b>14</b> |
| 4.1 Purpose and Scope .....   | 14        |
| 4.2 Recovery Scenarios .....  | 14        |
| 4.2.1 Recovery Scenario 1 (Partial Cluster Outage with Primary CMP Server Available).....                             | 14        |
| 4.2.2 Recovery Scenario 2 (Partial Cluster Outage with Georedundant CMP Server Available).....                        | 16        |
| 4.2.3 Recovery Scenario 3 (Full Cluster Outage of the CMP; Georedundancy Not Available; Other Servers as Needed)..... | 17        |
| <b>5. RESTORE PROCEDURES.....</b>   | <b>19</b> |
| 5.1 Procedure 1: Restore Standby CMP Node Using the Server Backup File.....   | 19        |
| 5.2 Procedure 2: Restore Standby CMP Node without Using the Server Backup File.....                                   | 24        |
| 5.3 Procedure 3: Restore Single MPE/MRA/Mediation Node Using the Server Backup File .....                             | 29        |
| 5.4 Procedure 4: Restore Single MPE/MRA/Mediation Node without Server Backup File.....                                | 35        |



|   |           |
|---|-----------|
| 5.5 Procedure 5: Restoring Complete Cluster Using Server Backup Files .....       | 40        |
| 5.6 Procedure 6: Restoring Complete Cluster without Using the Server Backup ..... | 49        |
| 5.7 Procedure 7: Restoring CMP Cluster Using the Available System Backup .....    | 57        |
| 5.8 Procedure 8: Promoting Georedundant CMP Cluster .....                         | 64        |
| <b>APPENDIX A. CONTACTING ORACLE.....</b>   | <b>68</b> |
| <b>APPENDIX B. RECOVERY OF THIRD PARTY COMPONENTS .....</b>                       | <b>69</b> |



## List of Tables

|                            |   |
|----------------------------|---|
| Table 1: Acronyms.....     | 7 |
| Table 2. Terminology ..... | 8 |



## List of Procedures

|   |    |
|---|----|
| Procedure 1 Restore standby CMP Node with server backup file .....                | 19 |
| Procedure 2 Restore standby CMP Node without server backup file .....             | 25 |
| Procedure 3 Restore single MPE/MRA/Mediation node with server backup file .....   | 30 |
| Procedure 4 Restore single MPE/MRA/Mediation node without server backup file..... | 36 |
| Procedure 5 Restoring complete cluster with the server backup files.....          | 41 |
| Procedure 6 Restoring complete cluster without the server backup.....             | 50 |
| Procedure 7 Restoring CMP cluster with system backup available .....              | 58 |
| Procedure 8 Promoting georedundant CMP cluster .....                              | 64 |



# 1. INTRODUCTION

## 1.1 Purpose and Scope

This document is a guide to describe procedures used to perform disaster recovery for Policy Management System, Release 12.5. This includes recovery of partial or a complete loss of one or more policy servers and policy components. This document provides step-by-step instructions to perform disaster recovery for Policy Management Systems. Executing this procedure also involves referring to and executing procedures in existing support documents.

## 1.2 References

- [1] E67765 Oracle Firmware Upgrade Release Notes, Release 3.1.5
- [2] E67825 Oracle Firmware Upgrade Pack Upgrade Guide, Release 3.1.5
- [3] E70315 Oracle Firmware Upgrade Release Notes, Release 3.1.6
- [4] E70316 Oracle Firmware Upgrade Pack Upgrade Guide, Release 3.1.6
- [5] E76846 HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.10
- [6] E64917 HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.9
- [7] E54387 PM&C Incremental Upgrade, current revision
- [8] E56282 TVOE 3.2 Disaster Recovery Procedure, Release 7.2, current revision
- [9] E53486 Tekelec Platform 7.0.x Configuration Procedure Reference, current revision
- [10] E54388-02 PM&C Disaster Recovery, Release 6.0
- [11] E67647 PM&C Disaster Recovery, Release 6.2
- [12] E53487 PM&C 6.2 Incremental Upgrade Procedure, current revision
- [13] E72270 Mediation Server User's Guide, Release 12.2
- [14] E82615-01 Oracle Communications Policy Management 12.2 Installation Procedure
- [15] E89552-01 Policy Management 12.4 Disaster Recovery\_Final.docx

These documents are available on the [Oracle Help Center](#).

**Note:** The HP Solutions firmware upgrade pack is provided if you 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     | ISO is taken from the ISO 9660 file system used with CD-ROM media, but an ISO image might also contain a UDF (ISO/IEC 13346) file system |
| c-Class | HP marketing term for their enterprise blade server platform   |
| CMP     | Configuration Management Platform  |
| DR-CMP  | Configuration Management Product for Disaster Recovery<br><b>NOTE:</b> It refers to the CMP on the secondary site                        |
| DVD     | Digital Video Disc   |
| GRUB    | Grand Unified Boot loader  |
| iLO     | Integrated Lights-Out  |
| IPM     | Initial Product Manufacture—The process of installing TPD on a hardware platform   |



| Acronym | Meaning                                      |
|---------|--|
| MPE     | Multiprotocol Policy Engine                  |
| MRA     | Multiprotocol Routing Agent                  |
| OS      | Operating System (for example, TPD)          |
| PM&C    | Platform Management and 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 the standard passwords for root, admusr, admin, and other standard logins referenced in this procedure. Note that using SSH to Policy servers as the root user is restricted, but is allowed using admusr user. These passwords are not included in this document.

## 1.5 Software Release Numbering

This guide applies to all Policy Management versions 12.5. It is assumed that PM&C Version 6.0.3 or above has been previously installed, configured in this deployment and in working condition, that is 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                          | Definition  |
|-------------------------------|---|
| 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).   |
| 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 return to normal operation and requires intrusive activities to re-install the software and/or hardware. |
| Perform Initial Configuration | The Perform Initial Configuration is added to the policy server through the platcfg utility. This configuration brings the network interface for the server online and enables management and configuration from the CMP  |



## 2. GENERAL DESCRIPTION

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

- Recovery of one or more servers with at least one CMP server intact
  - o 1 or more CMP servers (this can include GeoRedundant CMP (DR-CMP) servers)
  - o 1 or more MPE/MRA/Mediation servers failed
- Recovery of the entire network from a total outage
 

CMP servers are not available (neither primary, nor secondary) and other MPE, MRA, and Mediation servers are recovered

The existence of a georedundant system, including a georedundant CMP (DR-CMP), can mitigate massive outages by providing a running manager from which to synchronize the system as it is being 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 restored.

### NOTES:

- For disaster recovery of the PM&C server release 6.0 (E54388) or disaster recovery of the PM&C server release 6.2 (E67647), see Procedure 5: Post-Restoration Verification for Aggregate Switches, refer to Appendix A.
- Field Replacement Unit (FRU server) are deployed as type MPE, MRA, Mediation, or CMP. The FRU is required to physically replace the failed server, the cables for the server are connected to the same as the failed one.

### 2.1 Single Node Outage MRA/MPE/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. Perform initial configuration information is 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 to recover one server of a MRA/Mediation/MPE cluster or one server of a CMP cluster. The SSH exchange keys with cluster mate from active CMP is also required.

### 2.2 Recovery of Complete MRA/MPE/Mediation Cluster, with CMP Server Available

The failure of a complete cluster is recovered by replacing all nodes of the cluster. All nodes are recovered using base recovery of hardware and software. Perform initial configuration information are 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 cluster.

### 2.3 Recovery of the CMP Cluster when a Georedundant CMP Does Not Exist

The complete failure of the CMP requires re-installation using base recovery of hardware and software. Perform initial configuration information is 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 in order to recover application level configuration including policies and configuration of the MPE/MRA/Mediation clusters in the network.



## 2.4 Recovery of the CMP Cluster when a Georedundant CMP (DR-CMP) is Available

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

## 2.5 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 georedundant CMP is not 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 before the outage). If a backup file is not available, the only option is to rebuild the network from scratch. The network data is reconstructed from whatever sources are available, including entering all data manually.

## 2.6 Performing Initial Configuration

The information required for initial configuration is not extensive, and is readily available from site documents, or from the topology configuration for the CMP. In some cases it is easier to manually enter the initial configuration using the platcfg utility 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.

## 2.7 Using the Server Backup File

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

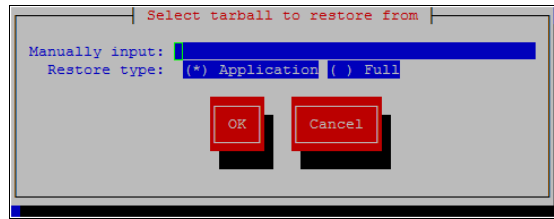


You must enter the complete path and filename in order to restore from a file that is not in the `/var/camiant/backup/local-archive/serverbackup` directory.



## 2.8 Using the System Restore File

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



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

## 2.9 PM&C Usage

When working with a c-Class enclosure, the PM&C establishes connectivity with DHCP to the blades in the enclosure. This allows the PM&C to act as your central contact point in the work on a c-Class system. It is a staging point for restoration files sent to c-Class blades 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.

#### Disaster recovery strategy

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

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 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. Perform appropriate recovery procedures.

#### Required materials

The following items are needed for disaster recovery:

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

#### Policy server backup

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

- Server Backup

There is one server configuration backup for each server in the system. The server backup is a Back-up of the OS information unique to the server. Information includes hostname, IP Addresses, NTP, DNS, Static Route configuration. This operation creates a server configuration Backup file, and is run on each of the servers in the network.

- System Backup

There is one Application Configuration backup for the Policy system. The system backup gathers PCRF configuration information that is unique to this system. Information such as:



Topology, Policys, 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 network when the CMP is not available.



## 4. PROCEDURE PREPARATION

### 4.1 Purpose and Scope

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. The first step is to evaluate the failure scenario and determine the procedures that are required to restore operations. A series of procedures are included that are 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 return 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 the version of TPD installed.
3. Load application for corresponding server HW types.
4. Check FW versions and upgraded if necessary.
5. Check NTP status after recovery.
6. Check active alarms from GUI and both syscheck the alarmMgr and alarmStatus from CLI.

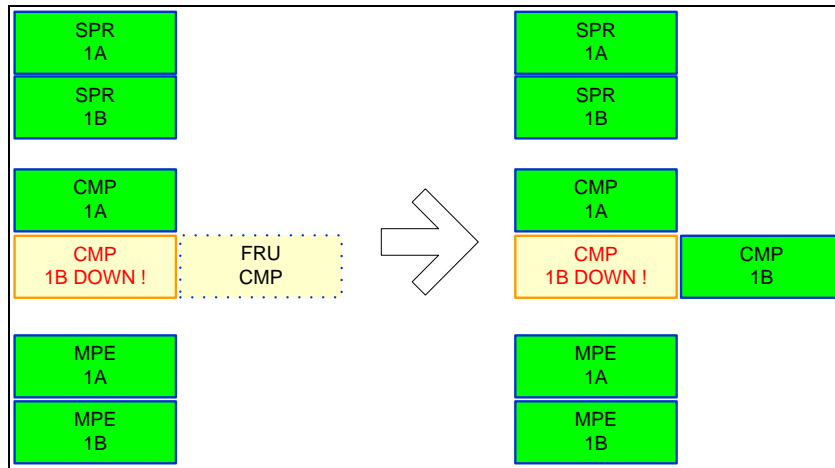
### 4.2 Recovery Scenarios

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

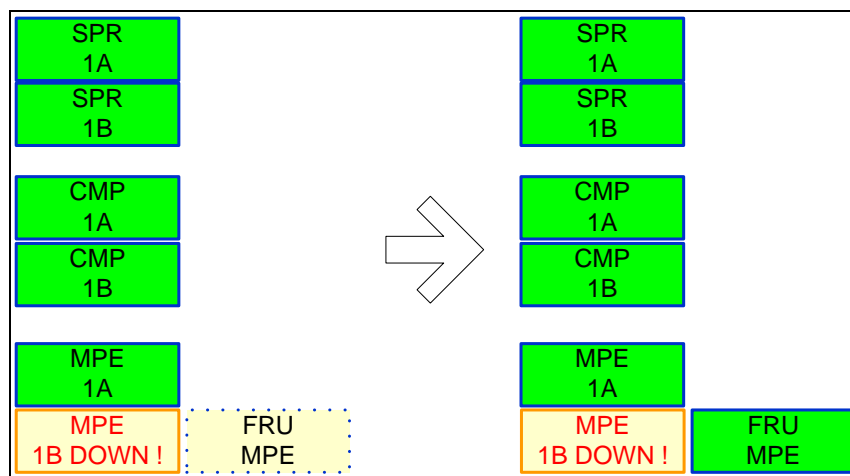
For a partial outage with a CMP server available, only base recovery of hardware and software and initial Policy configuration is needed. A single CMP server is capable of restoring the configuration database via replication to all MPE/MRA/Mediation servers, or to the other CMP node of a cluster. The major activities are summarized in the following list. Use this list to understand the recovery procedure summary. Do not use this list to perform the procedure. The detailed steps for the procedures 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.
  - o Recover the base hardware.
  - o Recover the software.
  - o Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - o 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 configuration is re-installed, either through the platcfg menu, or from the server backup file
  - The configuration database is available at the active CMP server and does not require restoration on the CMP. Configuration is pushed from the CMP to the MPE/MRA/Mediation servers using re-apply configuration



Follow the procedure for your specific needs.

- Use [Procedure 2: Restore Standby CMP Node without Using the Server Backup File](#)  
Or [Procedure 1: Restore Standby CMP Node Using the 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 4: Restore Single MPE/MRA/Mediation Node without [Server Backup File](#)
- Use [Procedure 5: Restoring Complete Cluster Using Server Backup Files](#)  
Or [Procedure 6: Restoring Complete Cluster without Using the Server Backup](#) to recover complete MPE/MRA/Mediation clusters that have gone down.
- Use [Procedure 7: Restoring CMP Cluster Using the Available System Backup files](#) to recover the first of 2 nodes in CMP cluster



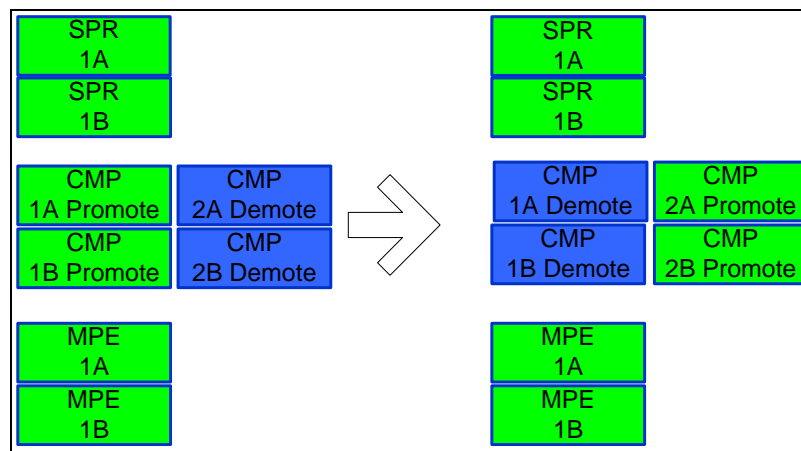
Use [Procedure 4: Restore Single MPE/MRA/Mediation Node without Server Backup File](#) to recover the second node of MPE/MRA/Mediation cluster.

#### 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 is manually promoted to Primary status as the controlling CMP for the policy network. Then base recovery of hardware and software and initial Policy configuration is needed. The 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. Use these procedures to understand the recovery procedure summary. Do not use this list to perform the procedure. The detailed steps for the procedures are in the [Restore Procedures](#) section. The major activities are summarized as follows:

1. Promote the georedundant CMP server.

This step is performed by logging into the OAM VIP address of the second site CMP cluster. Use [Procedure 7 Restoring CMP cluster with system backup available](#).



