Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Policy Management

Policy Management
Cloud Disaster Recovery 12.23

E85339-01

July 2017

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

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

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

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

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

EMAIL: support@oracle.com

Oracle Communications Policy Management Cloud Disaster Recovery 12.2

Table of Contents

List of Tables

1. INTRODUCTION

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for Policy Management System, Release 12.3. 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 execute disaster recovery for Policy Management Systems. Executing this procedure also involves referring to and executing procedures in existing support documents.

1.1 References

[1] E85332-01—Oracle Communications Policy Management Cloud Installation Guide 12.3

The above document is available on the Oracle Help Center.

1.2 Acronyms

Table 1: Acronyms

Acronym	Meaning
BIOS	Basic Input Output System
CD	Compact Disk
ISO	The name ISO is taken from the ISO 9660 file system used with CD-ROM media, but an ISO image might also contain a UDF (ISO/IEC 13346) file system
CMP	Configuration Management Platform
DR-CMP	Configuration Management Product for Disaster Recovery NOTE: It refers to the CMP on the secondary site
DVD	Digital Video Disc
GRUB	Grand Unified Boot loader
iLO	Integrated Lights-Out
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MPE	Multiprotocol Policy Engine
MRA	Multiprotocol Routing Agent
OS	Operating System (for example, TPD)
PM&C	Platform Management & Configuration
RMM	Remote Management Module
RMS	Rack Mount Server
SOL	Serial Over LAN
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
FRU	Field Replaceable Unit
USB	Universal Serial Bus
VM	Virtual Machine
VIP	Virtual IP address

1.3 Logins and Passwords

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

1.4 Software Release Numbering

This guide applies to all Policy Management versions 12.3.

1.5 Terminology

Table 2. Terminology

Term	Definition
Base software	Base software includes deploying the VM image.
Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.
Perform initial configuration	The perform initial configuration put into the policy server through the platcfg utility that brings the network interface for the server online and allows management and configuration from the CMP
Cluster mate	There are 2 or 3 blades in one cluster. Each is cluster mate in this cluster.
c-Class	HP marketing term for their enterprise blade server platform

2. GENERAL DESCRIPTION

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

- Recovery of one or more VM instance with at least one CMP VM instance intact
    - 1 or more CMP VM instances intact (this can include georedundant CMP(DR-CMP) VM instances)
    - 1 or more MPE/MRA instances failed
- Recovery of the entire network from a total outage
    - No CMP instances are available (neither primary, nor secondary) and other MPE/MRA VM instances must be recovered

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

No matter the number of VM instances 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 VM instances are offline and must be restored.

Single node outage MRA/MPE/ CMP, with CMP VM instance available

The simplest case of recovery is to recover a single node of a cluster with one or both CMP VM instances intact. Each failed VM instance is recovered by:

- Creating a new VM instance using section 4 as described in *Oracle Communications Policy Management Cloud Installation Guide* [1].
- Performing the initial configuration of the VM instance manually or from a server backup file

After this recovery, the cluster reforms, and database replication from the active node of the cluster recovers the restored VM instance. This scenario can be used to recover one VM instance of a MRA/MPE/ cluster or one VM instance of a CMP cluster. The SSH exchange keys with cluster mate from active CMP is also required.

Recovery of complete MRA/MPE cluster, with CMP VM instance available

The failure of a complete cluster can be recovered by creating new VM instances for the failed cluster. Each failed VM instance is recovered by:

- Creating a new VM instance using section 4 as described in *Oracle Communications Policy Management Cloud Installation Guide* [1].
- Performing the initial configuration of the VM instance manually or from a server backup file.

After this recovery, the CMP can push application level configuration to the restored cluster.

Recovery of the CMP Cluster when no georedundant CMP exists.

The complete failure of all CMP VM instances when no georedundant CMP exists is recovered by:

- Creating a new VM instance using as described in *Oracle Communications Policy Management Cloud Installation Guide* [1].
- Performing the initial configuration of the CMP VM instances manually or from a server backup file.

Disaster Recovery

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.

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

The availability of a georedundant CMP (DR-CMP) simplifies restoration of a failed CMP cluster. The georedundant CMP is promoted to active primary, and the failed CMP VM instances are recovered by:

- Creating a new VM instance using as described in *Oracle Communications Policy Management Cloud Installation Guide* [1]
- Performing the initial configuration of the CMP VM instances manually or from a server backup file

After the cluster is available, the primary running georedundant CMP replicates databases to the replaced CMP cluster.

Complete Outage (All VM instances)

This is the worst case scenario where all the VM instances in the network have suffered complete failure, and no georedundant CMP is available. Each VM instance in the network is recovered by:

- Creating a new VM instance using as described in *Oracle Communications Policy Management Cloud Installation Guide* [1]
- Performing the initial configuration of the VM instance manually or from a server backup file

After the VM instances are installed and available, completion of the recovery requires restoration of a stored system backup in order to recover the application level configuration including policies and configuration of the MPE/MRA clusters in the network.

If no backup file is available, the only option is to rebuild the entire network from scratch in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1]. The network data must be reconstructed from whatever sources are available, including entering all data manually.

A note on performing the initial configuration of a VM instance:

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

Initial configuration information:

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

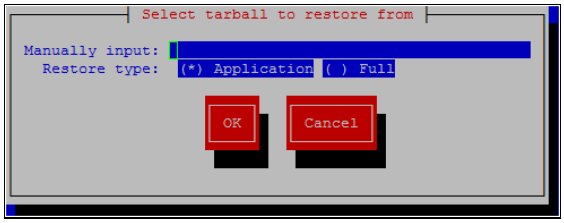
Using the server backup file

When asked to restore from server backup, the platcfg utility looks in `/var/camiant/backup/local-archive/serverbackup` directory. If no files are in that directory, the manual input dialog is presented.

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.

Using the system restore file

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

3.1 Disaster Recovery Strategy

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

1. Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedures. This means the failure conditions in the network match one of the failure scenarios described in Recovery Scenarios
2. Evaluate the availability of server and system backup files for the servers that are to be restored.
3. Read and review the content in this document.
4. Determine whether a georedundant CMP(DR-CMP) is available
5. From the failure conditions, determine the Recovery Scenario and procedure to follow.
6. Execute appropriate recovery procedures.

Required materials

The following items are required for disaster recovery:

1. A copy of this document and copies of all documents in the reference list.
2. Copy of all site surveys performed at the initial installation and network configuration of the site. If the site surveys cannot be found, escalate this issue within Oracle CGBU Customer Service until the site survey documents can be located.
3. Policy management system backup file: electronic backup file (preferred) or hardcopy of all Policy system configuration and provisioning data.
4. Policy Application installation: OVA for CMP, MPE, MRA of the target release.

3.2 Policy Server Backup

Backup of the policy server can be done either manually from the platcfg utility, or on a schedule as configured in the platcfg utility. There are two 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 should be executed on each of the server in the network.

- System Backup

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

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

4. PROCEDURE PREPARATION

1.1 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 below that can be combined to recover one or more policy management nodes or clusters in the network.

Note: A failed VM instance in disaster recovery context refers to a VM instance that is no longer available to be restored. Examples of scenarios where this can happen are: host server failure and user deletion of VM instance.

The general steps recovering VM instances are:

1. Create a new VM as described in *Oracle Communications Policy Management Cloud Installation Guide* **Error! Reference source not found.**
2. Perform the initial configuration of the VM or restore the initial configuration from a server backup file
3. Check NTP status after recovery
4. Check Active Alarms from CMP GUI page.

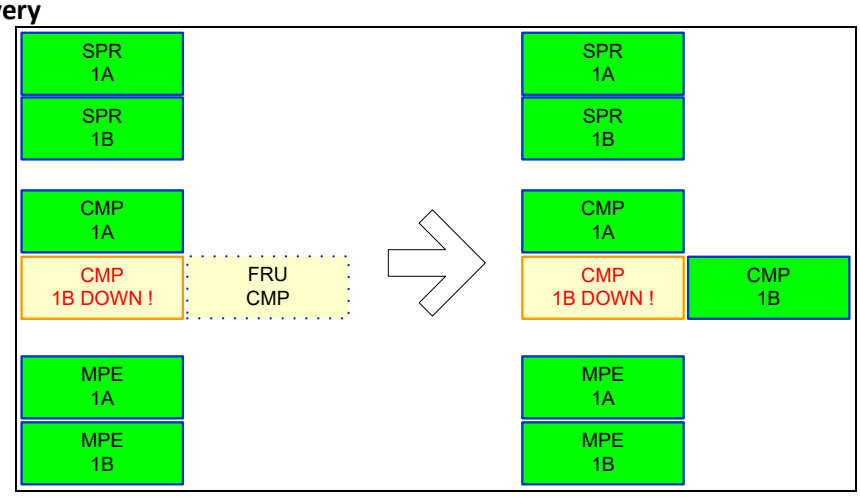
4.1 Recovery Scenarios

4.1.1 Recovery Scenario 1: Partial Cluster Outage with Primary CMP VM Instance Available

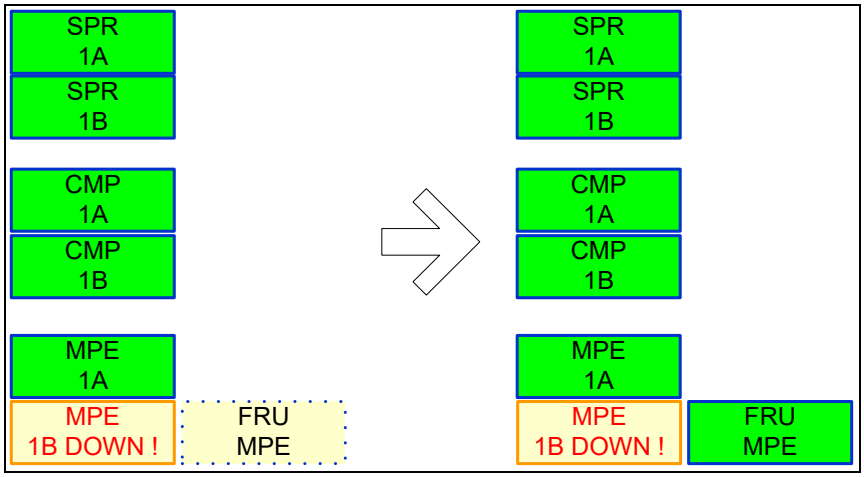
A single CMP VM instance is capable of restoring the configuration database via replication to all MPE/MRA servers, or to the other CMP node of a cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The detailed steps for the procedures are in the Restore Procedures section. The major activities are summarized as follows:

- Recover Standby CMP VM instance (if necessary)
  - Create a new CMP VM instance
  - 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 VM instance and is replicated to the standby CMP VM instance.

