

Oracle® Communications

Disaster Recovery

Policy Management Disaster Recovery Guide Release 15.1

G60309-01

August 2026



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

Oracle Communications Policy Management Disaster Recovery for Release 15.1
Copyright © 2013, 2026 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

Table of Contents

1. INTRODUCTION.....	7
1.1 Purpose and Scope	7
1.2 References.....	7
1.3 Acronyms.....	7
1.3 Logins and Passwords	8
1.4 Software Release Numbering.....	8
1.5 Terminology.....	8
2. GENERAL DESCRIPTION	9
2.1 Single Node Outage MPE/MRA/CMP, with CMP Server Available	9
2.2 Recovery of Complete MPE/MRA 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
3. PROCEDURE OVERVIEW	12
4. PROCEDURE PREPARATION	13
4.1 Purpose and Scope	13
4.2 Recovery Scenarios.....	13
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)	15
4.2.3 Recovery Scenario 3 (Full Cluster Outage of the CMP; Georedundancy Not Available; Other Servers as Needed).....	17
5. RESTORE PROCEDURES	20
5.1 Procedure 1: Restore Standby CMP Node Using the Server Backup File	20
5.2 Procedure 2: Restore Standby CMP Node without Using the Server Backup File.....	26
5.3 Procedure 3: Restore Single MPE/MRA Node Using the Server Backup File.....	31
5.4 Procedure 4: Restore Single MPE/MRA Node without Server Backup File	37
5.5 Procedure 5: Restoring Complete Cluster Using Server Backup Files	43
5.6 Procedure 6: Restoring Complete Cluster without Using the Server Backup	52
5.7 Procedure 7: Restoring CMP Cluster Using the Available System Backup.....	60

5.8 Procedure 8: Promoting Georedundant CMP Cluster.....	67
A. CONTACTING ORACLE.....	70

List of Tables

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

List of Procedures

Procedure 1 Restore standby CMP Node with server backup file	21
Procedure 2 Restore standby CMP Node without server backup file	27
Procedure 3 Restore single MPE/MRA node with server backup file	32
Procedure 4 Restore single MPE/MRA node without server backup file	38
Procedure 5 Restoring complete cluster with the server backup files.....	44
Procedure 6 Restoring complete cluster without the server backup	53
Procedure 7 Restoring CMP cluster with system backup available	61
Procedure 8 Promoting georedundant CMP cluster	67

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 15.1. 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] E53486 Tekelec Platform 7.0.x Configuration Procedure Reference, current revision

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

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
CMP	Configuration Management Platform
DR-CMP	Configuration Management Product for Disaster Recovery NOTE: It refers to the CMP on the secondary site
DVD	Digital Video Disc
GRUB	Grand Unified Boot loader
IPM	Initial Product Manufacture—The process of installing TPD on a hardware platform
FE	Front Endpoint
DRA	Diameter Route 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

Acronym	Meaning
USB	Universal Serial Bus

1.2 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.

1.3 Software Release Numbering

This guide applies to all Policy Management versions 15.1.

1.4 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 servers failed
- Recovery of the entire network from a total outage

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

2.1 Single Node Outage MPE/MRA/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 /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 MPE/MRA Cluster, with CMP Server Available

This scenario applies when all nodes of an MPE or MRA cluster require reconstruction while an operational CMP containing the required Policy Management configuration remains available.

Each failed MPE/MRA node is reconstructed and its initial node configuration is restored either from the corresponding server backup file or manually using Perform Initial Configuration, thus reforming the cluster. 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

When the complete primary CMP cluster has been lost and no usable georedundant CMP exists, the CMP application configuration must first be re-established.

Recover the first CMP node by using its corresponding server backup file or manually using Perform Initial Configuration, followed by doing a system restore using a stored system backup file. This recovers the application-level configuration on the CMP node including policies and configuration of MPE/MRA clusters in the network.

After the first CMP is operational and contains the application configuration, recover the remaining CMP node using the applicable standby-CMP recovery procedure selected for the available backup condition.

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)

A complete-server outage is the most severe recovery condition and can require reconstruction of all Policy Management nodes.

If no CMP is available, recover one CMP first. Restore its Policy Management application configuration from a valid system backup taken from offsite backup storage locations (assuming these were performed and stored offsite before the outage). After the CMP is available, recover the remaining CMP, MPE, and MRA nodes using the applicable procedures.

Server backup files, when available, restore node-specific initial configuration. They do not restore the complete Policy application configuration.

If no usable system backup or georedundant CMP exists, Policy Management application configuration must be reconstructed manually from whatever sources available.

2.6 Performing Initial Configuration

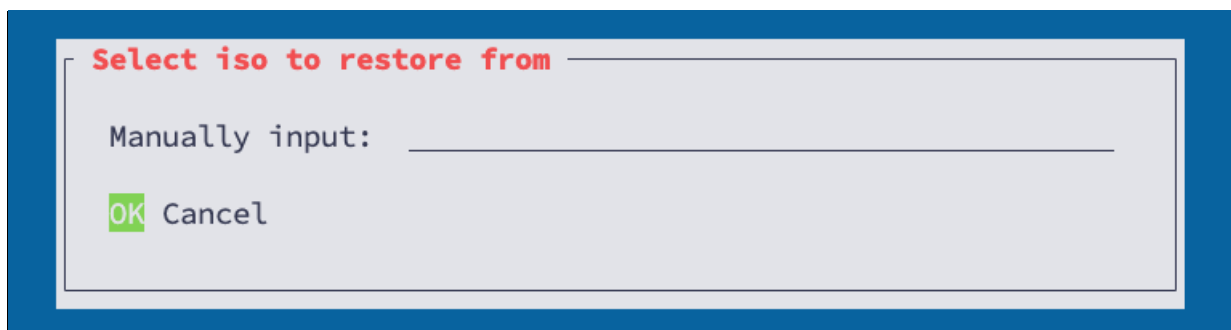
The information required for initial configuration is not extensive, and is readily available from site documents, or from the topology configuration for the CMP. In some cases it is easier to manually enter the initial configuration using the platcfg utility than to try to load a server backup file 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/eth0)

2.7 Using the Server Backup File

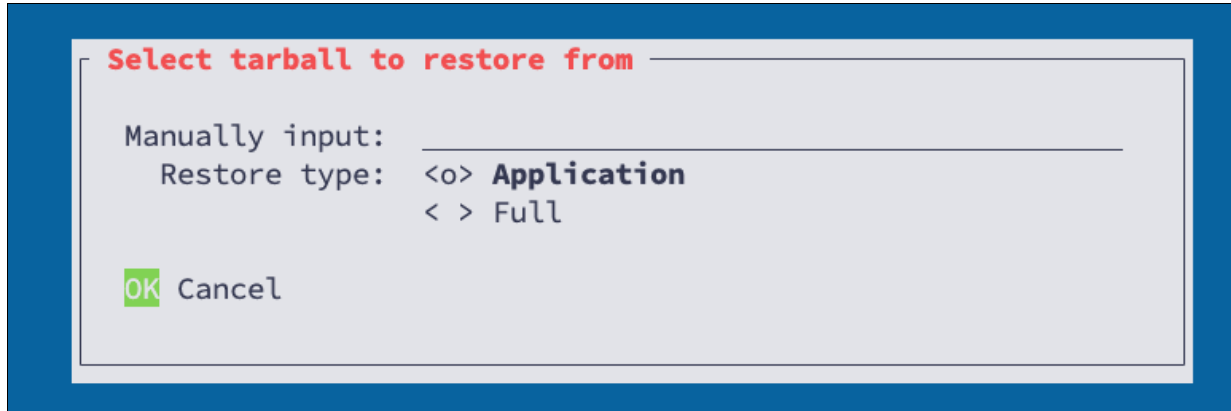
When asked to restore from server backup, the platcfg utility looks in `/var/camiant/backup/local-archive/serverbackup` directory. If the directory is empty, the manual selection dialogue opens.



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.

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. Policy Application installation QCOW/OVA for CMP, MPE, MRA of the target release.
5. 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 Policy configuration information that is unique to this system. Information such as: Topology, 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

The following table highlights all the possible recovery scenarios. As per your failure scenario, choose that specific procedure to follow:

Table: Various failure scenarios and procedure to follow

Failure Scenario	Backup Condition	Procedure to Follow
Standby CMP node failed; surviving CMP available	Server backup available	Procedure 1
Standby CMP node failed; surviving CMP available	Server backup unavailable	Procedure 2
Single MPE/MRA node failed; active CMP and cluster peer available	Server backup available	Procedure 3
Single MPE/MRA node failed; active CMP and cluster peer available	Server backup unavailable	Procedure 4
Primary CMP unavailable; healthy georedundant CMP available	Not applicable to promotion decision	Procedure 8 , followed by the applicable node/cluster recovery procedure
Primary CMP application configuration lost; no usable georedundant CMP	System backup available	Procedure 7 establishes the recovered CMP configuration; then use the applicable CMP- node procedure for the remaining node

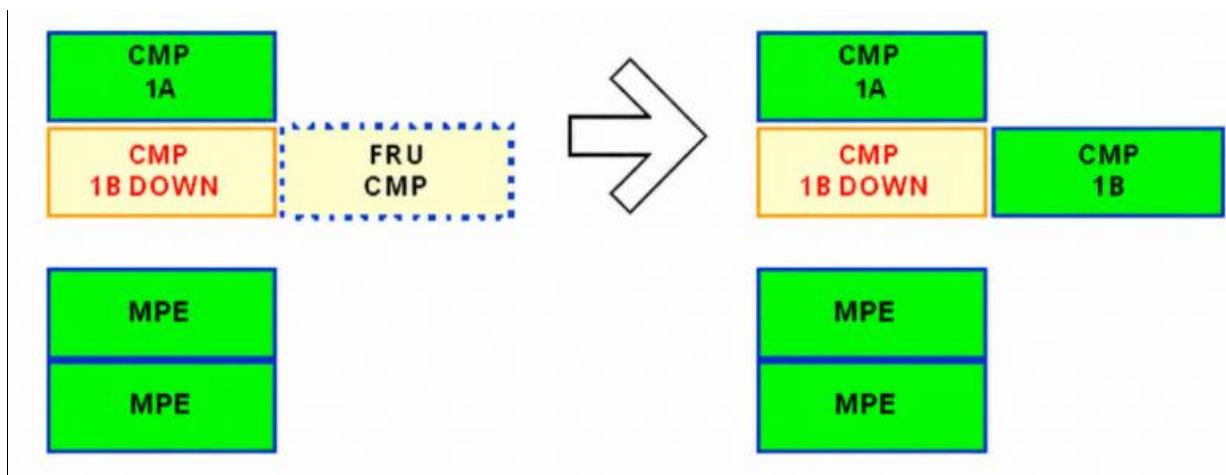
Complete MPE/MRA cluster requires reconstruction; active CMP available	Server backups available	Procedure 5
Complete MPE/MRA cluster requires reconstruction; active CMP available	Server backups unavailable	Procedure 6

If a scenario has both server backups and a system backup, remember that the backup types serve different purposes. The server backup restores node-specific initial configuration. The system backup restores Policy Management application configuration to the CMP.

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

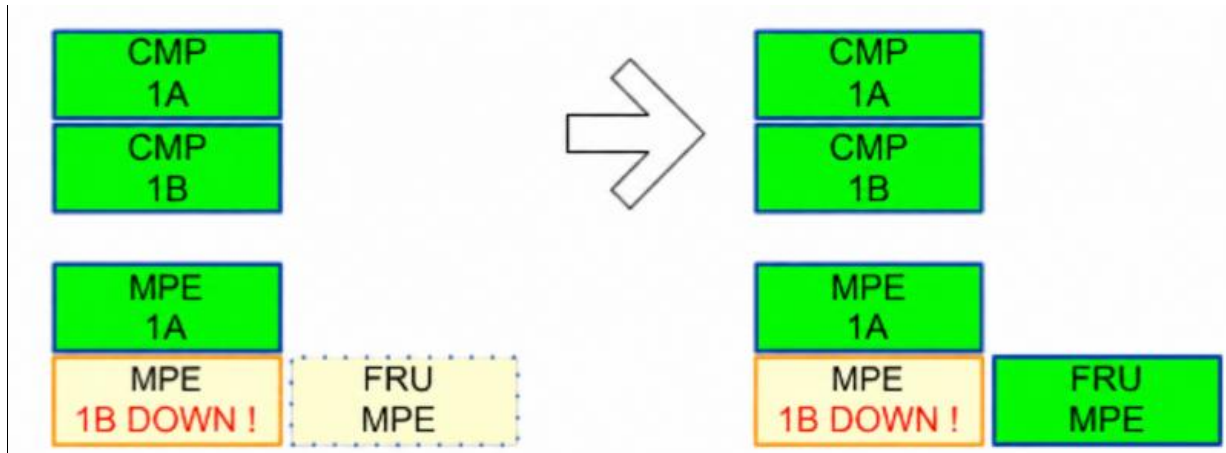
For a partial outage with a CMP server available, only base recovery of hardware and software and initial Policy configuration is needed. A single CMP server is capable of restoring the configuration database via replication to all MPE/MRA servers, or to the other CMP node of a cluster. The major activities are summarized in the 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. Refer the documentation provided by underlying hardware and host for more details. For example, Link for Oracle X9-2 troubleshooting is <https://docs.oracle.com/en/servers/x86/x9-2/service-manual/index.html>
 - 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 servers by recovering base hardware and software.
 - o Recover the base hardware. Refer the documentation provided by underlying hardware and host for more details. For example, Link for Oracle X9-2 troubleshooting is <https://docs.oracle.com/en/servers/x86/x9-2/service-manual/index.html>
 - 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 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 Node without Server Backup File](#) to recover MPE/MRA nodes when one of the peers of the cluster is still available.
Or Procedure 4: Restore Single MPE/MRA 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 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 Node without Server Backup File](#) to recover the second node of MPE/MRA cluster.

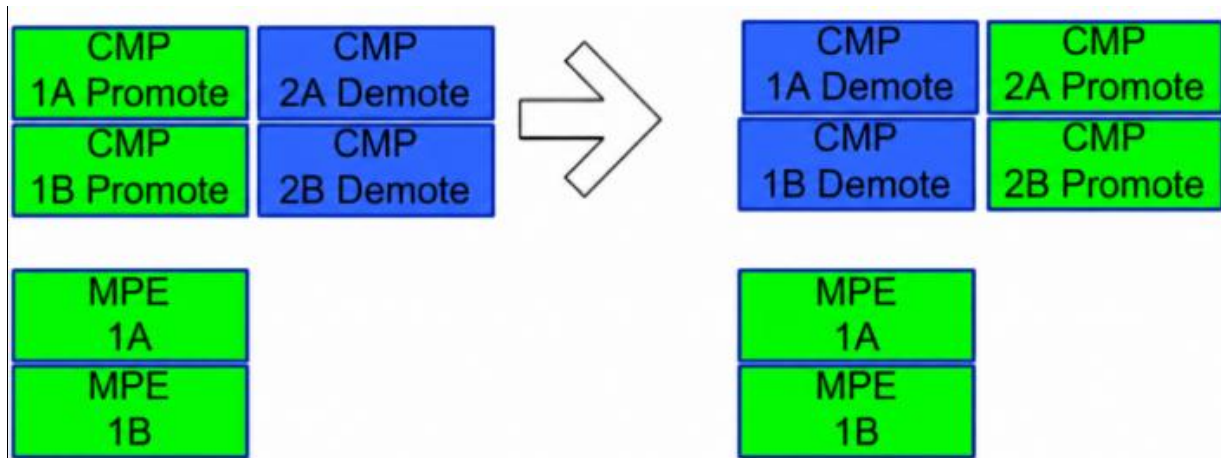
4.2.2 Recovery Scenario 2 (Partial Cluster Outage with Georedundant CMP Server Available)

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 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 MPE, MRA cluster, do not promote the georedundant CMP.

2. Recover any failed MPE/MRA servers by recovering base hardware and software.
 - o Recover the base hardware. Refer the documentation provided by underlying hardware and host for more details. For example, Link for Oracle X9-2 troubleshooting is <https://docs.oracle.com/en/servers/x86/x9-2/service-manual/index.html>
 - 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 servers using the re-apply configuration operation.
3. Recover other site CMP server by recovering base hardware and software.
 - o Recover the base hardware. Refer the documentation provided by underlying hardware and host for more details. For example, Link for Oracle X9-2 troubleshooting is <https://docs.oracle.com/en/servers/x86/x9-2/service-manual/index.html>
 - 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.

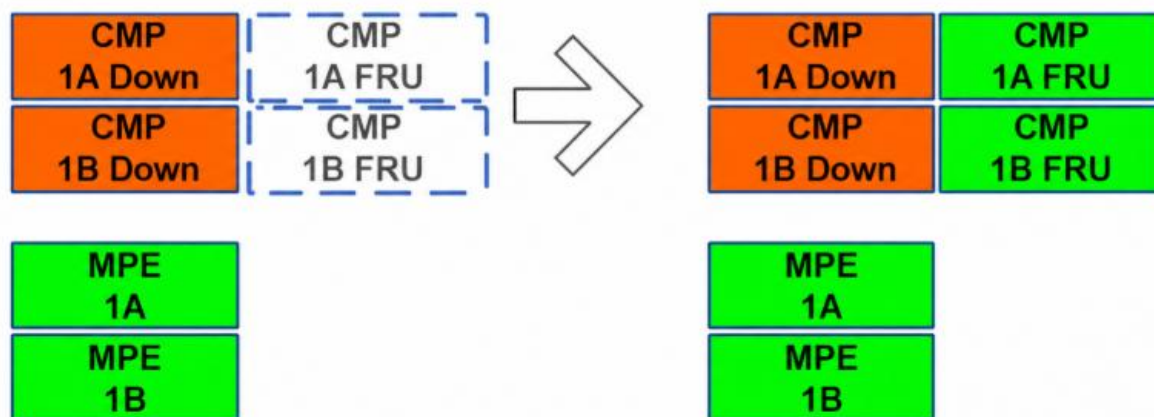
1. Use [Procedure 8: Promoting Georedundant CMP Cluster](#) to promote the georedundant CMP
2. Use [Procedure 4: Restore Single MPE/MRA Node without Server Backup File](#) to recover MPE/MRA nodes when one of the peers of the cluster is still available.
Or [Procedure 4: Restore Single MPE/MRA Node without](#) 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 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 Node without Server Backup File](#) to recover the second node of MPE/MRA 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. Refer the documentation provided by underlying hardware and host for more details. For example, Link for Oracle X9-2 troubleshooting is <https://docs.oracle.com/en/servers/x86/x9-2/service-manual/index.html>
 - 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. Refer the documentation provided by underlying hardware and host for more details. For example, Link for Oracle X9-2 troubleshooting is <https://docs.oracle.com/en/servers/x86/x9-2/service-manual/index.html>
 - 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 servers by recovering base hardware and software.
 - o Recover the base hardware. Refer the documentation provided by underlying hardware and host for more details. For example, Link for Oracle X9-2 troubleshooting is <https://docs.oracle.com/en/servers/x86/x9-2/service-manual/index.html>
 - 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 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 Node without Server Backup File](#) to recover MPE/MRA nodes when one of the peers of the cluster is still available.