This is done only if the Primary CMP cluster is restored. If the cluster is an MRA, Mediation, or MPE cluster, do not promote the georedundant CMP.

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

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

Go to each procedure for detailed steps.

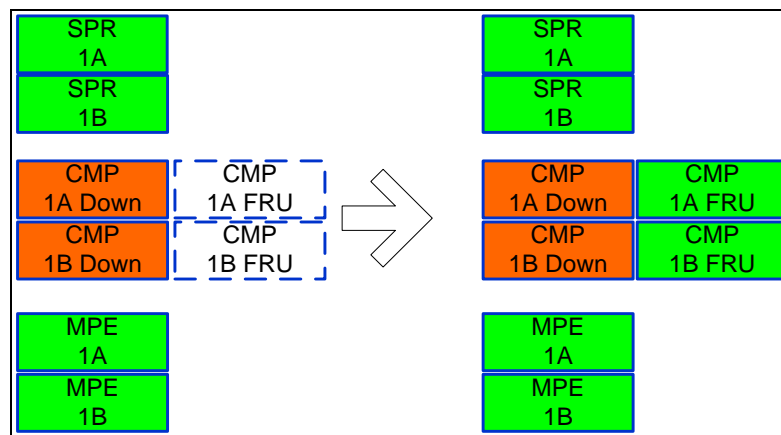
1. Use [Procedure 8: Promoting Georedundant CMP Cluster](#) to promote the georedundant CMP



2. 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 4: Restore Single MPE/MRA/Mediation Node](#) without Server Backup File
3. Use [Procedure 5: Restoring Complete Cluster Using Server Backup Files](#)  
Or [Procedure 6: Restoring Complete Cluster without Using the Server Backup](#) to recover complete MPE, MRA, and Mediation clusters that are down.
4. Use [Procedure 5: Restoring Complete Cluster Using Server Backup Files](#)  
Or [Procedure 6: Restoring Complete Cluster without Using the Server Backup](#) to recover the secondary site CMP. Recovery of the secondary site CMP is completed late in the process because the active CMP can handle all application level configuration as the network is brought back online.
5. Use [Procedure 7: Restoring CMP Cluster Using the Available System Backup](#) files to recover the first of 2 nodes in CMP cluster
6. Use [Procedure 4: Restore Single MPE/MRA/Mediation Node without 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 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. Use this list to understand the recovery procedure summary. Do not use this list to perform the procedure. The detailed steps for the procedure are in the [Restore Procedures](#) section. The major activities are summarized as follows:



- Recover one Primary CMP server (if necessary) by recovering base hardware and software.
  - o Recover the base hardware.
  - o Recover the software.
  - o Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file.
  - o The database of the CMP is restored from a system backup.
  - o If a system backup is not available, use the 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 is good) to verify that the re-entered data on the CMPs matches the previous



configuration that was in-use. Also, check with engineering team for possible approach to verify if the data at the operational MPEs matches the data that has been re-entered at the CMP after re-entering the Policies and other application level data to the CMP.

- Recover the second CMP server by recovering base hardware and software.
  - o Recover the base hardware.
  - o Recover the software.
  - o Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - o The configuration database is available on the active CMP server and does not require restoration on the second CMP node. Configuration is replicated when the two CMP nodes form a cluster.
- Recover any failed MPE/MRA/Mediation servers by recovering base hardware and software.
  - o Recover the base hardware.
  - o Recover the software.
  - o Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - o The configuration database is available at the active CMP server and does not require restoration on the CMP. Configuration is pushed from the CMP to the MPE/MRA/Mediation servers.

Go to these procedures for detailed steps.

- Use [Procedure 7: Restoring CMP Cluster Using the Available System Backup](#) to recover the first of 2 nodes in the CMP cluster.
- Use [Procedure 2: Restore Standby CMP Node](#) 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 4: Restore Single MPE/MRA/Mediation Node without Server Backup File](#)
- Use [Procedure 5: Restoring Complete Cluster Using Server Backup Files](#)  
Or [Procedure 6: Restoring Complete Cluster without Using the Server Backup](#) to recover complete MPE, MRA, and Mediation clusters that are down.
- Use [Procedure 7: Restoring CMP Cluster Using the Available System Backup](#) files to recover the first of 2 nodes in CMP cluster  
Use [Procedure 4: Restore Single MPE/MRA/Mediation Node without Server Backup File](#) to recover the second node of MPE/MRA/Mediation cluster.



## 5. RESTORE PROCEDURES

### 5.1 Procedure 1: Restore Standby CMP Node Using the Server Backup File

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

#### Required resources:

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

#### Prerequisites:

1. Power down the failed server gracefully

**Note:** Access the iLO with Administrator privilege, then go to **Power Management → Server Power** and click **Momentary Press**

2. Remove failed hardware and replace.
3. Verify that the node has TPD on it, or install TPD
4. Install application software—CMP


**Note:** Refer to the *Policy Management Bare Metal Installation Guide* Release 12.5, the documents are available at the Oracle Help Center

This Procedure restores the standby CMP node when a server level backup is available.

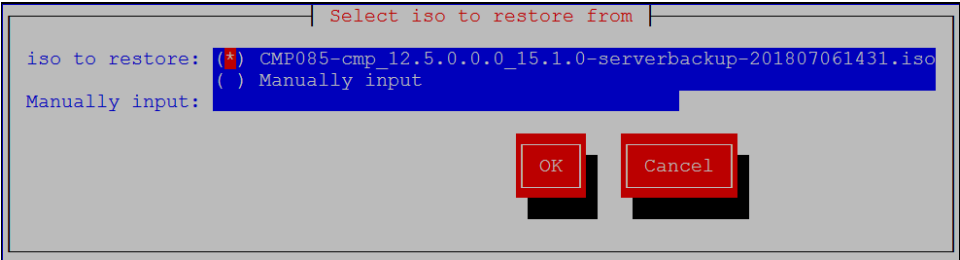

Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

#### Procedure 1 Restore standby CMP Node with server backup file

| Step                        | Procedure                             | Details  |
|-----------------------------|---------------------------------------|--|
| 1. <input type="checkbox"/> | Set the failed node to Forced Standby | <ol style="list-style-type: none"> <li>1. In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Settings → All Clusters</b></li> <li>2. Determine the cluster with the failed node</li> <li>3. Determine the failed node</li> <li>4. Click the <b>Modify Server-X</b> for the failed node</li> <li>5. Click the <b>Forced Standby</b> checkbox so that it is checked, then click <b>Save</b></li> </ol>  |

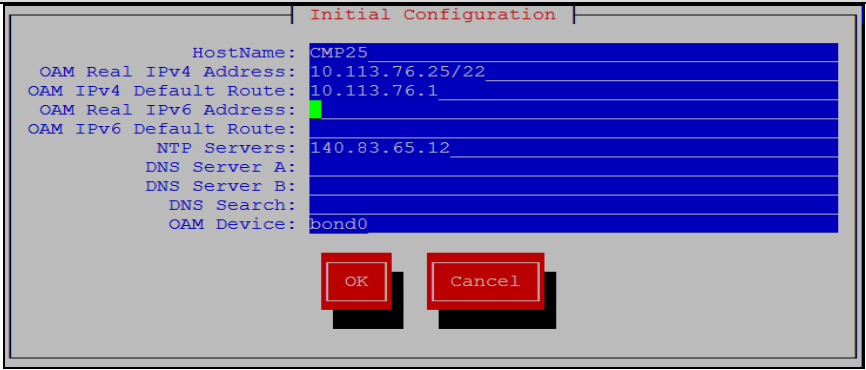
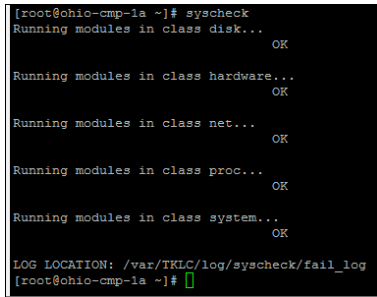


| Step                        | Procedure  | Details  |
|-----------------------------|--|--|
| 2. <input type="checkbox"/> | Load the ISO for server restore                              | <p>Obtain the <i>*serverbackup.iso*</i> for the restored node. When the replacement node is available (IPM/App installation complete), the server backup file is copied via secure copy (pscp, scp, or WinSCP) to the following directory:</p> <pre>/var/camiant/backup/local_archive/serverbackup</pre> <p><b>NOTE:</b> Later in this procedure, the platcfg restore function checks this directory and offers a convenient menu. The platcfg utility also allows the manual enter of any mounted path on the server.</p>   |
| 3. <input type="checkbox"/> | Login via SSH to the node                                    | <ul style="list-style-type: none"> <li>For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt;</pre> <pre>\$ sudo su -</pre> </li> <li>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul>                                    |
| 4. <input type="checkbox"/> | Perform platcfg restore from SSH session to replacement node | <ol style="list-style-type: none"> <li>Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>Navigate to:<br/> <b>Policy Configuration → Backup and Restore → Server Restore</b> </li> <li>Select the <i>*serverbackup*.ISO</i> that you just put on the system and click <b>OK</b>.</li> <li>Click <b>Yes</b> to confirm.</li> </ol>   |
| 5. <input type="checkbox"/> | Verify the status  | A window opens indicating that the restore operation is 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 <a href="#">My Oracle Support</a> or engineering team for assistance.   |
| 6. <input type="checkbox"/> | Perform Initial configuration                                | <ol style="list-style-type: none"> <li>Click <b>Exit</b> until you return to the Main Menu of the platcfg utility.</li> <li>Navigate to:<br/> <b>Policy Configuration → Verify Initial Configuration</b> </li> </ol>   |

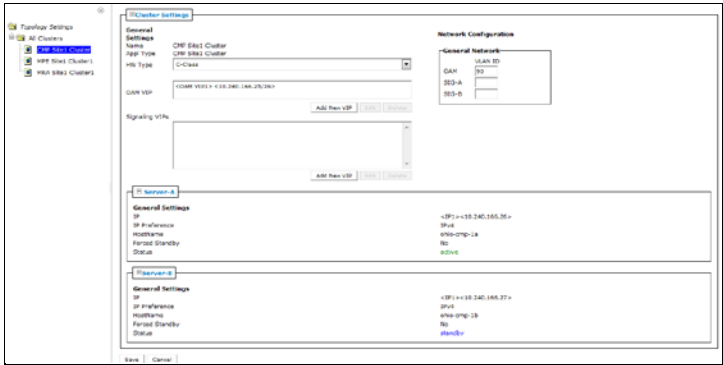
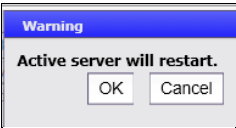
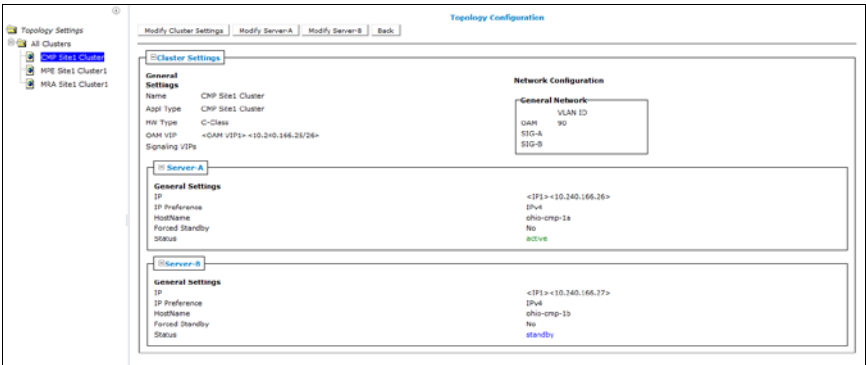


| Step | Procedure | Details   |
|------|-----------|---|
|      |           | <div><div>Copyright (C) 2002, 2010, Oracle and/or its affiliates. All rights reserved.<br/>Hostname: CMP085<br/>Date/Time: 07/06/2018 14:36:41<br/>Hardware Type: KVM<br/>DNS Search: ""<br/>DNSServerA: ""<br/>DNSServerB: ""<br/>DefaultGw: "10.11.0.1"<br/>DefaultIPv6Gw: ""<br/>Device: "eth0"<br/>HostName: "CMP085"<br/>LayoutProfile: "cloudinit"<br/>NtpServIpAddr: "10.11.0.26"<br/>OAMDevice: "eth0"<br/>OAMMTU: "1450"<br/>SIGDevice: "eth4"<br/>SIGAMTU: "1450"<br/>SIGBDevice: "eth2"<br/>SIGBMTU: "1450"<br/>SIGCDevice: "eth3"<br/>ServIpAddr: "10.11.0.85/16"<br/>ServIPv6Addr: ""<br/>NTP Status:<br/>remote refid st t when poll reach delay offset jitter<br/>*10.11.0.26 10.210.60.196 2 u 184 1024 377 2.708 -0.297 0.457</div><div>ForwardBackwardTopBottomExit</div><div>Use arrow keys to move between options   &lt;Enter&gt; selects</div></div> <div>3. If the configuration does not exist, navigate to the Perform Initial Configuration page and enter the hostname, OAM IP, and configuration.</div> <div>For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)</div> <div><div>Initial Configuration</div><div>HostName: CMP169-152<br/>OAM Real IPv4 Address: 10.75.169.152/25<br/>OAM IPv4 Default Route: 10.75.169.129<br/>OAM Real IPv6 Address:<br/>OAM IPv6 Default Route:<br/>NTP Servers: 10.250.32.10<br/>DNS Server A:<br/>DNS Server B:<br/>DNS Search:<br/>OAM Device: bond0<br/>OAM VLAN: 22<br/>SIGA VLAN: 23<br/>SIGB VLAN: 6<br/>SIGC VLAN: 7</div><div>OKCancel</div></div> <div>4. Ensure that your data is correct, and click <b>OK</b>.</div> <div>5. Click <b>Yes</b> to save and apply.</div> <div>6. Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</div> <div>For RMS (DL360/DL380):</div> <div>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</div> |



| Step                        | Procedure  | Details  |
|-----------------------------|--|--|
|                             |  |    |
| 7. <input type="checkbox"/> | Reboot the server                                    | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>   |
| 8. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>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.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol>  |



| Step                         | Procedure   | Details  |
|------------------------------|---|--|
| 9. <input type="checkbox"/>  | Remove the Forced Standby designation on the blade. | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Settings → All Clusters → &lt;Current Cluster&gt;</b></li> <li>Click modify for the server that is in Forced Standby.</li> <li>Clear the <b>Forced Standby</b> checkbox</li> <li>Click <b>Save</b></li> </ol>  <ol style="list-style-type: none"> <li>Accept the warning message by clicking <b>OK</b>.</li> </ol>  |
| 10. <input type="checkbox"/> | Verify cluster status                               | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Settings → All Clusters → &lt;Current Cluster&gt;</b></li> <li>Monitor the clustering of the node to its peer. Do not proceed until both nodes have a status of either Active or Standby, and that there are not any CMP related active alarms.</li> </ol>    |



| Step                         | Procedure  | Details  |
|------------------------------|--|--|
| 11. <input type="checkbox"/> | Alternative method to check replication status                         | <p>You can monitor the clustering of the blade from the shell on the primary node using the <b>irepstat</b> command. To do so, SSH to the active node of the cluster and run the <b>irepstat</b> command:</p> <pre># irepstat</pre> <p>Expected irepstat output while waiting reconnection:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AC To  ocpm-12r1-brbg-g6-mpe-a  Active    0    0.50 1%R 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mpe-b  Active    0    0.25 1%R 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-a  Active    0    0.50 1%R 0.04%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-b  Active    0    0.25 1%R 0.05%cpu 85B/s</pre> <p>Expected irepstat output after cluster has formed:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AA To  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> |
| 12. <input type="checkbox"/> | Exchange keys with cluster mate(This step need to run from active CMP) | <p>Exchanging SSH keys Utility</p> <ul style="list-style-type: none"> <li>As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code></li> <li>As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code></li> </ul> <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>  |
| ---End of Procedure---       |  |  |

## 5.2 Procedure 2: Restore Standby CMP Node without Using the Server Backup File

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

### Required resources:

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

### Prerequisites:

- Power down the failed server gracefully

**Note:** Access the iLO with administrator privilege, then go to **Power Management** → **Server Power** and click **Momentary Press**

- Remove failed hardware and replace.



