Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Disaster Recovery

Policy Management Disaster Recovery Guide Release 15.0

F88873-01

December 2023

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

Table of Contents

List of Tables

List of Procedures

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 15.0. 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 15.0.

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
  - 1 or more CMP servers (this can include GeoRedundant CMP (DR-CMP) servers)
  - 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 is 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

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

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

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

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

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

2.5 Complete Server Outage (All servers)

This is the worst case scenario where all the servers in the network have suffered partial or complete software and/or hardware failure, and georedundant CMP is not available. The servers are recovered using base recovery of hardware and software and then restoring a system backup to the active CMP server. Database backups are taken from offsite backup storage locations (assuming these were performed and stored offsite before the outage). If a backup file is not available, the only option is to rebuild the network from scratch. The network data is reconstructed from whatever sources are available, including entering all data manually.

2.6 Performing Initial Configuration

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

Needed initial configuration information:

- Hostname
- OAM real IP address and network mask
- OAM default router address
- NTP server
- DNS server (optional)
- DNS search (optional)
- Interface device (usually bond0/eth0)

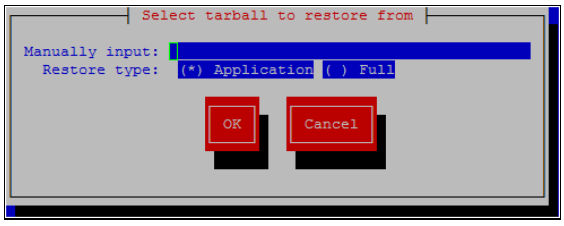
2.7 Using the Server Backup File

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:

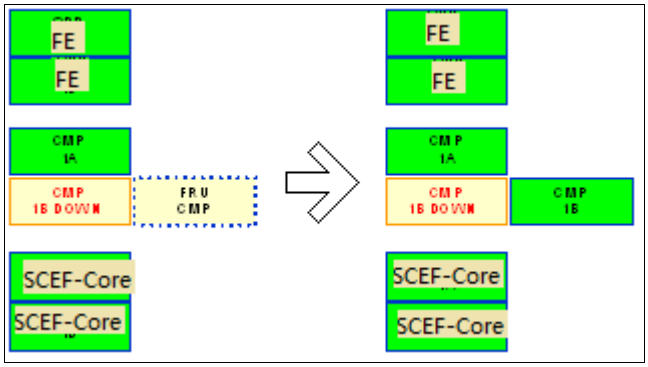
1. Verify BIOS time is correct on servers.
2. Verify the version of TPD installed.
3. Load application for corresponding server HW types.
4. Check FW versions and upgraded if necessary.
5. Check NTP status after recovery.
6. Check active alarms from GUI and both syscheck the alarmMgr and alarmStatusfrom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

4.2 Recovery Scenarios

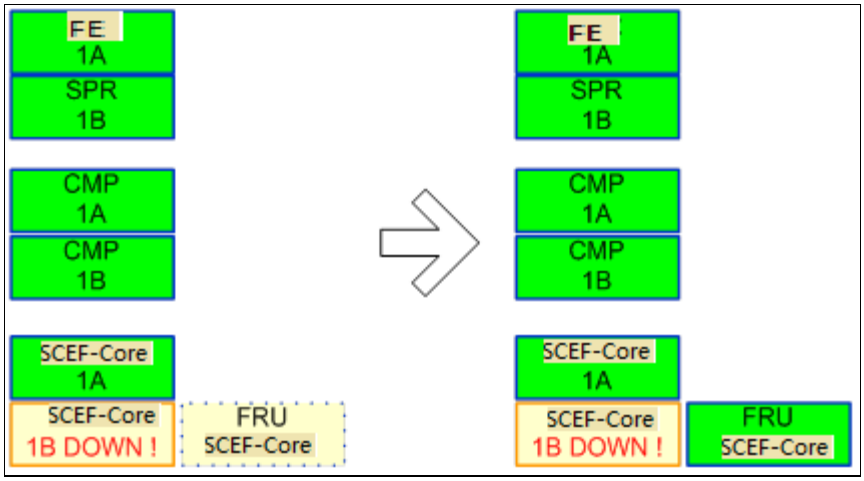
4.2.1 Recovery Scenario 1 (Partial Cluster Outage with Primary CMP Server Available)

For a partial outage with a CMP server available, only base recovery of hardware and software and initial Policy configuration is needed. A single CMP server is capable of restoring the configuration database via replication to all MPE/MRA servers, or to the other CMP node of a cluster. The major activities are summarized in the 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.
    - 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
    - Recover the software.
    - Initial policy configuration is re-installed, either through the platcfg menu, or from the server backup file
    - The database is intact at the active CMP server and is replicated to the standby CMP server.



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

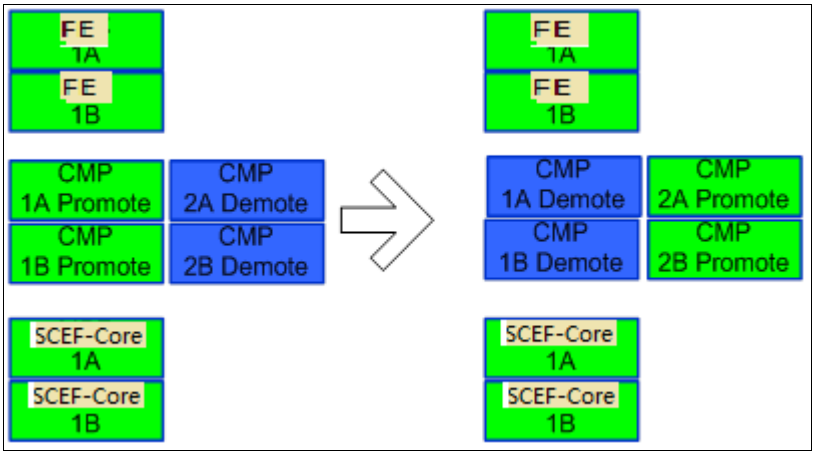
  Use Procedure 4: Restore Single MPE/MRA Node without Server Backup File to recover the second node of MPE/MRA cluster.

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.

   - 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
   - Recover the software.
   - Initial policy configuration is re-installed, either through the platcfg menu, or from the server backup file
   - The configuration database is available at the active CMP server and does not require restoration on the CMP. Configuration is pushed from the CMP to the MPE/MRA servers using the re-apply configuration operation.

3. Recover other site CMP server by recovering base hardware and software.

   - 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

- Recover the software.
- Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file.

The database of the active 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.

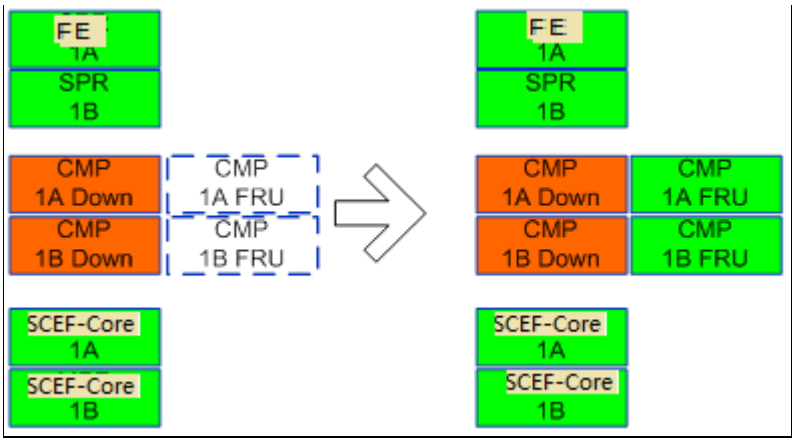
   Or Procedure 4: Restore Single MPE/MRA Node without Server Backup File
3. Use Procedure 5: Restoring Complete Cluster Using Server Backup Files

   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.

- 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
- Recover the software.
- Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file.
- The database of the CMP is restored from a system backup.
- 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.
  - 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
  - Recover the software.
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - The configuration database is available 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.
  - 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
  - Recover the software.
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - The configuration database is available at the active CMP server and does not require restoration on the CMP. Configuration is pushed from the CMP to the MPE/MRA 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.

5. RESTORE PROCEDURES

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

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

Required resources:

- 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.

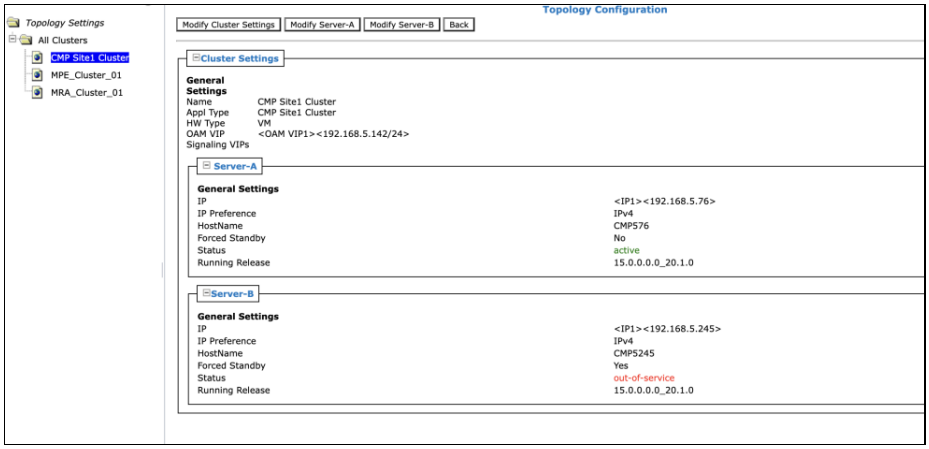
Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center**.**

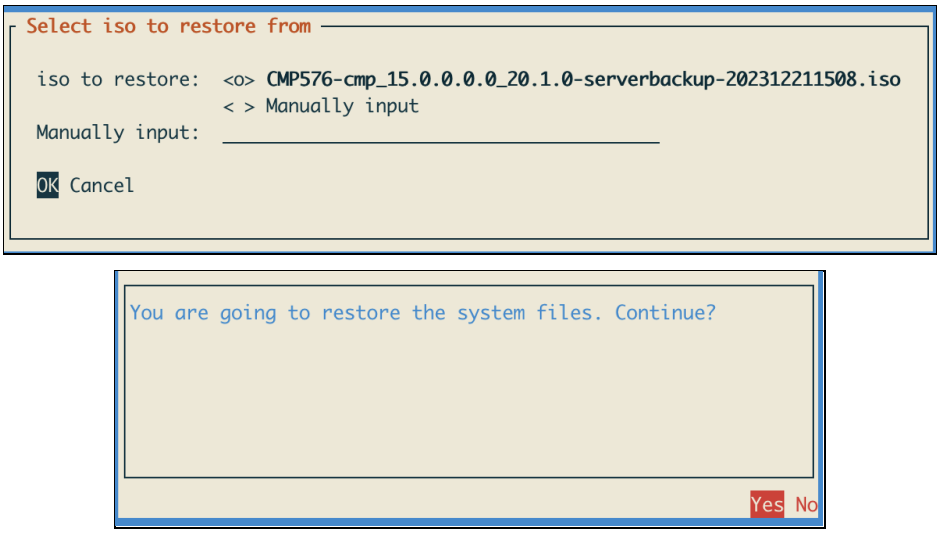
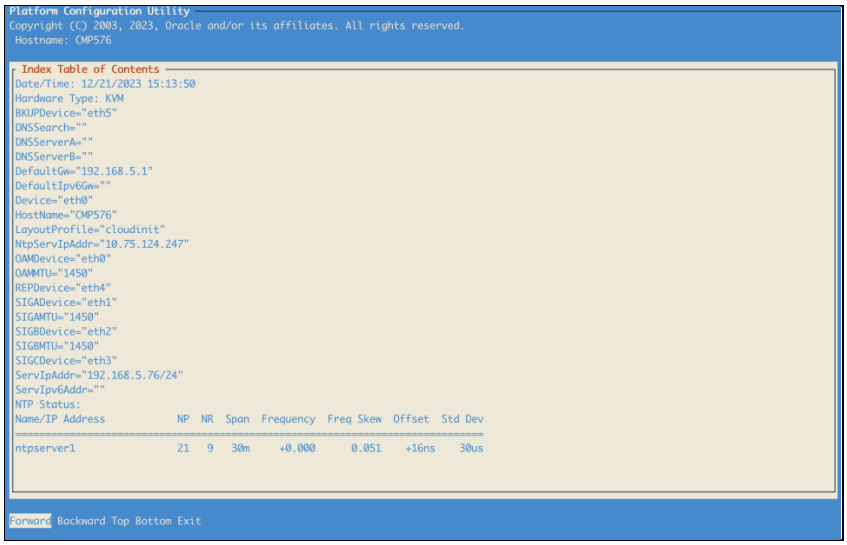
This Procedure restores the standby CMP node when a server level backup is available.