Disaster Recovery



- Recover any failed MPE/MRA servers by:
  - Create a new MPE/MRA VM instance
  - 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 VM instance and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/MRA VMs using re-apply configuration.



Follow the procedure below for detailed steps.

- Use Procedure 2: Restore Standby CMP Node without Server Backup File

  Or Procedure 1: Restore Standby CMP Node with Server Backup File to recover the second CMP node if necessary.

- Use Procedure 4: Restore Single MPE/MRA Node without Server Backup File to recover MPE / MRA nodes when one of the peers of the cluster is still available.

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

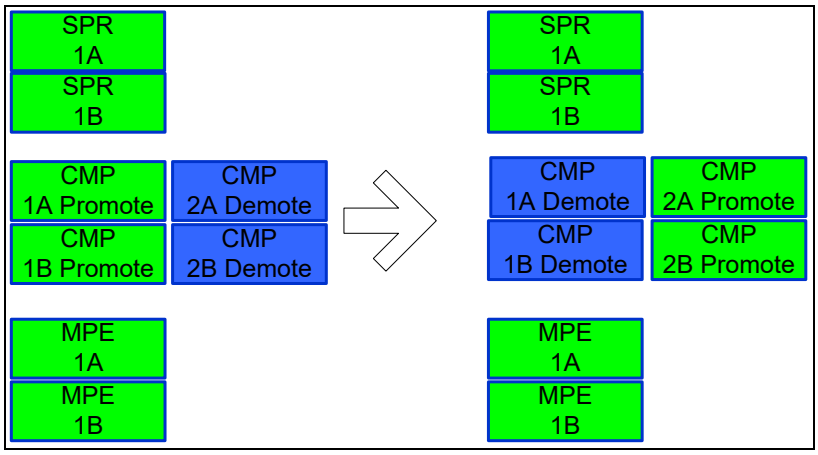
- Use Procedure 5: Restoring Complete Cluster with the Server Backup Files

  Or Procedure 6: Restoring Complete Cluster without Server Backup File to recover complete MPE / MRA clusters that have gone down.

4.1.2 Recovery Scenario 2: Partial Cluster Outage with Georedundant CMP Server Available

For a partial outage with a Georedundant CMP VM instance available, the secondary site CMP must be manually promoted to Primary status as the controlling CMP for the policy network. Then creation of a new CMP VM instance and initial Policy configuration is required. The now active CMP VM instance is capable of restoring the configuration database via replication to all MPE/MRA servers, and to the other CMP cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The detailed steps are in the Restore Procedures section. The major activities are summarized as follows:

- Promote the Georedundant CMP VM instance.
  - This step is done by logging into the OAM VIP address of the second site CMP cluster. Use procedure 8 below.



  This is done if the Primary CMP cluster must be restored. If it is an MRA, MPE, or secondary CMP cluster that must be restored, it is not required to promote the georedundant CMP.

- Recover any failed MPE/MRA VM instances by:
  - Creating a new VM instance for the failed MPE/MRA.
  - 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 VM instance and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/MRA VM instances using re-apply configuration.
- Recover other site CMP VM instance by:
  - Creating a new CMP VM instance.
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file.

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

Follow the procedure below for detailed steps.

- Use Procedure 8: Promoting Georedundant CMP Cluster below to promote the georedundant CMP
- Use Procedure 4: Restore Single MPE/MRA Node without Server Backup File to recover MPE/MRA nodes when one of the peers of the cluster is still available.

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

- Use Procedure 5: Restoring Complete Cluster with the Server Backup Files

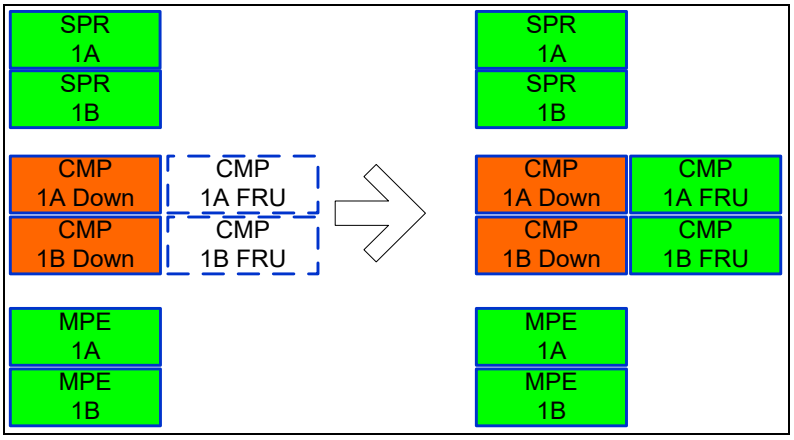
  Or Procedure 6: Restoring Complete Cluster without Server Backup File to recover complete MPE / MRA clusters that have gone down.

- Use Procedure 5: Restoring Complete Cluster with the Server Backup Files

  Or Procedure 6: Restoring Complete Cluster without Server Backup File to recover the secondary site CMP. Recovery of the secondary site CMP can be left for late in the process because the now active CMP can handle all application level configuration as the network is brought back online.

4.1.3 Recovery Scenario 3: Full Cluster Outage of the CMP; Georedundancy Not Available; Other VM instances as Required

For a full outage with a CMP VM instance unavailable, creation of new CMP VM instances is required, then the recovery from system backup of the application configuration for the policy network. The first CMP VM instance is built and restored with the configuration database from a system backup. Replication of the restored database to a second rebuilt CMP node forms a CMP cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The detailed steps are in the Restore Procedures section. The major activities are summarized as follows:



- Recover one Primary CMP VM instance (if necessary) by:
  - creating a new CMP VM instance
  - 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 to be restored from a system backup.
  - If a system backup is not available, use site survey and site installation documentation to restore application level configuration to the CMP. It is possible to use the data at the MPEs (that should still be good) to verify that the re-entered data on the CMPs matches the previous configuration that was in-use. Also, check with engineering team for possible approach to verify if the data at the operational MPEs matches the data that has been re-entered at the CMP after re-entering the Policies and other application level data to the CMP.
- Recover the second CMP VM instance by:

- creating a new CMP VM instance
- Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
- The configuration database is available at the now active CMP VM instance and does not require restoration on the second CMP node. Configuration is replicated when the two new CMP nodes form a cluster.

- Recover any failed MPE/MRA VM instances by:
  - Creating a new MPE/MRA VM instance for the failed VM instance
  - Initial Policy configuration is re-installed, either through the platcfg menu, or from the server backup file
  - The configuration database is available at the now active CMP VM instance and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/MRA VM instances.

Follow the procedure below for detailed steps.

- Use Procedure 7: Restoring CMP Cluster with System Backup Available below to recover the first of 2 nodes in the CMP cluster.
- Use Procedure 2: Restore Standby CMP Node below to recover the second node of the CMP cluster
- Use Procedure 4: Restore Single MPE/MRA Node without Server Backup File to recover MPE/MRA nodes when one of the peers of the cluster is still available.

  Or Procedure 4: Restore Single MPE/MRA Node without Server Backup File
- Use Procedure 5: Restoring Complete Cluster with the Server Backup Files

  Or Procedure 6: Restoring Complete Cluster without Server Backup File to recover complete MPE/MRA clusters that have gone down.

5. RESTORE PROCEDURES

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

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

Required resources:

- Host server identified for the new VM instance.
- OVA file or equivalent (depending on hypervisor or NFV manager).
- **serverbackup**.iso of the node to be replaced.

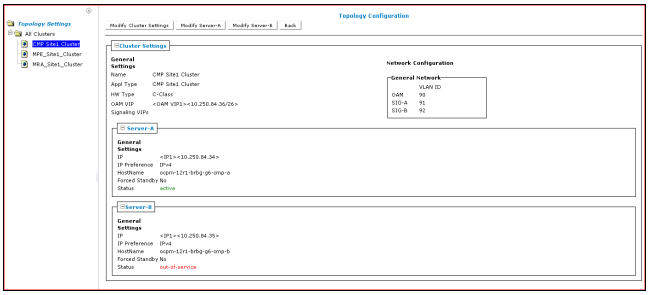
Prerequisites:

- Failed VM is not available (for example, it has been removed from the hypervisor/NFV manager).
- A new VM has been created in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1].