3. Verify that the node has TPD on it, or install TPD
4. Install application software—CMP

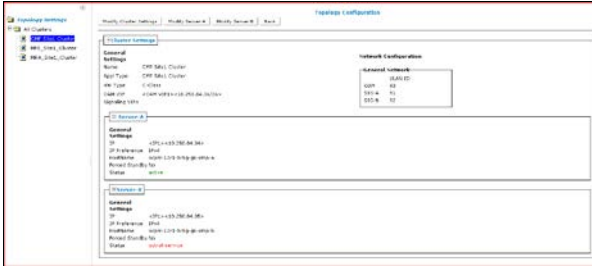
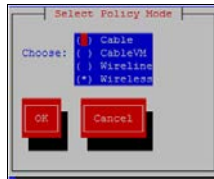
**Note:** Refer to the *Policy Management Bare Metal Installation Guide* Release 12.5, the documents are available at the Oracle Help Center

This Procedure restores the standby CMP node when a server level backup file is not available.

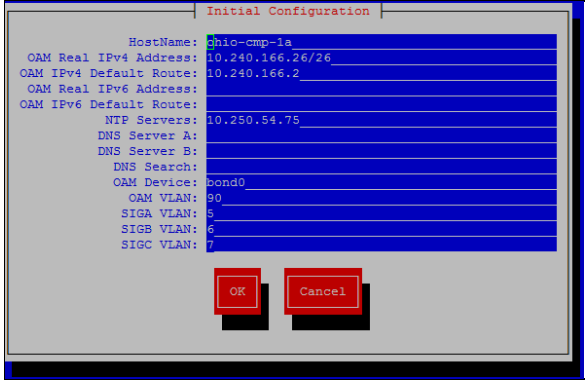
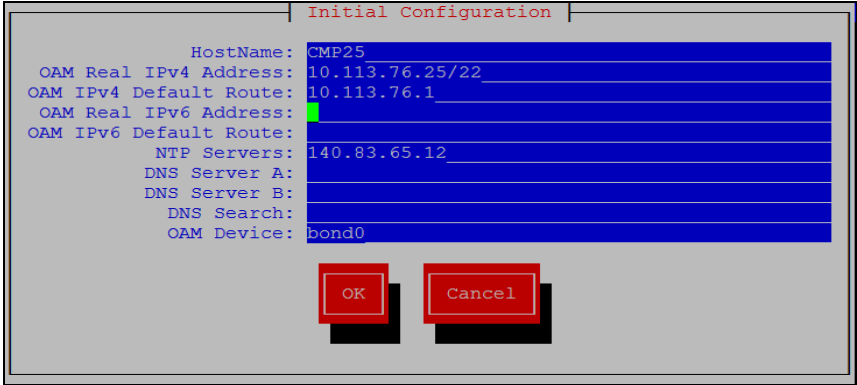
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

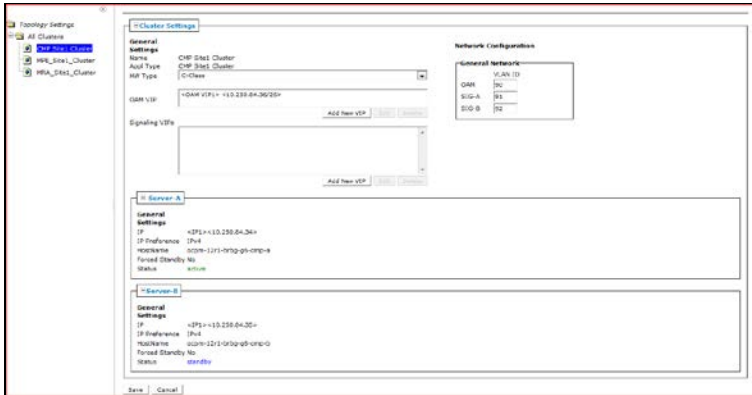
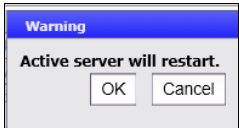
#### Procedure 2 Restore standby CMP Node without server backup file

| Step                        | Procedure   | Details   |
|-----------------------------|---|---|
| 1. <input type="checkbox"/> | Set the failed node to Forced Standby   | <ol style="list-style-type: none"> <li>1. In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Setting → All Clusters</b></li> <li>2. Determine the cluster with the failed node</li> <li>3. Determine the failed node</li> <li>4. Click the <b>Modify Server-X</b> for the failed node</li> <li>5. Click the <b>Forced Standby</b> checkbox so that it is checked, then click Save</li> </ol>  <p><b>NOTE:</b> The Network Configuration/General Network(VLAN ID) does not display for RMS (DL360/DL380) Hardware.</p> |
| 2. <input type="checkbox"/> | Login via SSH to the node   | <ul style="list-style-type: none"> <li>• For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt; \$ sudo su -</pre> </li> <li>• For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul>   |
| 3. <input type="checkbox"/> | Perform platcfg restore from SSH session to replacement node<br><br>Perform Initial configuration | <ol style="list-style-type: none"> <li>1. Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>2. Navigate to:<br/><b>Policy Configuration → Set Policy Mode</b></li> </ol>  <ol style="list-style-type: none"> <li>3. Leave the mode as <b>Wireless</b> and click <b>OK</b> to continue. You can skip this step.</li> <li>4. Navigate to:</li> </ol>   |

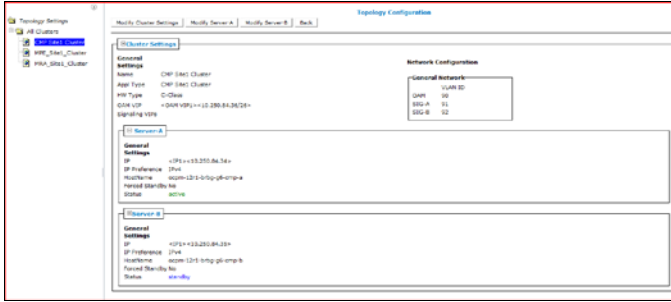
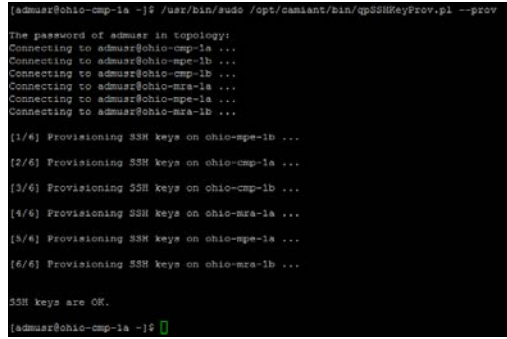


| Step                        | Procedure         | Details   |
|-----------------------------|-------------------|---|
|                             |                   | <p><b>Policy Configuration → Perform Initial Configuration</b></p> <ol style="list-style-type: none"> <li>Enter the configuration details for this node.</li> <li>Verify that entries are correct, and click <b>OK</b> to continue.</li> <li>Accept the dialog that opens asking to apply the configuration.</li> <li>After the operation is complete, click <b>Exit</b> on each platcfg menu until you are returned to the shell.</li> </ol> <p><b>For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)</b></p>  <ol style="list-style-type: none"> <li>Verify that the information is correct, and click <b>OK</b>.</li> <li>Click <b>Yes</b> to save and apply.</li> <li>Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</li> </ol> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p>  |
| 4. <input type="checkbox"/> | Reboot the server | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>  |



| Step                        | Procedure  | Details   |
|-----------------------------|--|---|
| 5. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>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.<br/> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> </li> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.<br/> <pre>[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 ~]#</pre> </li> </ol> |
| 6. <input type="checkbox"/> | Remove the Forced Standby designation on the blade.  | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/> <b>Platform Setting → Topology Setting → &lt;Current_Cluster&gt;</b> </li> <li>Click modify for the server that is in Forced Standby.</li> <li>Clear the <b>Forced Standby</b> checkbox</li> <li>Click <b>Save</b></li> </ol>   |
|                             |  | <ol style="list-style-type: none"> <li>Accept the warning message by clicking <b>OK</b>.<br/>  </li> </ol>  |



| Step                        | Procedure  | Details  |
|-----------------------------|--|--|
| 7. <input type="checkbox"/> | Verify cluster status  | <p>1. In the CMP GUI, navigate to:</p> <p><b>Platform Setting → Topology Settings → All Clusters → &lt;Current CMP Cluster&gt;</b></p> <p>2. Monitor the clustering of the node to its peer. Do not proceed until both nodes have a status of either Active or Standby, and that there are not any CMP related active alarms.</p>    |
| 8. <input type="checkbox"/> | Alternative method to check replication status                         | <p>You can monitor the clustering of the blade from the shell on the primary node using the <b>irepstat</b> command. To do so, SSH to the active node of the cluster and run the <b>irepstat</b> command:</p> <pre># irepstat</pre> <p>Expected irepstat output while waiting reconnection:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AC To  ocpm-12r1-brbg-g6-mpe-a Active      0   0.50 1kR 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mpe-b Active      0   0.25 1kR 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-a Active      0   0.50 1kR 0.04%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-b Active      0   0.25 1kR 0.05%cpu 85B/s</pre> <p>Expected irepstat output after cluster has formed:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AA To  ohio-cmp-1b Active      0   0.25 1kR 0.07%cpu 79B/s AC To  ohio-mpe-1a Active      0   0.50 1kR 0.05%cpu 65B/s AC To  ohio-mpe-1b Active      0   0.25 1kR 0.07%cpu 78B/s AC To  ohio-mra-1a Active      0   0.50 1kR 0.05%cpu 65B/s AC To  ohio-mra-1b Active      0   0.25 1kR 0.07%cpu 79B/s</pre> |
| 9. <input type="checkbox"/> | Exchange keys with cluster mate(This step need to run from active CMP) | <p>Exchanging SSH keys Utility</p> <ul style="list-style-type: none"> <li>As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code></li> <li>As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code></li> </ul>    |
| ---End of Procedure---      |  |  |



### 5.3 Procedure 3: Restore Single MPE/MRA/Mediation Node Using the Server Backup File

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

**Required resources:**

- Replacement node hardware
- TPD installation ISO
- Policy APP installation ISO.
- \*serverbackup\*.ISO for the replacement node

**Prerequisites:**

1. Power down the failed server gracefully

**Note:** Access the iLO with Administrator privilege, then go to **Power Management → Server Power** and click **Momentary Press**

2. Remove failed hardware and replace.
3. Verify that the hardware had TPD on it, or install TPD
4. Install application software—MPE or MRA or Mediation

**Note:** Refer to the Policy Management Bare Metal Installation Guide Release 12.5, the documents are available at the Oracle Help Center

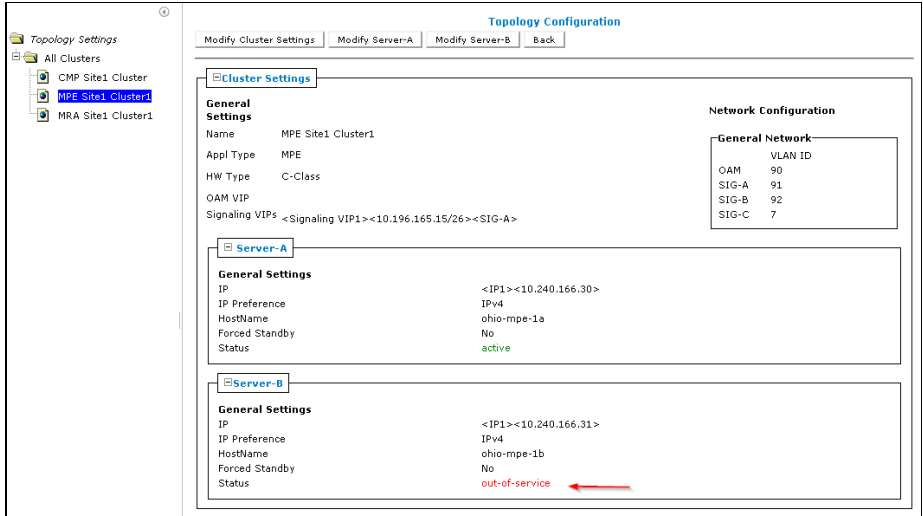


This procedure performs Restore single MPE/MRA/Mediation node with server backup file.

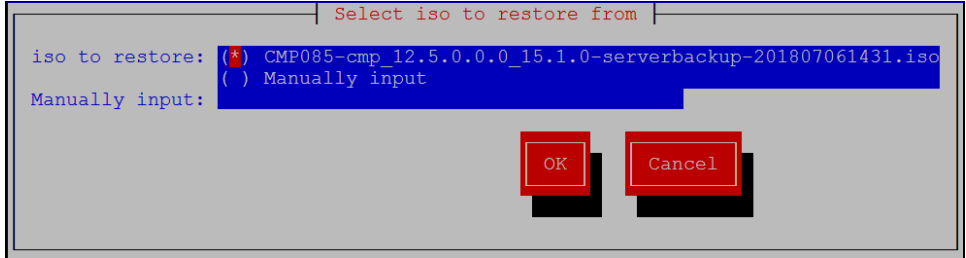
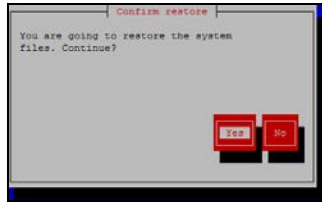

Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

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

| Step                        | Procedure                             | Details  |
|-----------------------------|---------------------------------------|--|
| 1. <input type="checkbox"/> | Set the failed node to Forced Standby | <p>1. In the CMP GUI, navigate to:<br/> <b>Platform Setting → Topology Setting → All Clusters</b></p> <p>2. Determine the cluster with the failed node</p> <p>3. Determine the failed node</p> <p>4. Click the <b>Modify Server-X</b> for the failed node</p> <p>5. Click the <b>Forced Standby</b> checkbox so that it is checked, then click Save</p>   |
| 2. <input type="checkbox"/> | Load the ISO for server backup        | <p>Obtain the *serverbackup.iso* for the restored node. When the replacement node is available (IPM/App installation complete), the server backup file is copied via secure copy (pscp, scp, or WinSCP) to the following directory:</p> <p style="text-align: center;">/var/camiant/backup/local_archive/serverbackup</p> <p><b>NOTE:</b> Later in this procedure, the platcfg restore function checks this directory and offers you a convenient menu to select from. The platcfg utility also allows you to manually enter any mounted path on the server.</p> |
| 3. <input type="checkbox"/> | Login via SSH to the node             | <ul style="list-style-type: none"> <li>For c-Class System:<br/> SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt;</pre> <pre>\$ sudo su -</pre> </li> <li>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:<br/> Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul>  |