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

Notes:

The procedure step sequence in this section is normative and must be followed as documented.

The following conventions apply to Procedures 1 through 8:

Replacement VM: References to the replacement node after VM creation mean the newly instantiated CMP, MPE, or MRA VM, not the previously failed VM.

Console access: Accessing the replacement VM console through the virtualization host.

Server backup: A server backup restores node-specific initial configuration only.

System backup: A system backup restores Policy Management application configuration to the CMP.

Forced Standby: Forced Standby operations in the detailed procedure are retained exactly as documented.

Health verification: ping, syscheck, alarm verification, cluster-status checks, irepstat, SSH-key provisioning, and Reapply Configuration operations remain at the positions defined by the detailed procedure.

5. RESTORE PROCEDURES

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

Use this procedure when one CMP node has failed, the peer CMP remains operational, and a valid server backup for the failed CMP node is available. Using server backup, we restore the initial perform initial configuration information for that node. The surviving CMP retains the CMP database and it re-syncs that database to the replacement node as it joins the cluster.

Required resources:

- Policy APP installation QCOW/OVA.
- *serverbackup*.ISO of the replaced node

Prerequisites:

Remove the failed VM and spawn a CMP VM instance using appropriate VM installation commands for CMP.

For example, Reference command using virt-install:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network
bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network
bridge:bridge2,model=virtio --graphics none --connect qemu:///system --
disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the name, RAM and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

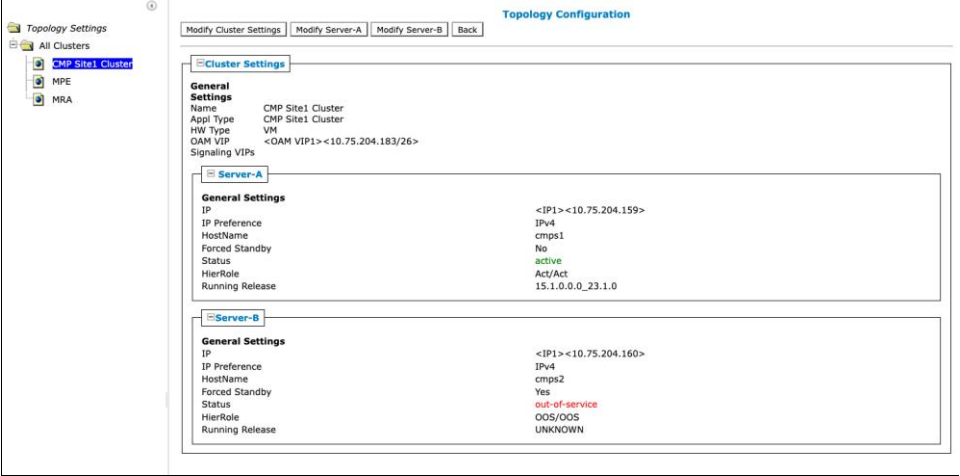
Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

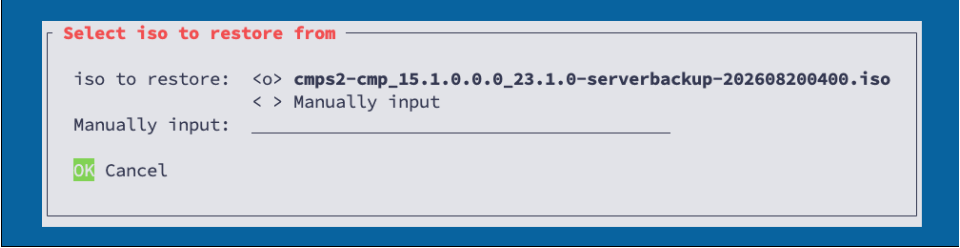
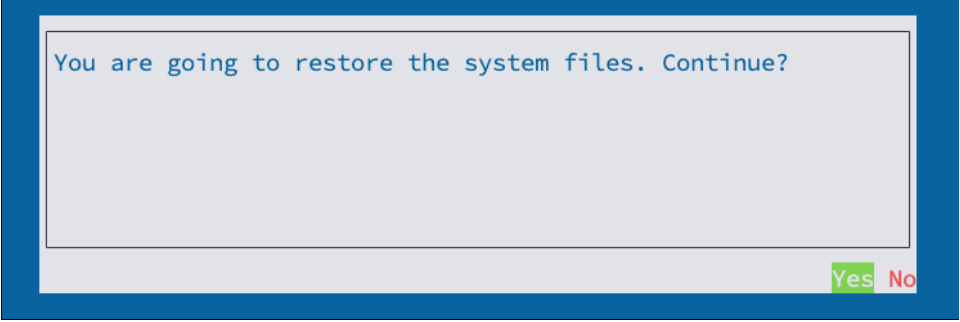
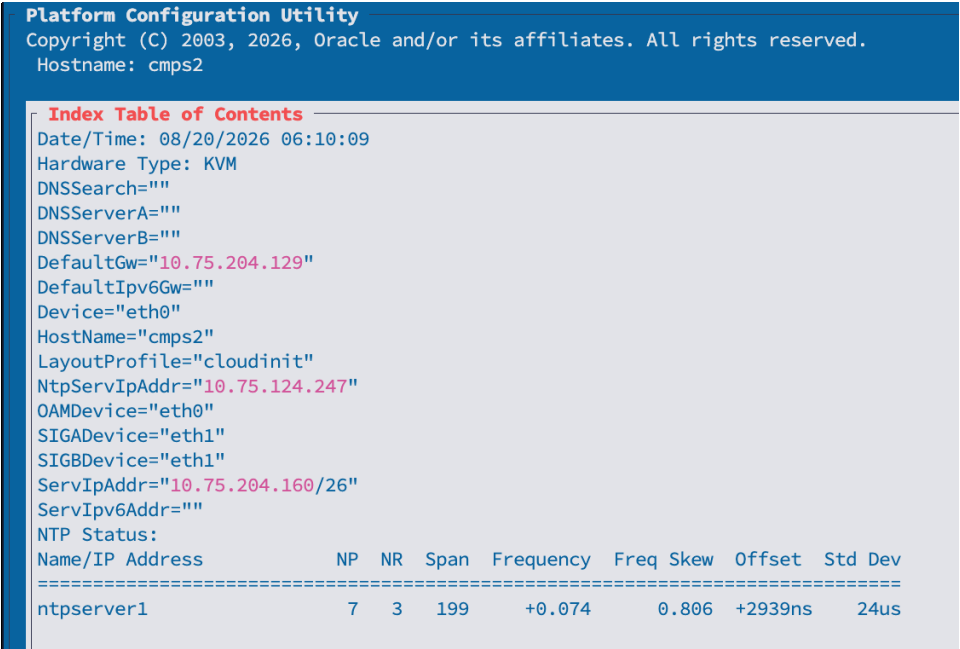
This Procedure restores the standby CMP node when a server level backup is available.

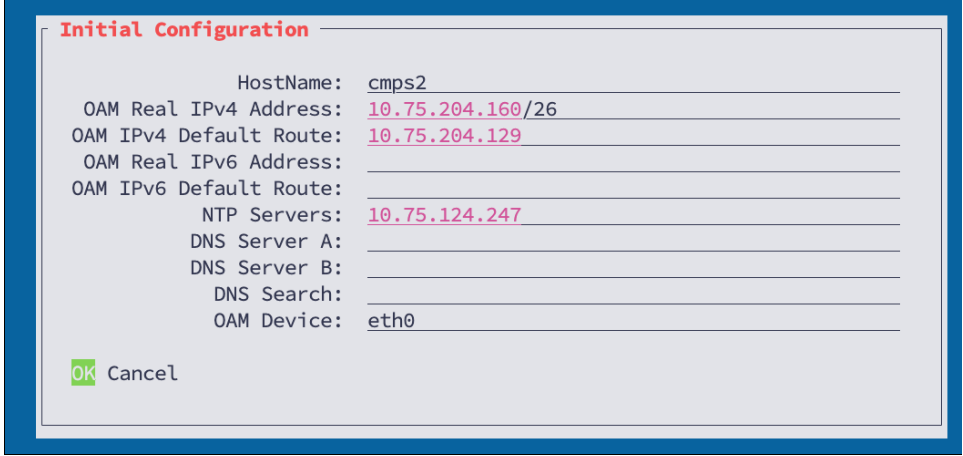
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

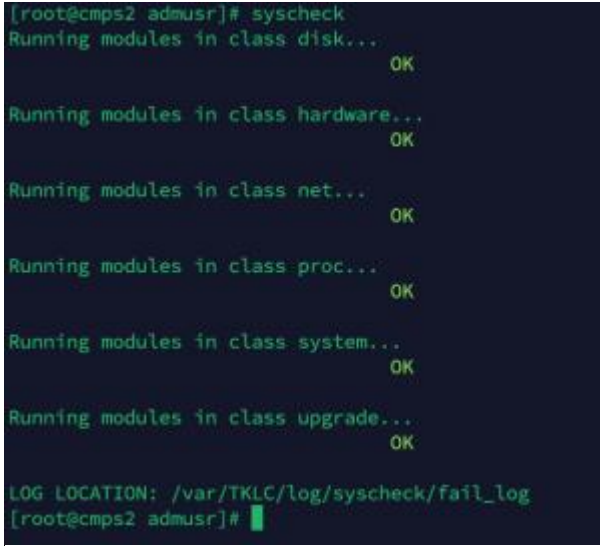
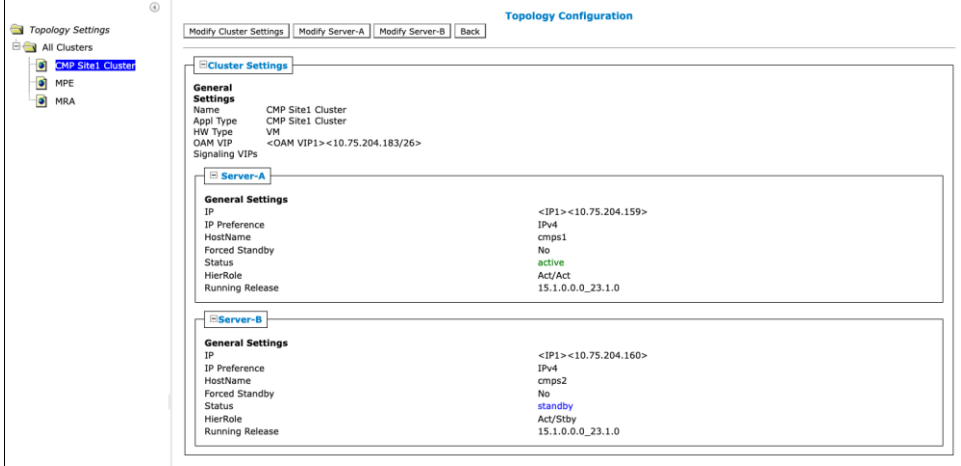
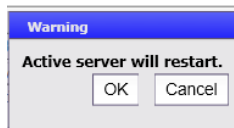
If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

Procedure 1 Restore standby CMP Node with server backup file

Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to: Platform Setting → Topology Settings → All Clusters 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click the Modify Server-X for the failed node 5. Click the Forced Standby checkbox so that it is checked, then click Save 
2. ☐	Load the ISO for server restore	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: <code>/var/camiant/backup/local_archive/serverbackup</code> NOTE: 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.
3. ☐	Access the console of the replacement VM	Access the replacement node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
4. ☐	Perform initial configuration to restore the node's initial information	1. Open the platcfg utility. <pre># su - platcfg</pre> 2. Navigate to: Policy Configuration → Backup and Restore → Server Restore 3. Select the *serverbackup*.ISO that you just put on the system and click OK. 4. Click Yes to confirm.  
5. ☐	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 My Oracle Support or engineering team for assistance.
6. ☐	Perform Initial configuration	1. Click Exit until you return to the Main Menu of the platcfg utility. 2. Navigate to: Policy Configuration → Verify Initial Configuration 

Step	Procedure	Details
		3. If the configuration does not exist, navigate to the Perform Initial Configuration page and enter the hostname, OAM IP, and configuration. 4. Ensure that your data is correct, and click OK. 5. Click Yes to save and apply. 6. Exit the platcfg utility by clicking Exit on each platcfg menu until you are returned to the shell. 
7. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Allow the server time to reboot. Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
8. ☐	Verify basic network connectivity and server health.	- From the installed server, ping the OAM/XML 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. <pre># ping <XMI or OAM gateway address></pre> - Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  <pre>[root@cmps2 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@cmps2 admusr]#</pre>
9. ☐	Remove the Forced Standby designation on the node.	- In the CMP GUI, navigate to: Platform Setting → Topology Settings → All Clusters → <Current Cluster> - Click modify for the server that is in Forced Standby. - Clear the Forced Standby checkbox - Click Save 
		Accept the warning message by clicking OK. 

Step	Procedure	Details
10. ☐	Verify cluster status	1. In the CMP GUI, navigate to: Platform Setting → Topology Settings → All Clusters → <Current Cluster> 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. Topology Settings All Clusters CMP Site1 Cluster MPE MRA Cluster Settings General Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type VM OAM VIP <OAM VIP1><10.75.204.183/26> Signaling VIPs Server-A General Settings IP <IP1><10.75.204.159> IP Preference IPv4 HostName cmps1 Forced Standby No Status active HierRole Act/Act Running Release 15.1.0.0_23.1.0 Server-B General Settings IP <IP1><10.75.204.160> IP Preference IPv4 HostName cmps2 Forced Standby No Status standby HierRole Act/Stby Running Release 15.1.0.0_23.1.0
11. ☐	Alternative method to check replication status	You can monitor the clustering of the de from the shell on the primary node using the irepstat command. To do so, SSH to the active node of the cluster and run the irepstat command: # irepstat Expected irepstat output after cluster has formed: cmps1 A1773.018 cmps1,10.75.204.159 06:18:59 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmps2 Active 0 0.00 1%R 0.06%cpu 65.1/s AC To D0 mpes2 Active 0 0.00 1%R 0.05%cpu 80.8/s AC To D0 mpes1 Active 0 0.01 1%R 0.06%cpu 66.0/s AC To D0 mras1 Active 0 0.01 1%R 0.05%cpu 94.5/s AC To D0 mras2 Active 0 0.01 1%R 0.05%cpu 77.3/s

Step	Procedure	Details
12. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility - As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code> - As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code> <pre>[admusr@cmps1 ~]\$ sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov Subroutine CMNodeInfo::pack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::unpack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. The password of admusr in topology: Connecting to admusr@cmps2 ... Connecting to admusr@mpes2 ... Connecting to admusr@mras1 ... Connecting to admusr@mras2 ... Connecting to admusr@mpes1 ... Connecting to admusr@cmps1 ... [1/6] Provisioning SSH keys on mpes2 ... [2/6] Provisioning SSH keys on cmps2 ... [3/6] Provisioning SSH keys on mpes1 ... [4/6] Provisioning SSH keys on mras2 ... [5/6] Provisioning SSH keys on cmps1 ... [6/6] Provisioning SSH keys on mras1 ... SSH keys are OK. [admusr@cmps1 ~]\$</pre> ---End of Procedure---

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

Use this procedure when one CMP node has failed, the peer CMP remains operational, but a valid server backup for the failed CMP node is NOT available. Initial node configuration is entered manually through Perform Initial Configuration menu in platcfg utility, and wait for the node to re-sync to the existing node to form a complete CMP cluster.

Required resources:

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

Prerequisites:

Remove the failed VM and spawn a CMP VM instance using appropriate VM installation commands for CMP.