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

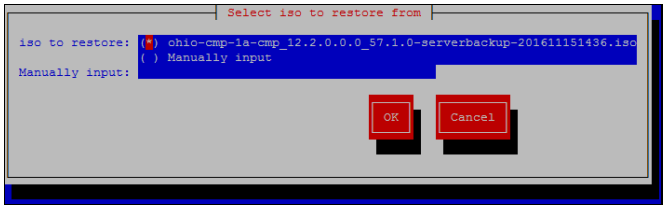
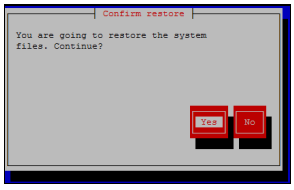
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

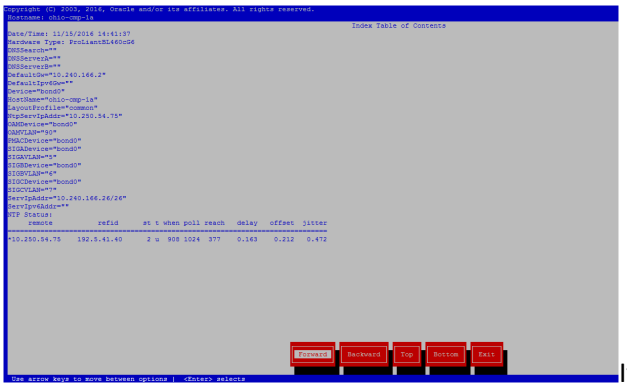
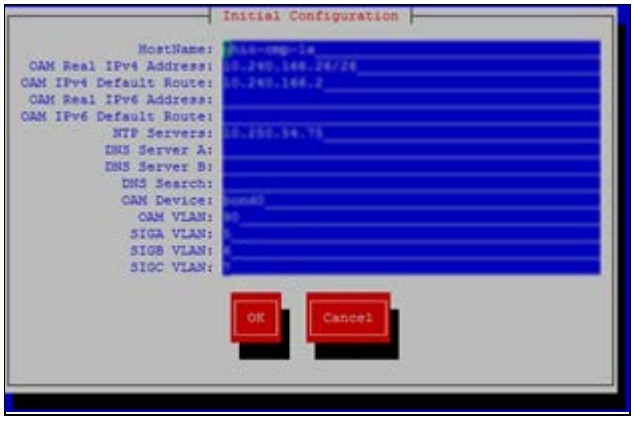
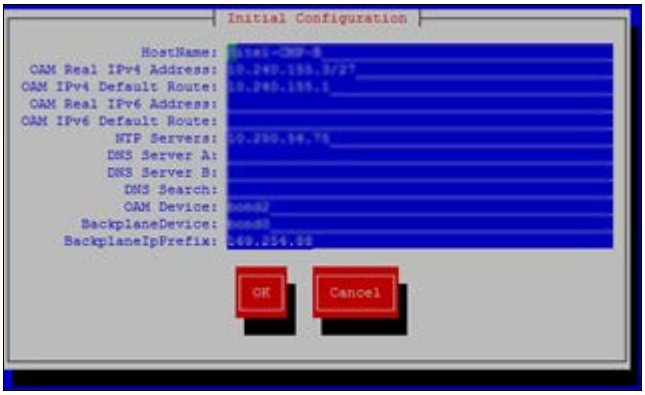
If this procedure fails, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

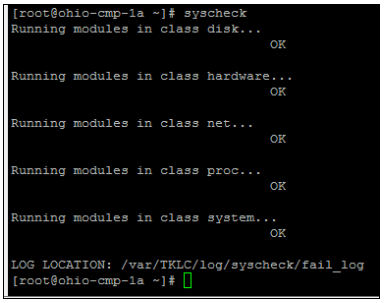
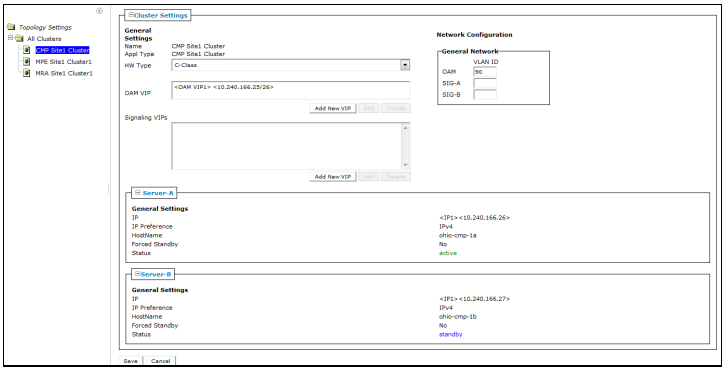
Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to: **Platform Setting → Topology Settings → All Clusters** 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click the Modify Server-X for the failed node 5. Click the Forced Standby checkbox so that it is checked, then click Save 
2. ☐	Create the VM instance	Create the new VM instance in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1]

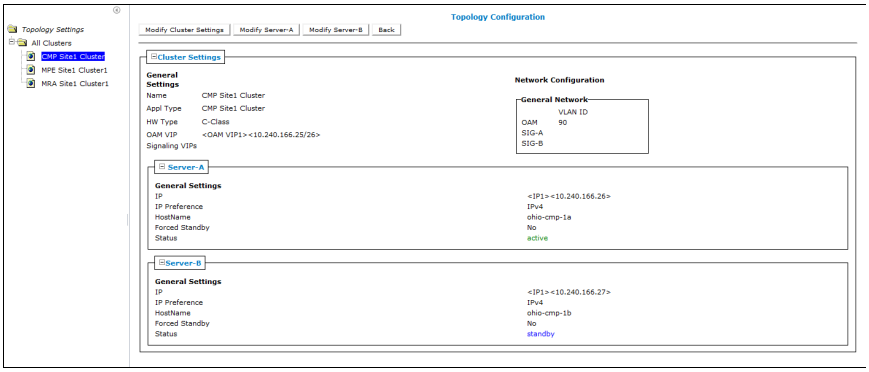
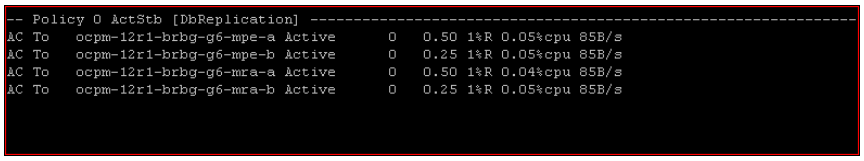
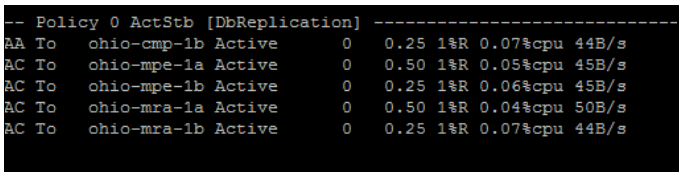
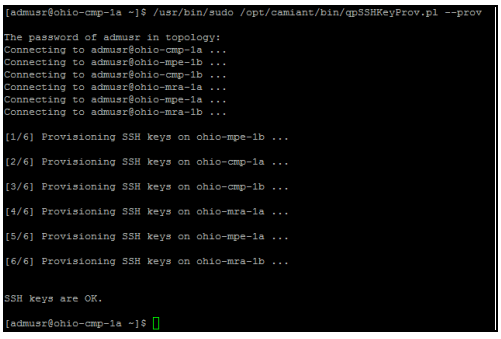
Step	Procedure	Details
3. ☐	Load the ISO for server restore	Obtain the **serverbackup*.iso* for the node to be restored. The server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE:** Later in this procedure, the platcfg restore function checks this directory and opens a menu of options. The platcfg utility also enables you to manually enter any mounted path on the server.

1. ☐	Login via SSH to new node	SSH to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

2. ☐	Perform platcfg restore from SSH session to replacement node	1. Run the following command: `# su - platcfg` 2. From the platcfg utility, navigate to **Policy Configuration → Backup and Restore → Server Restore** 3. Select the **serverbackup*.iso* that you just put on the system and click **OK**, then click **Yes** to confirm.  
3. ☐	Verify the status	A window opens indicating that the restore operation was successful and prompts you to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

Step	Procedure	Details
4. ☐	Perform Initial configuration	4. Click **Exit** until back to the Main Menu of the platcfg utility. 5. While in the platcfg utility, navigate to **Policy Configuration → Verify Initial Configuration**.  If the configuration does not exist, navigate to Perform Initial Configuration and enter the hostname, OAM IP and configuration information as shown below:  6. Verify that the data is correct. 7. Click **OK**, and then click **Yes** to save and apply. 8. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell.  **NOTE:** The above snapshot is for Cable mode, for Wireless mode the Backplane Device" and Backplane IP Prefix parameters do not exist.

Step	Procedure	Details
5. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot.
6. ☐	Verify basic network connectivity and server health.	From the installed VM, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **`syscheck`** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
7. ☐	Remove Forced Standby designation on current node.	1. In the CMP GUI, navigate to **Platform Setting → Topology Settings → All Clusters → Current Cluster.** 2. Modify for the server that has Forced Standby. 3. Clear the Forced Standby checkbox. 4. Click **Save**.  5. Click **OK** to restart the server. 

Step	Procedure	Details
8. ☐	Verify cluster status	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters→ Current CMP Cluster**. 2. Monitor clustering of the new node to its peer, do not proceed until both nodes have a status of either Active or Standby, and that there are no CMP related Active Alarms as shown below. 
9. ☐	Alternative method to check replication status	You can monitor the clustering of the new node from the shell on the primary node using the **`irepstat`** command. To do so, SSH to the Active node of the current cluster and run the **`irepstat`** command: `# irepstat` Expected **`irepstat`** command output while waiting reconnection:  Expected **`irepstat`** command output after cluster has formed: 
10. ☐	Exchange keys with cluster mate (This step must be run from the 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 Server Backup File

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

Required resources:

- Host server identified for the new VM instance
- OVA file or equivalent (depending on hypervisor or NFV manager)
- Node IP addresses, VLANs, NTP IP address, and hostname from CMP GUI

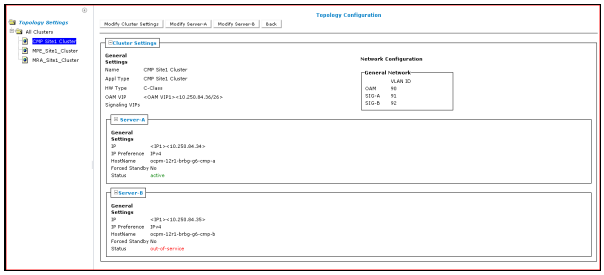
Prerequisites:

- Failed VM is not available (for example, it has been removed from the hypervisor/NFV manager).
- A new VM has been created in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1].