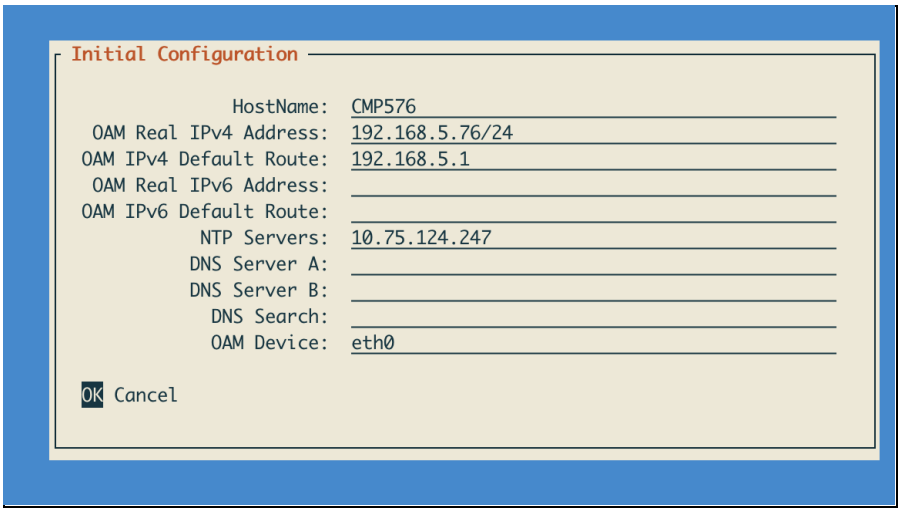
Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

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

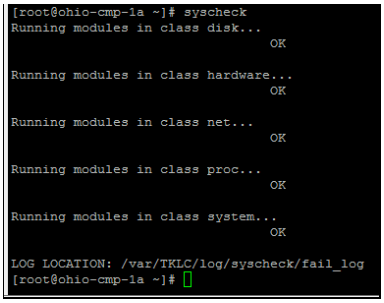
Procedure 1 Restore standby CMP Node with server backup file

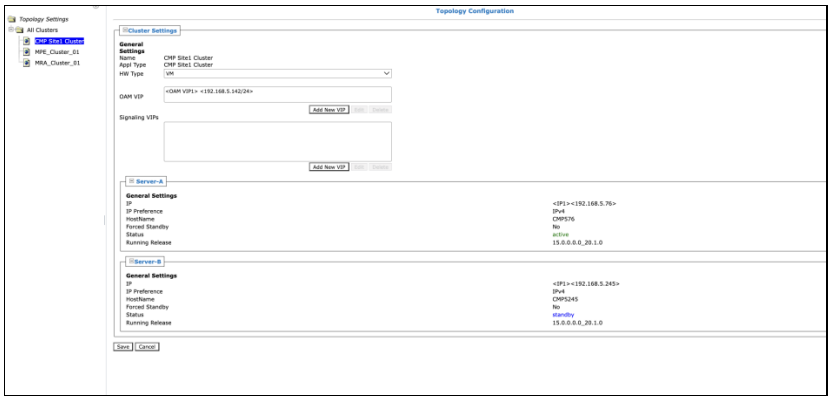
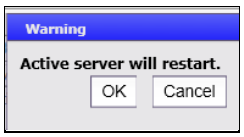
Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to: **Platform Setting → Topology Settings → All Clusters** 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click the **Modify Server-*X*** for the failed node 5. Click the **Forced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

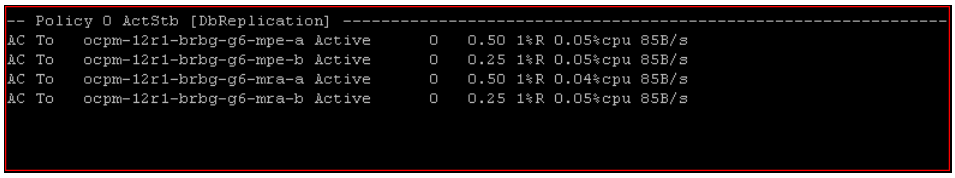
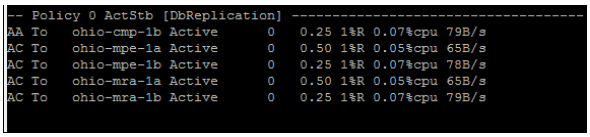
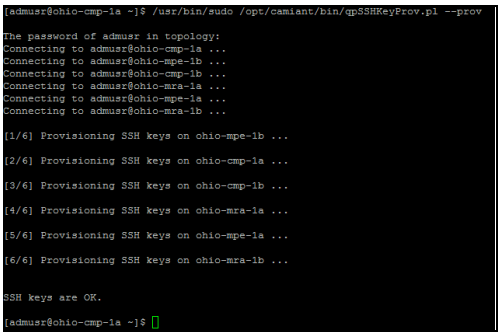
Step	Procedure	Details
4. ☐	Perform platcfg restore from SSH session to replacement node	1. Open the platcfg utility. `# su - platcfg` 2. Navigate to: **Policy Configuration → Backup and Restore → Server Restore** 3. Select the *serverbackup*.ISO that you just put on the system and click **OK**. 4. Click **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**  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

Step	Procedure	Details
		to the shell. 

7. ☐	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>`

8. ☐	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. `# 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. 

Step	Procedure	Details
9. ☐	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**  5. Accept the warning message by clicking **OK**. 
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. 

Step	Procedure	Details
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 while waiting reconnection:  Expected irepstat output after cluster has formed: 
12. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility • As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root` • As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov` 
---End of Procedure---		

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

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

Required resources:

- Replacement node hardware
- 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.

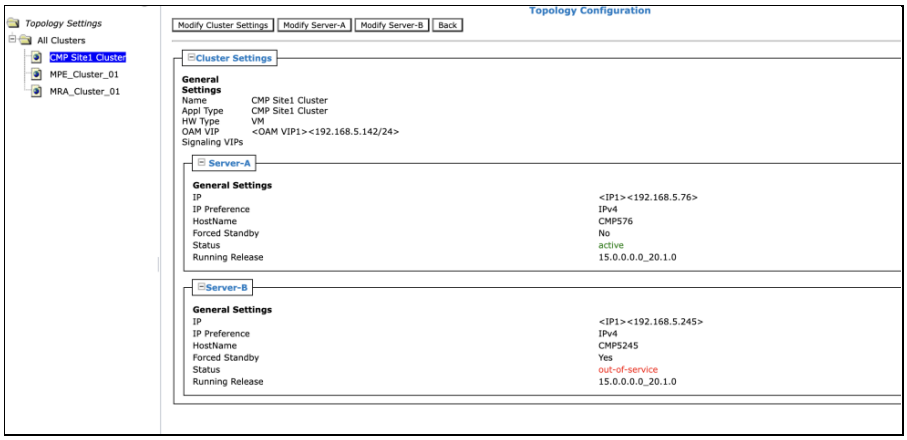
Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center.

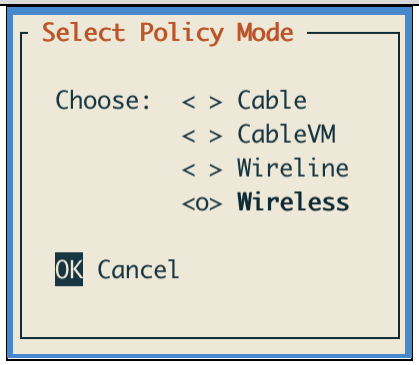
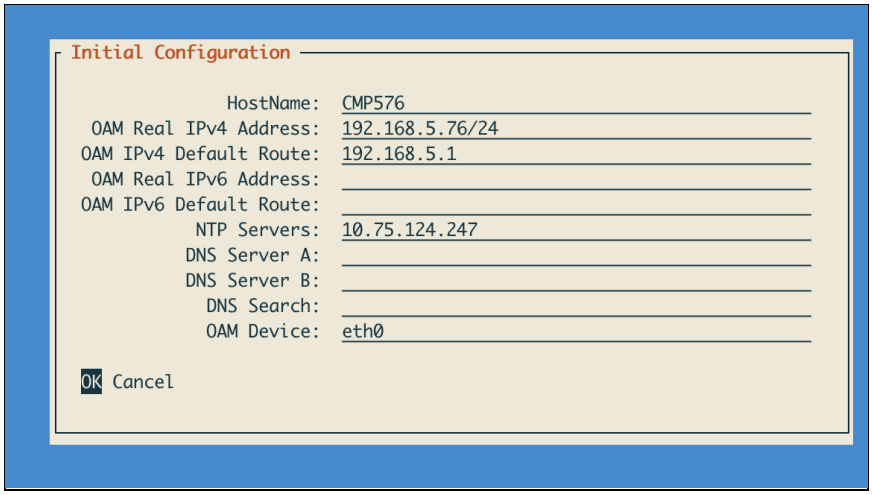
This Procedure restores the standby CMP node when a server level backup file is not available.