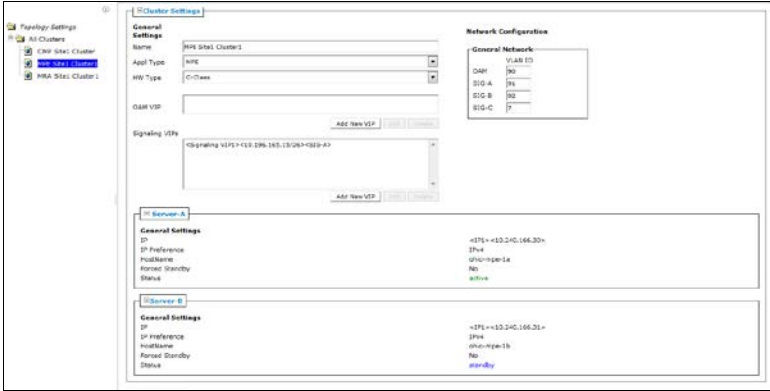
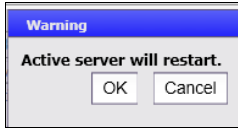


| Step                        | Procedure  | Details  |
|-----------------------------|--|--|
| 4. <input type="checkbox"/> | Perform platcfg restore from SSH session to replacement hardware | <ol style="list-style-type: none"> <li>Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>Navigate to:<br/> <b>Policy Configuration → Backup and Restore → Server Restore</b> </li> <li>Select the *serverbackup*.ISO that you just put on the system and click <b>OK</b>.</li> <li>Click <b>Yes</b> to confirm.</li> </ol>    |
| 5. <input type="checkbox"/> | Verify the status  | A window opens indicating that the restore operation is 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 <a href="#">My Oracle Support</a> or engineering team for assistance.  |
| 6. <input type="checkbox"/> | Perform Initial configuration                                    | <ol style="list-style-type: none"> <li>Click <b>Exit</b> on each platcfg menu until you are returned to the Main Menu of the platcfg utility.</li> <li>Navigate to:<br/> <b>Policy Configuration → Verify Initial Configuration</b> </li> </ol>  <ol style="list-style-type: none"> <li>If the configuration does not exist, navigate to <b>Perform Initial Configuration</b> and enter the initial configuration hostname, OAM IP, and NTP servers configurations.</li> </ol> <p><b>For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)</b></p> |


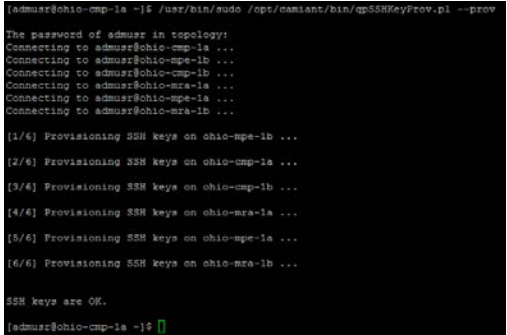


| Step                        | Procedure         | Details  |
|-----------------------------|-------------------|--|
|                             |                   | <div data-bbox="748 165 1289 512"> </div> <ol style="list-style-type: none"> <li>4. Ensure the information is correct.</li> <li>5. Click <b>OK</b> and then click <b>Yes</b> to save to apply</li> <li>6. Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</li> </ol> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p> <div data-bbox="620 833 1419 1176"> </div> |
| 9. <input type="checkbox"/> | Reboot the server | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>   |

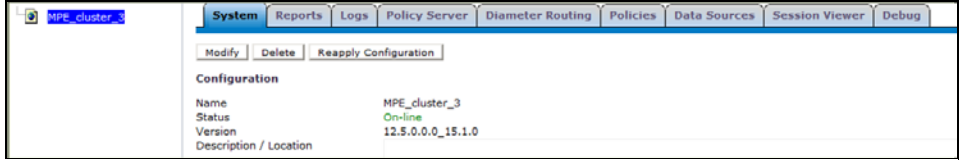


| Step                         | Procedure  | Details  |
|------------------------------|--|--|
| 10. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>From the installed server, ping the OAM/XMI gateway. If the ping is not successful, 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.<br/><br/># ping &lt;XMI or OAM gateway address&gt;</li> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol> <pre> [root@MPE168-131 admusr]# syscheck Running modules in class disk...                                 OK  Running modules in class hardware...                                 OK  Running modules in class net... *   ipbond: FAILURE:: MINOR::5000000000002000 -- Device Interface Warning *   ipbond: FAILURE:: Enslaved device eth02 is down One or more module in class "net" FAILED  Running modules in class proc...                                 OK  Running modules in class system...                                 OK  LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@MPE168-131 admusr]# </pre> |
| 11. <input type="checkbox"/> | Remove the Forced Standby designation on the blade.  | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Settings → All Clusters → &lt;Current Cluster&gt;</b></li> <li>Click modify for the server that is in Forced Standby.</li> <li>Clear the <b>Forced Standby</b> checkbox</li> <li>Click <b>Save</b></li> </ol>  <ol style="list-style-type: none"> <li>Accept the warning message by clicking <b>OK</b>.</li> </ol>    |



| Step                         | Procedure  | Details  |
|------------------------------|--|--|
| 12. <input type="checkbox"/> | Check status   | <ol style="list-style-type: none"> <li>In the CMP GUI, depending on the type of the blade, perform the following: <ul style="list-style-type: none"> <li>If this is an MPE node, navigate to:<br/><b>Policy Server → Configuration → All → &lt;Recovered MPE Cluster&gt; → Reports</b> tab</li> <li>If this is an MRA node, navigate to:<br/><b>MRA → Configuration → All → &lt;Recovered MRA Cluster&gt; → Reports</b> tab</li> <li>If this is an Mediation node, navigate to:<br/><b>Mediation → Configuration → All → &lt;Recovered Mediation Cluster&gt; → Reports</b> tab</li> </ul> </li> <li>Monitor clustering of the blade to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.</li> </ol>  |
| 13. <input type="checkbox"/> | Alternative method to check replication status                         | <p>You can monitor the clustering of the blade from the shell on the primary node using the <b>irepstat</b> command. To do so, SSH to the active node of the cluster and run the <b>irepstat</b> command:</p> <pre># irepstat</pre> <p>Expected irepstat output while waiting reconnection:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AC From ocpm-12r1-brbg-g6-cmp-a Active      0    0.25 ^0.04%cpu 45B/s  A=me</pre> <p>Expected irepstat output after cluster has formed:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AC From ocpm-12r1-brbg-g6-cmp-a Active      0    0.25 ^0.04%cpu 52B/s  A=C2488.184 CC From ocpm-12r1-brbg-g6-mpe-a Active      0    0.50 ^0.06 2.45%cpu 35B/s  A=C2488.184</pre>   |
| 14. <input type="checkbox"/> | Exchange keys with cluster mate(This step need to run from active CMP) | <p>Exchanging SSH keys Utility</p> <ul style="list-style-type: none"> <li>As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code></li> <li>As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code></li> </ul>    |



| Step                         | Procedure             | Details  |
|------------------------------|-----------------------|--|
| 15. <input type="checkbox"/> | Reapply Configuration | <p>In the CMP GUI, click <b>Reapply Configuration</b> on the MPE/MRA/Mediation cluster. The CMP displays the message: The configuration was applied successfully.</p>  <p>---End of Procedure---</p> |

## 5.4 Procedure 4: Restore Single MPE/MRA/Mediation Node without Server Backup File

The purpose of this procedure is to create a policy cluster from the replacement of one node of the cluster. The active primary node synchronizes the installed node to complete the cluster. In this example, initial policy configuration is restored to the node manually.

### Required resources:

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

Hostname, OAM IP address, and VLAN configuration is gleaned from:

**Platform Setting → Topology Setting → <Cluster\_Name>**

NTP server configuration (and optionally DNS configuration is contained in the platcfg of the running node)

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

### Prerequisites:

- Power down the failed server gracefully
 

**Note:** Access the iLO with Administrator privilege, then go to **Power Management → Server Power** and click **Momentary Press**
- Remove failed hardware and replace.
- Verify that the node has TPD on it, or install TPD
- Install application software—MPE or MRA or Mediation
 

**Note:** Refer to the *Policy Management Bare Metal Installation Guide* Release 12.5, the documents are available at the Oracle Help Center

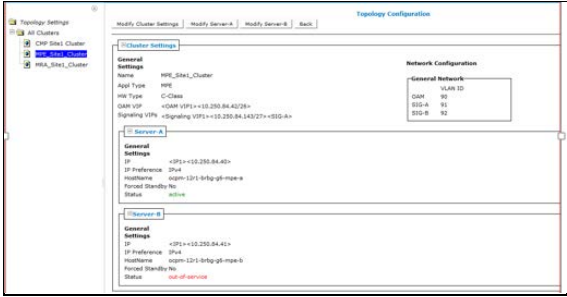
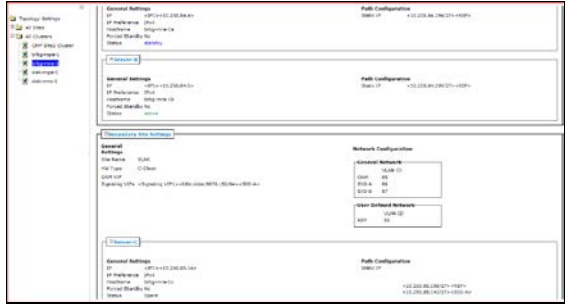


This Procedure performs Restore single MPE/MRA/Mediation node without server backup file

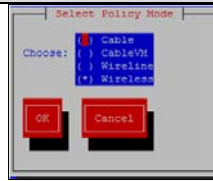
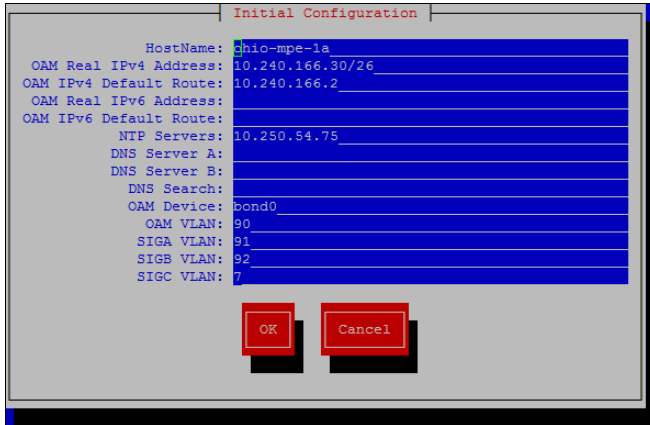
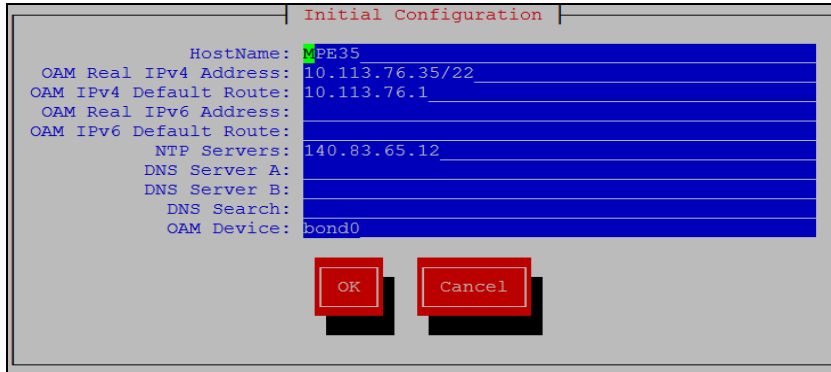
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

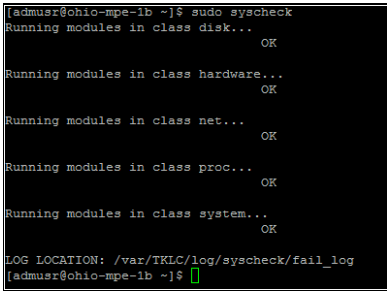
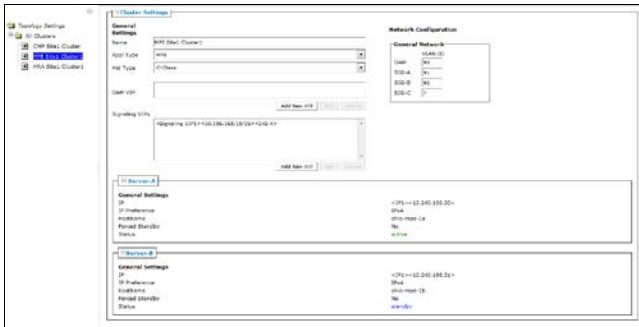
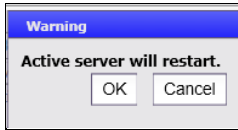
#### Procedure 4 Restore single MPE/MRA/Mediation node without server backup file

| Step                        | Procedure  | Details   |
|-----------------------------|--|---|
| 1. <input type="checkbox"/> | Set the failed node to Forced Standby  | <p>1. In the CMP GUI, navigate to:</p> <p><b>Platform Setting → Topology Setting → All Clusters</b></p> <p>2. Determine the cluster with the failed node</p> <p>3. Determine the failed node</p> <p><b>NOTE:</b> It is possible for a GeoRedundant Topology, that the failed server C node is the spare Server-C.</p> <p>4. Click the <b>Modify Server-X</b> for the failed node</p> <p>5. Select <b>Forced Standby</b> so that it is checked, then click <b>Save</b></p>  <p><b>Server-C (spare): In a GeoRedundant Topology</b></p>  |
| 2. <input type="checkbox"/> | Login via SSH to the node  | <ul style="list-style-type: none"> <li>For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt;</pre> <pre>\$ sudo su -</pre> </li> <li>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul>   |
| 3. <input type="checkbox"/> | Perform Initial Policy Configuration using the platcfg utility on the installed node | <p>1. Open the platcfg utility.</p> <pre># su - platcfg</pre> <p>2. Navigate to:</p> <p><b>Policy Configuration → Set Policy Mode</b></p>   |

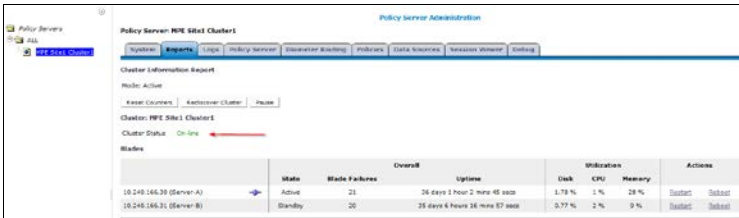
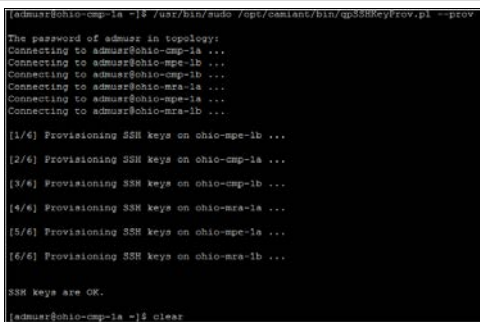


| Step | Procedure | Details   |
|------|-----------|---|
|      |           |  <p>3. Leave the mode as <b>Wireless</b> and click <b>OK</b> to continue. You can skip this step.</p> <p>4. Navigate to:</p> <p><b>Policy Configuration → Perform Initial Configuration</b></p> <p>5. Enter the configuration details from the node being replaced:</p> <p><b>For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)</b></p>  <p>6. After the server details are entered and verified, select <b>OK</b>.</p> <p>7. A menu displays asking to apply the settings, click <b>Yes</b> and wait for the operation to complete. A specific message is not given when the operation is successful, but an error displays if it was not completed. In this case, review the settings from the Perform Initial Configuration screen, if all values are as expected, contact My Oracle Support before proceeding.</p> <p>8. Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</p> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p>  |