For example, Reference command using virt-install:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network
bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network
bridge:bridge2,model=virtio --graphics none --connect qemu:///system --
disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the name, RAM and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

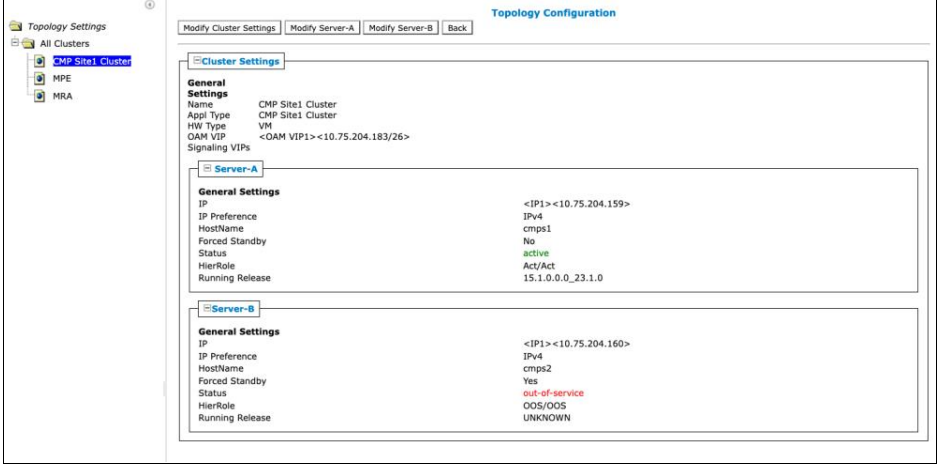
Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

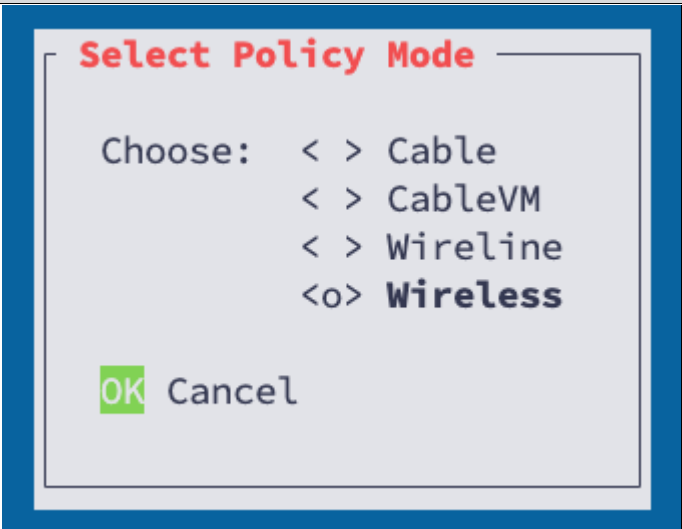
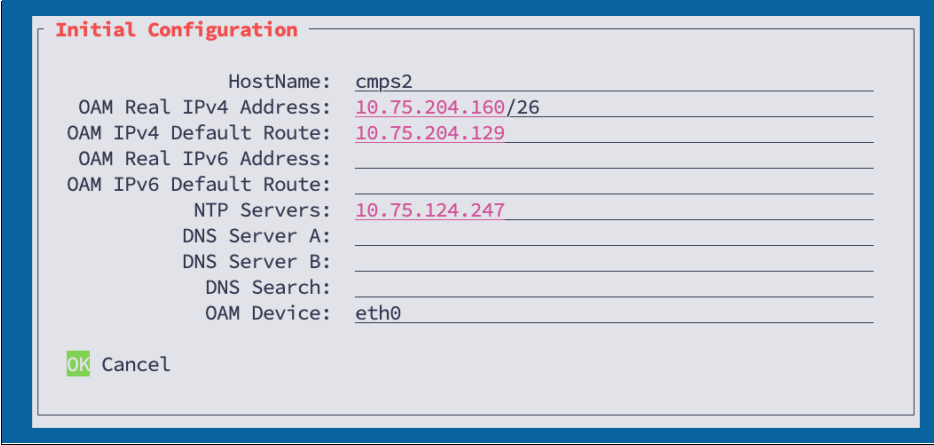
This Procedure restores the standby CMP node when a server level backup file is not available.

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

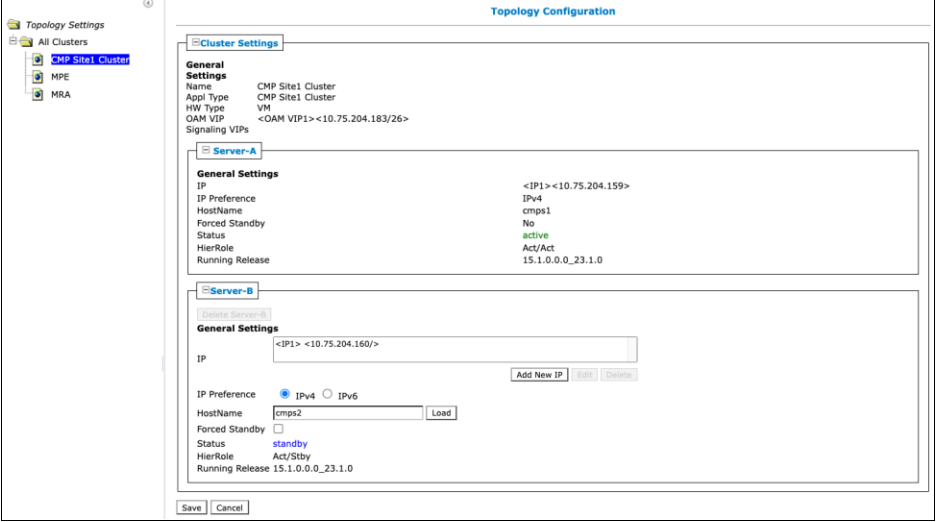
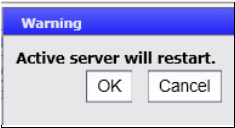
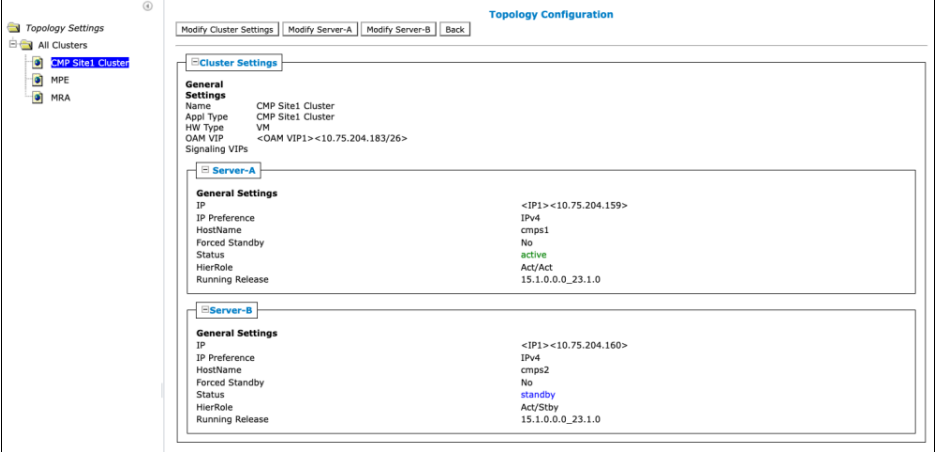
If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

Procedure 2 Restore standby CMP Node without server backup file

Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	- In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters - Determine the cluster with the failed node - Determine the failed node - Click the Modify Server-X for the failed node - Click the Forced Standby checkbox so that it is checked, then click Save 
2. ☐	Access the console of the replacement VM	Access the replacement node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
3. ☐	Perform initial configuration to restore the node's initial information	- Open the platcfg utility. <pre># su - platcfg</pre> - Navigate to: Policy Configuration → Set Policy Mode

Step	Procedure	Details
		 3. Leave the mode as Wireless and click OK to continue. You can skip this step. 4. Navigate to: Policy Configuration → Perform Initial Configuration 5. Enter the configuration details for this node. 6. Verify that entries are correct, and click OK to continue. 7. Accept the dialog that opens asking to apply the configuration. 8. After the operation is complete, click Exit on each platcfg menu until you are returned to the shell. 
4. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
5. ☐	Verify basic network connectivity and server health.	- From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. <pre># ping <XMI or OAM gateway address></pre> - Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. <pre>[root@cmps2 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@cmps2 admusr]#</pre>

Step	Procedure	Details
6. ☐	Remove the Forced Standby designation on the node.	- In the CMP GUI, navigate to: Platform Setting → Topology Setting → <Current_Cluster> - Click modify for the server that is in Forced Standby. - Clear the Forced Standby checkbox - Click Save  - Accept the warning message by clicking OK. 
7. ☐	Verify cluster status	- In the CMP GUI, navigate to: Platform Setting → Topology Settings → All Clusters → <Current CMP Cluster> - 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. 

Step	Procedure	Details
8. ☐	Alternative method to check replication status	You can monitor the clustering of the node from the shell on the primary node using the irepstat command. To do so, SSH to the active node of the cluster and run the irepstat command: <pre># irepstat</pre> Expected irepstat output after cluster has formed: <pre>cmpls1 A1773.018 cmpls1,10.75.204.159 06:18:59 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmpls2 Active 0 0.00 1%R 0.06%cpu 65.1/s AC To D0 mpls2 Active 0 0.00 1%R 0.05%cpu 80.8/s AC To D0 mpls1 Active 0 0.01 1%R 0.06%cpu 66.0/s AC To D0 mras1 Active 0 0.01 1%R 0.05%cpu 94.5/s AC To D0 mras2 Active 0 0.01 1%R 0.05%cpu 77.3/s</pre>
9. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility - As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code> - As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code> <pre>[admusr@cmpls1 ~]\$ sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov Subroutine CMNodeInfo::pack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::unpack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. The password of admusr in topology: Connecting to admusr@cmpls2 ... Connecting to admusr@mpes2 ... Connecting to admusr@mrsl ... Connecting to admusr@mrsl2 ... Connecting to admusr@mpes1 ... Connecting to admusr@cmpls1 ... [1/6] Provisioning SSH keys on mpes2 ... [2/6] Provisioning SSH keys on cmpls2 ... [3/6] Provisioning SSH keys on mpes1 ... [4/6] Provisioning SSH keys on mrsl2 ... [5/6] Provisioning SSH keys on cmpls1 ... [6/6] Provisioning SSH keys on mrsl1 ... SSH keys are OK. [admusr@cmpls1 ~]\$</pre> ---End of Procedure---

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

Use this procedure when one MPE or MRA node has failed, the other node of its cluster remains available, the active CMP is available, and a valid server backup exists for the failed node. 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.

Required resources:

- Policy APP installation QCOW/OVA.
- *serverbackup*.ISO for the replacment node

Prerequisites:

Remove the failed VM and spawn a MPE/MRA VM instance using appropriate VM installation commands for MPE/MRA.

For example, Reference command using virt-install:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network
bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network
bridge:bridge2,model=virtio --graphics none --connect qemu:///system --
disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the name, RAM and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

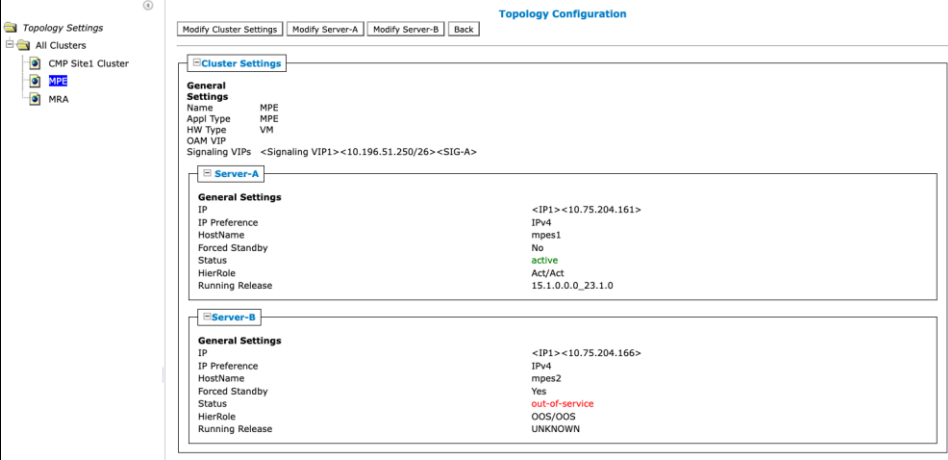
Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

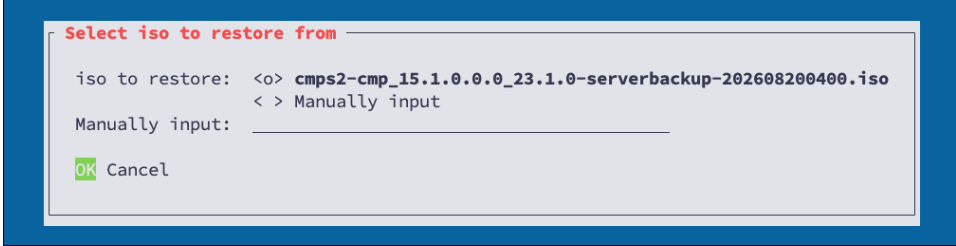
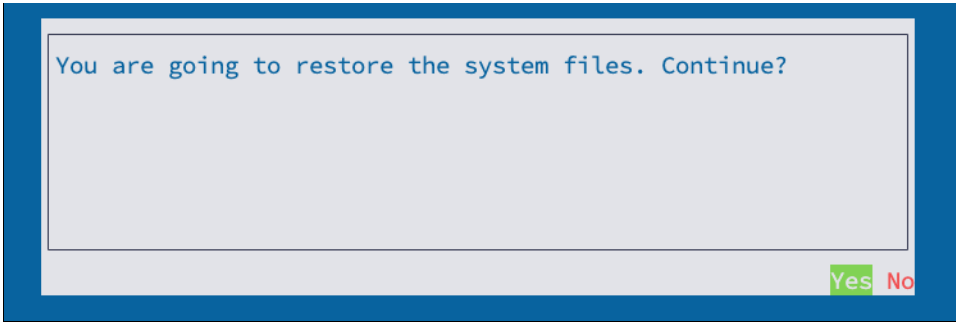
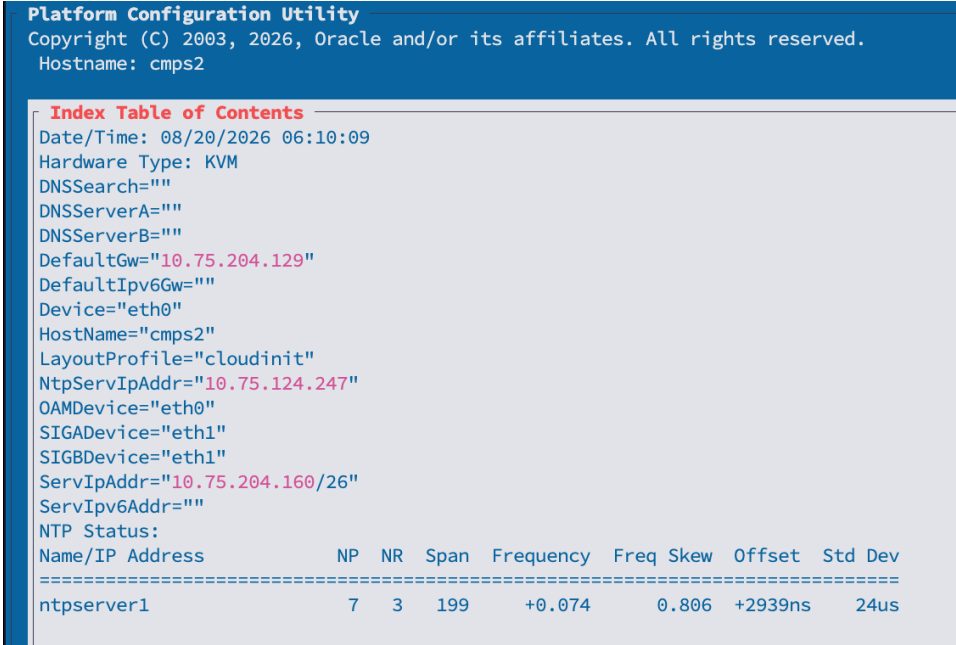
This procedure performs Restore single MPE/MRA node with server backup file.

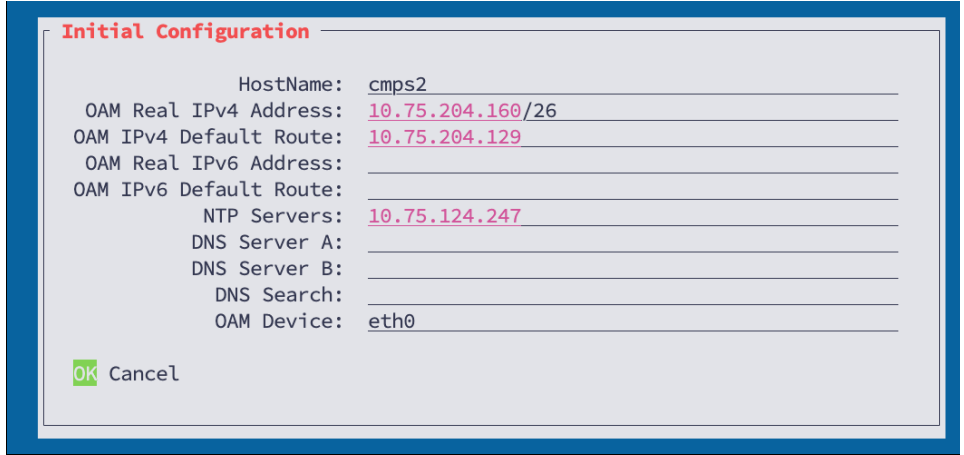
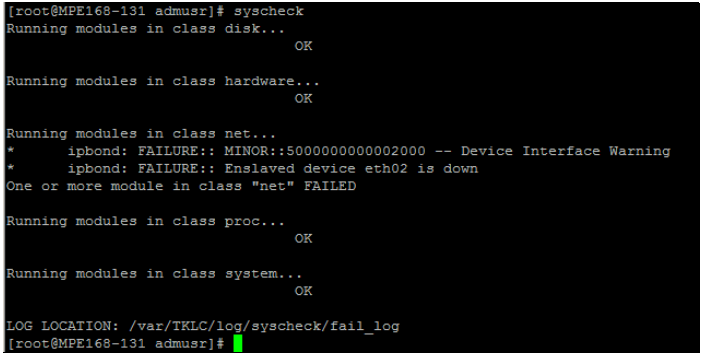
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

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

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

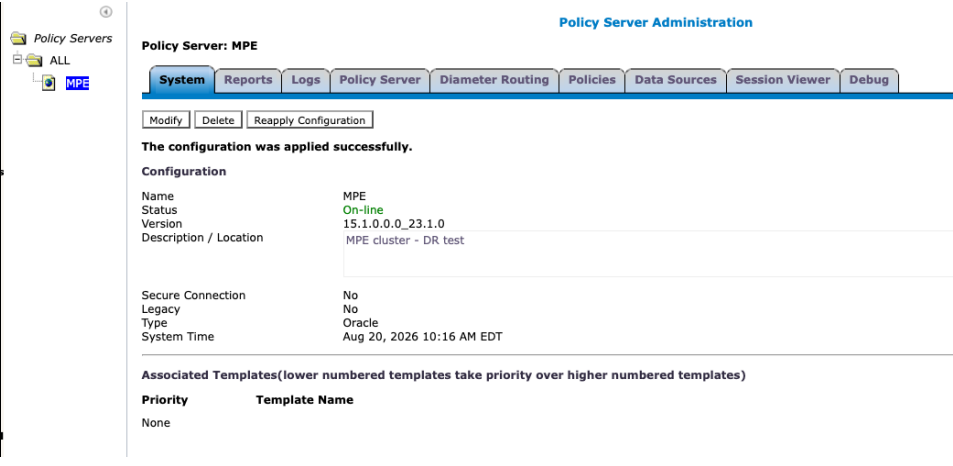
Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click the Modify Server-X for the failed node 5. Click the Forced Standby checkbox so that it is checked, then click Save 
2. ☐	Load the ISO for server backup	Obtain the *serverbackup.iso* for the 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: <pre>/var/camiant/backup/local_archive/serverbackup</pre> NOTE: 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.
3. ☐	Access the console of the replacement VM	Access the replacement node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
4. ☐	Perform platcfg restore from SSH session to replacement hardware	- Open the platcfg utility. <pre># su - platcfg</pre> - Navigate to: Policy Configuration → Backup and Restore → Server Restore - Select the *serverbackup*.ISO that you just put on the system and click OK. - Click Yes to confirm.  
5. ☐	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 My Oracle Support or engineering team for assistance.
6. ☐	Perform Initial configuration	- Click Exit on each platcfg menu until you are returned to the Main Menu of the platcfg utility. - Navigate to: Policy Configuration → Verify Initial Configuration 