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

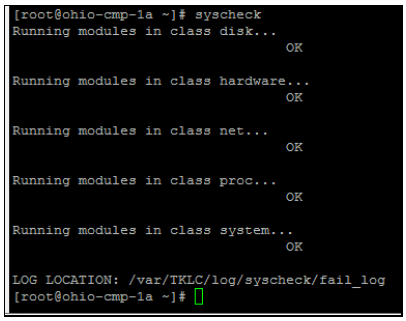
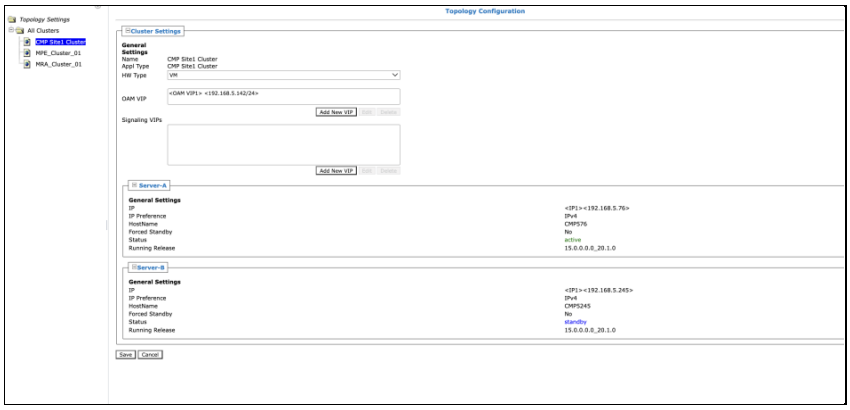
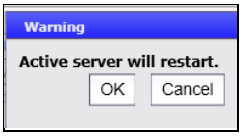
If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

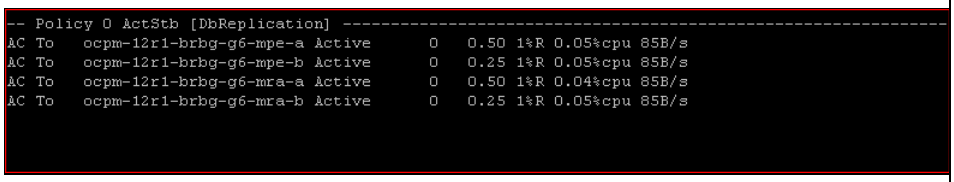
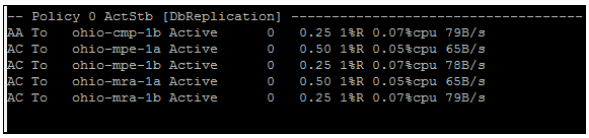
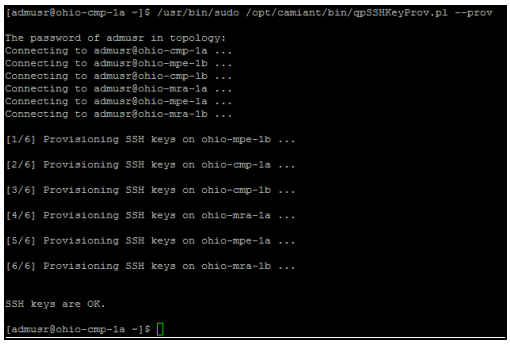
Procedure 2 Restore standby CMP Node without server backup file

Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	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. ☐	Login via SSH to the node	Login to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: `virsh console <SERVER_NAME>`
3. ☐	Perform platcfg restore from SSH session to replacement node Perform Initial configuration	1. Open the platcfg utility. `# su - platcfg` 2. 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:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

Step	Procedure	Details
5. ☐	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. `# 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. 
6. ☐	Remove the Forced Standby designation on the node.	1. In the CMP GUI, navigate to: **Platform Setting → Topology Setting →** <*Current_Cluster*> 2. Click modify for the server that is in Forced Standby. 3. Clear the **Forced Standby** checkbox 4. Click **Save**  5. Accept the warning message by clicking **OK**. 

Step	Procedure	Details
7. ☐	Verify cluster status	1. In the CMP GUI, navigate to: **Platform Setting → Topology Settings → All Clusters → <*Current CMP 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. 
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: `# irepstat` Expected irepstat output while waiting reconnection:  Expected irepstat output after cluster has formed: 
9. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility • As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root` • As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov` 
---End of Procedure---		

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

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

Required resources:

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

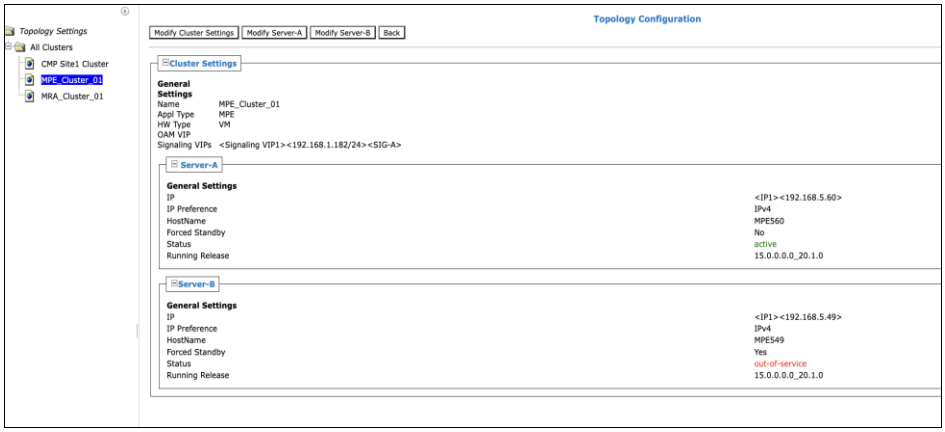
Note: Refer to the *Policy Management Cloud Installation Guide* Release 15.0, the documents are available at the Oracle Help Center**.**

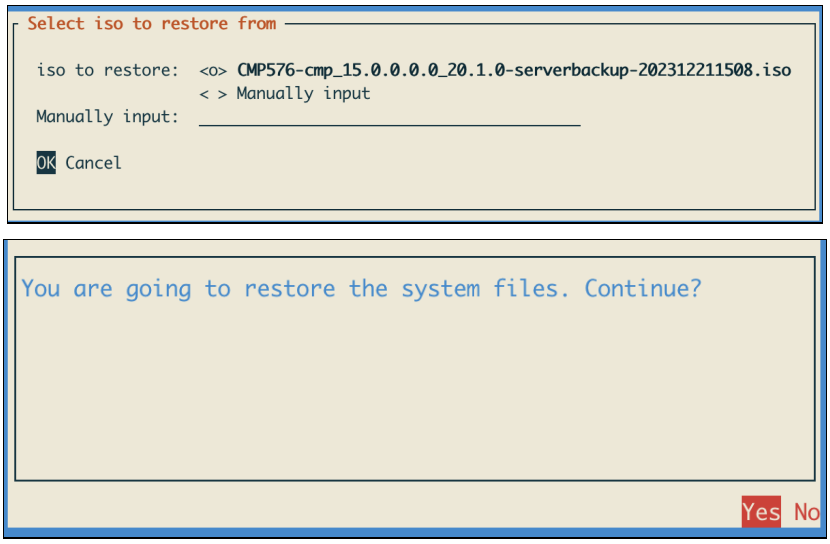
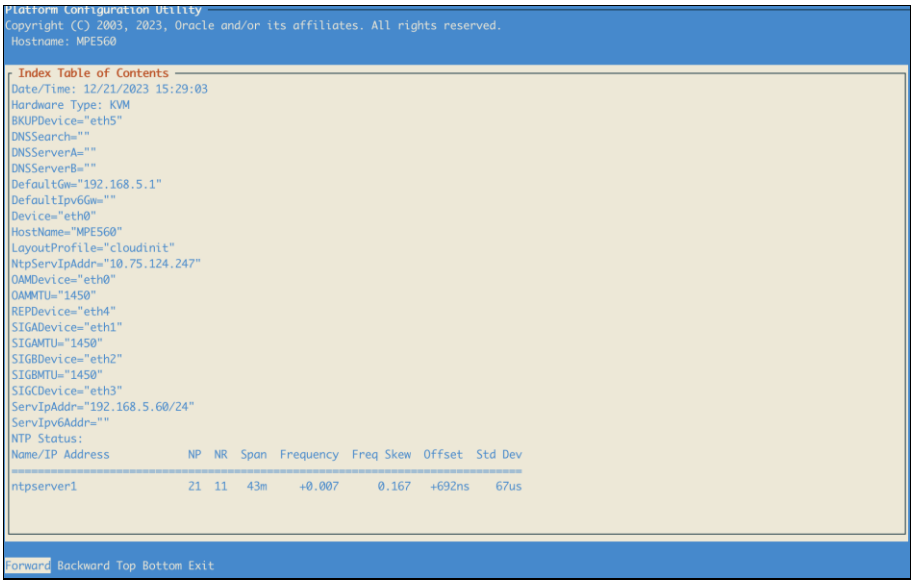
This procedure performs Restore single MPE/MRA node with server backup file.

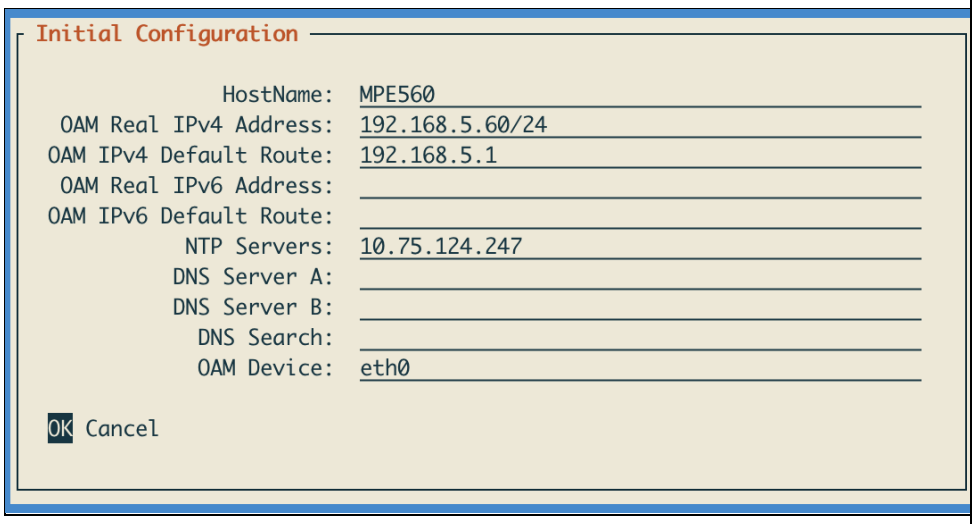
Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

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

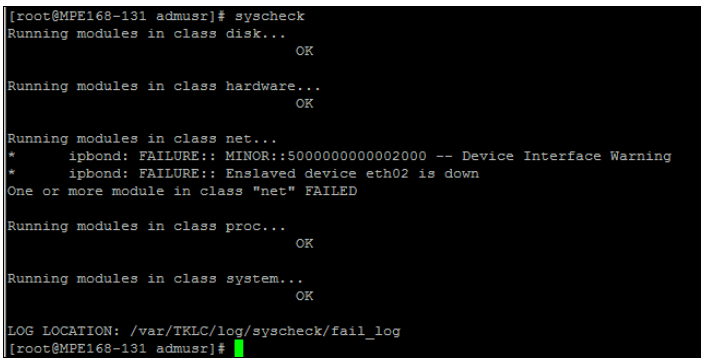
Procedure 3 Restore single MPE/MRA node with server backup file

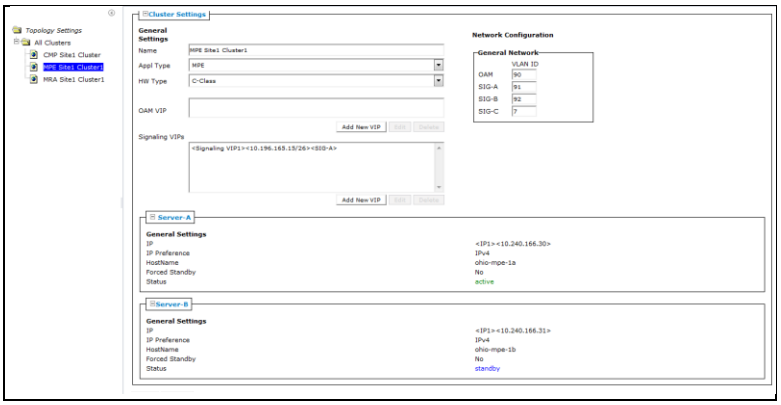
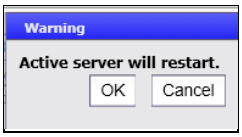
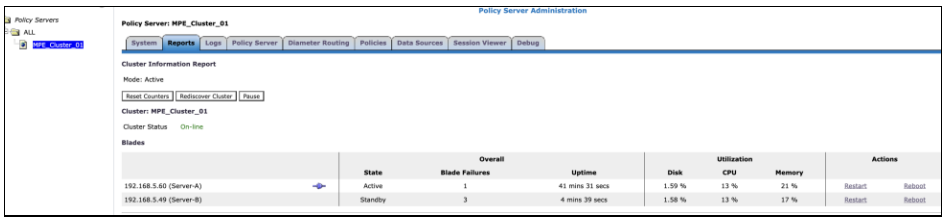
Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click the **Modify Server-*X*** for the failed node 5. Click the **Forced 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: `/var/camiant/backup/local_archive/serverbackup` **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. ☐	Login via SSH to the node	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: `virsh console <SERVER_NAME>`