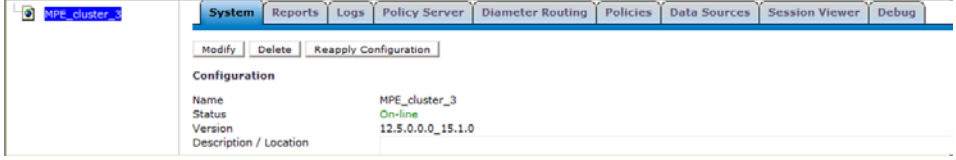


| Step                        | Procedure  | Details   |
|-----------------------------|--|---|
| 4. <input type="checkbox"/> | Reboot the server                                    | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>  |
| 5. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify that all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if the network ping tests still fail.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol>  |
| 6. <input type="checkbox"/> | Remove the Forced Standby designation on the blade.  | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Setting → Current Cluster</b></li> <li>Modify for the server that has Forced Standby</li> <li>Clear the Forced Standby checkbox</li> <li>Click <b>Save</b></li> </ol>  <ol style="list-style-type: none"> <li>Accept the warning dialog by clicking <b>OK</b>.</li> </ol>    |



| Step                         | Procedure  | Details  |
|------------------------------|--|--|
| 9. <input type="checkbox"/>  | Check status   | <div>1. In the CMP GUI, depending on the type of the blade, perform the following:<ul style="list-style-type: none"><li>If this is an MPE node, navigate to:<br/><b>Policy Server → Configuration → All →&lt;Recovered MPE Cluster&gt;→ Reports</b> tab</li><li>If this is an MRA node, navigate to:<br/><b>MRA → Configuration → All →&lt;Recovered MRA Cluster&gt;→ Reports</b> tab</li><li>If this is an Mediation node, navigate to:<br/><b>Mediation → Configuration → All →&lt;Recovered Mediation Cluster&gt;→ Reports</b> tab</li></ul><div>2. Monitor clustering of the blade to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.</div><div></div></div> |
| 10. <input type="checkbox"/> | Alternative method to check replication status                         | <div>Monitor the clustering of the blade from the shell on the primary node using the <b>irepstat</b> command. To do so, SSH to the active node of the cluster and run the <b>irepstat</b> command:</div> <div># irepstat</div> <div>Expected irepstat output while waiting reconnection:</div> <div><pre>-- Policy 0 ActStb [DbReplication] ----- AC From ocpm-12r1-brbg-g6-cmp-a Active      0   0.25 ^0.04%cpu 45B/s  A=me</pre></div> <div>Expected irepstat output after cluster has formed:</div> <div><pre>-- Policy 0 ActStb [DbReplication] ----- AC From ocpm-12r1-brbg-g6-cmp-a Active      0   0.25 ^0.04%cpu 52B/s  A=C2488.184 CC From ocpm-12r1-brbg-g6-mpe-a Active      0   0.50 ^0.06 2.45%cpu 35B/s  A=C2488.184</pre></div>  |
| 11. <input type="checkbox"/> | Exchange keys with cluster mate(This step need to run from active CMP) | <div>Exchanging SSH keys Utility</div> <div><ul style="list-style-type: none"><li>As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code></li><li>As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code></li></ul></div> <div></div>  |



| Step                         | Procedure             | Details  |
|------------------------------|-----------------------|--|
| 12. <input type="checkbox"/> | Reapply Configuration | <p>In the CMP GUI, click <b>Reapply Configuration</b> on the MPE/MRA/Mediation cluster. The CMP displays the message: The configuration was applied successfully.</p>  |
| ---End of Procedure---       |                       |  |

## 5.5 Procedure 5: Restoring Complete Cluster Using Server Backup Files

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

### Required resources:

- Replacement blade
- TPD installation ISO
- Policy APP installation ISO.
- \*serverbackup\*.iso for the replacment blade

### Prerequisites:

1. Power down the failed server gracefully

**Note:** Access the iLO with Administrator privilege, then go to **Power Management** → **Server Power** and click **Momentary Press**

2. Remove and replace both blades
3. IPM both blades
4. Install application on both blades(either CMP, MPE, MRA, Mediation)

**Note:** If it is a CMP Cluster that is being rebuilt, restore application data either from system backup or manually if a backup is not available.

**Note:** Refer to the *Policy Management Bare Metal Installation Guide* Release 12.5, the documents are available at the Oracle Help Center

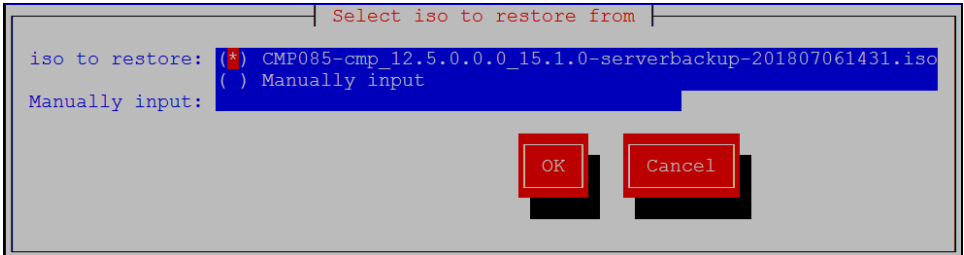


This Procedure performs Restoring complete cluster with the server backup files

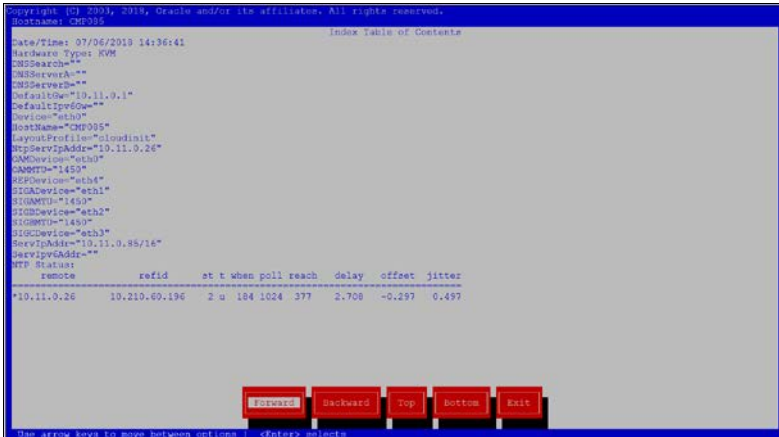
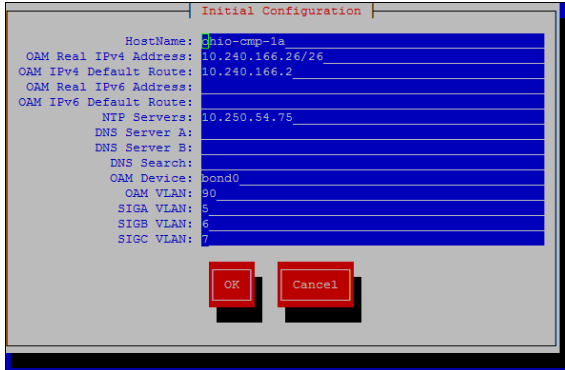
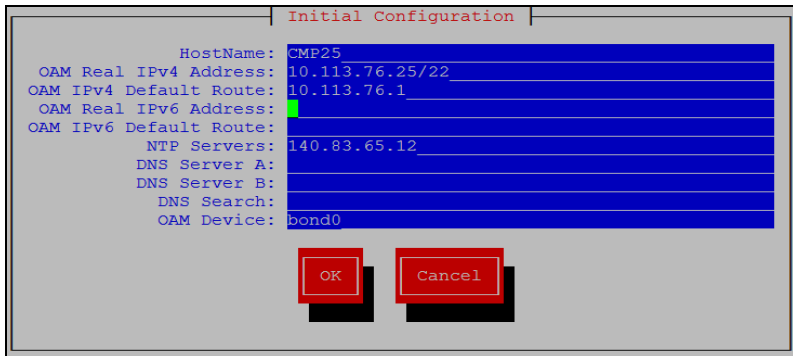
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

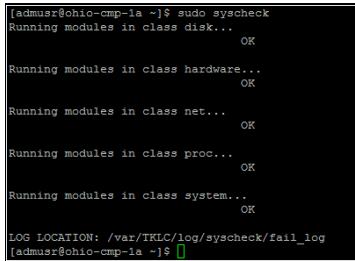
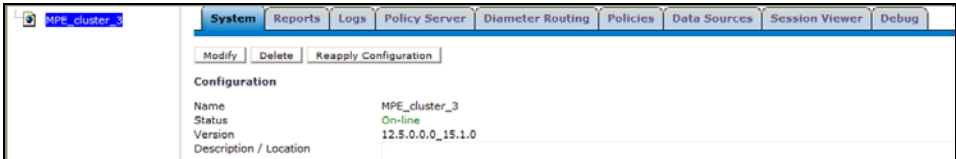
#### Procedure 5 Restoring complete cluster with the server backup files

| Step                        | Procedure   | Details  |
|-----------------------------|---|--|
| 1. <input type="checkbox"/> | SSH to replacement blade                                      | <ul style="list-style-type: none"> <li>For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt;</pre> <pre>\$ sudo su -</pre> </li> <li>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul>                    |
| 2. <input type="checkbox"/> | Load the ISO to restore 1 <sup>st</sup> server of the cluster | <p>Obtain the *serverbackup.iso* for the restored blade. When the replacement blade is available (IPM/App installation complete), the server backup file is copied via secure copy (pscp, scp, or WinSCP) to the following directory:</p> <pre>/var/camiant/backup/local_archive/serverbackup</pre> <p><b>NOTE:</b> Later in this procedure, the platcfg restore function checks this directory and opens a menu. The platcfg utility also enables you to manually enter any mounted path on the server.</p> |
| 3. <input type="checkbox"/> | Perform platcfg restore from SSH session to replacement blade | <ol style="list-style-type: none"> <li>Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>Navigate to:<br/> <b>Policy Configuration → Backup and Restore → Server Restore</b> </li> <li>Select the *serverbackup*.iso that you put on the system and click <b>OK</b></li> <li>Click <b>Yes</b> to confirm.</li> </ol>    |
| 4. <input type="checkbox"/> | Verify the status   | <p>A window opens indicating that the restore operation is 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 the support team or engineering team for assistance.</p>  |

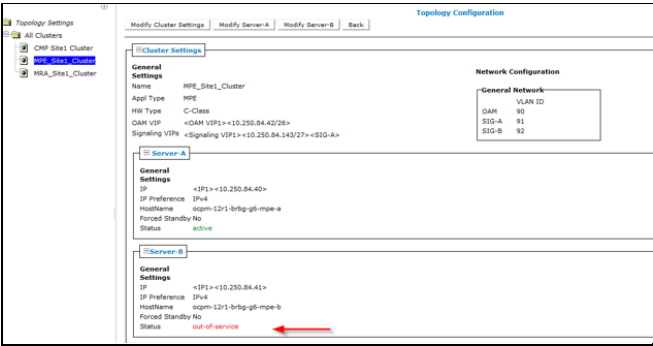


| Step                        | Procedure                    | Details  |
|-----------------------------|------------------------------|--|
| 5. <input type="checkbox"/> | Verify Initial configuration | <ol style="list-style-type: none"> <li>Click <b>Exit</b> on each platcfg menu until you are returned to the Main Menu of the platcfg utility.</li> <li>Navigate to:<br/><b>Policy Configuration → Verify Initial Configuration</b></li> </ol>  <ol style="list-style-type: none"> <li>If the configuration does not exist, navigate to <b>Perform Initial Configuration</b> and enter the initial configuration hostname, OAM IP, and NTP servers configurations.<br/><b>For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)</b></li> </ol>  <ol style="list-style-type: none"> <li>Verify that that the information is correct.</li> <li>Click <b>OK</b> and then <b>Yes</b> to save and apply</li> <li>Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</li> </ol> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p>  |

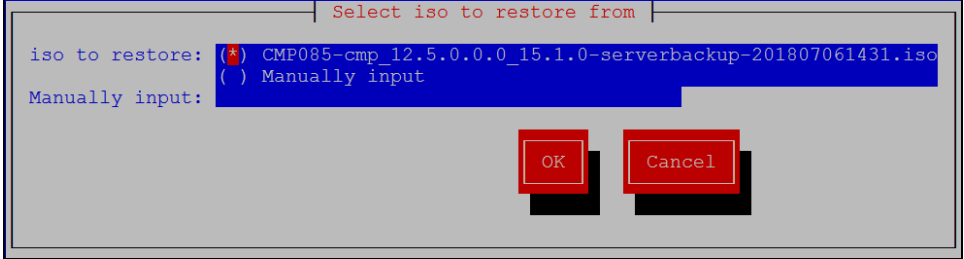


| Step                        | Procedure  | Details   |
|-----------------------------|--|---|
| 6. <input type="checkbox"/> | Reboot the server                                    | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>  |
| 7. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol>  <p><b>NOTE:</b> If you are restoring a CMP cluster, you must perform a system restoration for this server after this step, then perform a server restoration for the standby CMP server.</p> |
| 8. <input type="checkbox"/> | Check status   | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Settings → All Clusters</b></li> <li>Select a cluster.</li> <li>Click the <b>System</b> tab.</li> <li>If the Status field indicates Config Mismatch, click <b>Reapply Configuration</b> and wait for the Config Mismatch designation to disappear. If it does not, contact <a href="#">My Oracle Support</a> before proceeding.</li> </ol>   |


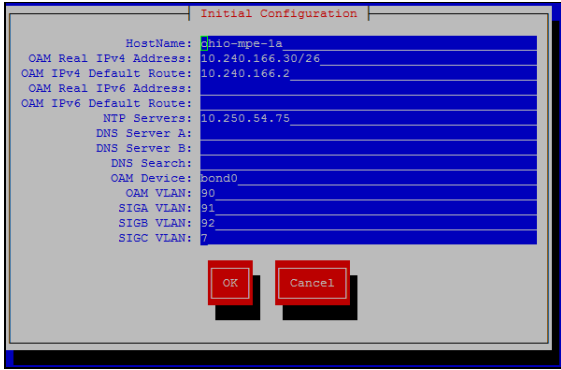
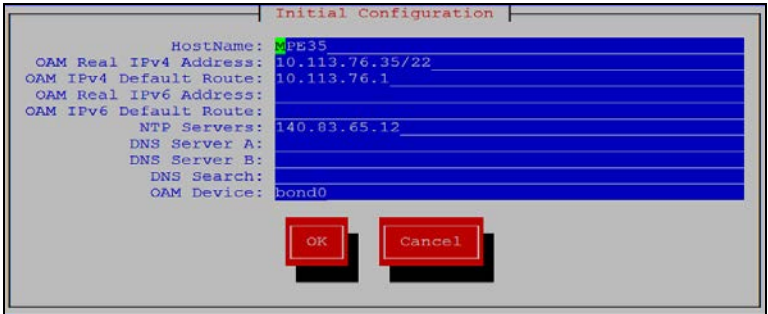


| Step                         | Procedure  | Details  |
|------------------------------|--|--|
| 11. <input type="checkbox"/> | Set Forced Standby designation on cluster node that is still out-of-service. | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Setting → &lt;Current Cluster&gt;</b></li> <li>Modify the server that has a status of out-of-service.</li> <li>Select <b>Forced Standby</b>.</li> <li>Click <b>Save</b>.</li> </ol>  <ol style="list-style-type: none"> <li>Accept the confirmation dialog by clicking <b>OK</b>.</li> </ol>                        |
| 12. <input type="checkbox"/> | SSH from the PM&C server to replacement blade                                | <ul style="list-style-type: none"> <li>For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt;</pre> <pre>\$ sudo su -</pre> </li> <li>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:<br/>Use the iLo to login, and start a remote console to run commands</li> </ul>  |
| 13. <input type="checkbox"/> | Load the ISO to restore 2 <sup>nd</sup> server of the cluster                | <p>Obtain the *serverbackup.iso* for the restored blade. When the replacement blade is available (IPM/App installation complete), the server backup file is copied via secure copy (pscp, scp, or WinSCP) to the following directory:</p> <pre>/var/camiant/backup/local_archive/serverbackup</pre> <p><b>NOTE:</b> Later in this procedure, the platcfg restore function checks this directory and opens a menu. The platcfg utility also enables you to manually enter any mounted path on the server.</p> |