Step	Procedure	Details
		3. If the configuration does not exist, navigate to Perform Initial Configuration and enter the initial configuration hostname, OAM IP, and NTP servers configurations. 
9. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
10. ☐	Verify basic network connectivity and server health.	1. 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. <pre># ping <XMI or OAM gateway address></pre> 2. Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 

Step	Procedure	Details																											
11. ☐	Remove the Forced Standby designation on the node.	1. In the CMP GUI, navigate to: Platform Setting → Topology Settings → All Clusters → <Current Cluster> 2. Click modify for the server that is in Forced Standby. 3. Clear the Forced Standby checkbox 4. Click Save Topology Settings All Clusters CMP Site1 Cluster MPE MRA Topology Configuration Cluster Settings General Settings NameMPE Appl TypeMPE HW TypeVM OAM VIP Signaling VIPs<Signaling VIP1><10.196.51.250/26><SIG-A> Server-A General Settings IP<IP1><10.75.204.161> IP PreferenceIPv4 HostNamempes1 Forced StandbyNo Statusactive HierRoleAct/Act Running Release15.1.0.0.0_23.1.0 Server-B Delete Server-B General Settings IP<IP1><10.75.204.166/> IP PreferenceIPv4IPv6 HostNamempes2 Forced Standby Statusstandby HierRoleAct/Stby Running Release15.1.0.0.0_23.1.0 SaveCancel 5. Accept the warning message by clicking OK. Warning Active server will restart. OKCancel																											
12. ☐	Check status	1. In the CMP GUI, depending on the type of the node, perform the following: If this is an MPE node, navigate to: Policy→ Configuration → All→<Recovered MPE Cluster>→ Reports tab If this is an MRA node, navigate to: MRA → Configuration → All →<Recovered MRA Cluster>→ Reports tab 2. Monitor clustering of the node to its peer, do not proceed until the Cluster Status changes from Degraded to On-line. Policy Server Administration SystemReportsLogsPolicy ServerDiameter RoutingPoliciesData SourcesSession ViewerDebug Cluster Information Report Mode: Active Reset CountersRediscover ClusterPause Cluster: MPE Cluster StatusOn-line Blades <table><thead><tr><th></th><th>State</th><th>HierRole</th><th>Blade Failures</th><th>Uptime</th><th>Disk</th><th>CPU</th><th>Memory</th><th>Actions</th></tr></thead><tbody><tr><td>10.75.204.161 (Server-A)</td><td>Active</td><td>Act/Act</td><td>1</td><td>1 day 7 hours 17 mins 13 secs</td><td>0.25 %</td><td>4 %</td><td>29 %</td><td>RestartReboot</td></tr><tr><td>10.75.204.166 (Server-B)</td><td>Standby</td><td>Act/Stby</td><td>2</td><td>3 mins 23 secs</td><td>0.22 %</td><td>5 %</td><td>17 %</td><td>RestartReboot</td></tr></tbody></table>		State	HierRole	Blade Failures	Uptime	Disk	CPU	Memory	Actions	10.75.204.161 (Server-A)	Active	Act/Act	1	1 day 7 hours 17 mins 13 secs	0.25 %	4 %	29 %	RestartReboot	10.75.204.166 (Server-B)	Standby	Act/Stby	2	3 mins 23 secs	0.22 %	5 %	17 %	RestartReboot
	State	HierRole	Blade Failures	Uptime	Disk	CPU	Memory	Actions																					
10.75.204.161 (Server-A)	Active	Act/Act	1	1 day 7 hours 17 mins 13 secs	0.25 %	4 %	29 %	RestartReboot																					
10.75.204.166 (Server-B)	Standby	Act/Stby	2	3 mins 23 secs	0.22 %	5 %	17 %	RestartReboot																					

Step	Procedure	Details
13. ☐	Alternative method to check replication status	You can monitor the clustering of the node from the shell on the primary node using the irepstat command. To do so, SSH to the active node of the cluster and run the irepstat command: <pre># irepstat</pre> Expected irepstat output while waiting reconnection: <pre>cmpls1 A1773.018 cmpls1,10.75.204.159 10:09:39 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmpls2 Active 0 0.00 1%R 0.06%cpu 90.0/s AC To D0 mpes1 Active 0 0.00 1%R 0.06%cpu 92.5/s AC To D0 mras1 Active 0 0.01 1%R 0.06%cpu 69.1/s AC To D0 mras2 Active 0 0.01 1%R 0.04%cpu 85.1/s ~</pre> Expected irepstat output after cluster has formed: <pre>cmpls1 A1773.018 cmpls1,10.75.204.159 10:15:23 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmpls2 Active 0 0.10 1%R 0.06%cpu 105.3/s AC To D0 mpes2 Active 0 0.11 1%R 0.05%cpu 94.4/s AC To D0 mpes1 Active 0 0.10 1%R 0.06%cpu 106.9/s AC To D0 mras1 Active 0 0.11 1%R 0.05%cpu 107.7/s AC To D0 mras2 Active 0 0.11 1%R 0.05%cpu 110.2/s ~</pre>
14. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility - As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code> - As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code> <pre>[admusr@cmpls1 ~]\$ sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov Subroutine CMNodeInfo::pack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::unpack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. The password of admusr in topology: Connecting to admusr@cmpls2 ... Connecting to admusr@mpes2 ... Connecting to admusr@mras1 ... Connecting to admusr@mras2 ... Connecting to admusr@mpes1 ... Connecting to admusr@cmpls1 ... [1/6] Provisioning SSH keys on mpes2 ... [2/6] Provisioning SSH keys on cmpls2 ... [3/6] Provisioning SSH keys on mpes1 ... [4/6] Provisioning SSH keys on mras2 ... [5/6] Provisioning SSH keys on cmpls1 ... [6/6] Provisioning SSH keys on mras1 ... SSH keys are OK. [admusr@cmpls1 ~]\$</pre>

Step	Procedure	Details
15. ☐	Reapply Configuration	In the CMP GUI, click Reapply Configuration on the MPE/MRA cluster. The CMP displays the message: The configuration was applied successfully.  ---End of Procedure---

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

Use this procedure when one MPE or MRA node has failed, the other node of its cluster and the active CMP remain available, and no valid server backup is available for the failed node. In this procedure, we manually perform the initial configuration on the replacement node and then the active node synchronizes data to the recovered node.

Required resources:

- Policy APP installation QCOW/OVA.
- 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:

Remove the failed VM and spawn a MPE/MRA VM instance using appropriate VM installation commands for MPE/MRA.

For example, Reference command using virt-install:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network
bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network
bridge:bridge2,model=virtio --graphics none --connect qemu:///system --
disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the name, RAM and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

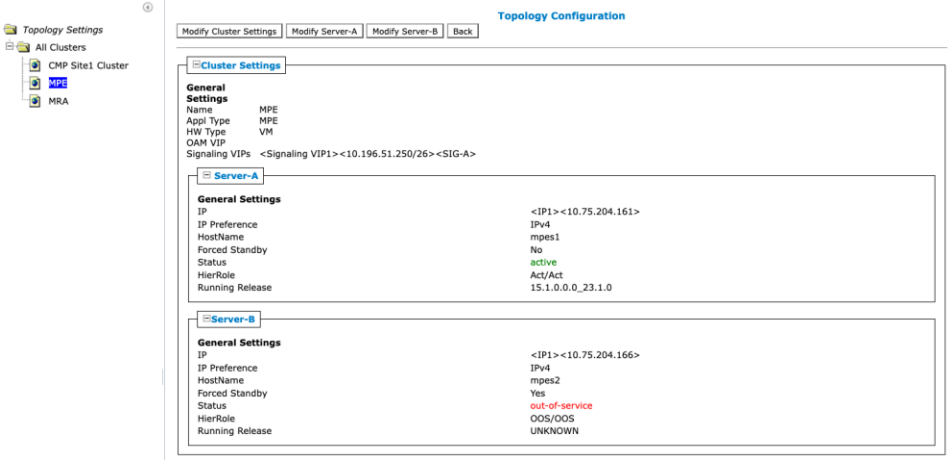
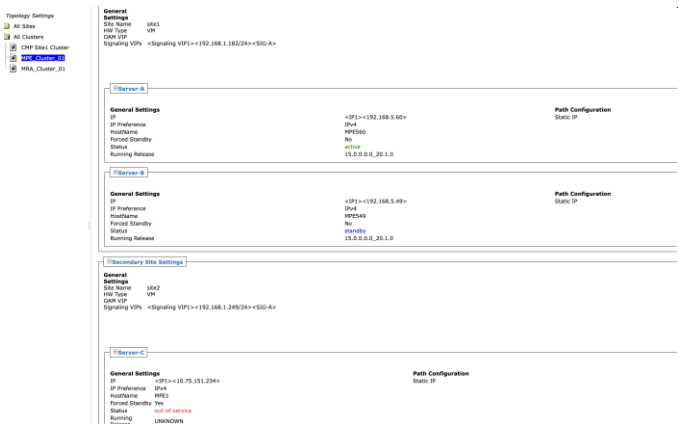
Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

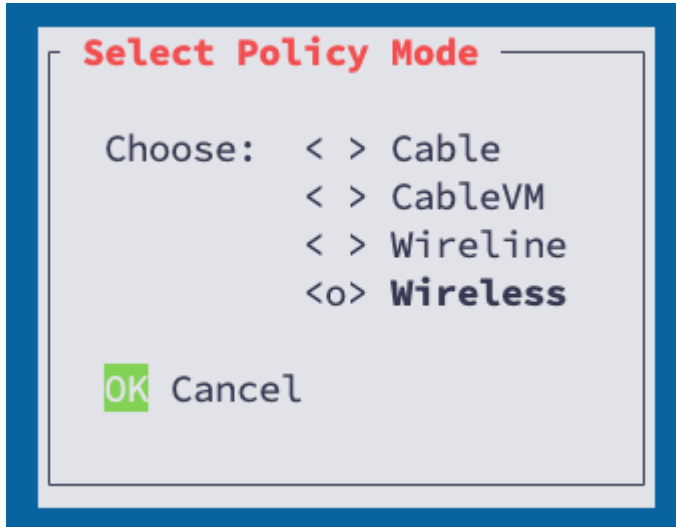
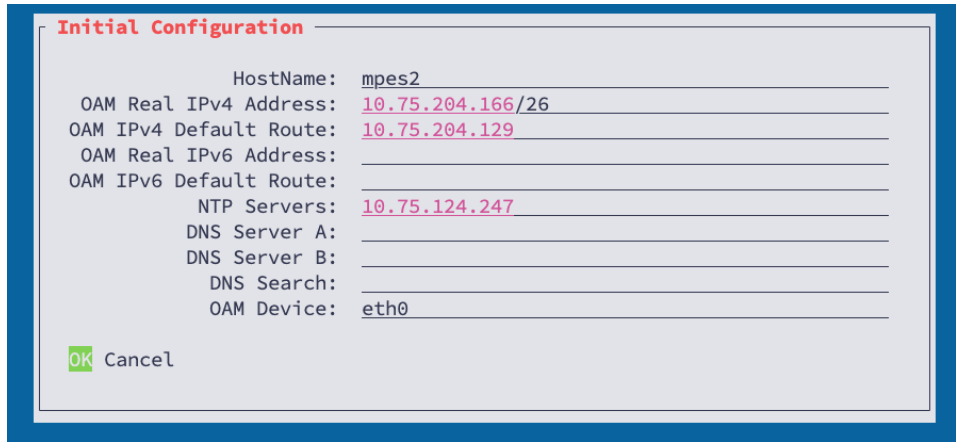
This Procedure performs Restore single MPE/MRA node without server backup file

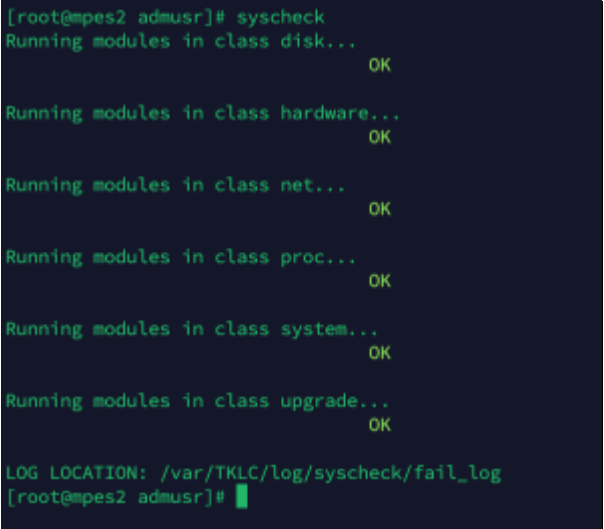
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

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

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

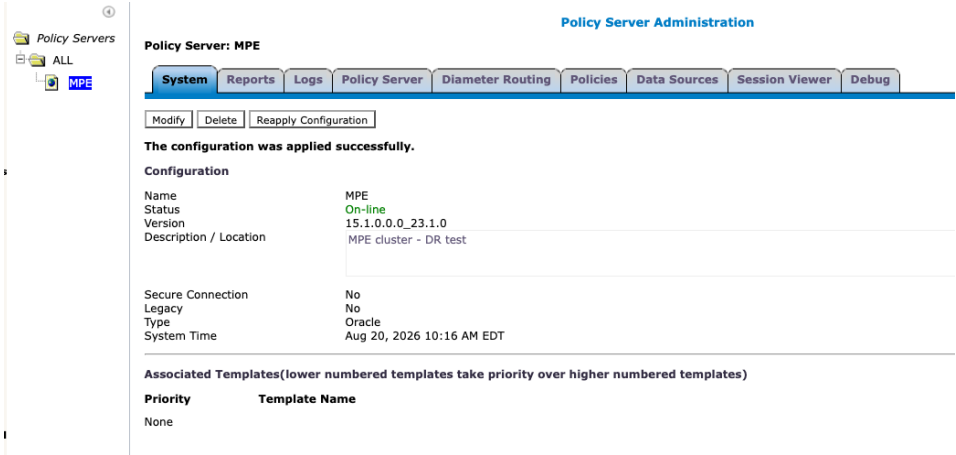
Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters 2. Determine the cluster with the failed node 3. Determine the failed node NOTE: It is possible for a GeoRedundant Topology, that the failed server C node is the spare Server-C. 4. Click the Modify Server-X for the failed node 5. Select Forced Standby so that it is checked, then click Save  Server-C (spare): In a GeoRedundant Topology 
2. ☐	Access the console of the replacement VM	Access the replacement node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
3. ☐	Perform Initial Policy Configuration using the platcfg utility on the installed node	- Open the platcfg utility. <pre># su - platcfg</pre> - Navigate to: Policy Configuration → Set Policy Mode  - Leave the mode as Wireless and click OK to continue. You can skip this step. - Navigate to: Policy Configuration → Perform Initial Configuration - Enter the configuration details from the node being replaced: 
4. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
5. ☐	Verify basic network connectivity and server health.	- From the installed server, ping the OAM/XML gateway. If the ping is not successful, verify that all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if the network ping tests still fail. <pre># ping <XMI or OAM gateway address></pre> - Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  <pre>[root@mpes2 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@mpes2 admusr]#</pre>