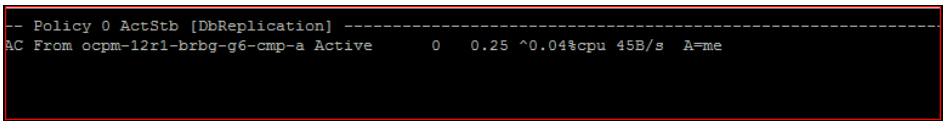
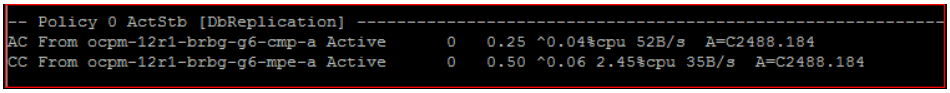
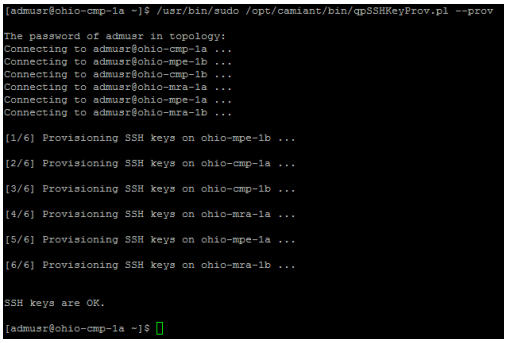
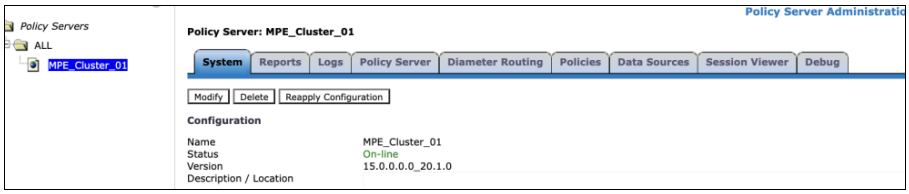
Step	Procedure	Details
4. ☐	Perform platcfg restore from SSH session to replacement hardware	1. Open the platcfg utility. `# su - platcfg` 2. Navigate to: **Policy Configuration → Backup and Restore → Server Restore** 3. Select the *serverbackup*.ISO that you just put on the system and click **OK**. 4. Click **Yes** to confirm. 
5. ☐	Verify the status	A window opens indicating that the restore operation is successful and 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	1. Click **Exit** on each platcfg menu until you are returned to the Main Menu of the platcfg utility. 2. Navigate to: **Policy Configuration → Verify Initial Configuration**  3. If the configuration does not exists, navigate to **Perform Initial Configuration** and enter the initial configuration hostname, OAM IP, and NTP servers configurations.

Step	Procedure	Details
		

9. ☐	Reboot the server	Reboot the server:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

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. `# 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. 

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**  5. Accept the warning message by clicking **OK**. 
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. 

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: `# irepstat` Expected irepstat output while waiting reconnection:  Expected irepstat output after cluster has formed: 
14. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility • As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root` • As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov` 
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

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

Required resources:

- Policy APP installation QCOW/OVA.
- 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 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 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**.**

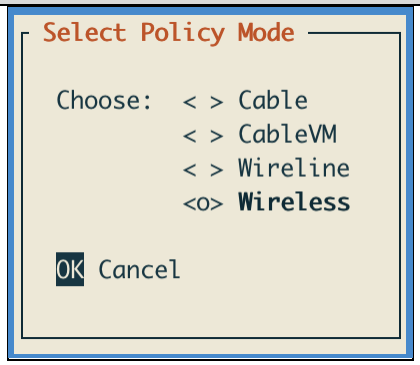
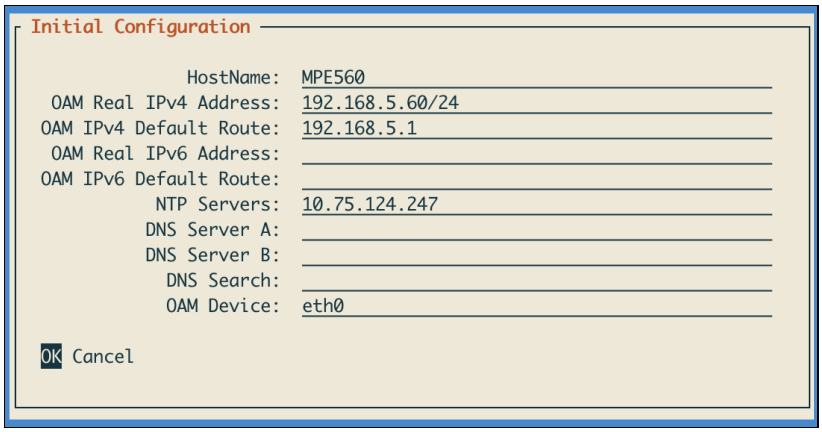
This Procedure performs Restore single MPE/MRA node without server backup file

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

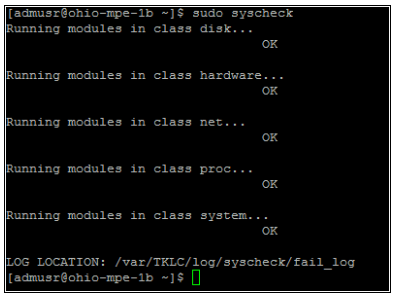
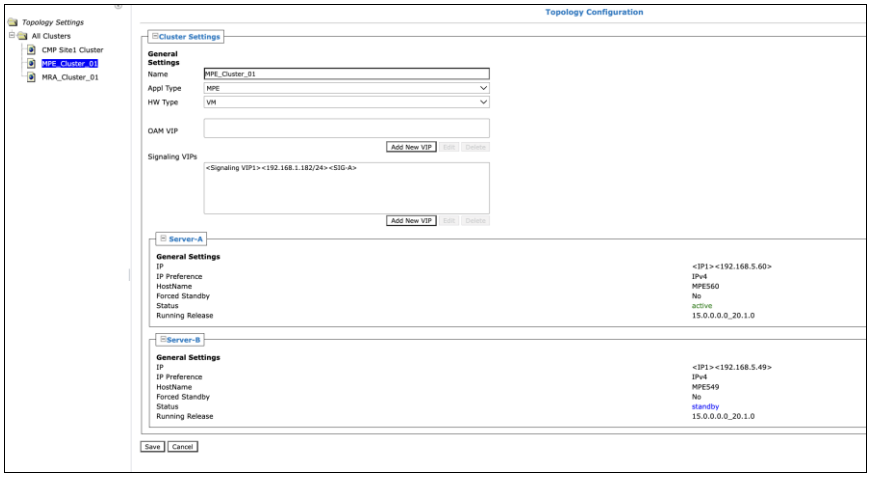
If this procedure fails, contact the My Oracle Support Customer Care Center and ask for assistance.

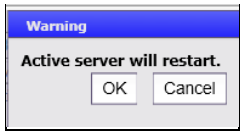
Procedure 4 Restore single MPE/MRA node without server backup file

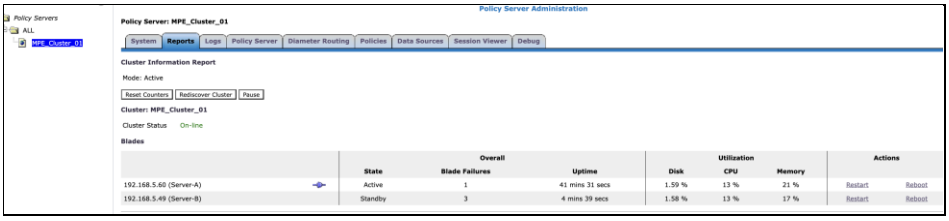
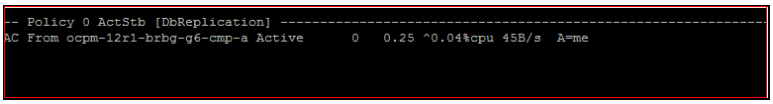
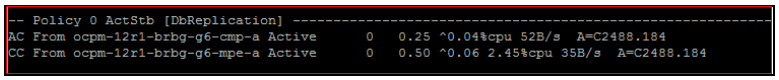
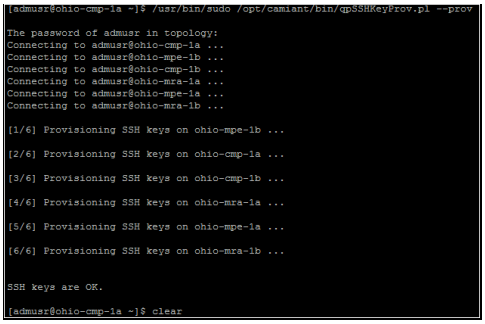
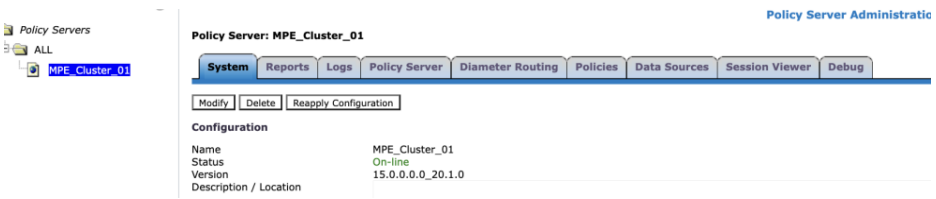
Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 2. Determine the cluster with the failed node 3. Determine the failed node **NOTE:** It is possible for a GeoRedudant Topology, that the failed server 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. ☐	Login via SSH to the node	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: `virsh console <SERVER_NAME>`
3. ☐	Perform Initial Policy Configuration using the platcfg utility on the	1. Open the platcfg utility. `# su - platcfg` 2. Navigate to: **Policy Configuration → Set Policy Mode**

Step	Procedure	Details
	installed node	 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 from the node being replaced: 

4. ☐	Reboot the server	Reboot the server:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>5. ☐</td><td>Verify basic network connectivity and server health.</td><td>1. From the installed server, ping the OAM/XMI 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.
<code># ping <XMI or OAM gateway address></code>
2. Run the syscheck command. Verify that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support.
 