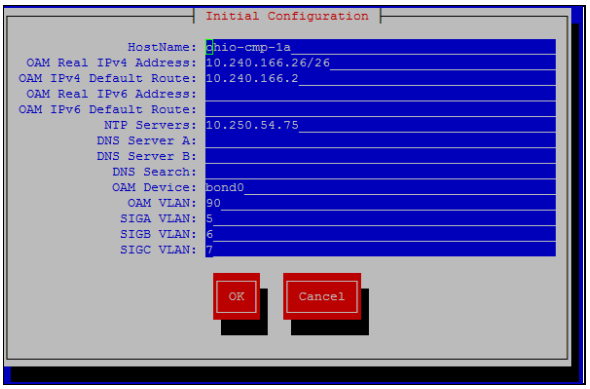
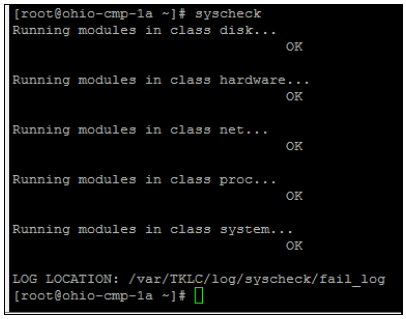
This Procedure restores the standby CMP node when a server level backup file is not available.

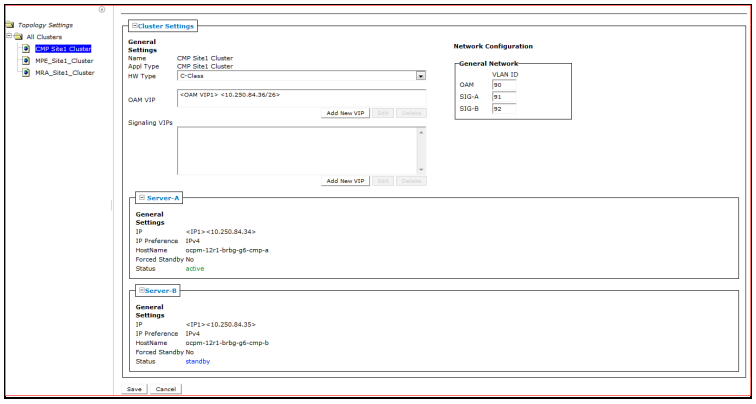
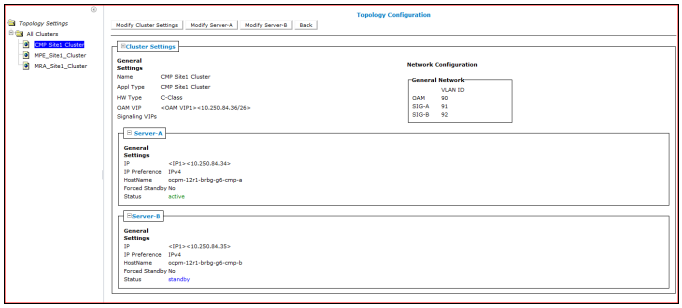
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

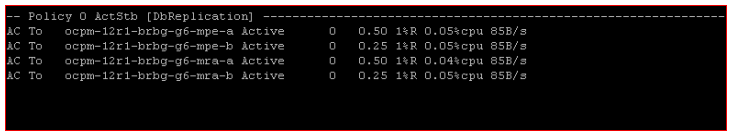
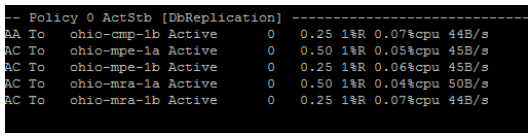
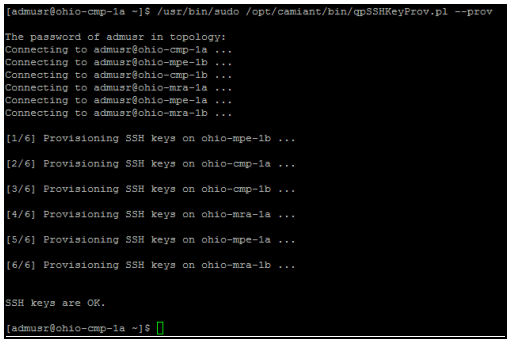
If this procedure fails, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters**. 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click the Modify Server-X for the failed node 5. Click the Forced Standby checkbox so that it is checked, then click Save  **NOTE:** From the above screenshot, the Network Configuration/General Network(VLAN ID) does not appear for RMS (DL 360/ DL380) Hardware
2. ☐	Create the VM instance	Create the new VM instance according to *Oracle Communications Policy Management Cloud Installation Guide* [1]

3. ☐	Login via SSH to new node	SSH session to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

Step	Procedure	Details
4. ☐	Perform platcfg restore from SSH session to replacement node Perform Initial configuration	1. Run the following command `# su - platcfg` 2. From within the platcfg utility, navigate to **Policy Configuration → Perform Initial Configuration**. 3. Enter the appropriate configuration details for this node, verify that entries are correct, and click **OK** to continue. Accept the resulting dialog that displays asking to apply the configuration. After the operation is complete, click **Exit** on the platcfg menu until you arereturned to the shell.  4. Ensure that configured data is correct, and click **OK**, then click **Yes** to save and apply. 5. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell.
5. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot;
6. ☐	Verify basic network connectivity and server health.	From the installed VM, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **syscheck** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 

Step	Procedure	Details
7. ☐	Remove Forced Standby designation on current node.	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → Current Cluster.** 2. Click **Modify** for the server that has Forced standby. 3. Clear the Forced Standby checkbox. 4. Click **Save**.  5. Click **OK** to restart the server. 
8. ☐	Verify cluster status	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All → Current CMP Cluster**. 2. Monitor clustering of the new node to its peer, do not proceed until both nodes have a status of either active or standby, and that there are no CMP related Active Alarms as shown below. 

Step	Procedure	Details
9. ☐	Alternative method to check replication status	You can monitor the clustering of the new node from the shell on the primary node using the **irepstat** command. To do so, SSH to the Active node of the current cluster and run the **irepstat** command: `# irepstat` Expected **irepstat** command output while waiting reconnection:  Expected **irepstat** command output after cluster has formed: 
10. ☐	Exchange keys with cluster mate (This step must be run from the 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 with Server Backup file

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

Required resources:

- Host server identified for the new VM instance
- OVA file or equivalent (depending on hypervisor or NFV manager)
- **serverbackup*.iso of the node to be replaced

Prerequisites:

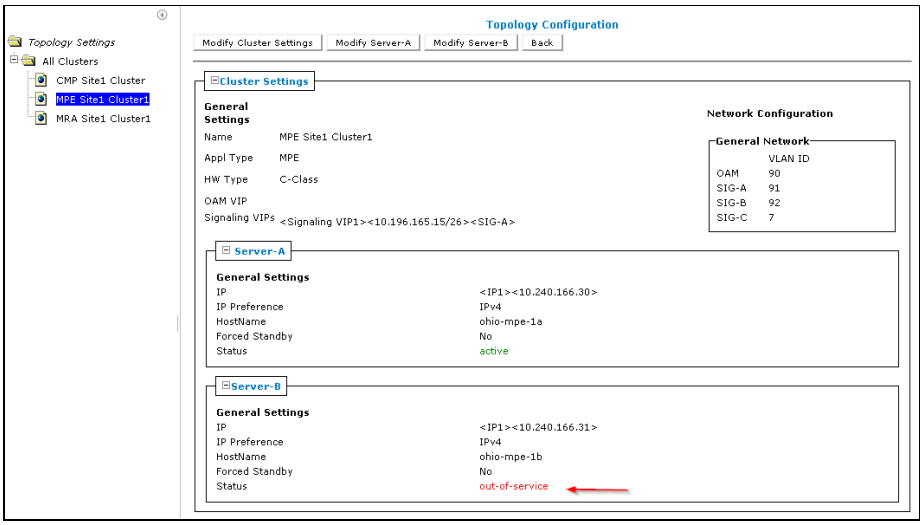
- Failed VM is not available (for example, it has been removed from the hypervisor/NFV manager).
- A new VM has been created in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1].

Disaster Recovery

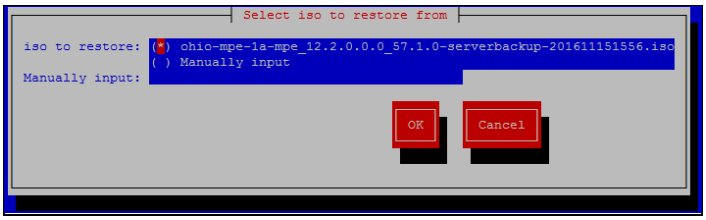
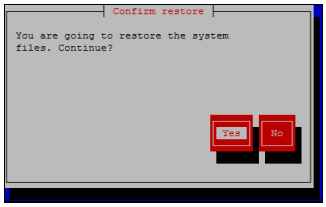
This procedure performs Restore single MPE/MRA node with server backup file.