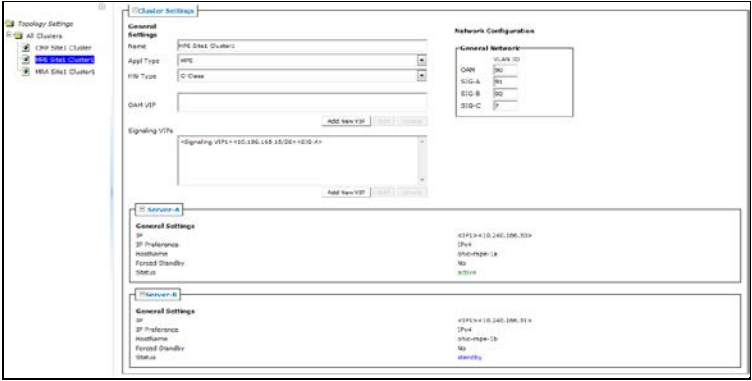
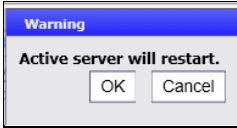


| Step                         | Procedure   | Details  |
|------------------------------|---|--|
| 14. <input type="checkbox"/> | Perform platcfg restore from SSH session to replacement blade | <ol style="list-style-type: none"> <li>1. Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>2. Navigate to:<br/> <b>Policy Configuration → Backup and Restore → Server Restore</b> </li> <li>3. Select the *serverbackup*.ISO that you just put on the system and click <b>OK</b>.</li> <li>4. Click <b>Yes</b> to confirm.</li> </ol>  |
| 15. <input type="checkbox"/> | Verify the status   | <p>If the restore is successful, 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. Ensure that results of the restore operation indicates success before proceeding.</p>   |




| Step                         | Procedure                    | Details  |
|------------------------------|------------------------------|--|
| 16. <input type="checkbox"/> | Verify Initial configuration | <ol style="list-style-type: none"> <li>Click <b>Exit</b> on each platcfg menu until you are returned to the Main Menu of the platcfg utility.</li> <li>Navigate to:<br/><b>Policy Configuration → Verify Initial Configuration</b></li> </ol>  <ol style="list-style-type: none"> <li>If the configuration does not exist, navigate to <b>Perform Initial Configuration</b> and enter the initial configuration: hostname, OAM IP, and NTP servers configurations.<br/><b>For c-Class or Sun X5-2/Sun Netra X5-2(belongs to hardware type Oracle RMS)</b></li> </ol>  <ol style="list-style-type: none"> <li>Verify that the information is correct.</li> <li>Click <b>OK</b> and then click <b>Yes</b> to save and apply</li> <li>Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</li> </ol> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p>  |

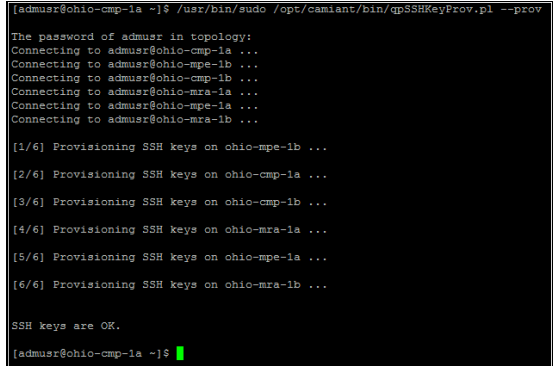


| Step                         | Procedure   | Details   |
|------------------------------|---|---|
| 17. <input type="checkbox"/> | Reboot the server                                   | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>  |
| 18. <input type="checkbox"/> | Remove the Forced Standby designation on the blade. | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Setting → &lt;Current Cluster&gt;</b></li> <li>Click modify for the server that is in Forced Standby</li> <li>Clear the Forced Standby checkbox</li> <li>Click <b>Save</b></li> </ol>  <ol style="list-style-type: none"> <li>Accept the warning message by clicking <b>OK</b>.</li> </ol>  |



| Step                         | Procedure                                      | Details   |
|------------------------------|--|---|
| 19. <input type="checkbox"/> | Check status                                   | <ol style="list-style-type: none"> <li>In the CMP GUI, depending on the type of the blade, perform the following: <ul style="list-style-type: none"> <li>If this is an MPE node, navigate to:<br/><b>Policy Server → Configuration → All → &lt;Recovered MPE Cluster&gt; → Reports</b> tab</li> <li>If this is an MRA node, navigate to:<br/><b>MRA → Configuration → All → &lt;Recovered MRA Cluster&gt; → Reports</b> tab</li> <li>If this is an Mediation node, navigate to:<br/><b>Mediation → Configuration → All → &lt;Recovered Mediation Cluster&gt; → Reports</b> tab</li> </ul> </li> <li>Check CMP cluster status (as indicated in the previous step), navigate to: <b>Platform Setting → Topology Setting → Current CMP Cluster</b></li> <li>Monitor clustering of the blade to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.</li> </ol>    |
| 20. <input type="checkbox"/> | Alternative method to check replication status | <p>You can monitor the clustering of the blade from the shell on the primary node using the <b>irepstat</b> command. To do so, SSH to the active node of the cluster and run the <b>irepstat</b> command:</p> <pre># irepstat</pre> <p>Expected irepstat output while waiting reconnection:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AC To  ocpm-12r1-brbg-g6-mpe-a Active      0    0.50 1%R 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mpe-b Active      0    0.25 1%R 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-a Active      0    0.50 1%R 0.04%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-b Active      0    0.25 1%R 0.05%cpu 85B/s</pre> <p>Expected irepstat output after cluster has formed:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- RA 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> |



| Step                         | Procedure  | Details  |
|------------------------------|--|--|
| 21. <input type="checkbox"/> | Exchange keys with cluster mate(This step need to run from active CMP) | <p>Exchanging SSH keys Utility</p> <ul style="list-style-type: none"> <li>As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code></li> <li>As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code></li> </ul>  |
| 22. <input type="checkbox"/> | Reapply Configuration  | In the CMP GUI, click <b>Reapply Configuration</b> on the MPE/MRA/Mediation cluster. The CMP displays the message: The configuration was applied successfully.   |
| ---End of Procedure---       |  |  |

## 5.6 Procedure 6: Restoring Complete Cluster without Using the Server Backup

The purpose of this procedure is to restore a policy cluster without the server backup file. The active primary blade synchronizes the installed blade to complete the cluster. In this example, initial Policy configuration is restored to the blade by manually.

### Required resources:

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

Hostname, OAM IP address, and VLAN configuration are gleaned from:

**Platform Setting → Topology Setting → <Cluster\_Name>**

NTP server configuration (and optionally DNS configuration is contained in the platcfg of the running blade)

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

### Prerequisites:

- Power down the failed server gracefully
  - Note: Access the iLO with Administrator privilege, then go to **Power Management → Server Power** and click **Momentary Press**
- Remove failed blade and replace.
- Verify that the blade had TPD on it, or install TPD
- Install application software—CMP, MPE, MRA, Mediation



**Notes:**

- o If it is a CMP Cluster that is being rebuilt, restore application data either from a system backup or manually if a backup is not available.
- o Refer to the *Policy Management Bare Metal Installation Guide* Release 12.5, this document is available on the Oracle Help Center

This Procedure performs Restoring complete cluster without the server backup

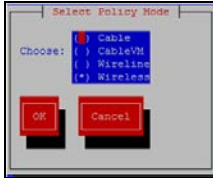
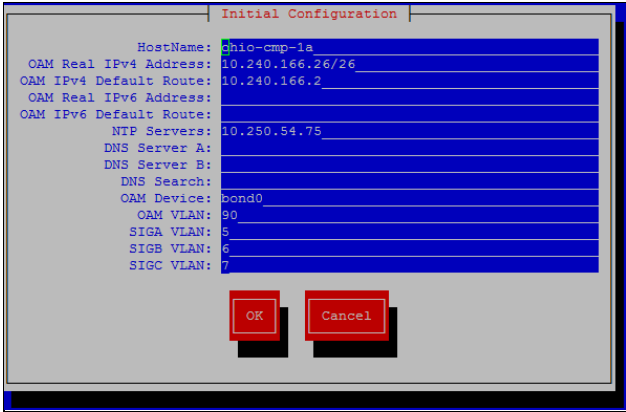
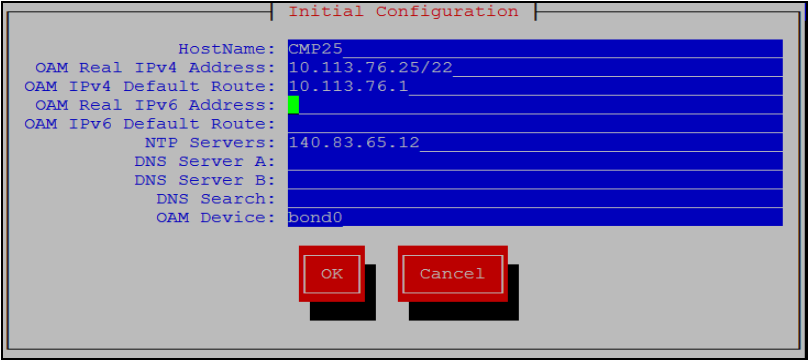
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

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

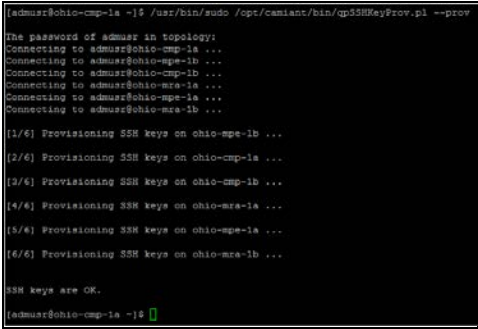
**Procedure 6 Restoring complete cluster without the server backup**

| Step                        | Procedure                  | Details  |
|-----------------------------|----------------------------|--|
| 1. <input type="checkbox"/> | Login via SSH to the blade | <ul style="list-style-type: none"> <li>• For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt;</pre> <pre>\$ sudo su -</pre> </li> <li>• For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul> |

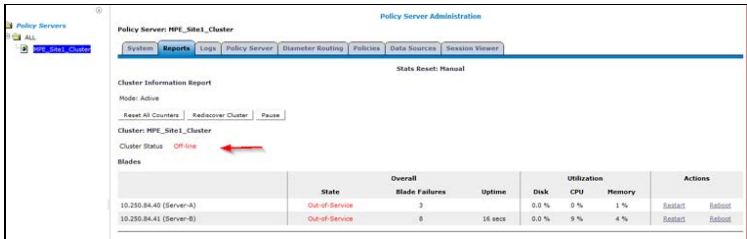
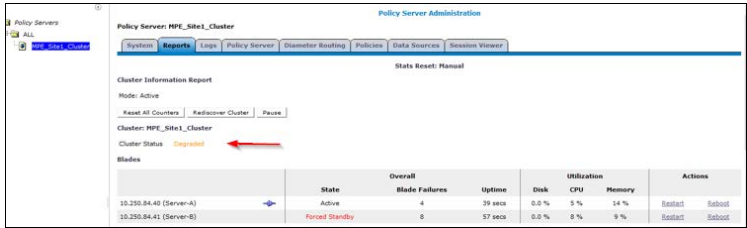
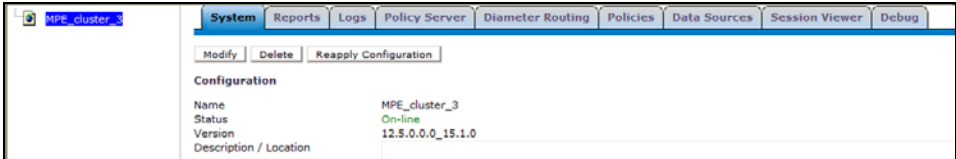


| Step                        | Procedure   | Details   |
|-----------------------------|---|---|
| 2. <input type="checkbox"/> | Perform Initial Policy Configuration using the platcfg utility on the installed blade | <ol style="list-style-type: none"> <li>Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>Navigate to:<br/> <b>Policy Configuration → Set Policy Mode</b>  </li> <li>Leave the mode as <b>Wireless</b> and click <b>OK</b> to continue. You can skip this step.</li> <li>Navigate to:<br/> <b>Policy Configuration → Perform Initial Configuration</b> </li> <li>Enter the configuration details for the blade being replaced:<br/>  </li> <li>After the server details are entered and verified, click <b>OK</b>.</li> <li>A menu displays asking to apply the settings, click <b>Yes</b> and wait for the operation to complete. A specific message is not given when the operation is successful, but an error displays if it was not completed. In this case, review the settings from the Perform Initial Configuration screen, if all values are as expected, contact My Oracle Support before proceeding.</li> <li>Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</li> </ol> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p>  |

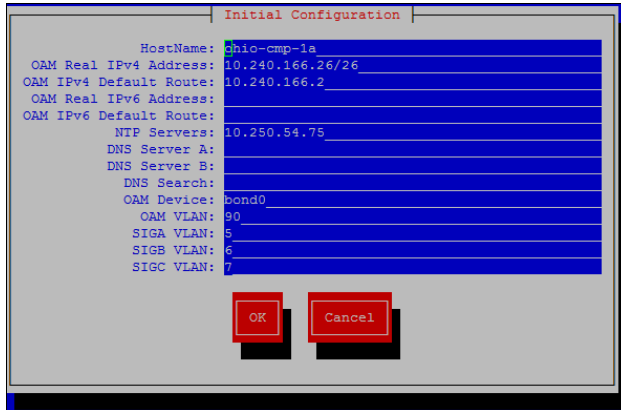


| Step                        | Procedure  | Details  |
|-----------------------------|--|--|
| 3. <input type="checkbox"/> | Reboot the server                                    | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>   |
| 4. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol>  <pre>(admusr@ohio-cmp-1a ~)\$ /usr/bin/sudo /opt/cwiant/bin/gpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@ohio-cmp-1a ... Connecting to admusr@ohio-cmp-1b ... Connecting to admusr@ohio-cmp-1b ... Connecting to admusr@ohio-mra-1a ... Connecting to admusr@ohio-mra-1a ... Connecting to admusr@ohio-mra-1b ... Connecting to admusr@ohio-mra-1b ...  [1/6] Provisioning SSH keys on ohio-cmp-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-mra-1a ... [6/6] Provisioning SSH keys on ohio-mra-1b ...  SSH keys are OK. (admusr@ohio-cmp-1a ~)\$</pre> |



| Step                        | Procedure    | Details   |
|-----------------------------|--------------|---|
| 5. <input type="checkbox"/> | Check status | <p>1. In the CMP GUI, depending on the type of the blade, perform the following:</p> <ul style="list-style-type: none"> <li>- If this is an MPE node, navigate to:<br/><b>Policy Server → Configuration → All → &lt;Recovered MPE Cluster&gt; → Reports</b> tab</li> <li>- If this is an MRA node, navigate to:<br/><b>MRA → Configuration → All → &lt;Recovered MRA Cluster&gt; → Reports</b> tab</li> <li>- If this is an Mediation node, navigate to:<br/><b>Mediation → Configuration → All → &lt;Recovered Mediation Cluster&gt; → Reports</b> tab</li> </ul> <p>2. Monitor clustering of the blade to its peer, do not proceed until the Cluster Status returns from Off-line to Degraded.</p> <p><b>Off-line</b></p>  <p><b>Degraded</b></p>  |
| 6. <input type="checkbox"/> | Check status | <p>1. In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Setting → All Clusters</b></p> <p>2. Select a cluster</p> <p>3. Click <b>System</b> tab.</p> <p>If the Status field indicates Config Mismatch, click the <b>Reapply Configuration</b> and wait for the Config Mismatch designation to disappear. If it does not, contact My Oracle Support before proceeding.</p>   |