</td></tr>
<tr><td>6. ☐</td><td>Remove the Forced Standby designation on the node.</td><td>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
 

5. Accept the warning dialog by clicking OK.
 
</td></tr>
</table>

Step	Procedure	Details
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. 
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: `# irepstat` Expected irepstat output while waiting reconnection:  Expected irepstat output after cluster has formed: 
11. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility • As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root` • As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov` 
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.` 

Step	Procedure	Details
---End of Procedure---		

5.5 Procedure 5: Restoring Complete Cluster Using Server Backup Files

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

Required resources:

- Policy APP installation QCOW/OVA.
- *serverbackup*.iso for the replacment 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: 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**.**

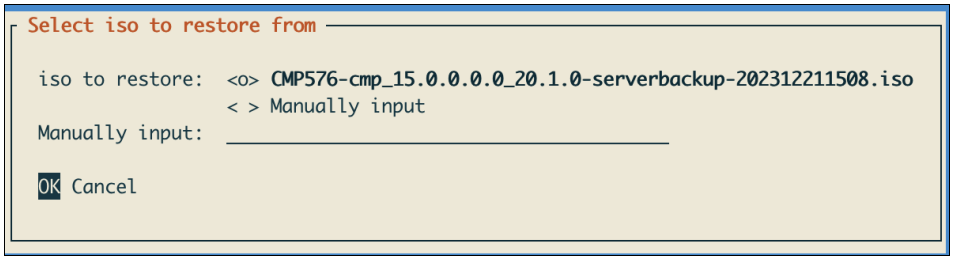
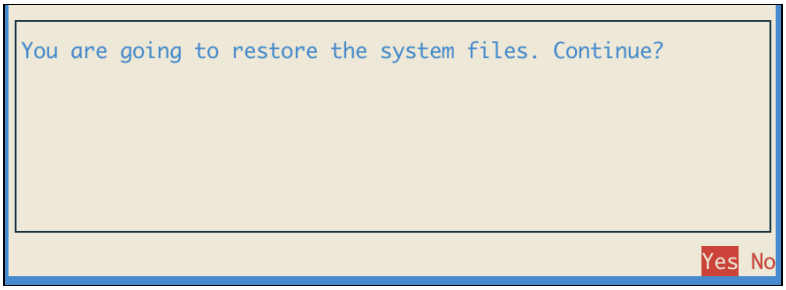
This Procedure performs Restoring complete cluster with the server backup files

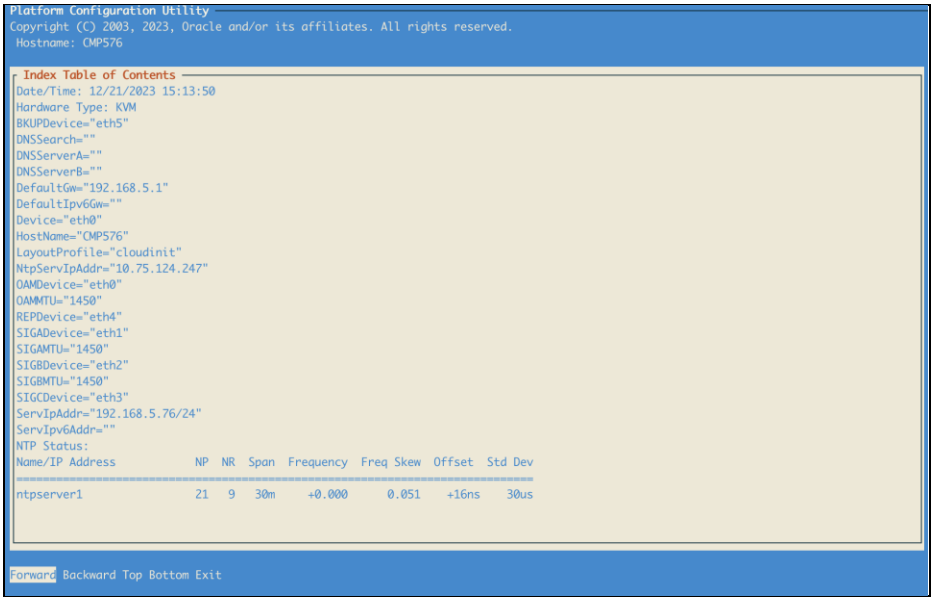
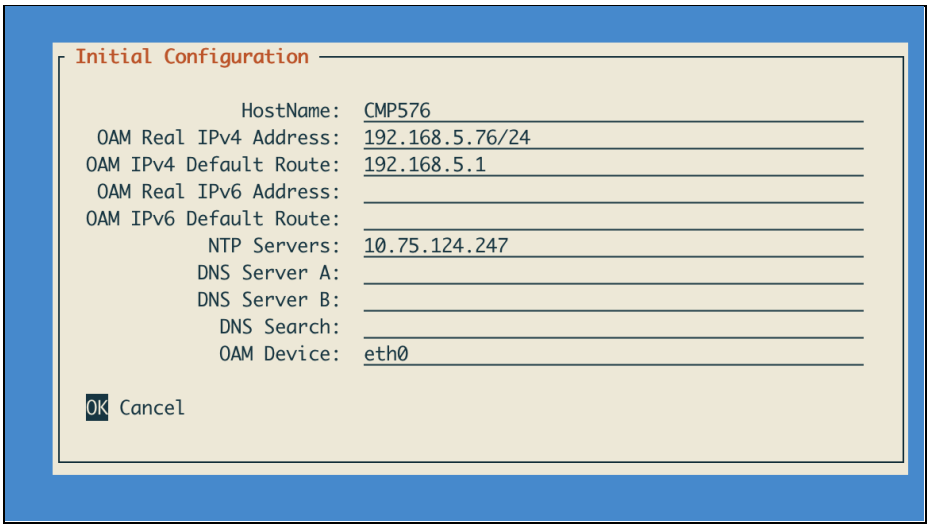
Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

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

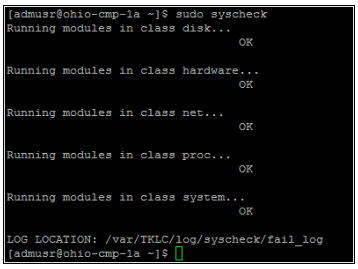
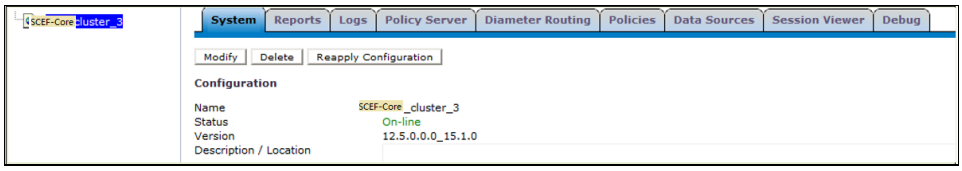
Procedure 5 Restoring complete cluster with the server backup files

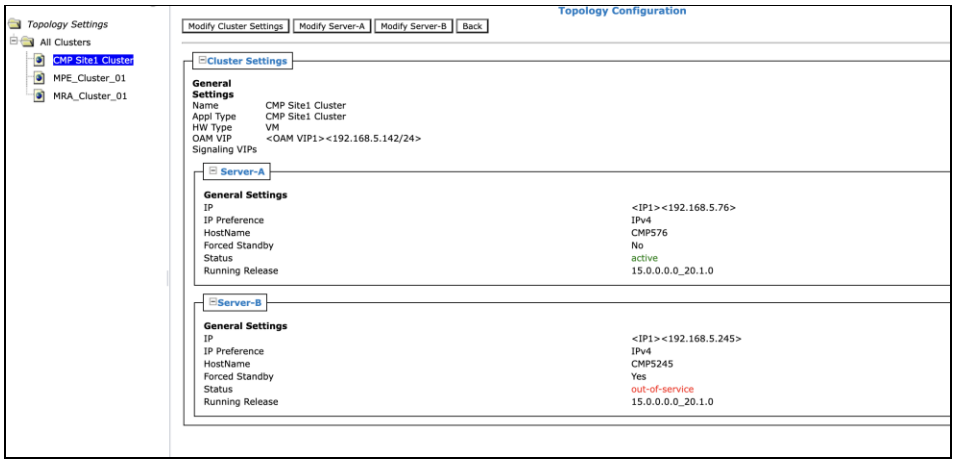
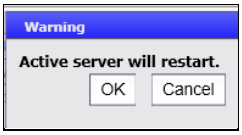
Step	Procedure	Details
1. ☐	SSH to replacement node	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: `virsh console <SERVER_NAME>`

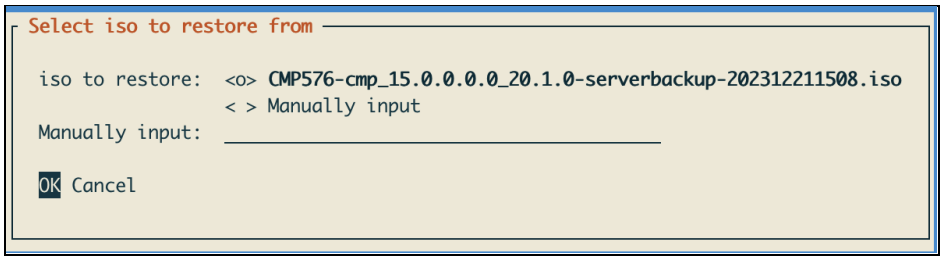
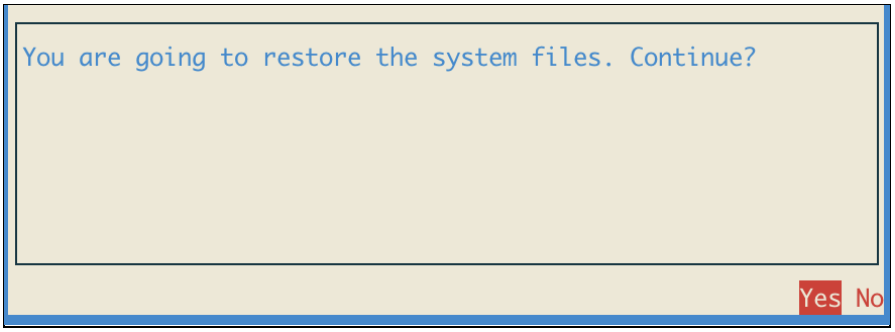
Step	Procedure	Details
2. ☐	Load the ISO to restore 1st server of the cluster	Obtain the *serverbackup.iso* for the restored node. When the replacement node is available (IPM/App installation complete), the server backup file is copied via secure copy (pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **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.
3. ☐	Perform platcfg restore from SSH session to replacement node	1. Open the platcfg utility. `# su - platcfg` 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.