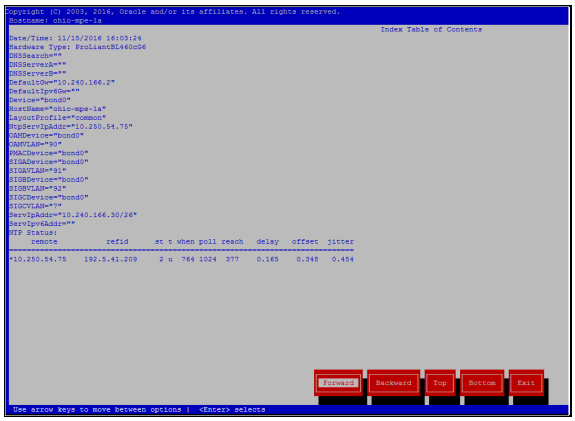
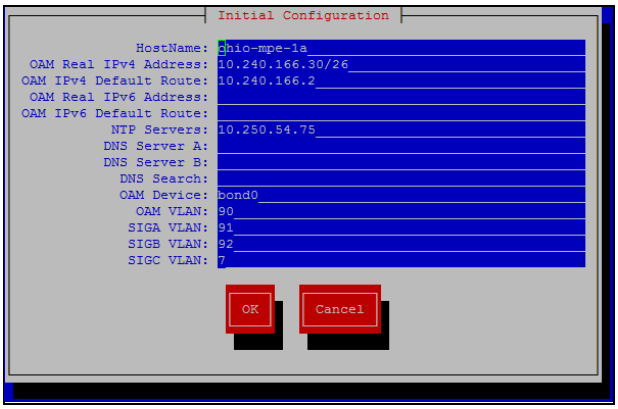
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

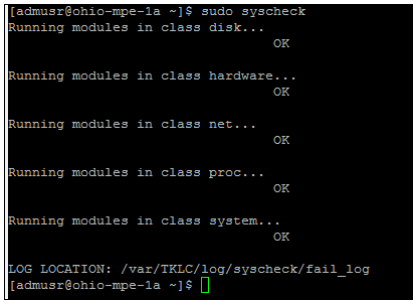
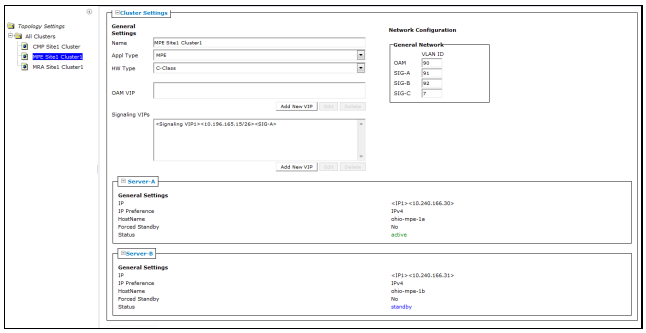
If this procedure fails, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

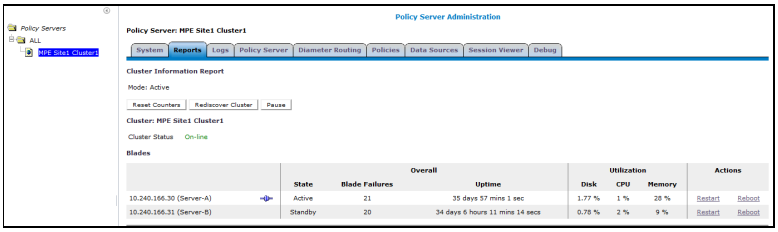
Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters**. 2. Determine the cluster with the failed node 3. Determine the failed node 4. Click the Modify Server-X for the failed node 5. Click the Forced Standby checkbox so that it is checked, then click Save 
2. ☐	Create the VM instance	Create the VM instance according to *Oracle Communications Policy Management Cloud Installation Guide* [1]
3. ☐	Load the ISO for server backup	Obtain the **serverbackup*.iso for the node to be restored. The server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE:** Later in this procedure, the platcfg restore function checks this directory and opens a menu of options. The platcfg utility also enables you to manually enter any mounted path on the server.

4. ☐	Login via SSH to new node	SSH to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

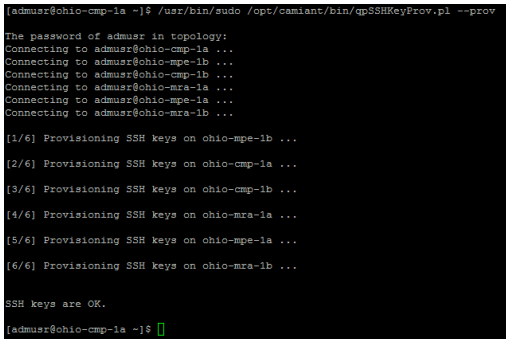
Step	Procedure	Details
5. ☐	Perform platcfg restore from SSH session to replacement hardware	1. Run the following command: `# su - platcfg` 2. From within the platcfg utility, navigate to **Policy Configuration → Backup and Restore → Server Restore.** 3. Select the **serverbackup**.iso that you just put on the system and click **OK** and then click **Yes** to confirm.  
6. ☐	Verify the status	A window opens, indicating restore operation was successful and instructs you to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

Step	Procedure	Details
7. ☐	Perform Initial configuration	1. Click **Exit** repeatedly until you are back to the Main Menu of the platcfg utility. 2. Navigate to **Policy Configuration → Verify Initial Configuration**.  3. If the configuration does not exist, then navigate to Perform Initial Configuration and enter the initial configuration: hostname, OAM IP and NTP servers configurations as shown below:  4. Verify the configured data is correct, and click **OK**, then click **Yes** to save and apply. 5. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell. **NOTE:** The above snapshot is for Cable mode, for Wireless mode the Backplane Device and Backplane IP Prefix parameters do not exist.
8. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot.

Step	Procedure	Details
9. ☐	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. 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. 
10. ☐	Remove Forced Standby designation on current node.	1. In the CMP GUI, navigate to **Platform Setting → Topology Settings → All Clusters → Current Cluster**. 2. Click **Modify** for the server that has Forced Standby. 3. Clear the Forced Standby checkbox. 4. Click **Save.**  5. Click **OK** to restart the server. 

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

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

13. ☐	Exchange keys with cluster mate(This step must be 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---		

5.4 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 new node by manual entry.

Required resources:

- Host server identified for the new VM instance
- OVA file or equivalent (depending on hypervisor or NFV manager)
- Initial configuration information about the node to be restored:
  - OAM IP address, default gateway, NTP & SNMP server IP addresses
  - VLAN configuration information.

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

Platform Setting → Topology Setting → <*Cluster_Name***>**

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

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

Prerequisites:

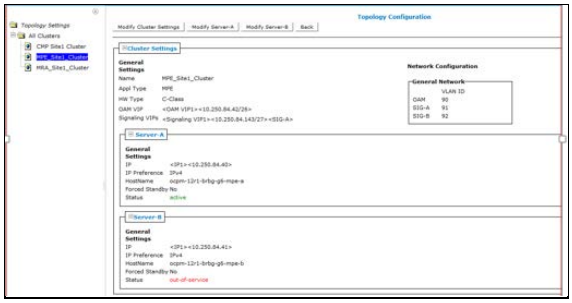
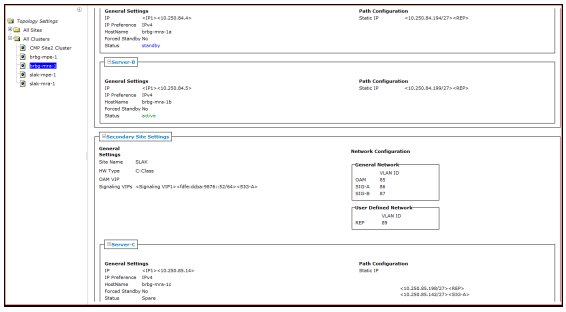
- Failed VM is not available (for example, it has been removed from the hypervisor/NFV manager).
- A new VM has been created in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1]

Disaster Recovery

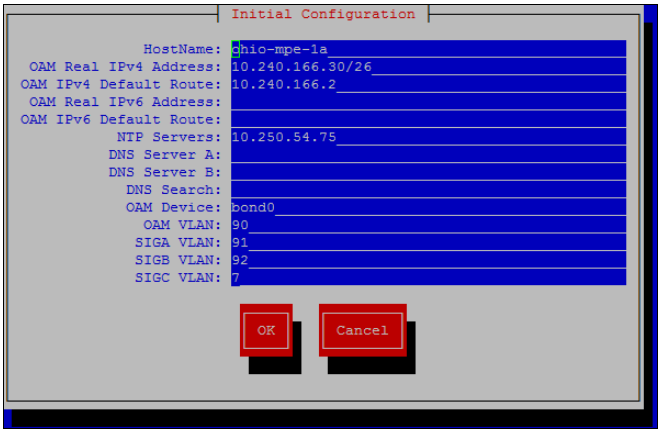
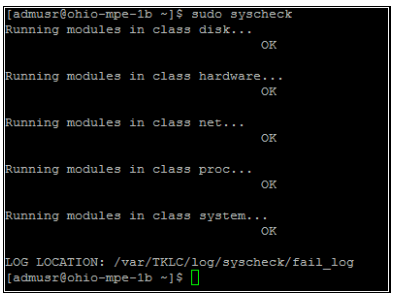
This Procedure performs Restore single MPE/MRA node without server backup file

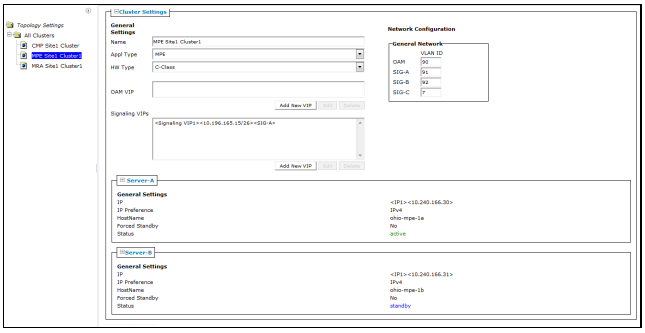
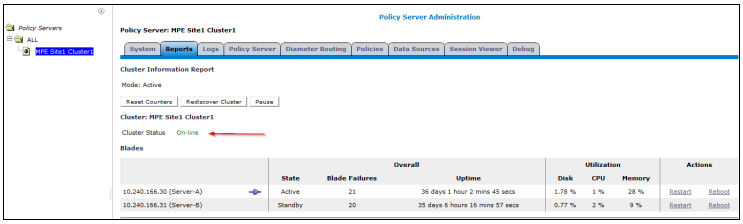
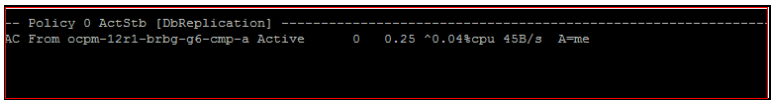
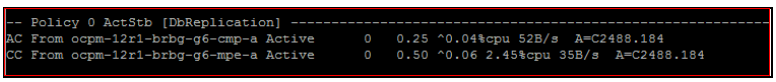
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