| Step                        | Procedure  | Details   |
|-----------------------------|--|---|
| 7. <input type="checkbox"/> | Login via SSH to second node of the cluster  | <ul style="list-style-type: none"> <li>For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt;</pre> <pre>\$ sudo su -</pre> </li> <li>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2)System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul>  |
| 8. <input type="checkbox"/> | Perform Initial Policy Configuration using the platcfg utility on second node of cluster | <ol style="list-style-type: none"> <li>Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>Navigate to:<br/> <b>Policy Configuration → Initial Configuration</b> </li> <li>Enter the details for the replacement blade:<br/>  </li> <li>After the server details are entered and verified, select <b>OK</b>.</li> <li>A menu displays asking to apply the settings, click <b>Yes</b> and wait for the operation to complete. A specific message is not given when the operation is successful, but an error displays if it was not completed. In this case, review the settings from the Perform Initial Configuration screen, if all values are as expected, contact My Oracle Support before proceeding.</li> <li>Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.</li> </ol> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p> |



| Step                         | Procedure  | Details  |
|------------------------------|--|--|
|                              |  | <div data-bbox="613 163 1425 588"> <p>Initial Configuration</p> <pre> 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 </pre> <p>OK Cancel</p> </div>   |
| 9. <input type="checkbox"/>  | Reboot the server                                    | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>   |
| 10. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol> <div data-bbox="833 1207 1203 1465"> <pre> [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 ~]\$ </pre> </div> |



| Step                         | Procedure    | Details   |
|------------------------------|--------------|---|
| 11. <input type="checkbox"/> | Check status | <p>1. In the CMP GUI, depending on the type of the blade, perform the following:</p> <ul style="list-style-type: none"> <li>If this is an MPE node, navigate to:<br/><b>Policy Server → Configuration → All → &lt;Recovered MPE Cluster&gt; → Reports</b> tab</li> <li>If this is an MRA node, navigate to:<br/><b>MRA → Configuration → All → &lt;Recovered MRA Cluster&gt; → Reports</b> tab</li> <li>If this is an Mediation node, navigate to:<br/><b>Mediation → Configuration → All → &lt;Recovered Mediation Cluster&gt; → Reports</b> tab</li> </ul> <p>2. Monitor clustering of the blade to its peer, do not proceed until the Cluster Status changes from Degraded to On-line</p> <p><b>MPE:</b></p>  <p><b>MRA:</b></p>  <p><b>Mediation:</b></p>  |



| Step                         | Procedure   | Details  |
|------------------------------|---|--|
| 12. <input type="checkbox"/> | Alternative method to check replication status                          | <p>You can also monitor the clustering of the blade from the shell on the primary node with the <b>irepstat</b> command. To do so, SSH to the active node of the cluster and run the <b>irepstat</b> command:</p> <pre># irepstat</pre> <p>Expected irepstat output while waiting reconnection:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AC To  ocpm-12r1-brbg-g6-mpe-a  Active    0    0.50 1%R 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mpe-b  Active    0    0.25 1%R 0.05%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-a  Active    0    0.50 1%R 0.04%cpu 85B/s AC To  ocpm-12r1-brbg-g6-mra-b  Active    0    0.25 1%R 0.05%cpu 85B/s</pre> <p>Expected irepstat output after cluster has formed:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- AA To  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> |
| 13. <input type="checkbox"/> | Exchange keys with cluster mate (This step need to run from active CMP) | <p>Exchanging SSH keys Utility</p> <ul style="list-style-type: none"> <li>As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code></li> <li>As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code></li> </ul> <pre>[admin@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. [admin@ohio-cmp-1a ~]\$</pre>  |
| 14. <input type="checkbox"/> | Reapply Configuration   | <p>In the CMP GUI, click <b>Reapply Configuration</b> on the MPE/MRA/Mediation cluster. The CMP displays The configuration was applied successfully message.</p>   |
| ---End of Procedure---       |   |  |

## 5.7 Procedure 7: Restoring CMP Cluster Using the Available System Backup

The purpose of this procedure is to re-create a CMP with the application level configuration of the policy network that is used to re-create the recovered policy network. After the CMP is online, all other servers of the policy network are re-created using Procedure 1 through Procedure 6 and then their application level configuration restored from this CMP. In the case of a massive outage that includes the CMP, at least one of the CMP blades is restored first.

### Required resources:

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



- Initial configuration information about the blade:
  - o OAM IP address, default gateway, NTP and SNMP server IP addresses
  - o VLAN configuration information.

Hostname, OAM IP address, and VLAN configuration are gleaned from:

**Platform Setting → Topology Setting → <Cluster\_Name>**

NTP server configuration (and optionally DNS configuration is contained in the platcfg utility of the running blade)

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

#### Prerequisites:

1. Power down the failed server gracefully

**Note:** Access the iLO with Administrator privilege, then go to **Power Management → Server Power** and click **Momentary Press**.

2. Remove failed blades and replace.
3. Verify that the blade had TPD on it, or install TPD
4. Install application software—CMP

**Note:** Refer to the *Policy Management Bare Metal Installation Guide* Release 12.5, this document is available at the Oracle Help Center

This Procedure performs Restoring CMP cluster with system backup available

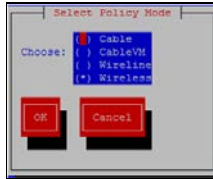
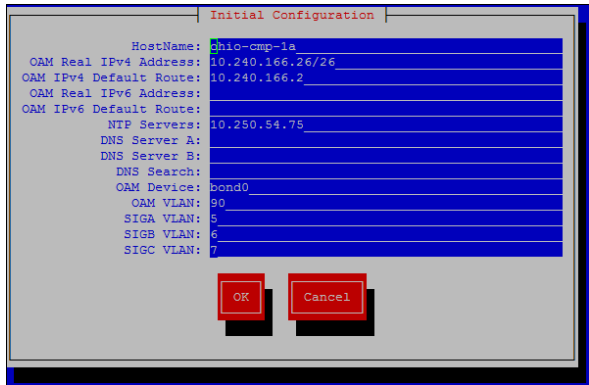
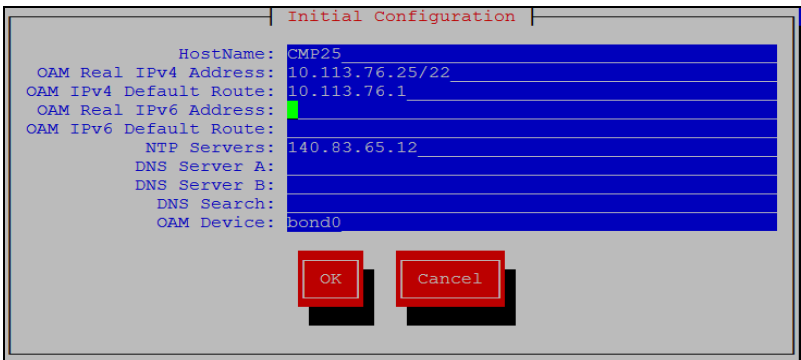
Check off (✓) each step as it is completed. Boxes been provided for this purpose under each step number.

If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

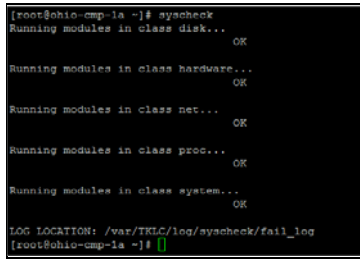
#### Procedure 7 Restoring CMP cluster with system backup available

| Step                        | Procedure              | Details  |
|-----------------------------|------------------------|--|
| 1. <input type="checkbox"/> | Login via SSH to blade | <ul style="list-style-type: none"> <li>• For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> screen to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt; \$ sudo su -</pre> </li> <li>• For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul> |

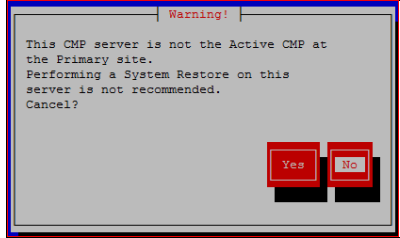
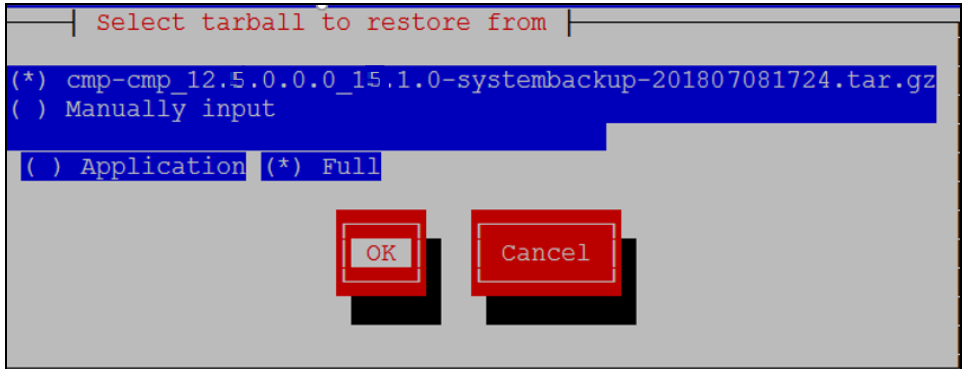


| Step                        | Procedure   | Details   |
|-----------------------------|---|---|
| 2. <input type="checkbox"/> | Perform Initial Policy Configuration using the platcfg utility on the installed blade | <ol style="list-style-type: none"> <li>Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>Navigate to:<br/> <b>Policy Configuration → Set Policy Mode</b>  </li> <li>Leave the mode as <b>Wireless</b> and click <b>OK</b> to continue. You can skip this step.</li> <li>Navigate to:<br/> <b>Policy Configuration → Perform Initial Configuration</b> </li> <li>Enter the relevant details from the replaced blade:<br/>  </li> <li>After the server details are entered and verified, click <b>OK</b>.</li> <li>A menu opens asking to apply the settings, click <b>Yes</b> and wait for the operation to complete. A specific message is not given 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 screen, if all is as expected, contact My Oracle Support before proceeding.</li> <li>Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu page until you are returned to the shell.</li> </ol> <p><b>For RMS (DL360/DL380):</b></p> <p>The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.</p>  |

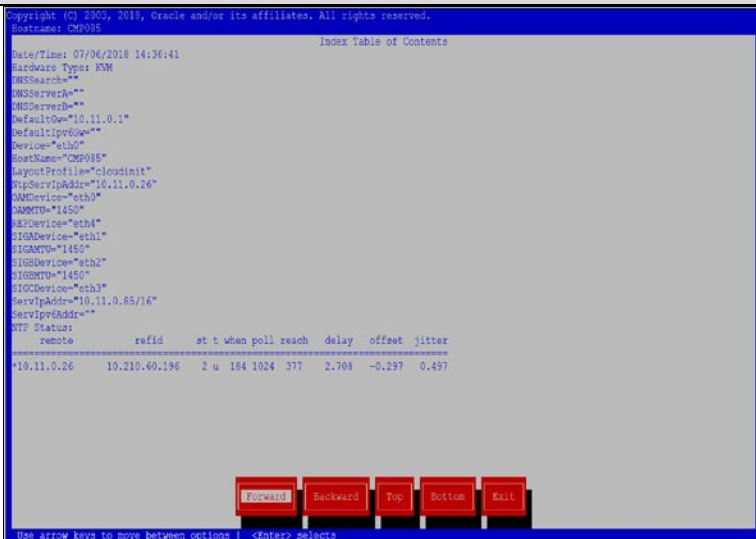
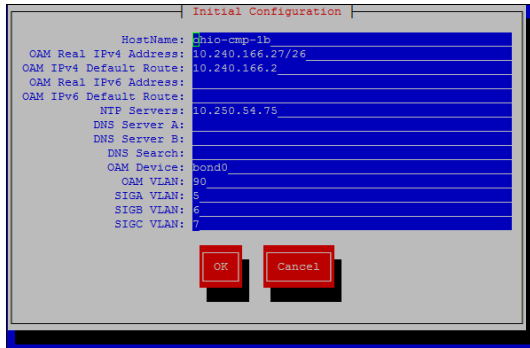


| Step                        | Procedure  | Details   |
|-----------------------------|--|---|
| 3. <input type="checkbox"/> | Reboot the server                                    | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>  |
| 4. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol>  <pre>[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 ~]#</pre> |
| 5. <input type="checkbox"/> | Load the system backup(ISO) file for server restore  | <p>The system backup file contains the database information for the application level configuration of the policy network. Without the backup, the application configuration is restored either using the platcfg menu or from the server backup file from site documentation.</p> <p>If the system backup file is available, put a copy of the file on the constructed CMP blade using secure copy (pscp scp, or WinSCP).</p> <pre>/var/camiant/backup/local_archive/systembackup/</pre>   |

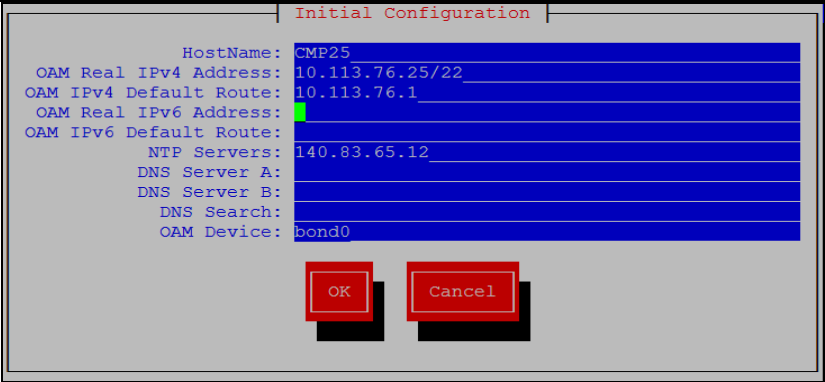
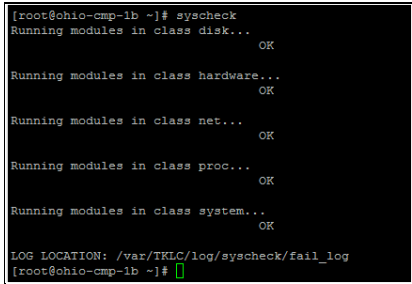


| Step                        | Procedure   | Details  |
|-----------------------------|---|--|
| 6. <input type="checkbox"/> | Perform platcfg restore from SSH session to replacement blade | <ol style="list-style-type: none"> <li>Open the platcfg utility.<br/> <pre># su - platcfg</pre> </li> <li>Navigate to:<br/> <b>Policy Configuration → Backup and Restore → System Restore</b> </li> <li>A message displays prompting confirmation to restore even though this node is not recognized as the active member. This is expected, continue by clicking <b>No</b>.<br/>  </li> <li>A page opens asking you to select the restoration file. If the file was copied correctly in the previous step, it is listed here as an option, otherwise select <b>Manually Input</b> and select <b>Full</b>.</li> <li>Click <b>OK</b> to proceed.<br/>  </li> </ol> <p><b>NOTE:</b> <b>Full</b> restores the Comcol data, but <b>Application</b> excludes Comcol.</p> |
| 7. <input type="checkbox"/> | Verify the status   | A window opens indicating that restore operation was successful and asks you to press any key to exit. If it is not successful, retry the restore operation. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.   |
| 8. <input type="checkbox"/> | Verify Initial configuration                                  | <ol style="list-style-type: none"> <li>Click <b>Exit</b> on each platcfg menu until you are back to the Main Menu of the platcfg utility.</li> <li>Navigate to:<br/> <b>Policy Configuration → Verify Initial Configuration</b> </li> </ol>  |