Step	Procedure	Details																																			
6. ☐	Remove the Forced Standby designation on the node.	1. In the CMP GUI, navigate to: Platform Setting → Topology Setting → Current Cluster 2. Modify for the server that has Forced Standby 3. Clear the Forced Standby checkbox 4. Click Save Topology Settings All Clusters CMP Site1 Cluster MPE MRA Topology Configuration Cluster Settings General Settings NameMPE Appl TypeMPE HW TypeVM OSAM VIP Signaling VIPs<Signaling VIP1><10.196.51.250/26><SIG-A> Server-A General Settings IP<IP1><10.75.204.161> IP PreferenceIPv4 HostNamempes1 Forced StandbyNo Statusactive HierRoleAct/Act Running Release15.1.0.0_23.1.0 Server-B Delete Server-B General Settings IP<IP1><10.75.204.166/> IP PreferenceIPv4IPv6 HostNamempes2 Forced Standby Statusstandby HierRoleAct/Stby Running Release15.1.0.0_23.1.0 SaveCancel 5. Accept the warning dialog by clicking OK. Warning Active server will restart. OKCancel <tr><td>9. ☐</td><td>Check status</td><td> 1. In the CMP GUI, depending on the type of the node, perform the following: If this is an MPE node, navigate to: Policy Server → Configuration → All→<Recovered MPE Cluster>→ Reports tab If this is an MRA node, navigate to: MRA → Configuration → All →<Recovered MRA Cluster>→ Reports tab 2. Monitor clustering of the node to its peer, do not proceed until the Cluster Status changes from Degraded to On-line. Policy Server Administration Policy Server: MPE SystemReportsLogsPolicy ServerDiameter RoutingPoliciesData SourcesSession ViewerDebug Cluster Information Report Mode: Active Reset CountersRediscover ClusterPause Cluster: MPE Cluster StatusOn-line Blades <table><thead><tr><th></th><th>State</th><th>HierRole</th><th>Blade Failures</th><th>Overall</th><th>Uptime</th><th>Utilization</th><th>Actions</th></tr><tr><th></th><th></th><th></th><th></th><th></th><th></th><th>DiskCPUMemory</th><th></th></tr></thead><tbody><tr><td>10.75.204.161 (Server-A)</td><td>Active</td><td>Act/Act</td><td>1</td><td></td><td>1 day 7 hours 17 mins 13 secs</td><td>0.25 %4 %29 %</td><td>RestartReboot</td></tr><tr><td>10.75.204.166 (Server-B)</td><td>Standby</td><td>Act/Stby</td><td>2</td><td></td><td>3 mins 23 secs</td><td>0.22 %5 %17 %</td><td>RestartReboot</td></tr></tbody></table> </td></tr>	9. ☐	Check status	1. In the CMP GUI, depending on the type of the node, perform the following: If this is an MPE node, navigate to: Policy Server → Configuration → All→<Recovered MPE Cluster>→ Reports tab If this is an MRA node, navigate to: MRA → Configuration → All →<Recovered MRA Cluster>→ Reports tab 2. Monitor clustering of the node to its peer, do not proceed until the Cluster Status changes from Degraded to On-line. Policy Server Administration Policy Server: MPE SystemReportsLogsPolicy ServerDiameter RoutingPoliciesData SourcesSession ViewerDebug Cluster Information Report Mode: Active Reset CountersRediscover ClusterPause Cluster: MPE Cluster StatusOn-line Blades <table><thead><tr><th></th><th>State</th><th>HierRole</th><th>Blade Failures</th><th>Overall</th><th>Uptime</th><th>Utilization</th><th>Actions</th></tr><tr><th></th><th></th><th></th><th></th><th></th><th></th><th>DiskCPUMemory</th><th></th></tr></thead><tbody><tr><td>10.75.204.161 (Server-A)</td><td>Active</td><td>Act/Act</td><td>1</td><td></td><td>1 day 7 hours 17 mins 13 secs</td><td>0.25 %4 %29 %</td><td>RestartReboot</td></tr><tr><td>10.75.204.166 (Server-B)</td><td>Standby</td><td>Act/Stby</td><td>2</td><td></td><td>3 mins 23 secs</td><td>0.22 %5 %17 %</td><td>RestartReboot</td></tr></tbody></table>		State	HierRole	Blade Failures	Overall	Uptime	Utilization	Actions							DiskCPUMemory		10.75.204.161 (Server-A)	Active	Act/Act	1		1 day 7 hours 17 mins 13 secs	0.25 %4 %29 %	RestartReboot	10.75.204.166 (Server-B)	Standby	Act/Stby	2		3 mins 23 secs	0.22 %5 %17 %	RestartReboot
9. ☐	Check status	1. In the CMP GUI, depending on the type of the node, perform the following: If this is an MPE node, navigate to: Policy Server → Configuration → All→<Recovered MPE Cluster>→ Reports tab If this is an MRA node, navigate to: MRA → Configuration → All →<Recovered MRA Cluster>→ Reports tab 2. Monitor clustering of the node to its peer, do not proceed until the Cluster Status changes from Degraded to On-line. Policy Server Administration Policy Server: MPE SystemReportsLogsPolicy ServerDiameter RoutingPoliciesData SourcesSession ViewerDebug Cluster Information Report Mode: Active Reset CountersRediscover ClusterPause Cluster: MPE Cluster StatusOn-line Blades <table><thead><tr><th></th><th>State</th><th>HierRole</th><th>Blade Failures</th><th>Overall</th><th>Uptime</th><th>Utilization</th><th>Actions</th></tr><tr><th></th><th></th><th></th><th></th><th></th><th></th><th>DiskCPUMemory</th><th></th></tr></thead><tbody><tr><td>10.75.204.161 (Server-A)</td><td>Active</td><td>Act/Act</td><td>1</td><td></td><td>1 day 7 hours 17 mins 13 secs</td><td>0.25 %4 %29 %</td><td>RestartReboot</td></tr><tr><td>10.75.204.166 (Server-B)</td><td>Standby</td><td>Act/Stby</td><td>2</td><td></td><td>3 mins 23 secs</td><td>0.22 %5 %17 %</td><td>RestartReboot</td></tr></tbody></table>		State	HierRole	Blade Failures	Overall	Uptime	Utilization	Actions							DiskCPUMemory		10.75.204.161 (Server-A)	Active	Act/Act	1		1 day 7 hours 17 mins 13 secs	0.25 %4 %29 %	RestartReboot	10.75.204.166 (Server-B)	Standby	Act/Stby	2		3 mins 23 secs	0.22 %5 %17 %	RestartReboot			
	State	HierRole	Blade Failures	Overall	Uptime	Utilization	Actions																														
						DiskCPUMemory																															
10.75.204.161 (Server-A)	Active	Act/Act	1		1 day 7 hours 17 mins 13 secs	0.25 %4 %29 %	RestartReboot																														
10.75.204.166 (Server-B)	Standby	Act/Stby	2		3 mins 23 secs	0.22 %5 %17 %	RestartReboot																														

Step	Procedure	Details
10. ☐	Alternative method to check replication status	Monitor the clustering of the node from the shell on the primary node using the irepstat command. To do so, SSH to the active node of the cluster and run the irepstat command: <pre># irepstat</pre> Expected irepstat output while waiting reconnection: <pre>cmps1 A1773.018 cmps1,10.75.204.159 10:09:39 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmps2 Active 0 0.00 1%R 0.06%cpu 90.0/s AC To D0 mpes1 Active 0 0.00 1%R 0.06%cpu 92.5/s AC To D0 mras1 Active 0 0.01 1%R 0.06%cpu 69.1/s AC To D0 mras2 Active 0 0.01 1%R 0.04%cpu 85.1/s ~</pre> Expected irepstat output after cluster has formed: <pre>cmps1 A1773.018 cmps1,10.75.204.159 10:15:23 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmps2 Active 0 0.10 1%R 0.06%cpu 105.3/s AC To D0 mpes2 Active 0 0.11 1%R 0.05%cpu 94.4/s AC To D0 mpes1 Active 0 0.10 1%R 0.06%cpu 106.9/s AC To D0 mras1 Active 0 0.11 1%R 0.05%cpu 107.7/s AC To D0 mras2 Active 0 0.11 1%R 0.05%cpu 110.2/s ~</pre>
11. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility - As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code> - As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code> <pre>[root@cmps1 admusr]# /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=admusr Subroutine CMNodeInfo::pack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::unpack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. The password of admusr in topology: Connecting to admusr@mpes1 ... Connecting to admusr@cmps2 ... Connecting to admusr@mpes2 ... Connecting to admusr@mras2 ... Connecting to admusr@mras1 ... Connecting to admusr@cmps1 ... [1/6] Provisioning SSH keys on mras2 ... [2/6] Provisioning SSH keys on mpes2 ... [3/6] Provisioning SSH keys on cmps1 ... [4/6] Provisioning SSH keys on mpes1 ... [5/6] Provisioning SSH keys on cmps2 ... [6/6] Provisioning SSH keys on mras1 ... SSH keys are OK. [root@cmps1 admusr]#</pre>

Step	Procedure	Details
12. ☐	Reapply Configuration	In the CMP GUI, click Reapply Configuration on the MPE/MRA cluster. The CMP displays the message: The configuration was applied successfully.  ---End of Procedure---

5.5 Procedure 5: Restoring Complete Cluster Using Server Backup Files

This procedure is directly applicable to complete MPE/MRA cluster recovery when an active CMP containing the required Policy Management configuration is available.

For MPE/MRA recovery, the server backups restore the node-specific initial configuration of the replacement nodes. After the nodes are restored and the cluster is re-established, the application-level policy configuration is reapplied from the active CMP.

For a complete CMP cluster recovery, the source of the application-level Policy configuration depends on the disaster-recovery scenario:

If the cluster being recovered is a CMP cluster, do not interpret the reference to configuration being pushed “from the active CMP” as universally applicable. CMP application-configuration recovery depends on the outage scenario:

→ If a georedundant CMP is available, it must first be made the active CMP according to procedure 8. The failed CMP cluster can then be restored using this Procedure 5, with the active CMP providing the application-level configuration.

→ If the entire CMP cluster is unavailable and no georedundant CMP is available, the CMP application configuration must first be restored from a valid system backup using Procedure 7: Restoring CMP Cluster Using the Available System Backup.

Required resources:

- Policy APP installation QCOW/OVA.
- *serverbackup*.iso for the replacement node

Prerequisites:

Remove the failed VM and spawn the appropriate replacement VMs for the cluster type being recovered.

For example, Reference command using virt-install:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network
bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network
```

```
bridge:bridge2,model=virtio --graphics none --connect qemu:///system --
disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the name, RAM and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

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 Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

This Procedure performs Restoring complete cluster with the server backup files

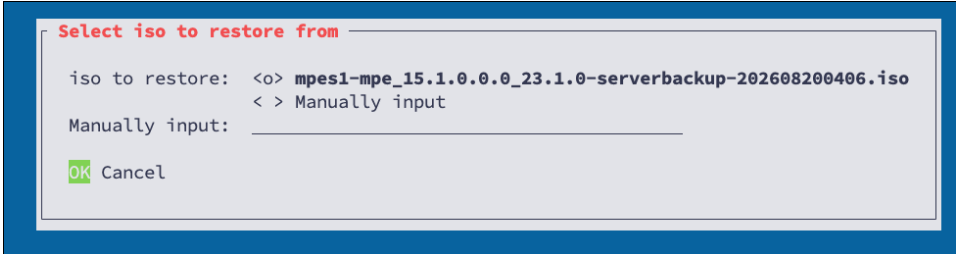
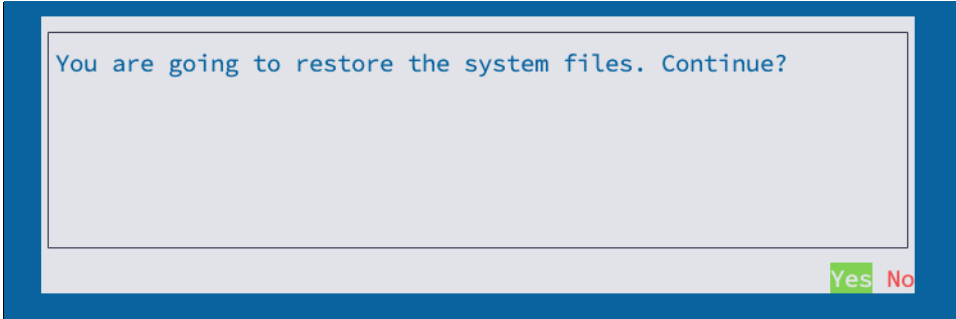
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

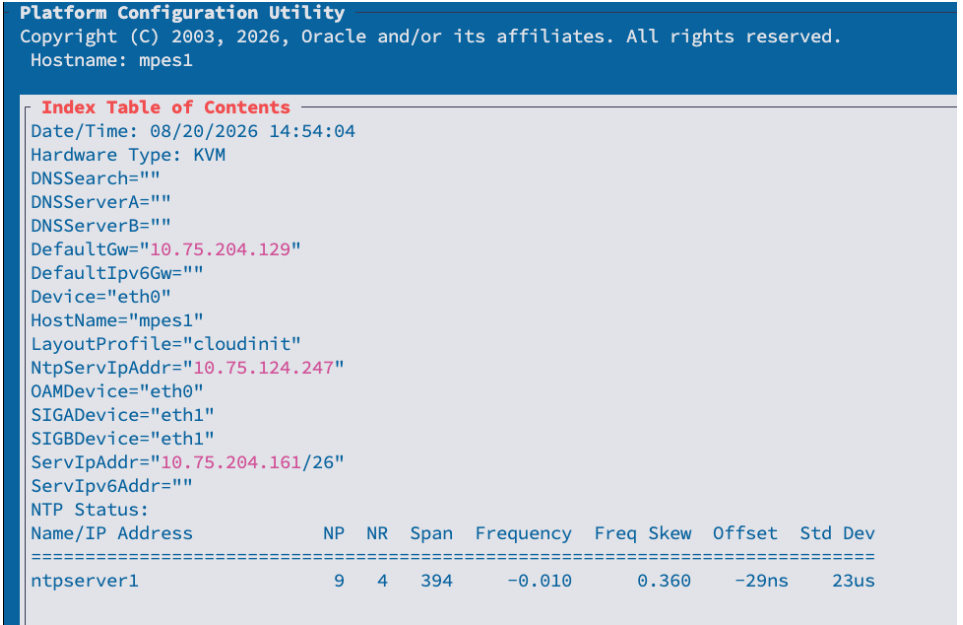
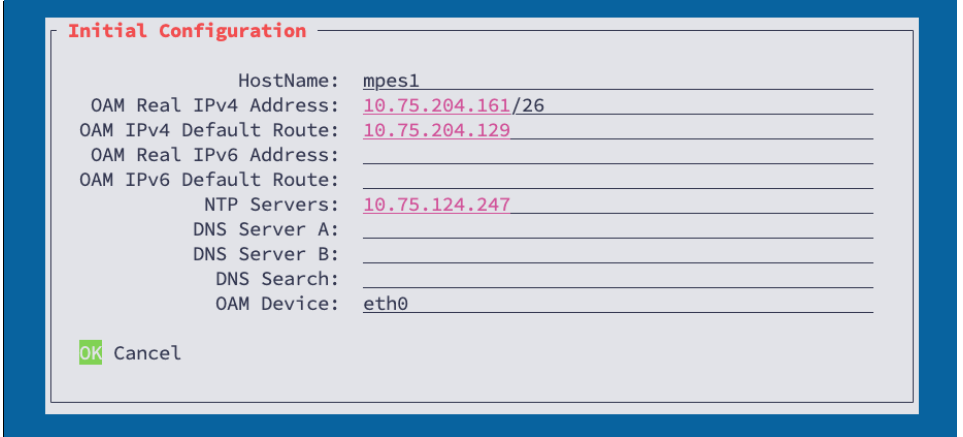
If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

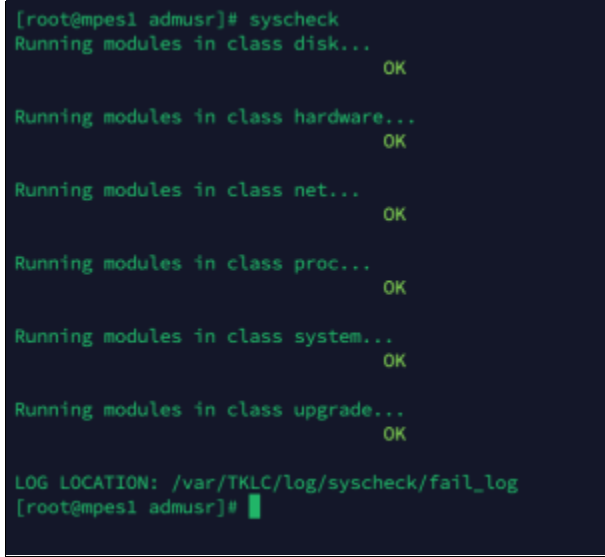
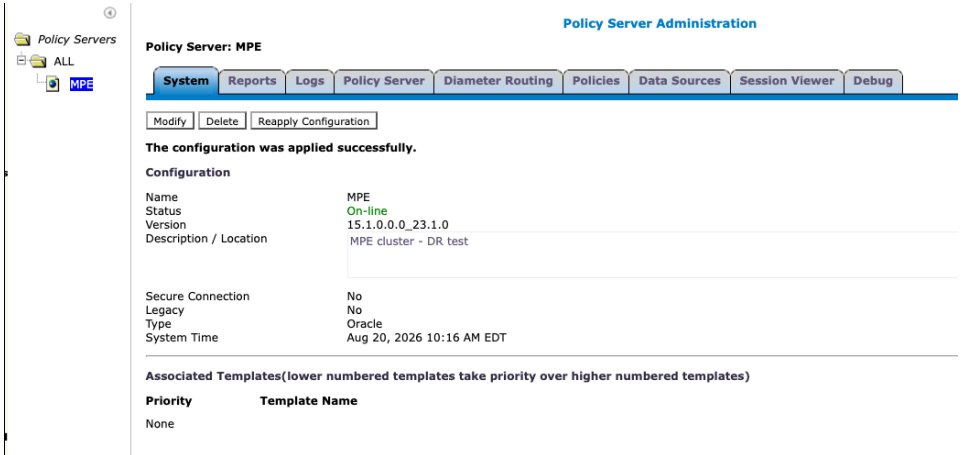
Procedure 5 Restoring complete cluster with the server backup files

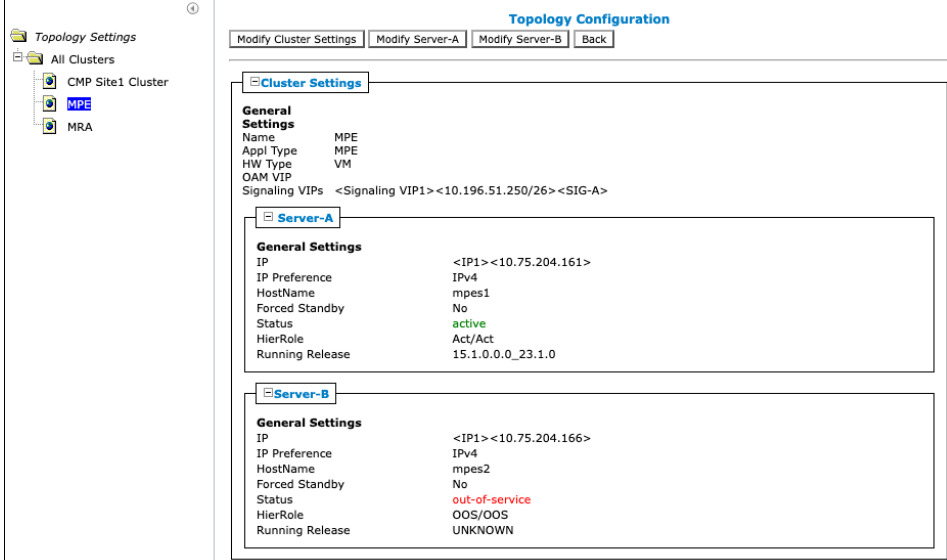
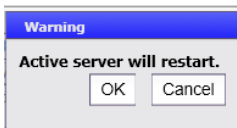
Note: The following steps demonstrate recovering a complete MPE/MRA high-availability (HA) cluster when there is still an active CMP available. The same steps can be followed in case there is an outage in a secondary CMP cluster with the primary active CMP still available:

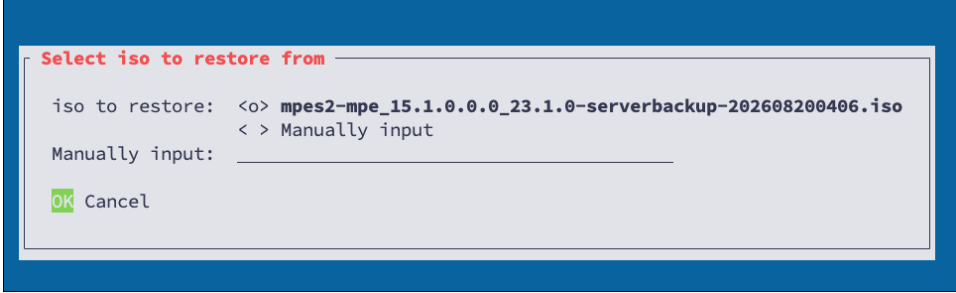
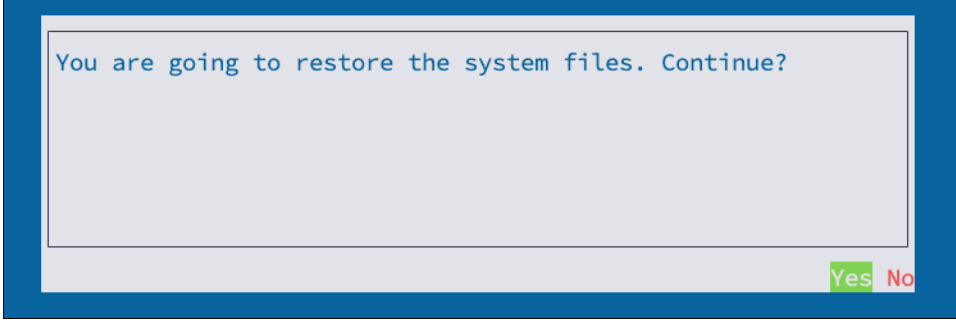
Step	Procedure	Details
1. ☐	Access the console of the 1st replacement node	Access the replacement node using respective console access command. For example, for KVM: <code>virsh console <SERVER_NAME></code>
2. ☐	Load the ISO to restore 1 st server of the cluster	Obtain the *serverbackup.iso* for the 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: <code>/var/camiant/backup/local_archive/serverbackup</code> NOTE: 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.