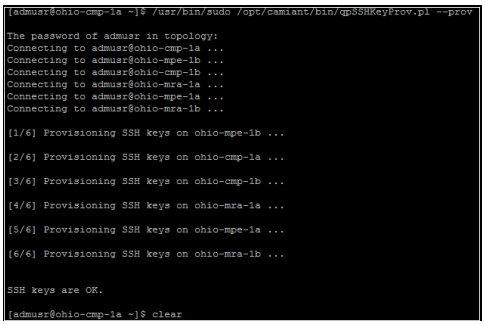
If this procedure fails, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

Step	Procedure	Details
1. ☐	Set the failed node to Forced Standby	1. In the CMP GUI, navigate to **Platform Setting → Topology Setting → All Clusters.** 2. Determine the cluster with the failed node 3. Determine the failed node **Note:** It is possible for a Georedudant Topology that server C is a 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  Server-C (spare): In a Georedundant Topology 
2. ☐	Create the VM instance	Create the VM instance according to *Oracle Communications Policy Management Cloud Installation Guide* [1]

3. ☐	Login via SSH to new node	SSH session to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

4. ☐	Perform Initial Policy Configuration from within platcfg utility on installed node	1. Execute the following command `# su - platcfg` 2. From the platcfg utility, navigate to **Policy Configuration → Perform Initial Configuration**. 3. Enter the configuration details from the node being replaced:  4. After the server details are entered and verified for correctness click **OK**. A dialog opens asking if the settings should be applied, click **Yes** and allow the operation to complete. No specific message is 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 again, if all appears as expected, contact My Oracle Support before proceeding. 5. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell. **NOTE:** The above snapshot is for Cable mode, for Wireless mode the "Backplane Device and Backplane IP Prefix parameters do not exist.
5. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot;
6. ☐	Verify basic network connectivity and server health.	From the installed server, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **`syscheck`** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 

7. ☐	Remove Forced Standby designation on current blade.	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. Click **OK** to restart the server. 
8. ☐	Check status	In the CMP GUI, depending on the type of the blade, perform the following: • If this is an MPE node, navigate to: **Policy Server → Configuration → All→**<*Recovered MPE Cluster*>**→ Reports** • If this is an MRA node, navigate to: **MRA → Configuration → All →**<*Recovered MRA Cluster*>**→ Reports** Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from Degraded to On-line. 
9. ☐	Alternative method to check replication status	You can monitor the clustering of the new node from the shell on the primary node using the **`irepstat`** command. To do so, SSH to the Active node of the current cluster and run the **`irepstat`** command: `# irepstat` Expected **`irepstat`** command output while waiting reconnection:  Expected **`irepstat`** command output after cluster has formed: 

10. ☐	Exchange keys with cluster mate (This step must be run from the 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---		

5.5 Procedure 5: Restoring Complete Cluster with the Server Backup Files

The purpose of this procedure is to create policy cluster VM instances, then restore application level configuration by pushing that configuration from the active CMP. In this example, initial Policy configuration is restored to the new blades through the use of server backup files for each server to be restored.

Required resources:

- Host server(s) identified for the new VM instances
- OVA file or equivalent (depending on hypervisor or NFV manager)
- **serverbackup*.iso of the blade to be replaced

Prerequisites:

- Failed VM is not available (for example, it has been removed from the hypervisor/NFV manager).
- New VM instances have been created in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1].
    - **NOTE:** In case it is a CMP Cluster that is being rebuilt, restore application data either from system backup or manually if no backup available.

This Procedure performs Restoring complete cluster with the server backup files

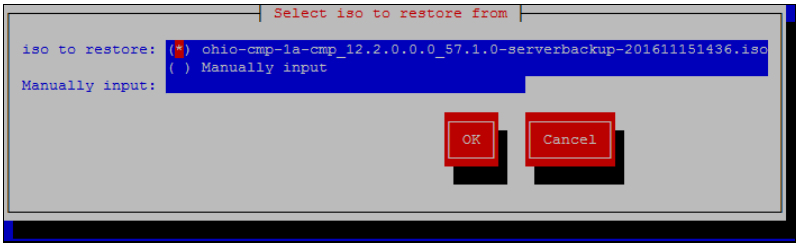
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

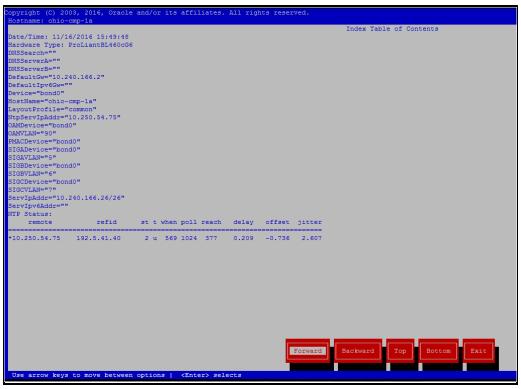
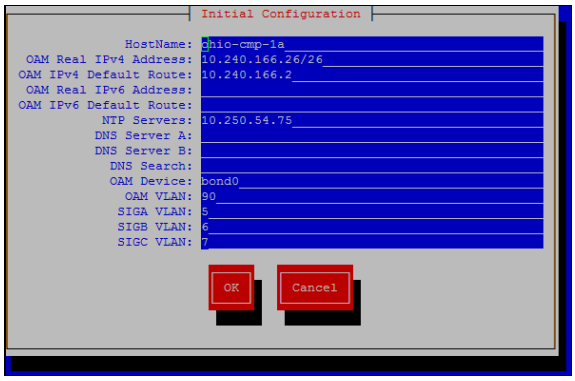
If this procedure fails, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

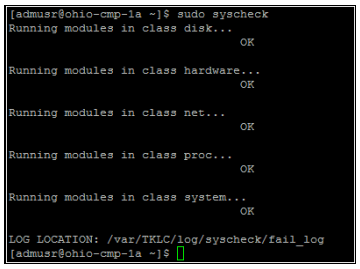
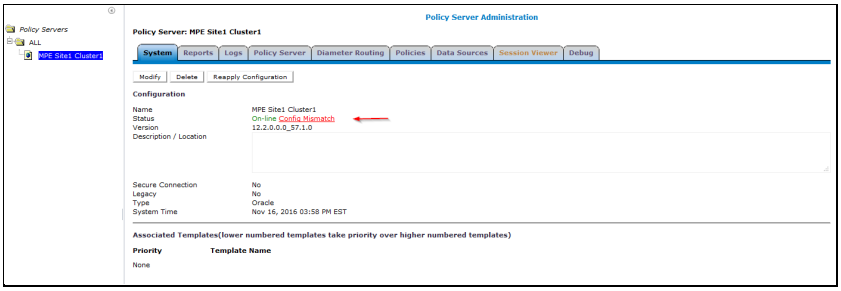
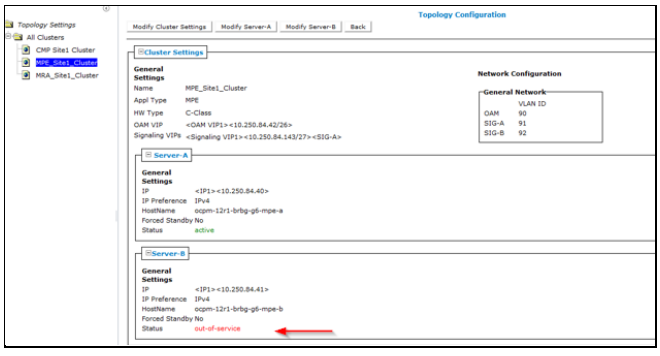
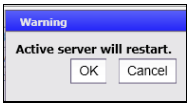
Step	Procedure	Details
1. ☐	Create the VM instance	Create the VM instance according to *Oracle Communications Policy Management Cloud Installation Guide* [1]

Step	Procedure	Details
2. ☐	Load the ISO to restore first server of the cluster	Obtain the **serverbackup**.iso for the blade to be restored. The server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE:** Later in this procedure, the platcfg restore function checks this directory and opens a menu of options. The platcfg utility also enables you to manually enter any mounted path on the server.

3. ☐	SSH to replacement VM instance	SSH to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

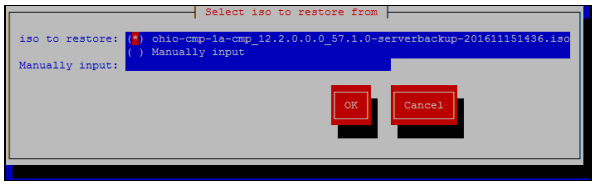
4. ☐	Perform platcfg restore from SSH session to replacement VM instance	1. Run the following command `# su - platcfg` 2. From the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** 3. Select the **serverbackup**.iso that you just put on the system and click **OK** and then click **Yes** to confirm. 
5. ☐	Verify the status	A window opens indicating that the restore operation was successful and instructs you to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