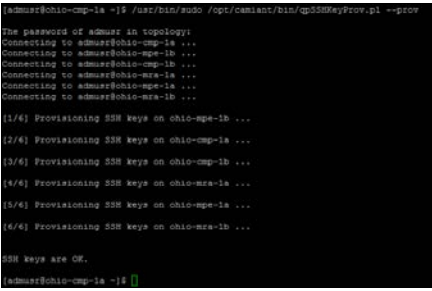


| Step        | Procedure  | Details   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |
|-------------|--|---|--------|-----------------|-------|--------|-----------------|-------|--------|--------|-------------|---------------|---|---|--------------|-------|--------|-------|
|             |  |  <p>Copyright (C) 2002, 2010, Oracle and/or its affiliates. All rights reserved.<br/>Hostname: OMS085</p> <p>Date/Time: 07/06/2018 14:36:41<br/>Hardware Type: KVM<br/>DNS Search: ""<br/>DNS Server A: ""<br/>DNS Server B: ""<br/>Default IPv4: 10.11.0.1<br/>Default IPv6: ""<br/>Device: eth0<br/>Host Name: "OMS085"<br/>Layout Profile: "cloudinit"<br/>NTP ServIP Addr: "10.11.0.26"<br/>OAM Device: "eth0"<br/>SIGMTO: "1450"<br/>SIGMTO: "eth4"<br/>SIGMTO: "eth1"<br/>SIGMTO: "1450"<br/>SIGMTO: "eth2"<br/>SIGMTO: "1450"<br/>SIGMTO: "eth3"<br/>ServIP Addr: "10.11.0.85/16"<br/>ServIP Addr: ""</p> <p>NTP Status:</p> <table><tr><th>remote</th><th>refid</th><th>st</th><th>t</th><th>when poll reach</th><th>delay</th><th>offset</th><th>jitter</th></tr><tr><td>*10.11.0.26</td><td>10.210.60.196</td><td>2</td><td>u</td><td>184 1024 377</td><td>2.708</td><td>-0.237</td><td>0.457</td></tr></table> <p>Forward Backward Top Bottom Exit</p> <p>Use arrow keys to move between options   &lt;Enter&gt; selects</p> | remote | refid           | st    | t      | when poll reach | delay | offset | jitter | *10.11.0.26 | 10.210.60.196 | 2 | u | 184 1024 377 | 2.708 | -0.237 | 0.457 |
| remote      | refid  | st  | t      | when poll reach | delay | offset | jitter          |       |        |        |             |               |   |   |              |       |        |       |
| *10.11.0.26 | 10.210.60.196  | 2   | u      | 184 1024 377    | 2.708 | -0.237 | 0.457           |       |        |        |             |               |   |   |              |       |        |       |
| 3.          | Verify that the information is correct. If the configuration is not there, navigate to <b>Perform Initial Configuration</b> and enter the hostname, OAM IP and so on.  |  <p>Initial Configuration</p> <p>HostName: oms0-cmp-1b<br/>OAM Real IPv4 Address: 10.240.166.27/26<br/>OAM IPv4 Default Route: 10.240.166.2<br/>OAM Real IPv6 Address: <br/>OAM IPv6 Default Route: <br/>NTP Servers: 10.250.54.75<br/>DNS Server A: <br/>DNS Server B: <br/>DNS Search: <br/>OAM Device: bond0<br/>OAM VLAN: 90<br/>SIGA VLAN: 5<br/>SIGB VLAN: 6<br/>SIGC VLAN: 7</p> <p>OK Cancel</p>   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |
| 4.          | Click <b>OK</b> and then click <b>YES</b> to save and apply.   |   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |
| 5.          | After the server details are entered and verified, select <b>OK</b> .  |   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |
| 6.          | A menu displays asking to apply settings, click <b>Yes</b> and wait for the operation to complete. A specific message is not given when the operation is successful, but an error displays if it was not completed. In this case, review the settings from the Perform Initial Configuration screen, if all values are as expected, contact My Oracle Support before proceeding. |   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |
| 7.          | Exit the platcfg utility by clicking <b>Exit</b> on each platcfg menu until you are returned to the shell.   |   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |
|             | <b>For RMS (DL360/DL380):</b>  |   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |
|             | The platcfg utility for RMS does not natively use VLANs. For example, the SIGA VLAN, SIGB VLAN, and SIGC VLAN configuration parameters are not listed for RMS based hardware.  |   |        |                 |       |        |                 |       |        |        |             |               |   |   |              |       |        |       |



| Step                         | Procedure  | Details  |
|------------------------------|--|--|
|                              |  |    |
| 9. <input type="checkbox"/>  | Reboot the server                                    | <p>Reboot the server:</p> <pre># init 6</pre> <p>Allow the server time to reboot.</p> <ul style="list-style-type: none"> <li>For c-Class or Netra X5-2(Oracle RMS)System:<br/>Reconnect via SSH from the PM&amp;C server to the node as admusr and then switch to root privileges.</li> <li>For RMS (DL360/DL380/Oracle X5-2)System without PM&amp;C:<br/>SSH directly to the node.</li> </ul>   |
| 10. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>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.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol>  |



| Step                         | Procedure  | Details   |
|------------------------------|--|---|
| 11. <input type="checkbox"/> | Exchange keys with cluster mate(This step need to run from active CMP) | <p>Exchanging SSH keys Utility</p> <ul style="list-style-type: none"> <li>As root,<br/> <pre>run /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</pre> </li> <li>As admusr, run<br/> <pre>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</pre> </li> </ul>   |
| 12. <input type="checkbox"/> | Check status   | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/> <b>Platform Setting → Topology Setting → All Clusters</b> </li> <li>When the server returns to online status, log into the GUI on the OAM virtual IP address</li> <li>Verify to that the manager has configuration for the MPE clusters in the network (whether those clusters are online or not)</li> <li>Verify other application configuration properties.</li> <li>After the CMP is in place, the replace the other node of the CMP cluster using this procedure, and any other clusters or individual nodes that require replacement are replaced using this procedures.</li> </ol> |
| ---End of Procedure---       |  |   |

## 5.8 Procedure 8: Promoting Georedundant CMP Cluster

This procedure is used to bring a georedundant secondary active CMP online before beginning restoration of other policy clusters in the network. After the CMP is online, all other servers of the policy network are re-created using Procedure 1 through Procedure 7 and then their application level configuration restored from this CMP.

This Procedure performs Promoting georedundant CMP cluster

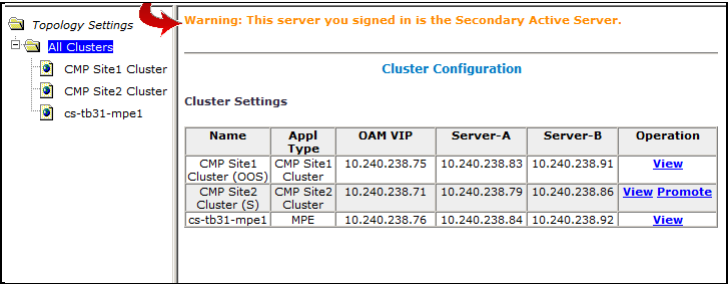
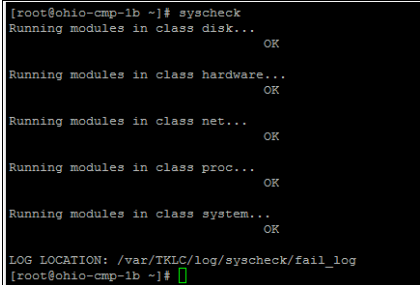
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

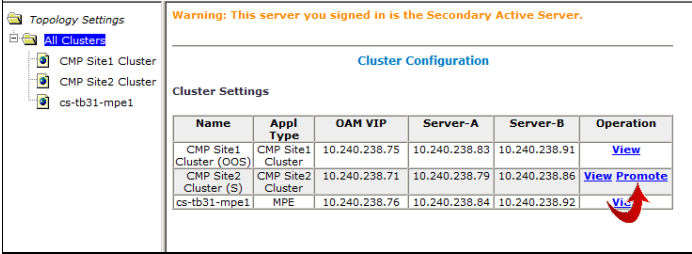
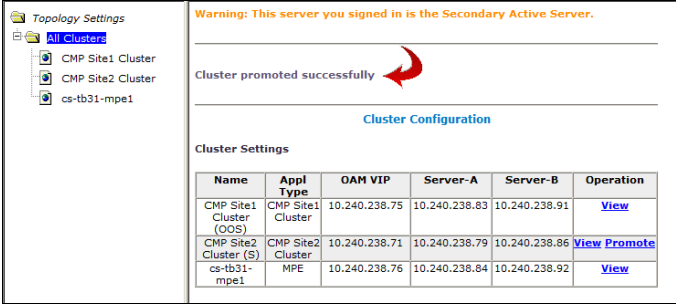
### Procedure 8 Promoting georedundant CMP cluster

| Step                        | Procedure            | Details  |
|-----------------------------|----------------------|--|
| 1. <input type="checkbox"/> | Access to the system | Log into the GUI on the OAM VIP of the georedundant CMP. |

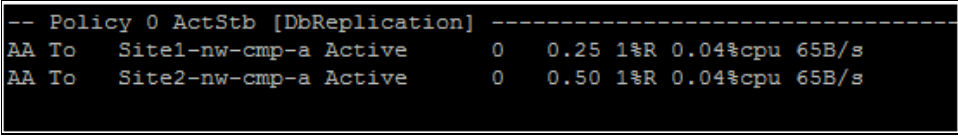
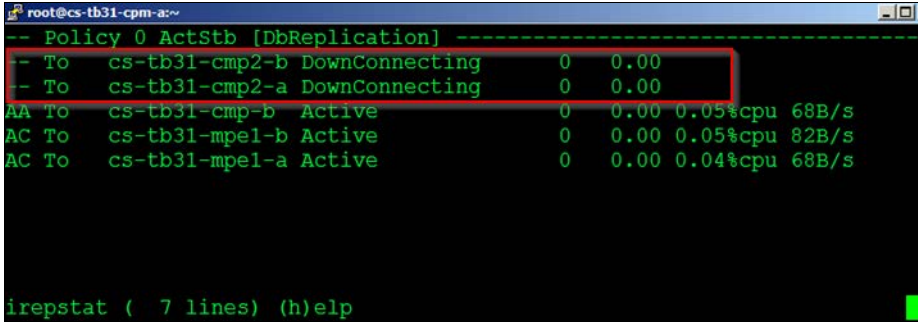


| Step                        | Procedure  | Details   |
|-----------------------------|--|---|
| 2. <input type="checkbox"/> | Check status   | <p>In the CMP GUI, navigate to:</p> <p><b>Platform Setting → Topology Setting → All Clusters</b></p> <p>You are warned that you are not on the primary cluster of the policy network. The secondary server has limited functionality.</p>   |
| 3. <input type="checkbox"/> | Verify basic network connectivity and server health. | <ol style="list-style-type: none"> <li>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.</li> </ol> <pre># ping &lt;XMI or OAM gateway address&gt;</pre> <ol style="list-style-type: none"> <li>Run the <b>syscheck</b> command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.</li> </ol>  |



| Step                        | Procedure                                  | Details   |
|-----------------------------|--|---|
| 4. <input type="checkbox"/> | Promote secondary CMP cluster              | <ol style="list-style-type: none"> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Setting → All Clusters</b></li> <li>Click Promote on the secondary server.</li> <li>Accept the resulting confirmation dialog by clicking OK.</li> </ol>  <p>You see a message display above the Cluster Configuration header indicating successful promotion (see example). If not, retry the operation and/or contact My Oracle Support.</p>  |
| 5. <input type="checkbox"/> | Logout of the CMP GUI                      | Logout of the CMP GUI by clicking <b>Logout</b> link or closing the browser window.   |
| 6. <input type="checkbox"/> | Verify operation via CMP GUI               | <ol style="list-style-type: none"> <li>Login to the CMP GUI using the VIP of CMP Site2</li> <li>In the CMP GUI, navigate to:<br/><b>Platform Setting → Topology Setting → All Clusters</b></li> <li>Ensure all clusters are performing as expected. Follow the procedures listed in this document to bring other failed servers/clusters back online.</li> </ol>  |
| 7. <input type="checkbox"/> | SSH to active node of the promoted cluster | <ul style="list-style-type: none"> <li>For c-Class System:<br/>SSH session from PM&amp;C to the server, using the <b>PM&amp;C GUI → Software → Software Inventory</b> page to obtain the blade IP address:<br/> <pre># ssh admusr@&lt;node_IP_Address&gt; \$ sudo su -</pre> </li> <li>For RMS (DL360/DL380/Oracle X5-2/Netra X5-2) System:<br/>Use the iLO/iLOM (for oracle HW Oracle X5-2 and Netra X5-2) to login, and start a remote console to run commands.</li> </ul>  |



| Step                        | Procedure   | Details   |
|-----------------------------|---|---|
| 8. <input type="checkbox"/> | Verify <b>irepstat</b> command output shows expected status | <ol style="list-style-type: none"> <li>1. Use the SSH session from PM&amp;C to the active node of the promoted CMP cluster.</li> <li>2. Run the <b>irepstat</b> command to verify that cluster replication is active. If not active after 5 minutes, check the CMP GUI for any active alarms.</li> </ol> <pre># irepstat</pre>  <pre>-- Policy 0 ActStb [DbReplication] ----- AA To  Site1-nw-cmp-a Active      0   0.25 1%R 0.04%cpu 65B/s AA To  Site2-nw-cmp-a Active      0   0.50 1%R 0.04%cpu 65B/s</pre> <p>The status of all clusters except known failed servers has a status of Active.</p> <p>Otherwise, if any of the replication paths show <code>DownConnecting</code> contact My Oracle Support.</p> <p>This example shows the installation with servers <code>cs-tb31-cmp2-a</code> and <code>cs-tb31-cmp2-b</code> failed, while all other cluster replication is working.</p>  <pre>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-mpel-b Active          0   0.00 0.05%cpu 82B/s AC To  cs-tb31-mpel-a Active          0   0.00 0.04%cpu 68B/s  irepstat ( 7 lines) (h)elp</pre> |
| 9. <input type="checkbox"/> | Rebuild failed CMP cluster                                  | Refer to <a href="#">Procedure 6: Restoring Complete Cluster without Using the Server Backup</a> to rebuild failed CMP cluster.   |
| ---End of Procedure---      |   |   |



## A. CONTACTING ORACLE

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

### A.1 My Oracle Support

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year:

- Web portal (preferred option): [My Oracle Support](https://support.oracle.com/) at <https://support.oracle.com/>
- Phone: +1.800.223.1711 (toll-free in the US),
- Retrieve your local hotline from [Oracle Global Customer Support Center](http://www.oracle.com/support/contact.html) at <http://www.oracle.com/support/contact.html>

Perform the following selections on the Support telephone menu:

1. Select **2** for New Service Request
2. Then select **3** for Hardware, Networking, and Solaris Operating System Support

- o Select **1** for Technical Issues,

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

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

- o Select **2** for Non-Technical Issues, for example, for My Oracle Support registration.

When talking to the agent, mention that you are a Tekelec Customer to My Oracle Support.

### 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.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 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 are defined as critical and agreed with Oracle.



## **APPENDIX B. RECOVERY OF THIRD PARTY COMPONENTS**

Refer to [9], E53486 Tekelec Platform 7.0.x Configuration Procedure Reference, current revision, for supported recovery procedures for 3<sup>rd</sup> 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