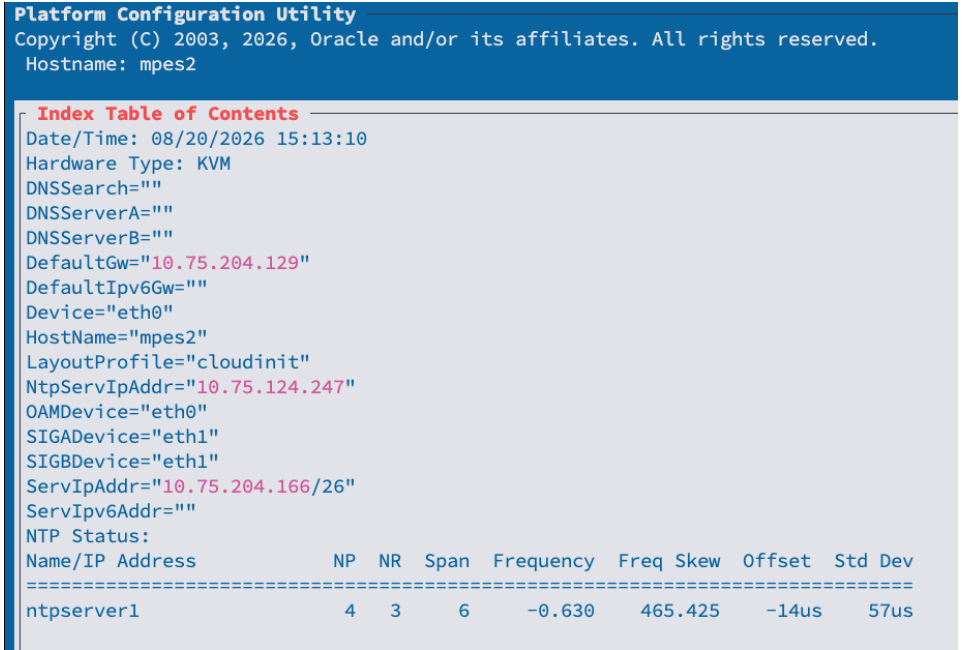
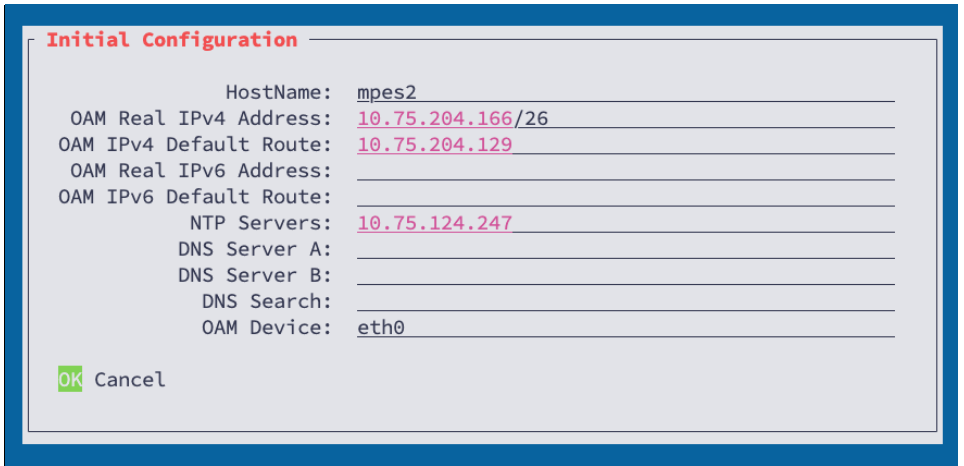
Step	Procedure	Details
3. ☐	Perform server restore from platcfg of this replacement node	1. Open the platcfg utility. <pre># su - platcfg</pre> 2. Navigate to: Policy Configuration → Backup and Restore → Server Restore 3. Select the *serverbackup*.iso that you put on the system and click OK 4. Click Yes to confirm.  
4. ☐	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 the support team or engineering team for assistance.

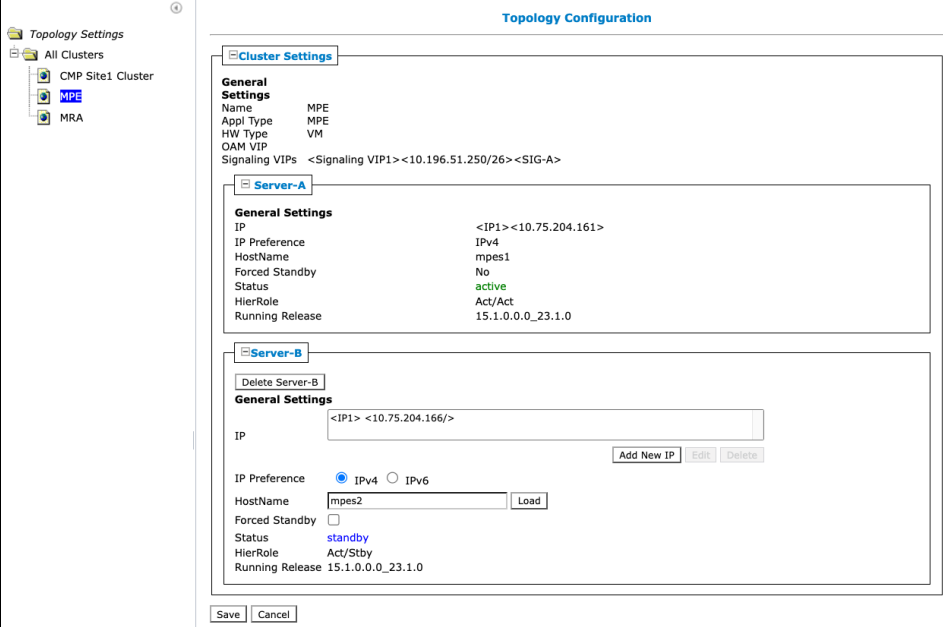
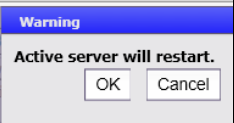
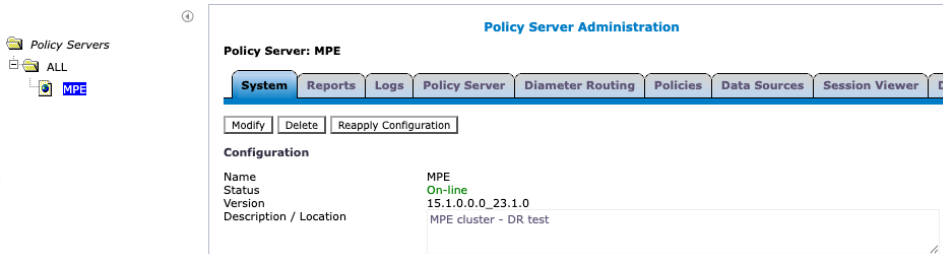
Step	Procedure	Details
5. ☐	Verify Initial configuration	- Click Exit on each platcfg menu until you are returned to the Main Menu of the platcfg utility. - Navigate to: Policy Configuration → Verify Initial Configuration  - If the configuration does not exist, navigate to Perform Initial Configuration and enter the initial configuration hostname, OAM IP, and NTP servers configurations. 
6. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
7. ☐	Verify basic network connectivity and server health.	- From the installed server, ping the OAM/XML gateway. If the ping is not successful, verify all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. <pre># ping <XMI or OAM gateway address></pre> - Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  <pre>[root@mpes1 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@mpes1 admusr]#</pre> NOTE: 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.
8. ☐	Check status	- In the CMP GUI, navigate to: Platform Setting → Topology Settings → All Clusters - Select a cluster. - Click the System tab. - If the Status field indicates Config Mismatch, click Reapply Configuration and wait for the Config Mismatch designation to disappear. If it does not, contact My Oracle Support before proceeding. 

Step	Procedure	Details
11. ☐	Enable Forced Standby on the 2nd failed node of the cluster	1. In the CMP GUI, navigate to: Platform Setting → Topology Setting → <Current Cluster> 2. Modify the server that has a status of out-of-service. 3. Select Forced Standby. 4. Click Save.  5. Accept the confirmation dialog by clicking OK. 
12. ☐	Access the console of the 2nd replacement node	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
13. ☐	Load the ISO to restore 2 nd server of the cluster	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: <pre>/var/camiant/backup/local_archive/serverbackup</pre> NOTE: 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.

Step	Procedure	Details
14. ☐	Perform server restore from platcfg of this replacement node.	1. Open the platcfg utility. <pre># su - platcfg</pre> 2. Navigate to: Policy Configuration → Backup and Restore → Server Restore 3. Select the *serverbackup*.ISO that you just put on the system and click OK. 4. Click Yes to confirm.  
15. ☐	Verify the status	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.

Step	Procedure	Details
16. ☐	Verify Initial configuration	- Click Exit on each platcfg menu until you are returned to the Main Menu of the platcfg utility. - Navigate to: Policy Configuration → Verify Initial Configuration  - If the configuration does not exist, navigate to Perform Initial Configuration and enter the initial configuration: hostname, OAM IP, and NTP servers configurations. - Verify that the information is correct. - Click OK and then click Yes to save and apply. - Exit the platcfg utility by clicking Exit on each platcfg menu until you are returned to the shell. 
17. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
18. ☐	Remove the Forced Standby designation on the node.	- In the CMP GUI, navigate to: Platform Setting → Topology Setting → <Current Cluster> - Click modify for the server that is in Forced Standby - Clear the Forced Standby checkbox - Click Save  - Accept the warning message by clicking OK. 
19. ☐	Check status	- In the CMP GUI, depending on the type of the node, perform the following: - If this is an MPE node, navigate to: Policy Server → Configuration → All → <Recovered MPE Cluster> → Reports tab - If this is an MRA node, navigate to: MRA → Configuration → All → <Recovered MRA Cluster> → Reports tab - Check CMP cluster status (as indicated in the previous step), navigate to: Platform Setting → Topology Setting → Current CMP Cluster - Monitor clustering of the node to its peer, do not proceed until the Cluster Status changes from Degraded to On-line. 

Step	Procedure	Details
20. ☐	Alternative method to check replication status	You can monitor the clustering of the node from the shell on the primary node using the irepstat command. To do so, SSH to the active node of the cluster and run the irepstat command: <pre># irepstat</pre> Expected irepstat output while waiting reconnection: <pre>cmps1 A1773.018 cmps1,10.75.204.159 10:09:39 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmps2 Active 0 0.00 1%R 0.06%cpu 90.0/s AC To D0 mpes1 Active 0 0.00 1%R 0.06%cpu 92.5/s AC To D0 mras1 Active 0 0.01 1%R 0.06%cpu 69.1/s AC To D0 mras2 Active 0 0.01 1%R 0.04%cpu 85.1/s ~</pre> Expected irepstat output after cluster has formed: <pre>cmps1 A1773.018 cmps1,10.75.204.159 10:15:23 [Rw] -- Policy 0 ActStb [DbReplication] ----- AA To P0 cmps2 Active 0 0.10 1%R 0.06%cpu 105.3/s AC To D0 mpes2 Active 0 0.11 1%R 0.05%cpu 94.4/s AC To D0 mpes1 Active 0 0.10 1%R 0.06%cpu 106.9/s AC To D0 mras1 Active 0 0.11 1%R 0.05%cpu 107.7/s AC To D0 mras2 Active 0 0.11 1%R 0.05%cpu 110.2/s ~</pre>
21. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility - As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code> - As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code> <pre>[root@cmps1 admusr]# /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=admusr Subroutine CMNodeInfo::pack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::unpack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. The password of admusr in topology: Connecting to admusr@mpes1 ... Connecting to admusr@cmps2 ... Connecting to admusr@mpes2 ... Connecting to admusr@mras2 ... Connecting to admusr@mras1 ... Connecting to admusr@cmps1 ... [1/6] Provisioning SSH keys on mras2 ... [2/6] Provisioning SSH keys on mpes2 ... [3/6] Provisioning SSH keys on cmps1 ... [4/6] Provisioning SSH keys on mpes1 ... [5/6] Provisioning SSH keys on cmps2 ... [6/6] Provisioning SSH keys on mras1 ... SSH keys are OK. [root@cmps1 admusr]#</pre>
22. ☐	Reapply Configuration	In the CMP GUI, click Reapply Configuration on the MPE/MRA 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

Use this procedure to reconstruct a complete cluster when server backup files are NOT available and node-specific initial configuration must be entered manually. The active primary node synchronizes the installed node to complete the cluster. On each failed node, the initial configuration information is manually restored using Perform Initial Configuration.

Required resources:

- Policy APP installation QCOW/OVA.
- Initial configuration information about the node is restored:
 - o OAM node Ip address, default gateway, ntp server ip address
 - 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 of the running node)

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

Prerequisites:

Remove the failed VM and spawn the appropriate replacement VMs for the cluster type being recovered.

For example, Reference command using virt-install:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network
bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network
bridge:bridge2,model=virtio --graphics none --connect qemu:///system --
disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the name, RAM and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

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 Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

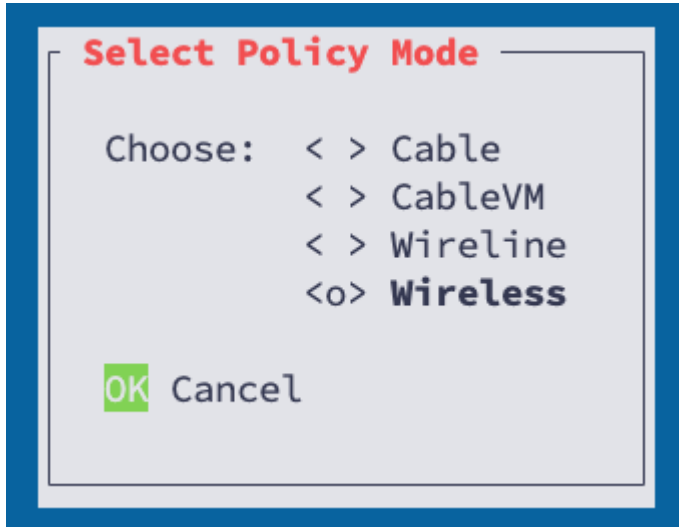
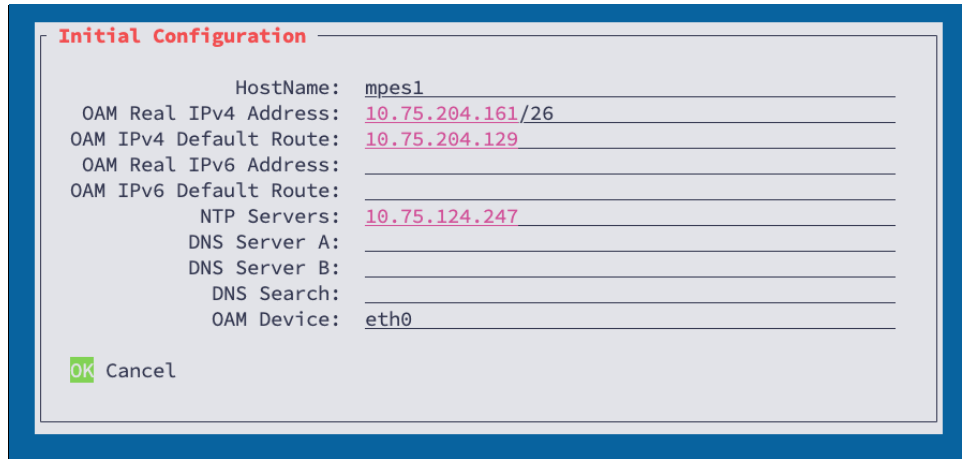
This Procedure performs Restoring complete cluster without the server backup

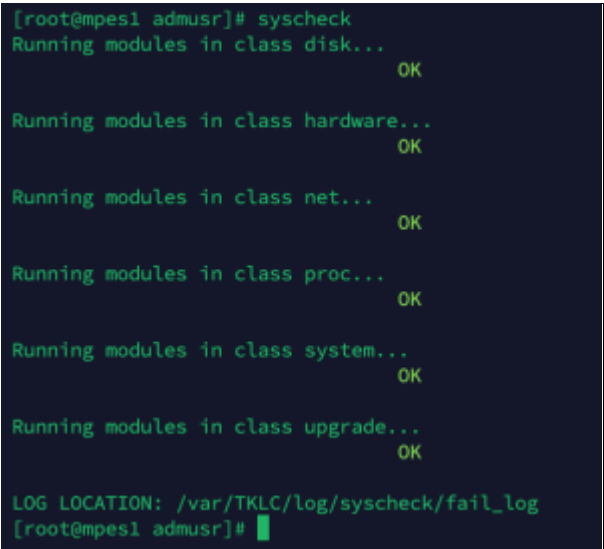
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

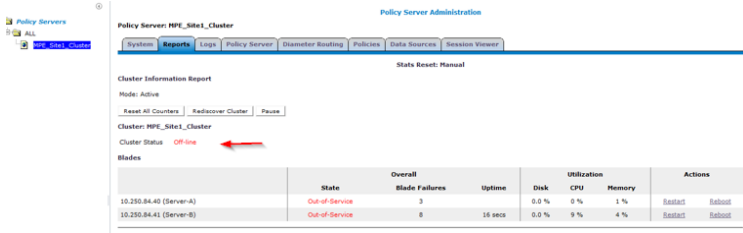
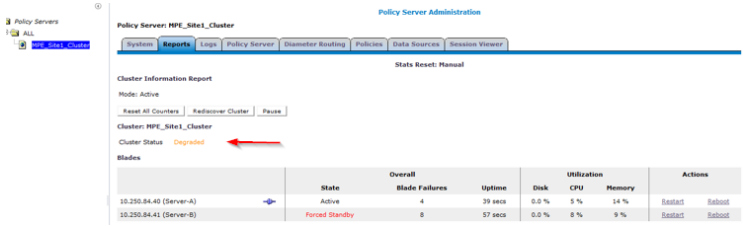
If this procedure fails, contact the My Oracle Support and ask for assistance.