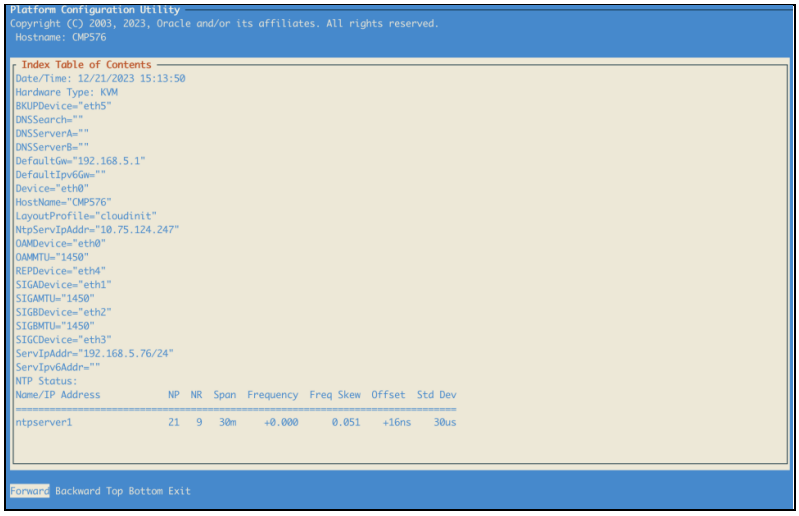
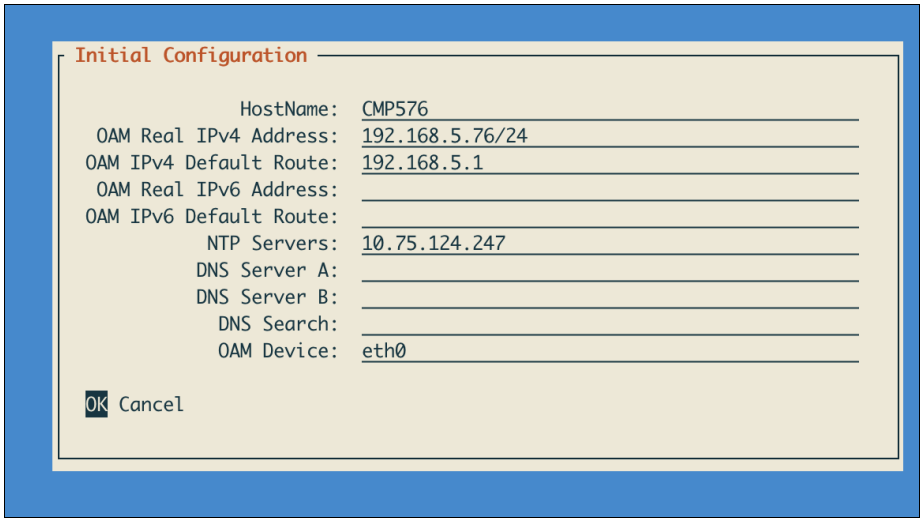
Step	Procedure	Details
5. ☐	Verify Initial configuration	1. Click **Exit** on each platcfg menu until you are returned to the Main Menu of the platcfg utility. 2. Navigate to: **Policy Configuration → Verify Initial Configuration**  3. If the configuration does not exist, navigate to **Perform Initial Configuration** and enter the initial configuration hostname, OAM IP, and NTP servers configurations. 

6. ☐	Reboot the server	Reboot the server:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

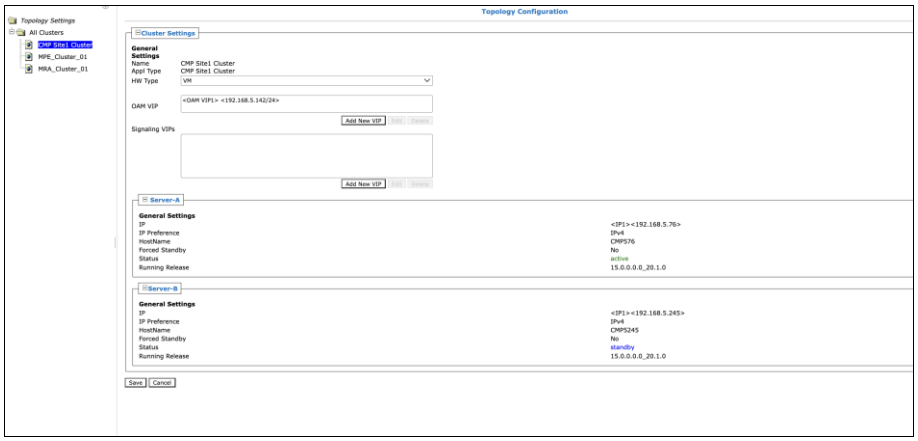
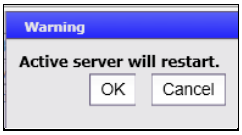
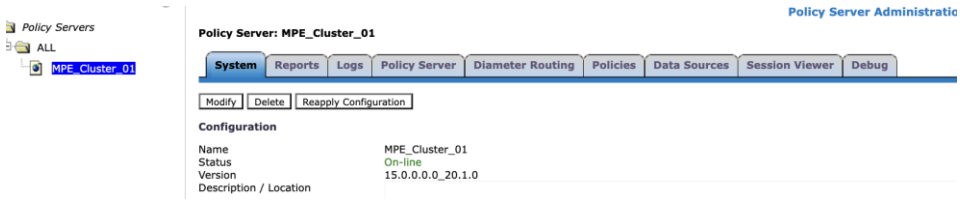
Step	Procedure	Details
7. ☐	Verify basic network connectivity and server health.	1. From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# 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.  **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	1. In the CMP GUI, navigate to: **Platform Setting → Topology Settings → All Clusters** 2. Select a cluster. 3. Click the **System** tab. 4. 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. 

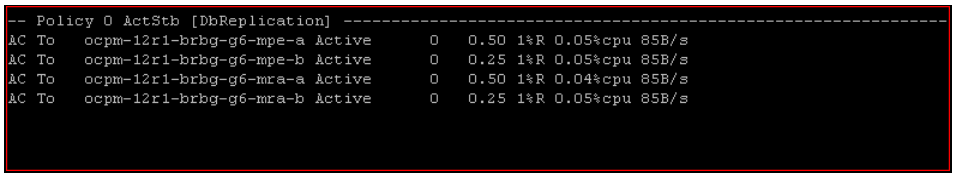
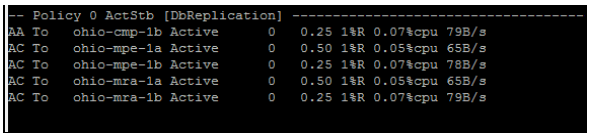
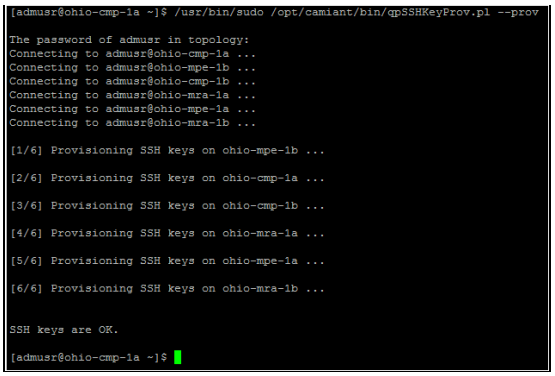
Step	Procedure	Details
11. ☐	Set Forced Standby designation on cluster node that is still out-of-service.	1. In the CMP GUI, navigate to: **Platform Setting → Topology Setting → <***Current Cluster***>** 2. Modify the server that has a status of out-of-service. 3. Select **Forced Standby**. 4. Click **Save**.  5. Accept the confirmation dialog by clicking **OK**. 
12. ☐	SSH from the VM Host server to 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: `virsh console <SERVER_NAME>`
13. ☐	Load the ISO to restore 2nd 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: `/var/camiant/backup/local_archive/serverbackup` **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 platcfg restore from SSH session to replacement node	1. Open the platcfg utility. `# su - platcfg` 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	1. Click **Exit** on each platcfg menu until you are returned to the Main Menu of the platcfg utility. 2. Navigate to: **Policy Configuration → Verify Initial Configuration**  3. If the configuration does not exists, navigate to **Perform Initial Configuration** and enter the initial configuration: hostname, OAM IP, and NTP servers configurations. 4. Verify that that the information is correct. 5. Click **OK** and then 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. 

17. ☐	Reboot the server	Reboot the server:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

Step	Procedure	Details
18. ☐	Remove the Forced Standby designation on the node.	1. In the CMP GUI, navigate to: **Platform Setting → Topology Setting → <***Current Cluster***>** 2. Click modify for the server that is in Forced Standby 3. Clear the Forced Standby checkbox 4. Click **Save**  5. Accept the warning message by clicking **OK**. 
19. ☐	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.** Check CMP cluster status (as indicated in the previous step), navigate to: **Platform Setting → Topology Setting → Current CMP Cluster** 3. 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: `# irepstat` Expected irepstat output while waiting reconnection:  Expected irepstat output after cluster has formed: 
21. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility • As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root` • As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov` 
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

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

Required resources:

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

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

Platform Setting → Topology Setting → <*Cluster_Name*>

NTP server configuration (and optionally DNS configuration is contained in the platcfg of the running 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: 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**.**

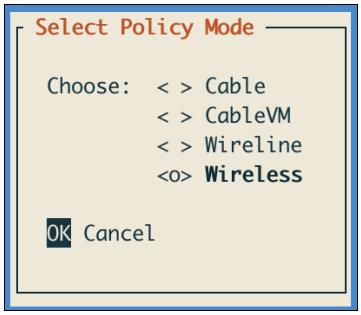
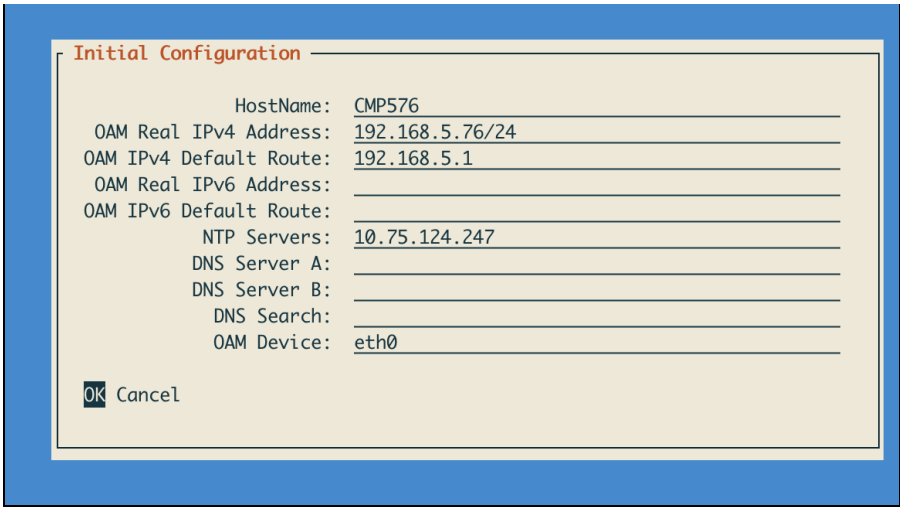
This Procedure performs Restoring complete cluster without the server backup

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

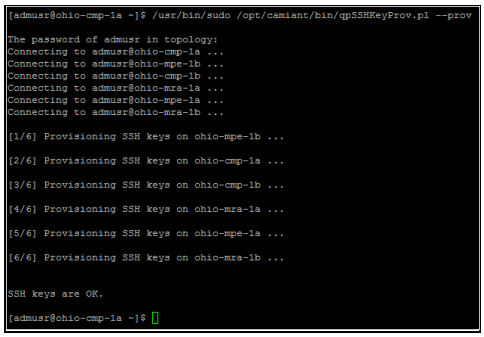
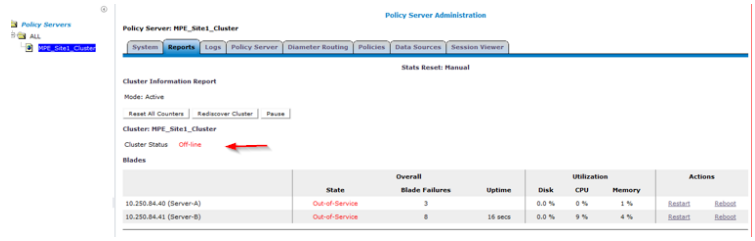
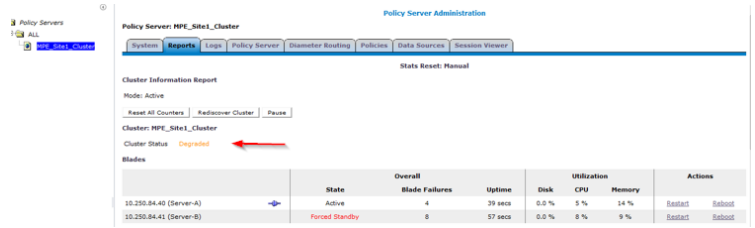
If this procedure fails, contact the My Oracle Support and ask for assistance.