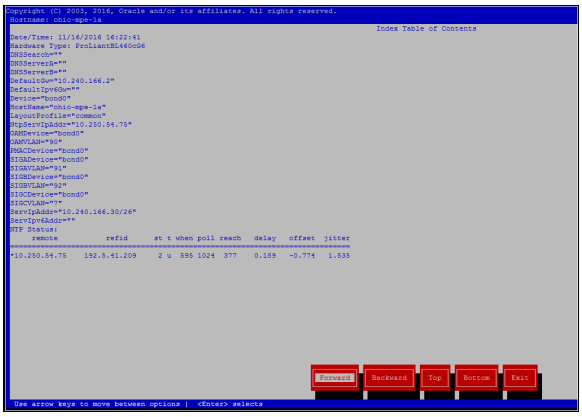
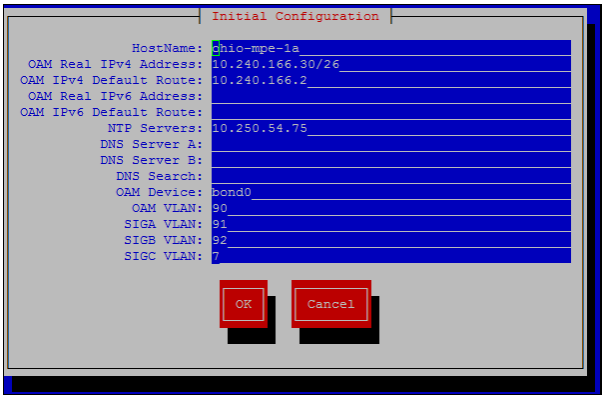
Step	Procedure	Details
6. ☐	Verify Initial configuration	1. Click **Exit** repeatedly until back to the Main Menu of the platcfg utility. 2. While in the platcfg utility, navigate to **Policy Configuration → Verify Initial Configuration**.  3. If the configuration does not exists, then navigate to Perform Initial Configuration and enter initial configuration for hostname, OAM IP and NTP servers configurations as shown below:  4. Verify that your data is correct. 5. Click **OK**, then click **Yes** to save and apply. 6. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell. **NOTE:** The above snapshot is for Cable mode, for Wireless mode the“Backplane Device and Backplane IP Prefix parameters do not exist.
7. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot.

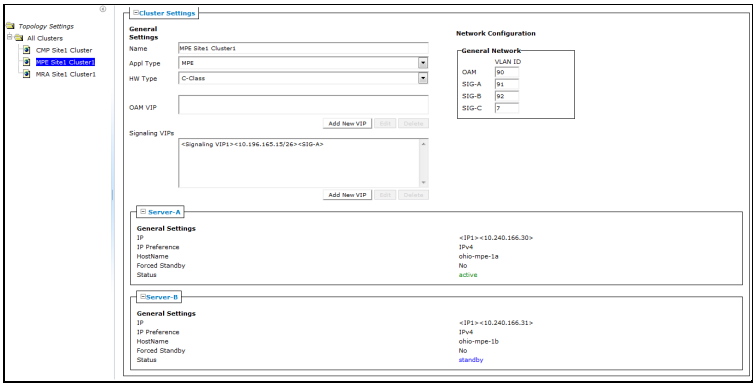
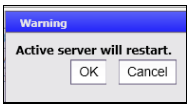
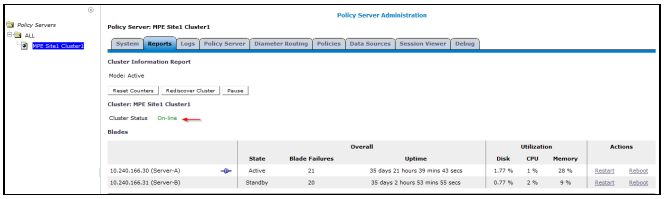
Step	Procedure	Details
8. ☐	Verify basic network connectivity and server health.	From the installed VM instance, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **syscheck** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
9. ☐	Check status	1. In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters 2. Check the System tab for the cluster. 3. 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. 
10. ☐	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 for the server that has an out-of-service status. 3. Check the Forced Standby checkbox 4. Click Save  5. Click **OK** to restart the server. 

Step	Procedure	Details
11. ☐	Create the VM instance	Create the VM instance according to *Oracle Communications Policy Management Cloud Installation Guide* [1]
12. ☐	Load the ISO to restore second server of the cluster	Obtain the **serverbackup*.iso for the blade to be restored. The server backup file should be copied via secure copy(pscp,scp, or WinSCP) to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE:** Later in this procedure, the platcfg restore function checks this directory and opens a menu of options. The platcfg utility also enables you to manually enter any mounted path on the server.

13. ☐	SSH to replacement VM instance	SSH to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

14. ☐	Perform platcfg restore from SSH session to replacement VM instance	1. Run the following command `# su - platcfg` 2. From the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore**. 3. Select the **serverbackup*.iso that you just put on the system and click **OK** and then click **Yes** to confirm. 
15. ☐	Verify the status	A window opens indicating that the restore operation was successful and informs you to press any key to exit. If it is not successful, retry the restore. If the second restore is not successful, stop and contact My Oracle Support or engineering team for assistance.

Step	Procedure	Details
16. ☐	Verify Initial configuration	1. Click **Exit** until you are back to the Main Menu of the platcfg utility. 2. Navigate to **Policy Configuration → Verify Initial Configuration**.  3. If the configuration does not exists, then navigate to Perform Initial Configuration and enter the initial configuration: hostname, OAM IP and NTP servers configurations as shown below:  4. Verify that your data is correct. 5. Click **OK** and then click **Yes** to save and apply. 6. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell. **NOTE:** The above snapshot is for Cable mode, for Wireless mode the Backplane Device and Backplane IP Prefix parameters do not exist.
17. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot;

Step	Procedure	Details
18. ☐	Remove Forced Standby designation on current blade.	1. In the CMP GUI, navigate to **Platform Setting → Topology Settings → Current Cluster.** 2. Modify for the server that has Forced Standby. 3. Clear the Forced Standby checkbox. 4. Click Save.  5. Click **OK** to restart the server: 
19. ☐	Check the status	In the CMP GUI, depending on the type of the blade, perform the following: • If this is an MPE node, navigate to: **Policy Server → Configuration → All→<*Recovered MPE Cluster*>→ Reports** • If this is an MRA node, navigate to: **MRA → Configuration → All →<*Recovered MRA Cluster*>→ Reports** Check CMP cluster status (as indicated in the previous step), navigate to **Platform Setting → Topology Setting → Current CMP Cluster**. Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from Degraded to On-line. 

Step	Procedure	Details

20. ☐	Alternative method to check replication status	You can monitor the clustering of the new node from the shell on the primary node using the **irepstat** command. To do so, SSH to the Active node of the current cluster and run the **irepstat** command:
		`# irepstat`
		Expected **irepstat** command output while waiting reconnection:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1%R 0.05%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.25 1%R 0.05%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.50 1%R 0.04%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.25 1%R 0.05%cpu 85B/s`
		Expected **irepstat** command output after cluster has formed:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To ohio-cmp-1b Active 0 0.25 1%R 0.07%cpu 79B/s`
		`AC To ohio-mpe-1a Active 0 0.50 1%R 0.05%cpu 65B/s`
		`AC To ohio-mpe-1b Active 0 0.25 1%R 0.07%cpu 78B/s`
		`AC To ohio-mra-1a Active 0 0.50 1%R 0.05%cpu 65B/s`
		`AC To ohio-mra-1b Active 0 0.25 1%R 0.07%cpu 79B/s`

21. ☐	Exchange keys with cluster mate (This step must be run from the 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**
		`[admusr@ohio-cmp-1a ~]$ /usr/bin/sudo /opt/camiant/bin/qpSSHKeyProv.pl --prov`
		`The password of admusr in topology:`
		`Connecting to admusr@ohio-cmp-1a ...`
		`Connecting to admusr@ohio-mpe-1b ...`
		`Connecting to admusr@ohio-cmp-1b ...`
		`Connecting to admusr@ohio-mra-1a ...`
		`Connecting to admusr@ohio-mpe-1a ...`
		`Connecting to admusr@ohio-mra-1b ...`
		`[1/6] Provisioning SSH keys on ohio-mpe-1b ...`
		`[2/6] Provisioning SSH keys on ohio-cmp-1a ...`
		`[3/6] Provisioning SSH keys on ohio-cmp-1b ...`
		`[4/6] Provisioning SSH keys on ohio-mra-1a ...`
		`[5/6] Provisioning SSH keys on ohio-mpe-1a ...`
		`[6/6] Provisioning SSH keys on ohio-mra-1b ...`
		`SSH keys are OK.`
		`[admusr@ohio-cmp-1a ~]$`

---End of Procedure---		

5.6 Procedure 6: Restoring Complete Cluster without Server Backup File

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

Required resources:

- Host server(s) identified for the new VM instances
- OVA file or equivalent (depending on hypervisor or NFV manager)
- Initial configuration information about the blade to be restored:
  - OAM blade Ip address, default gateway, ntp server ip address
  - Vlan configuration information.

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

Platform Setting → Topology Setting → <*Cluster_Name*>

Disaster Recovery

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

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

Prerequisites:

- Failed VM is not available (for example, it has been removed from the hypervisor/NFV manager).
- New VM instances have been created in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1]
- Install application software – CMP, MPE, MRA

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

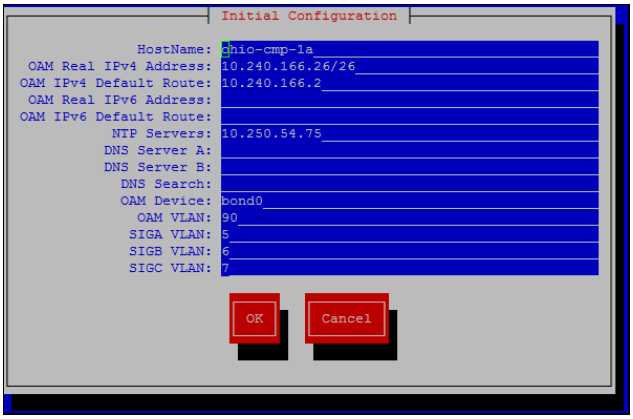
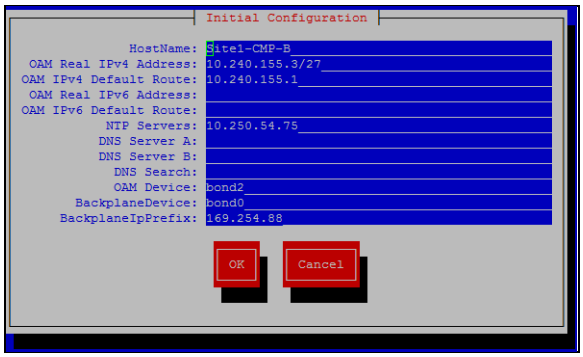
This Procedure performs Restoring complete cluster without the server backup