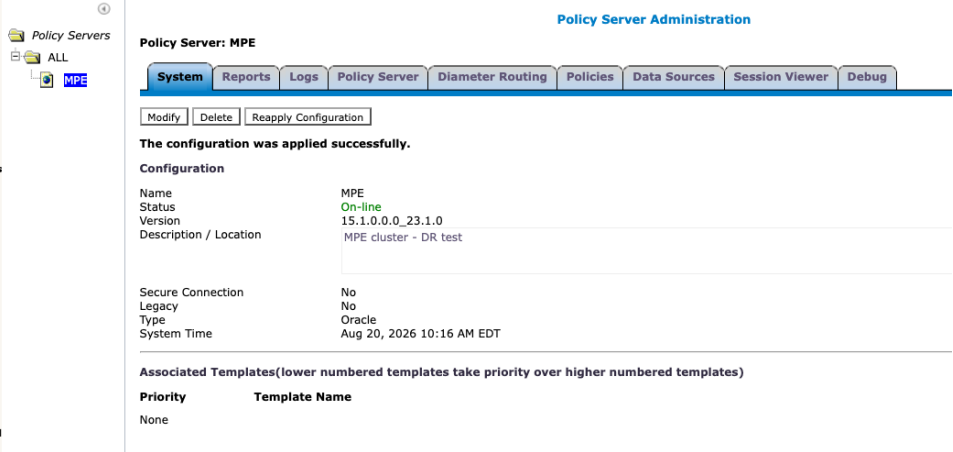
Procedure 6 Restoring complete cluster without the server backup

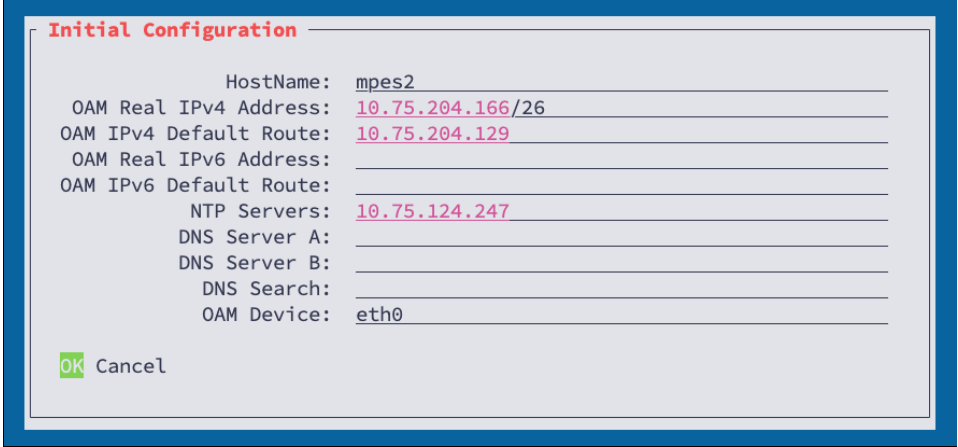
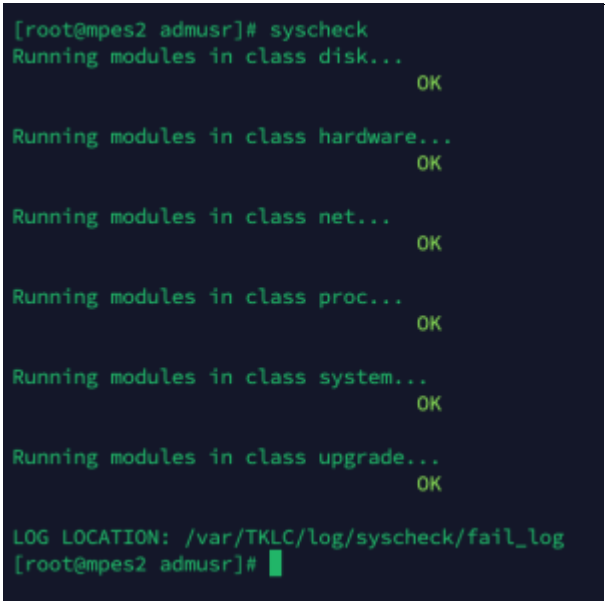
Step	Procedure	Details
1. ☐	Access the console of the 1st replacement VM	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
2. ☐	Perform Initial Policy Configuration using the platcfg utility on the installed node	- Open the platcfg utility. <pre># su - platcfg</pre> - Navigate to: Policy Configuration → Set Policy Mode  - Leave the mode as Wireless and click OK to continue. You can skip this step. - Navigate to: Policy Configuration → Perform Initial Configuration - Enter the configuration details for the node being replaced: - After the server details are entered and verified, click OK. - A menu displays asking to apply the settings, click Yes 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. - Exit the platcfg utility by clicking Exit on each platcfg menu until you are returned to the shell. 

Step	Procedure	Details
3. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
4. ☐	Verify basic network connectivity and server health.	1. From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. <pre># ping <XMI or OAM gateway address></pre> 2. Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  <pre>[root@mpes1 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@mpes1 admusr]#</pre>

Step	Procedure	Details
5. ☐	Check Status	1. In the CMP GUI, depending on the type of the node, perform the following: - If this is an MPE node, navigate to: Policy Server → Configuration → All → <Recovered MPE Cluster> → Reports tab - If this is an MRA node, navigate to: MRA → Configuration → All → <Recovered MRA Cluster> → Reports tab 2. Monitor clustering of the node to its peer, do not proceed until the Cluster Status returns from Off-line to Degraded. Off-line  Degraded 

Step	Procedure	Details
6. ☐	Check status	- In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters - Select a cluster - Click System tab. If the Status field indicates Config Mismatch, click the Reapply Configuration and wait for the Config Mismatch designation to disappear. If it does not, contact My Oracle Support before proceeding. 
7. ☐	Access the console of the 2nd replacement VM	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
8. ☐	Perform Initial Policy Configuration using the platcfg utility on second node of cluster	- Open the platcfg utility. <pre># su - platcfg</pre> - Navigate to: Policy Configuration → Initial Configuration - Enter the details for the replacement node: - After the server details are entered and verified, select OK. - A menu displays asking to apply the settings, click Yes 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. - Exit the platcfg utility by clicking Exit on each platcfg menu until you are returned to the shell.

Step	Procedure	Details
		 Initial Configuration HostName: <u>mpes2</u> OAM Real IPv4 Address: <u>10.75.204.166/26</u> OAM IPv4 Default Route: <u>10.75.204.129</u> OAM Real IPv6 Address: _____ OAM IPv6 Default Route: _____ NTP Servers: <u>10.75.124.247</u> DNS Server A: _____ DNS Server B: _____ DNS Search: _____ OAM Device: <u>eth0</u> OK Cancel
9. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
10. ☐	Verify basic network connectivity and server health.	- From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. <pre># ping <XMI or OAM gateway address></pre> - Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  <pre>[root@mpes2 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@mpes2 admusr]#</pre>

Step	Procedure	Details
11. ☐	Check status	

Step	Procedure	Details
13. ☐	Exchange keys with cluster mate (This step need to run from active CMP)	Exchanging SSH keys Utility - As root, run <code>/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</code> - As admusr, run <code>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</code> <pre>[root@cmps1 admusr]# /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=admusr Subroutine CMNodeInfo::pack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::unpack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. The password of admusr in topology: Connecting to admusr@mpes1 ... Connecting to admusr@cmps2 ... Connecting to admusr@mpes2 ... Connecting to admusr@mras2 ... Connecting to admusr@mras1 ... Connecting to admusr@cmps1 ... [1/6] Provisioning SSH keys on mras2 ... [2/6] Provisioning SSH keys on mpes2 ... [3/6] Provisioning SSH keys on cmps1 ... [4/6] Provisioning SSH keys on mpes1 ... [5/6] Provisioning SSH keys on cmps2 ... [6/6] Provisioning SSH keys on mras1 ... SSH keys are OK. [root@cmps1 admusr]#</pre>
14. ☐	Reapply Configuration	In the CMP GUI, click Reapply Configuration on the MPE/MRA cluster. The CMP displays The configuration was applied successfully message.
---End of Procedure---		

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

This procedure is applicable when there an entire CMP cluster has failed and there is no georedundant CMP cluster available. In this case, we first re-create a CMP with the application-level configuration. This CMP will then be used to re-create the whole policy network. The overall process for this is as follows:

→ The first CMP is recovered by using its server backup file or by manually entering the Perform Initial Configuration information in platcfg.

→ After recovering all the node-level information by server backup or Perform Initial Configuration, we perform system restore on this CMP to recover all the application-level data.

→ After this CMP is online, all other servers of the policy network can be re-created using Procedure 1 through Procedure 7.

→ The first CMP we recovered which will be the primary active CMP in the policy network re-syncs all the application-level configuration data to all other nodes recovered.

Required resources:

- Recent server backup file
- Policy APP installation QCOW/OVA.
- Recent System backup file.

- Initial configuration information about the node:
 - OAM IP address, default gateway, NTP and SNMP server IP addresses
 - 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 node)

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

Prerequisites:

Remove the failed VM and spawn a CMP VM instance using appropriate VM installation commands for CMP.

For example, Reference command using virt-install:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network
bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network
bridge:bridge2,model=virtio --graphics none --connect qemu:///system --
disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the name, RAM and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

This Procedure performs Restoring CMP cluster with system backup available

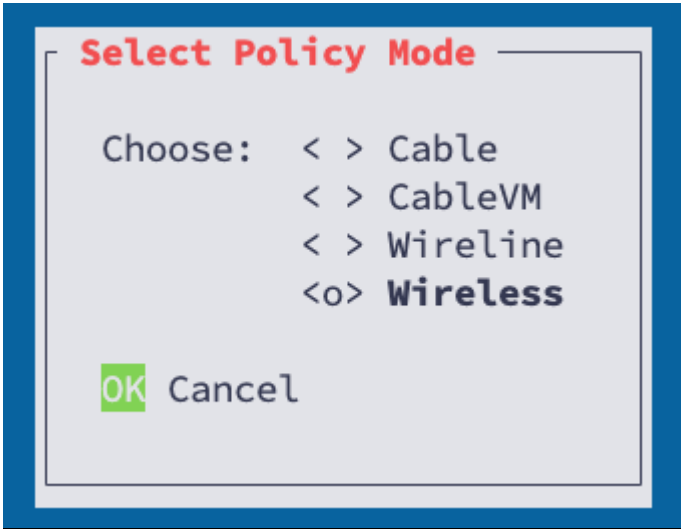
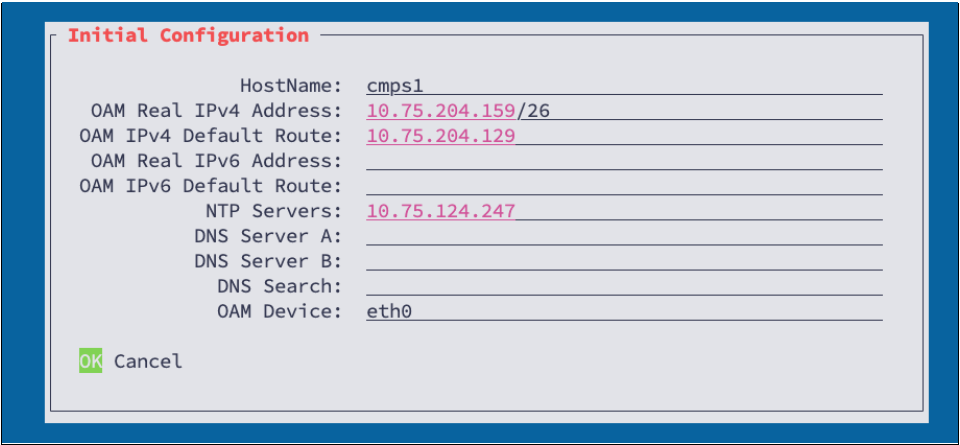
Check off (✓) each step as it is completed. Boxes been provided for this purpose under each step number.

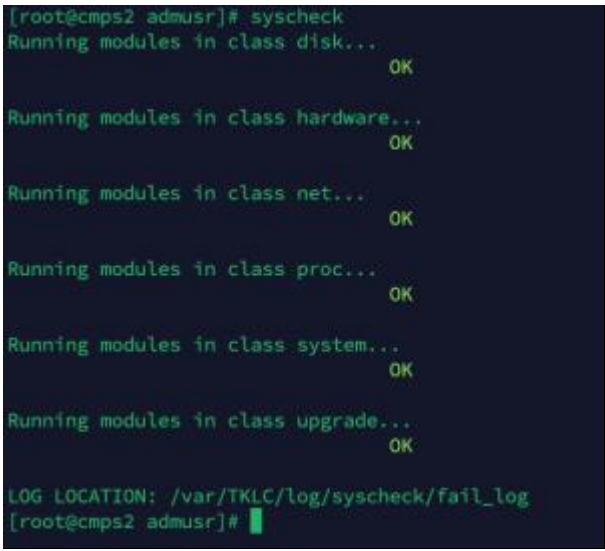
If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

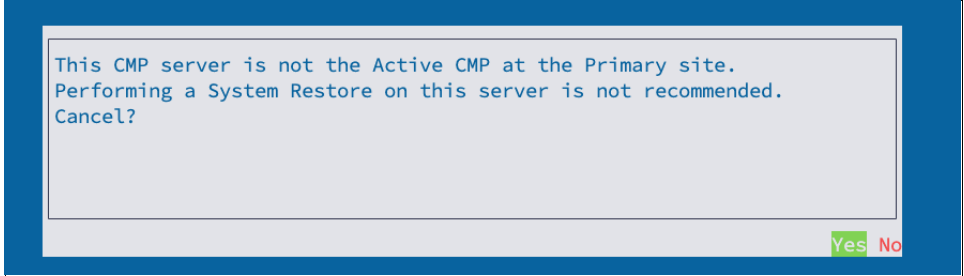
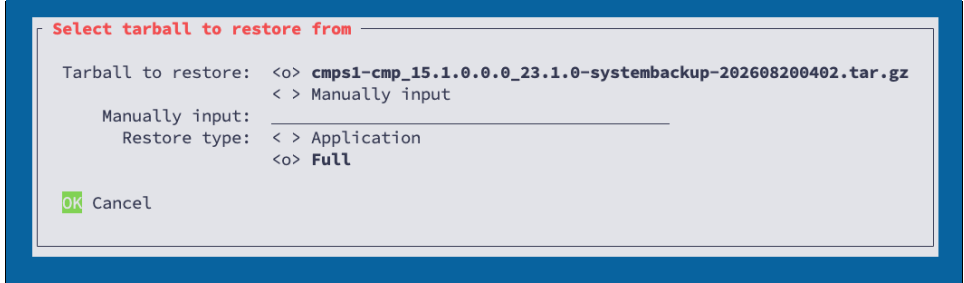
Procedure 7 Restoring CMP cluster with system backup available

Note: Here, we show recovering node-level info of the first CMP using Perform Initial Configuration. The same can be performed using server backup file. After the first CMP is recovered with node-level info, we perform system restore to recover all the application-related configuration in it. After that, we can recover other nodes using the relevant procedures (procedures 1 to 6).