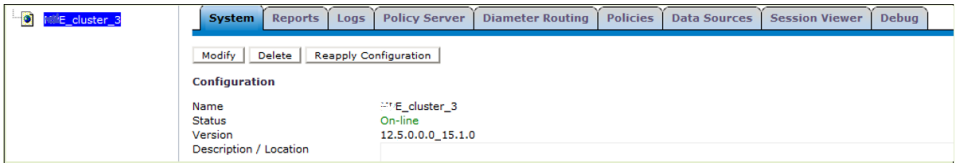
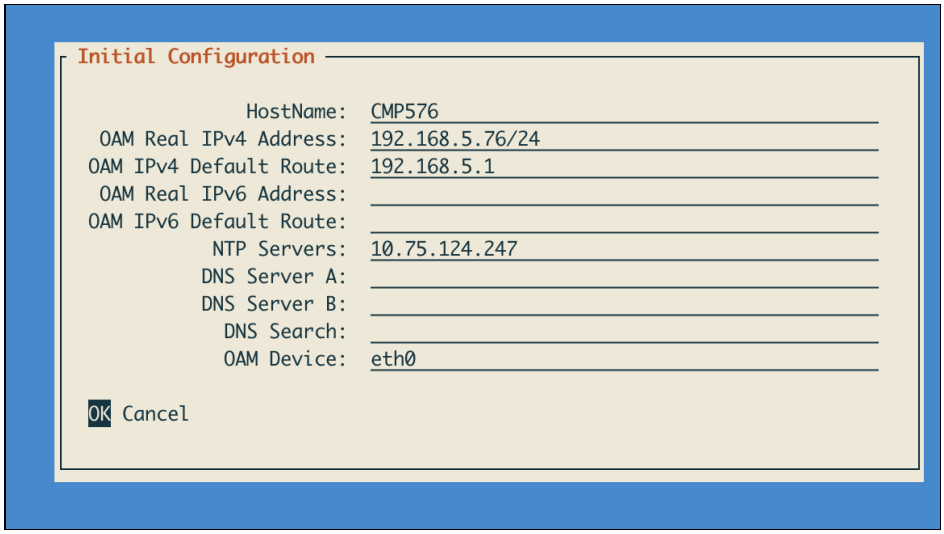
Procedure 6 Restoring complete cluster without the server backup

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

Step	Procedure	Details
2. ☐	Perform Initial Policy Configuration using the platcfg utility on the installed node	1. Open the platcfg utility. `# su - platcfg` 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 configuration details for the node being replaced: 6. After the server details are entered and verified, click **OK**. 7. 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. 8. Exit the platcfg utility by clicking **Exit** on each platcfg menu until you are returned to the shell. 

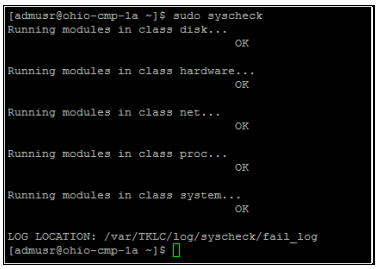
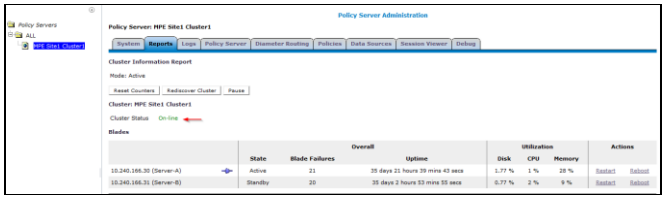
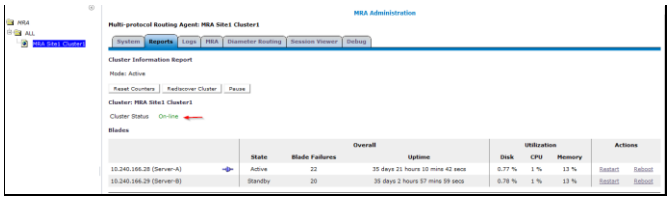
3. ☐	Reboot the server	Reboot the server:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

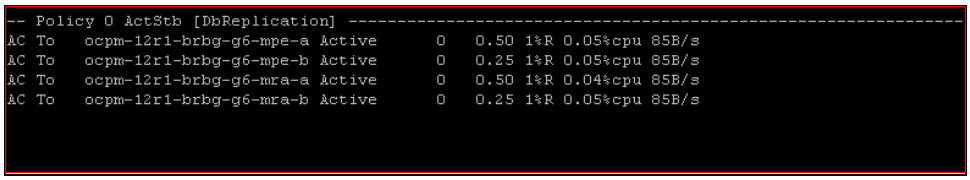
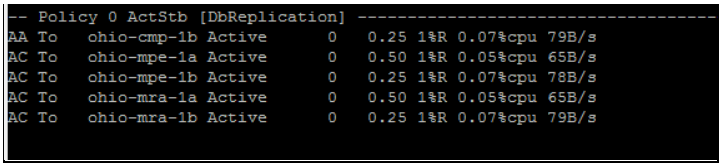
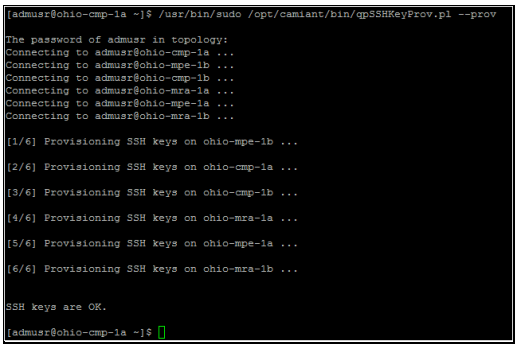
Step	Procedure	Details
4. ☐	Verify basic network connectivity and server health.	1. From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# 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. 
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	1. In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 2. Select a cluster 3. 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. ☐	Login via SSH to second node of the cluster	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: `virsh console <SERVER_NAME>`
8. ☐	Perform Initial Policy Configuration using the platcfg utility on second node of cluster	1. Open the platcfg utility. `# su - platcfg` 2. Navigate to: **Policy Configuration → Initial Configuration** 3. Enter the details for the replacement node: 4. After the server details are entered and verified, select **OK**. 5. 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. 6. Exit the platcfg utility by clicking **Exit** on each platcfg menu until you are returned to the shell. 

Step	Procedure	Details

9. ☐	Reboot the server	Reboot the server:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

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 node 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. 
11. ☐	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 **MPE:**  **MRA:** 

Step	Procedure	Details
12. ☐	Alternative method to check replication status	You can also monitor the clustering of the node from the shell on the primary node with the **irepstat** command. To do so, SSH to the active node of the cluster and run the **irepstat** command: `# irepstat` Expected irepstat output while waiting reconnection:  Expected irepstat output after cluster has formed: 
13. ☐	Exchange keys with cluster mate (This step need to run from active CMP)	Exchanging SSH keys Utility • As root, run `/opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root` • As admusr, run `/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov` 
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

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

Required resources:

- 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**.**

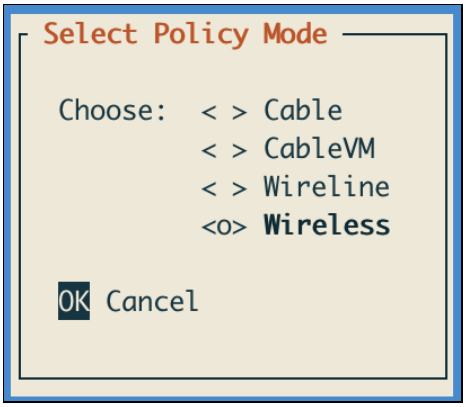
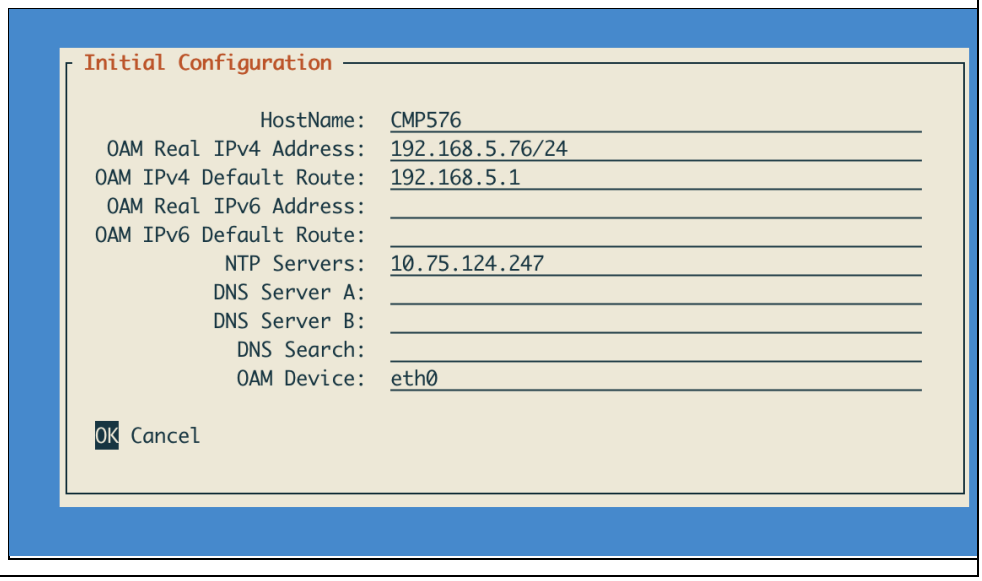
This Procedure performs Restoring CMP cluster with system backup available

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.