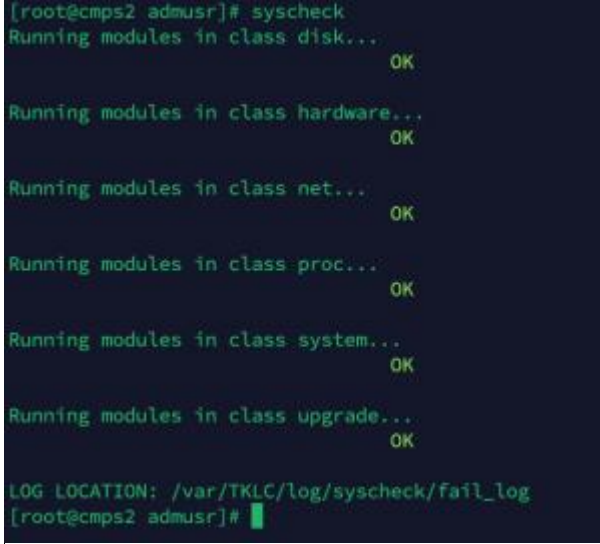
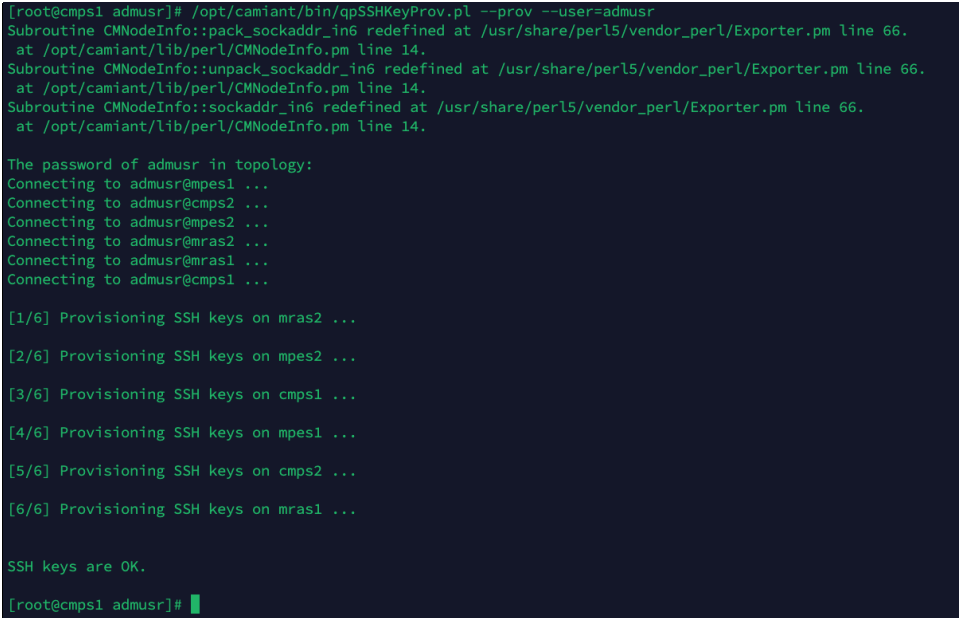
Step	Procedure	Details
1. ☐	Login via SSH to node	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>

Step	Procedure	Details
2. ☐	Perform Initial Policy Configuration using the platcfg utility on the installed node	1. Open the platcfg utility. <pre># su - platcfg</pre> 2. Navigate to: Policy Configuration → Set Policy Mode  3. Leave the mode as Wireless and click OK to continue. You can skip this step. 4. Navigate to: Policy Configuration → Perform Initial Configuration 5. Enter the relevant details from the replaced node: 6. After the server details are entered and verified, click OK. 7. A menu opens asking to apply the settings, click Yes 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. 8. Exit the platcfg utility by clicking Exit on each platcfg menu page until you are returned to the shell. 

Step	Procedure	Details
3. ☐	Reboot the server	Reboot the server: <pre># init 6</pre> Reconnect to the server using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
4. ☐	Verify basic network connectivity and server health.	1. From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. <pre># ping <XMI or OAM gateway address></pre> 2. Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  <pre>[root@cmps2 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@cmps2 admusr]#</pre>
5. ☐	Load the system backup file for system restore	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. If the system backup file is available, put a copy of the file on the constructed CMP node using secure copy (pscp scp, or WinSCP). <pre>/var/camiant/backup/local_archive/systembackup/</pre>

Step	Procedure	Details
6. ☐	Perform system restore from platcfg on the replacement node	- Open the platcfg utility. <pre># su - platcfg</pre> - Navigate to: Policy Configuration → Backup and Restore → System Restore - A message displays prompting confirmation to restore even though this node is not recognized as the active member. This is expected, continue by clicking Yes.  - 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 Manually Input and select Full. - Click OK to proceed.  NOTE: Full restores the Comcol data, but Application excludes Comcol.
7. ☐	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. ☐	Verify Initial configuration	- Click Exit on each platcfg menu until you are back to the Main Menu of the platcfg utility. - Navigate to: Policy Configuration → Verify Initial Configuration

Step	Procedure	Details																			
		Platform Configuration Utility Copyright (C) 2003, 2026, Oracle and/or its affiliates. All rights reserved. Hostname: cmps1 Index Table of Contents Date/Time: 08/20/2026 16:35:23 Hardware Type: KVM DNSSearch="" DNSServerA="" DNSServerB="" DefaultGw="10.75.204.129" DefaultIpv6Gw="" Device="eth0" HostName="cmps1" LayoutProfile="cloudinit" NtpServIpAddr="10.75.124.247" OAMDevice="eth0" SIGADevice="eth1" SIGBDevice="eth1" ServIpAddr="10.75.204.159/26" ServIpv6Addr="" NTP Status: <table><thead><tr><th>Name/IP Address</th><th>NP</th><th>NR</th><th>Span</th><th>Frequency</th><th>Freq Skew</th><th>Offset</th><th>Std Dev</th></tr></thead><tbody><tr><td>ntpserver1</td><td>23</td><td>14</td><td>32m</td><td>-0.000</td><td>0.022</td><td>-27ns</td><td>15us</td></tr></tbody></table> 3. Verify that the information is correct. If the configuration is not there, navigate to Perform Initial Configuration and enter the hostname, OAM IP and so on. 4. Click OK and then click YES to save and apply. 5. After the server details are entered and verified, select OK. 6. A menu displays asking to apply settings, click Yes 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 Exit on each platcfg menu until you are returned to the shell. Initial Configuration HostName: cmps1 OAM Real IPv4 Address: 10.75.204.159/26 OAM IPv4 Default Route: 10.75.204.129 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 10.75.124.247 DNS Server A: DNS Server B: DNS Search: OAM Device: eth0 OK Cancel <tr><td>9. ☐</td><td>Reboot the server</td><td> Reboot the server: # init 6 Allow the server time to reboot. Reconnect to the server using respective console access command. For example, for KVM: virsh console <SERVER_NAME> </td></tr>	Name/IP Address	NP	NR	Span	Frequency	Freq Skew	Offset	Std Dev	ntpserver1	23	14	32m	-0.000	0.022	-27ns	15us	9. ☐	Reboot the server	Reboot the server: # init 6 Allow the server time to reboot. Reconnect to the server using respective console access command. For example, for KVM: virsh console <SERVER_NAME>
Name/IP Address	NP	NR	Span	Frequency	Freq Skew	Offset	Std Dev														
ntpserver1	23	14	32m	-0.000	0.022	-27ns	15us														
9. ☐	Reboot the server	Reboot the server: # init 6 Allow the server time to reboot. Reconnect to the server using respective console access command. For example, for KVM: virsh console <SERVER_NAME>																			

Step	Procedure	Details
10. ☐	Verify basic network connectivity and server health.	- From the installed server, ping the OAM/XML 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. <pre># ping <XMI or OAM gateway address></pre> - Run the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.  <pre>[root@cmps2 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@cmps2 admusr]#</pre>
11. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility - As root, <pre>run /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root</pre> - As admusr, run <pre>/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov</pre>  <pre>[root@cmps1 admusr]# /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=admusr Subroutine CMNodeInfo::pack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::unpack_sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. Subroutine CMNodeInfo::sockaddr_in6 redefined at /usr/share/perl5/vendor_perl/Exporter.pm line 66. at /opt/camiant/lib/perl/CMNodeInfo.pm line 14. The password of admusr in topology: Connecting to admusr@mpes1 ... Connecting to admusr@cmps2 ... Connecting to admusr@mpes2 ... Connecting to admusr@mras2 ... Connecting to admusr@mras1 ... Connecting to admusr@cmps1 ... [1/6] Provisioning SSH keys on mras2 ... [2/6] Provisioning SSH keys on mpes2 ... [3/6] Provisioning SSH keys on cmps1 ... [4/6] Provisioning SSH keys on mpes1 ... [5/6] Provisioning SSH keys on cmps2 ... [6/6] Provisioning SSH keys on mras1 ... SSH keys are OK. [root@cmps1 admusr]#</pre>

Step	Procedure	Details
12. ☐	Check status	1. In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters 2. When the server returns to online status, log into the GUI on the OAM virtual IP address 3. Verify to that the manager has configuration for the MPE clusters in the network (whether those clusters are online or not) 4. Verify other application configuration properties. 5. After the CMP is in place, recover the other CMP node of this cluster using procedure 1 if this scenario is applicable. Recover any other clusters or nodes using any of the application procedures from procedure 1 to 6.
13.	Now recover other nodes of the topology	Since the first CMP has been restored and it contains the application-level configuration and database information, we can now restore other nodes of the topology. Refer the procedures 1 through 6 and identify relevant failure scenario and choose the procedure that recovers the nodes/clusters in your topology.
---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

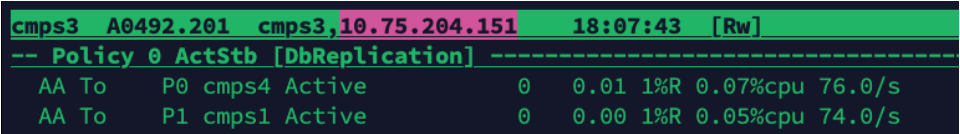
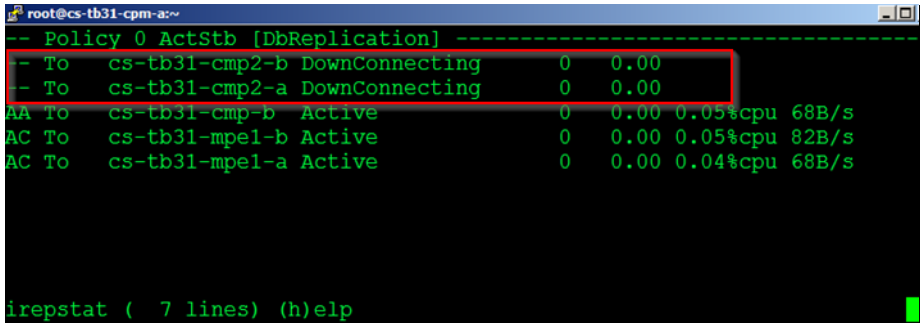
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.

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. ☐	Access to the system	Log into the GUI on the OAM VIP of the georedundant CMP.																														
2. ☐	Check status	In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters You are warned that you are not on the primary cluster of the policy network. The secondary server has limited functionality. Topology Settings All Clusters Warning: This server you signed in is the Secondary Active Server. Cluster Configuration <table><tr><th>Name</th><th>Appl Type</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Operation</th></tr><tr><td>CMP Site1 Cluster (S)</td><td>CMP Site1 Cluster</td><td>10.75.204.183/26</td><td>10.75.204.159</td><td>10.75.204.160</td><td>View</td></tr><tr><td>CMP Site2 Cluster (OOS)</td><td>CMP Site2 Cluster</td><td>10.75.204.188/26</td><td>10.75.204.151</td><td>10.75.204.162</td><td>View Promote</td></tr><tr><td>MPE</td><td>MPE</td><td>N/A</td><td>10.75.204.161</td><td>10.75.204.166</td><td>View</td></tr><tr><td>MRA</td><td>MRA</td><td>N/A</td><td>10.75.204.167</td><td>10.75.204.181</td><td>View</td></tr></table>	Name	Appl Type	OAM VIP	Server-A	Server-B	Operation	CMP Site1 Cluster (S)	CMP Site1 Cluster	10.75.204.183/26	10.75.204.159	10.75.204.160	View	CMP Site2 Cluster (OOS)	CMP Site2 Cluster	10.75.204.188/26	10.75.204.151	10.75.204.162	View Promote	MPE	MPE	N/A	10.75.204.161	10.75.204.166	View	MRA	MRA	N/A	10.75.204.167	10.75.204.181	View
Name	Appl Type	OAM VIP	Server-A	Server-B	Operation																											
CMP Site1 Cluster (S)	CMP Site1 Cluster	10.75.204.183/26	10.75.204.159	10.75.204.160	View																											
CMP Site2 Cluster (OOS)	CMP Site2 Cluster	10.75.204.188/26	10.75.204.151	10.75.204.162	View Promote																											
MPE	MPE	N/A	10.75.204.161	10.75.204.166	View																											
MRA	MRA	N/A	10.75.204.167	10.75.204.181	View																											

Step	Procedure	Details																																																												
3. ☐	Verify basic network connectivity and server health.	1. From the active server of site 2 CMP (Promote server), ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. # ping <XMI or OAM gateway address> 2. Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. <pre>[root@cmps2 admusr]# 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 Running modules in class upgrade... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@cmps2 admusr]#</pre>																																																												
4. ☐	Promote secondary CMP cluster	1. In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters 2. Click Promote on the secondary server. 3. Accept the resulting confirmation dialog by clicking OK. Topology Settings All Clusters Warning: This server you signed in is the Secondary Active Server. Cluster Configuration <table><thead><tr><th>Name</th><th>Appl Type</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Operation</th></tr></thead><tbody><tr><td>CMP Site1 Cluster (S)</td><td>CMP Site1 Cluster</td><td>10.75.204.183/26</td><td>10.75.204.159</td><td>10.75.204.160</td><td>View</td></tr><tr><td>CMP Site2 Cluster (OOS)</td><td>CMP Site2 Cluster</td><td>10.75.204.188/26</td><td>10.75.204.151</td><td>10.75.204.162</td><td>View Promote</td></tr><tr><td>MPE</td><td>MPE</td><td>N/A</td><td>10.75.204.161</td><td>10.75.204.166</td><td>View</td></tr><tr><td>MRA</td><td>MRA</td><td>N/A</td><td>10.75.204.167</td><td>10.75.204.181</td><td>View</td></tr></tbody></table> Due to the design changes in Release 15.1, the “Cluster Promoted Successfully” and “Cluster Demoted Successfully” pop-up messages are not displayed when we demote/promote a CMP cluster. To check if a CMP cluster has been promoted successfully, the nodes of that cluster will have Active and Standby roles. If not, retry the operation and/or contact My Oracle Support. Topology Settings All Clusters Cluster Configuration Add CMP Site1 ClusterAdd CMP Site2 ClusterAdd MPE/MRA Cluster <table><thead><tr><th>Name</th><th>Appl Type</th><th>OAM VIP</th><th>Server-A</th><th>Server-B</th><th>Operation</th></tr></thead><tbody><tr><td>CMP Site1 Cluster (S)</td><td>CMP Site1 Cluster</td><td>10.75.204.183/26</td><td>10.75.204.159</td><td>10.75.204.160</td><td>View Delete</td></tr><tr><td>CMP Site2 Cluster (P)</td><td>CMP Site2 Cluster</td><td>10.75.204.188/26</td><td>10.75.204.151</td><td>10.75.204.162</td><td>View Demote</td></tr><tr><td>MPE</td><td>MPE</td><td>N/A</td><td>10.75.204.161</td><td>10.75.204.166</td><td>View Delete</td></tr><tr><td>MRA</td><td>MRA</td><td>N/A</td><td>10.75.204.167</td><td>10.75.204.181</td><td>View Delete</td></tr></tbody></table>	Name	Appl Type	OAM VIP	Server-A	Server-B	Operation	CMP Site1 Cluster (S)	CMP Site1 Cluster	10.75.204.183/26	10.75.204.159	10.75.204.160	View	CMP Site2 Cluster (OOS)	CMP Site2 Cluster	10.75.204.188/26	10.75.204.151	10.75.204.162	View Promote	MPE	MPE	N/A	10.75.204.161	10.75.204.166	View	MRA	MRA	N/A	10.75.204.167	10.75.204.181	View	Name	Appl Type	OAM VIP	Server-A	Server-B	Operation	CMP Site1 Cluster (S)	CMP Site1 Cluster	10.75.204.183/26	10.75.204.159	10.75.204.160	View Delete	CMP Site2 Cluster (P)	CMP Site2 Cluster	10.75.204.188/26	10.75.204.151	10.75.204.162	View Demote	MPE	MPE	N/A	10.75.204.161	10.75.204.166	View Delete	MRA	MRA	N/A	10.75.204.167	10.75.204.181	View Delete
Name	Appl Type	OAM VIP	Server-A	Server-B	Operation																																																									
CMP Site1 Cluster (S)	CMP Site1 Cluster	10.75.204.183/26	10.75.204.159	10.75.204.160	View																																																									
CMP Site2 Cluster (OOS)	CMP Site2 Cluster	10.75.204.188/26	10.75.204.151	10.75.204.162	View Promote																																																									
MPE	MPE	N/A	10.75.204.161	10.75.204.166	View																																																									
MRA	MRA	N/A	10.75.204.167	10.75.204.181	View																																																									
Name	Appl Type	OAM VIP	Server-A	Server-B	Operation																																																									
CMP Site1 Cluster (S)	CMP Site1 Cluster	10.75.204.183/26	10.75.204.159	10.75.204.160	View Delete																																																									
CMP Site2 Cluster (P)	CMP Site2 Cluster	10.75.204.188/26	10.75.204.151	10.75.204.162	View Demote																																																									
MPE	MPE	N/A	10.75.204.161	10.75.204.166	View Delete																																																									
MRA	MRA	N/A	10.75.204.167	10.75.204.181	View Delete																																																									
5. ☐	Logout of the CMP GUI	Logout of the CMP GUI by clicking Logout link or closing the browser window.																																																												

Step	Procedure	Details
6. ☐	Verify operation via CMP GUI	1. Login to the CMP GUI using the VIP of CMP Site2 2. In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters 3. Ensure all clusters are performing as expected. Follow the procedures listed in this document to bring other failed servers/clusters back online.
7. ☐	SSH to active node of the promoted cluster	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: <pre>virsh console <SERVER_NAME></pre>
8. ☐	Verify irepstat command output shows expected status	1. Use the SSH session from VM Host to the active node of the promoted CMP cluster. 2. Run the irepstat command to verify that cluster replication is active. If not active after 5 minutes, check the CMP GUI for any active alarms. <pre># irepstat</pre>  The status of all clusters except known failed servers has a status of Active. Otherwise, if any of the replication paths show <code>DownConnecting</code> contact My Oracle Support. 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.  <pre>irepstat (7 lines) (h)elp</pre>
9. ☐	Rebuild failed CMP cluster	Refer to Procedure 6: Restoring Complete Cluster without Using the Server Backup 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.