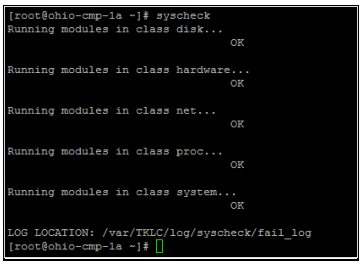
Procedure 7 Restoring CMP cluster with system backup available

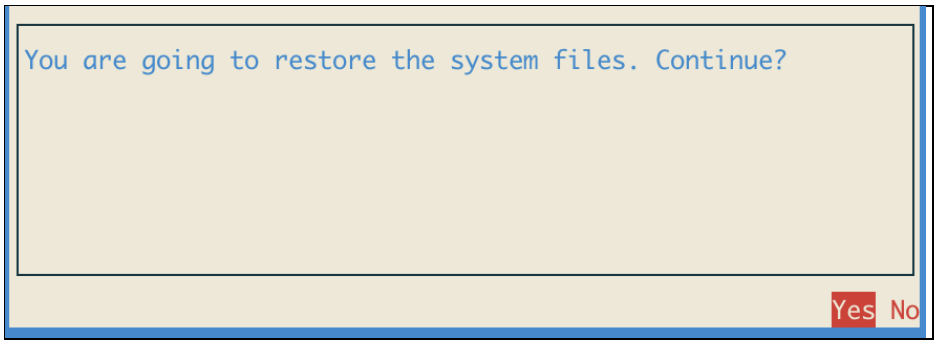
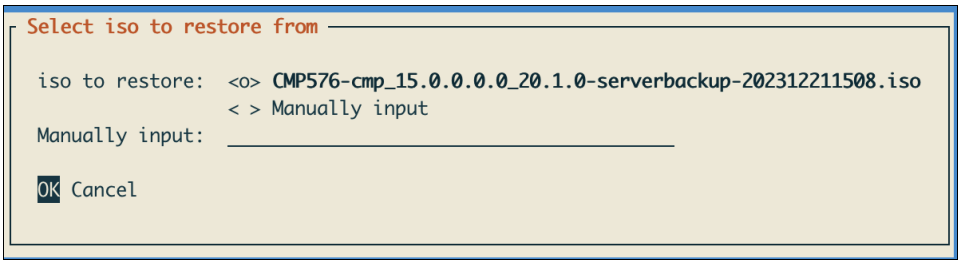
Step	Procedure	Details
1. ☐	Login via SSH to node	Log in to the underlying Virtual host (for example, KVM). Access the failed node using respective console access command. For example, for KVM: `virsh console <SERVER_NAME>`

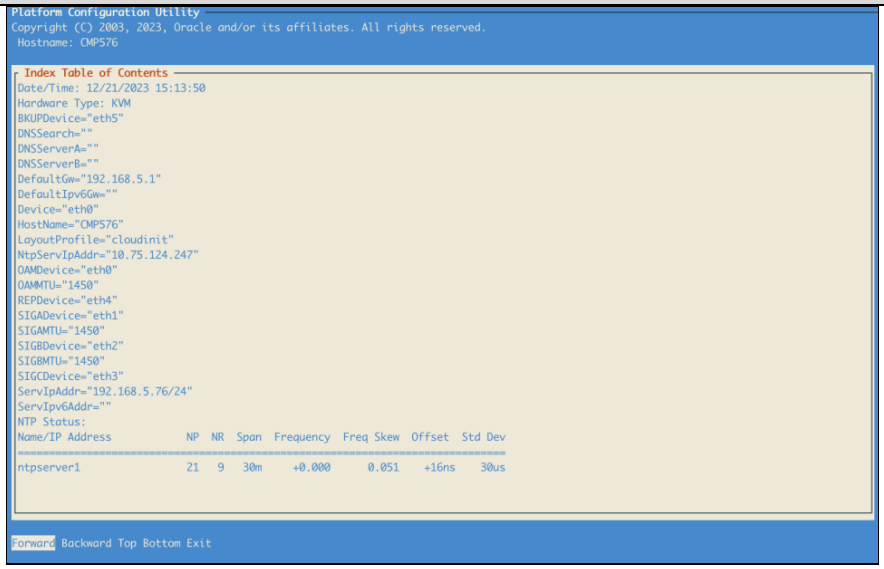
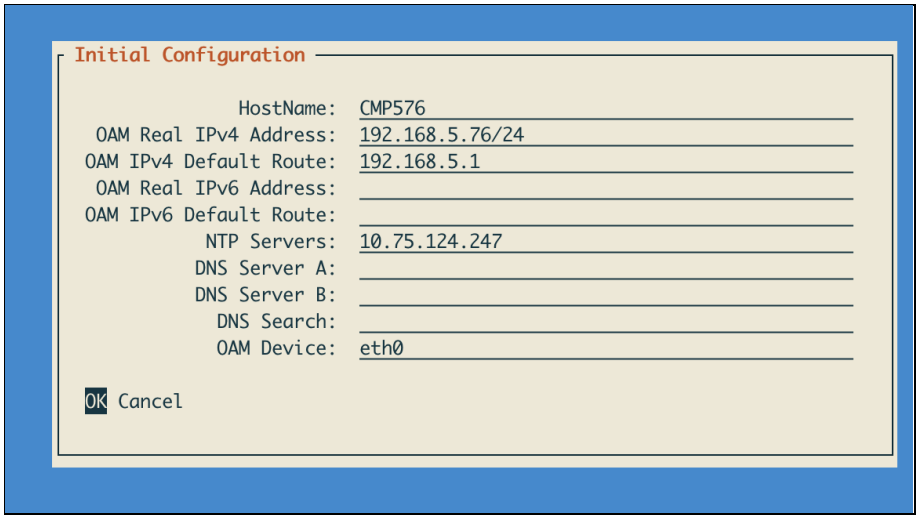
Step	Procedure	Details
2. ☐	Perform Initial Policy Configuration using the platcfg utility on the installed node	1. Open the platcfg utility. `# su - platcfg` 2. Navigate to: **Policy Configuration → Set Policy Mode**  3. Leave the mode as **Wireless** and click **OK** to continue. You can skip this 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

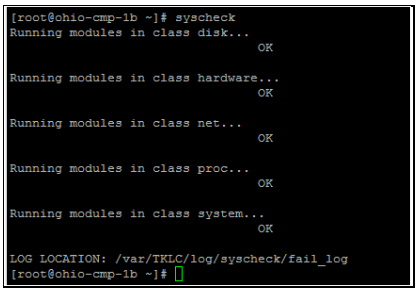
3. ☐	Reboot the server	Reboot the server:
		`# init 6`
		Reconnect to the server using respective console access command. For example, for KVM:
		`virsh console <SERVER_NAME>`

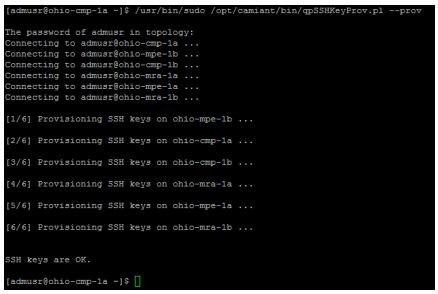
4. ☐	Verify basic network connectivity and server health.	1. From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old node configuration and reconfigure if needed. Contact My Oracle Support before proceeding if network ping tests still fail. `# 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. 
5. ☐	Load the system backup(ISO) file for server 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). `/var/camiant/backup/local_archive/systembackup/`

Step	Procedure	Details
6. ☐	Perform platcfg restore from SSH session to replacement node	1. Open the platcfg utility. `# su - platcfg` 2. Navigate to: **Policy Configuration → Backup and Restore → System Restore** 3. 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**.  4. 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**. 5. 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	1. Click **Exit** on each platcfg menu until you are back to the Main Menu of the platcfg utility. 2. Navigate to: **Policy Configuration → Verify Initial Configuration**

Step	Procedure	Details
		 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. 

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.	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. `# ping <XMI or OAM gateway address>` 2. Run the **syscheck** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 

11. ☐	Exchange keys with cluster mate(This step need to run from active CMP)	Exchanging SSH keys Utility
		• As root,
		`run /opt/camiant/bin/qpSSHKeyProv.pl --prov --user=root`
		• As admusr, run
		`/usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`
		 

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, the replace the other node of the CMP cluster using this procedure, and any other clusters or individual nodes that require replacement are replaced using this procedures.
---End of Procedure---		

5.8 Procedure 8: Promoting Georedundant CMP Cluster

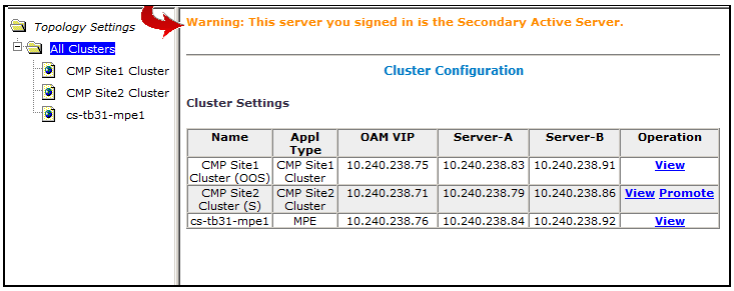
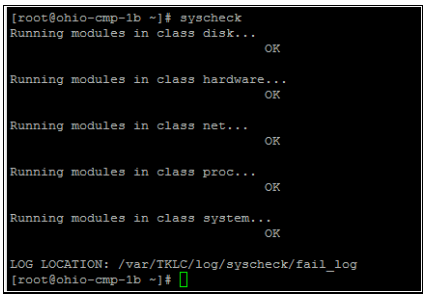
This procedure is used to bring a georedundant secondary active CMP online before beginning restoration of other policy clusters in the network. After the CMP is online, all other servers of the policy network are re-created using Procedure 1 through Procedure 7 and then their application level configuration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

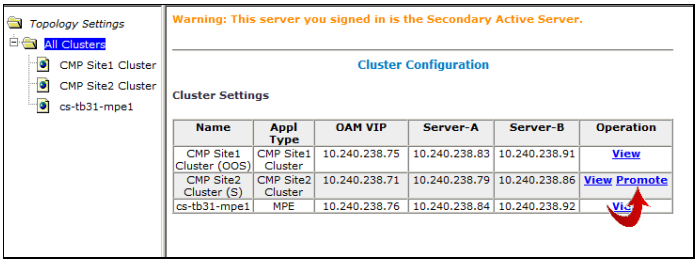
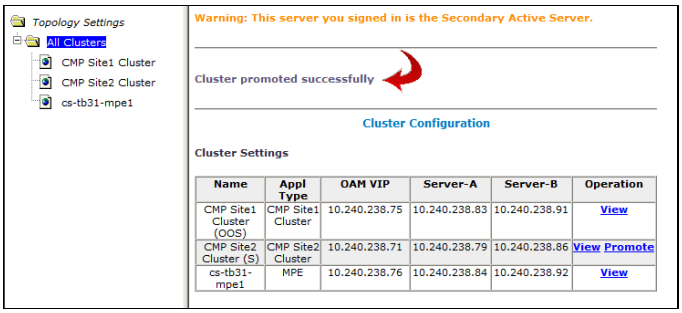
This Procedure performs Promoting georedundant CMP cluster

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. 
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. 

Step	Procedure	Details
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.  You see a message display above the Cluster Configuration header indicating successful promotion (see example). If not, retry the operation and/or contact My Oracle Support. 
5. ☐	Logout of the CMP GUI	Logout of the CMP GUI by clicking **Logout** link or closing the browser window.
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: `virsh console <SERVER_NAME>`

Step	Procedure	Details

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.
		`# irepstat`
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To Site1-nw-cmp-a Active 0 0.25 1%R 0.04%cpu 65B/s`
		`AA To Site2-nw-cmp-a Active 0 0.50 1%R 0.04%cpu 65B/s`
		The status of all clusters except known failed servers has a status of Active.
		Otherwise, if any of the replication paths show `DownConnecting` contact My Oracle Support.
		This example shows the installation with servers cs-tb31-cmp2-a and cs-tb31-cmp2-b failed, while all other cluster replication is working.
		`root@cs-tb31-cpm-a:~`
		`-- Policy 0 ActStb [DbReplication] ----------`
		`-- To cs-tb31-cmp2-b DownConnecting 0 0.00`
		`-- To cs-tb31-cmp2-a DownConnecting 0 0.00`
		`AA To cs-tb31-cmp-b Active 0 0.00 0.05%cpu 68B/s`
		`AC To cs-tb31-mpe1-b Active 0 0.00 0.05%cpu 82B/s`
		`AC To cs-tb31-mpe1-a Active 0 0.00 0.04%cpu 68B/s`
		`irepstat ( 7 lines) (h)elp`

9. ☐	Rebuild failed CMP cluster	Refer to Procedure 6: Restoring Complete Cluster without 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 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 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
   - 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.
   - 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.