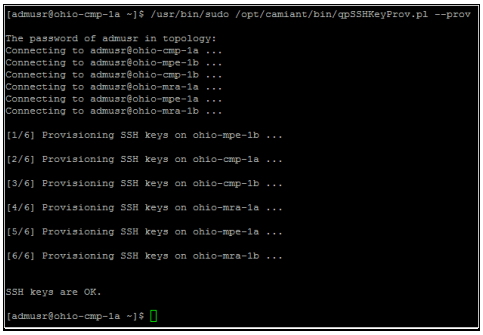
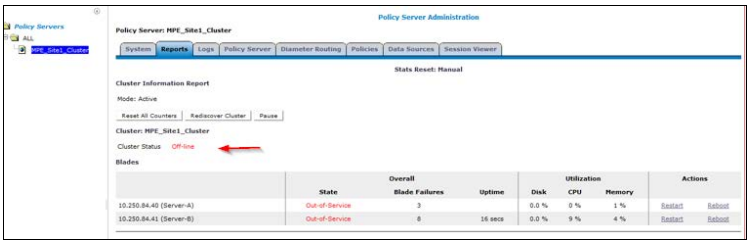
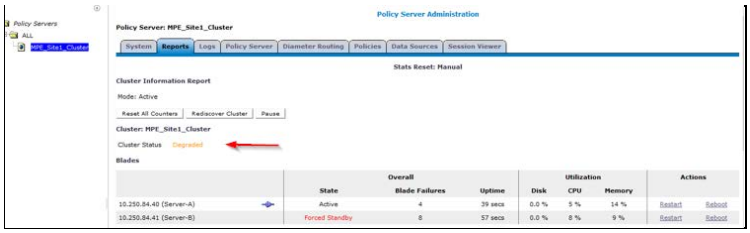
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

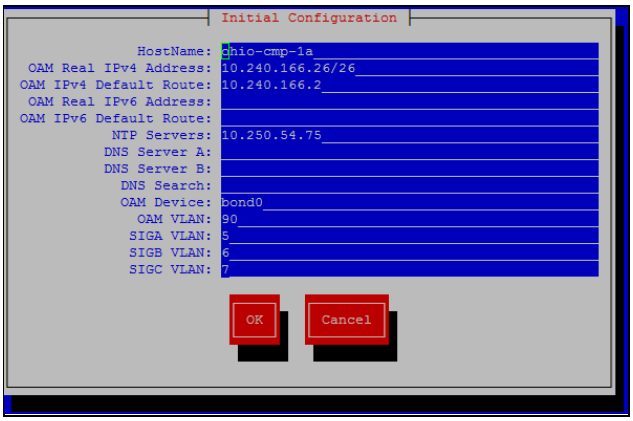
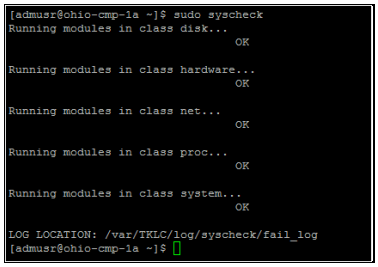
Step	Procedure	Details
1. ☐	Create the VM	Create the VM instance according to *Oracle Communications Policy Management Cloud Installation Guide* [1]

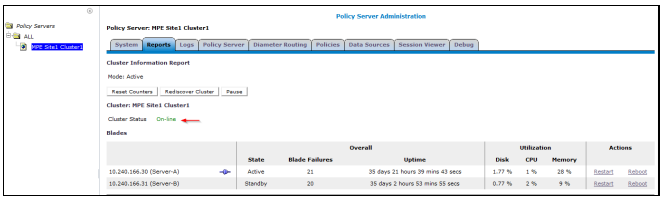
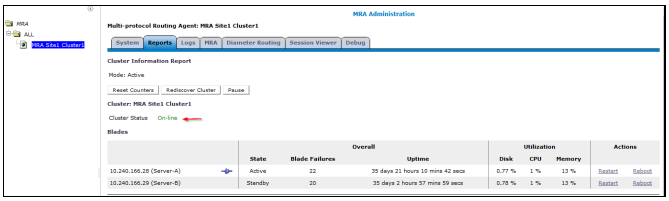
2. ☐	Login via SSH to replacement VM instance	SSH to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

Step	Procedure	Details
3. ☐	Perform Initial Policy Configuration from within platcfg utility on installed VM instance.	1. Run the following command `# su - platcfg` 2. From within the platcfg utility, navigate to: Policy Configuration → Perform Initial Configuration 3. Enter the relevant configuration details from the blade being replaced:  4. After the server details are entered and verified for correctness click **OK**. A menu opens asking if the new settings should be applied, click **Yes** and allow the operation to complete. No specific message is 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 again, if all appears as expected, contact My Oracle Support before proceeding. 5. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell.  **NOTE:** The above snapshot is for Cable mode, for Wireless mode the Backplane Device and Backplane IP Prefix parameters does not exist.
4. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot.

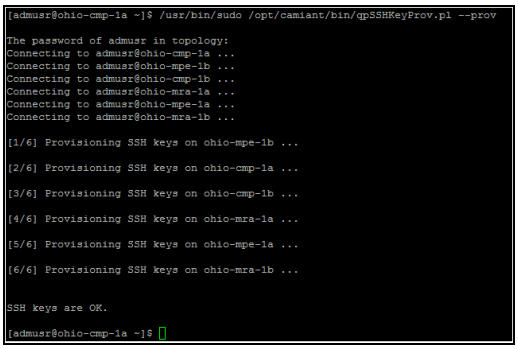
Step	Procedure	Details
5. ☐	Verify basic network connectivity and server health.	From the installed VM, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **syscheck** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
6. ☐	Check status	In the CMP GUI, depending on the type of the blade, perform the following: • If this is an MPE node, navigate to: **Policy Server → Configuration → All→<*Recovered MPE Cluster*>→ Reports** • If this is an MRA node, navigate to: **MRA → Configuration → All →<*Recovered MRA Cluster*>→ Reports** Monitor clustering of the new blade to its peer, do not proceed until the Cluster Status returns from Off-line to Degraded. **Off-line**  **Degraded** 
7. ☐	Create the VM	Create the VM according to *Oracle Communications Policy Management Cloud Installation Guide* [1]

8. ☐	Login via SSH to second node of the current cluster	SSH to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

Step	Procedure	Details
9. ☐	Perform Initial Policy Configuration from within platcfg utility on second node of cluster	1. Run the following command `# su - platcfg` 2. From the platcfg utility, navigate to **Policy Configuration → Initial Configuration**. 3. Enter the relevant details from the blade being replaced:  4. Aftr the server details are entered and verified for correctness, click **OK**. 5. A menu opens asking if the new settings should be applied, click **YES** and allow the operation to complete. No specific message is 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 again, if all appears as expected, contact My Oracle Support before proceeding. 6. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell. **NOTE:** The above snapshot is for Cable mode, for Wireless mode the Backplane Device and Backplane IP Prefix parameters do not exist.
10. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot.
11. ☐	Verify basic network connectivity and server health.	From the installed VM, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **`syscheck`** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 

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

13. ☐	Alternative method to check replication status	You can monitor the clustering of the new node from the shell on the primary node using the **`irepstat`** command. To do so, SSH to the Active node of the current cluster and run the **`irepstat`** command:
		`# irepstat`
		Expected **`irepstat`** command output while waiting reconnection:
		`-- Policy 0 ActStb [DbReplication] --------------------------------------------------------`
		`AC To ocpm-12r1-brbg-g6-mpe-a Active 0 0.50 1%R 0.05%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mpe-b Active 0 0.25 1%R 0.05%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mra-a Active 0 0.50 1%R 0.04%cpu 85B/s`
		`AC To ocpm-12r1-brbg-g6-mra-b Active 0 0.25 1%R 0.05%cpu 85B/s`
		Expected **`irepstat`** command output after cluster has formed:
		`-- Policy 0 ActStb [DbReplication] ----------------------------------`
		`AA To ohio-cmp-1b Active 0 0.25 1%R 0.07%cpu 79B/s`
		`AC To ohio-mpe-1a Active 0 0.50 1%R 0.05%cpu 65B/s`
		`AC To ohio-mpe-1b Active 0 0.25 1%R 0.07%cpu 78B/s`
		`AC To ohio-mra-1a Active 0 0.50 1%R 0.05%cpu 65B/s`
		`AC To ohio-mra-1b Active 0 0.25 1%R 0.07%cpu 79B/s`

Step	Procedure	Details
14. ☐	Exchange keys with cluster mate (This step must be run from the 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---		

5.7 Procedure 7: Restoring CMP Cluster with System Backup Available

The purpose of this procedure is to re-create a CMP with the application level configuration of the policy network that can be used to re-create the policy network that is to be recovered. After a CMP is online, all other VM instances of the policy network can be re-created using the above procedures and then their application level configuration restored from this CMP. In the case of a massive outage that includes the CMP, at least one of the CMP VM instances should be restored first.

Required resources:

- Host server(s) identified for the new VM instances
- OVA file or equivalent (depending on hypervisor or NFV manager)
- Recent System backup file.
- Initial configuration information about the blade to be restored:
  - OAM IP address, default gateway, NTP & SNMP server IP addresses
  - VLAN configuration information.

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

Platform Setting → Topology Setting → <*Cluster_Name***>**

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

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

Prerequisites:

- Failed VM is not available (for example, it has been removed from the hypervisor/NFV manager).
- New VM instances have been created in accordance with *Oracle Communications Policy Management Cloud Installation Guide* [1].

Disaster Recovery

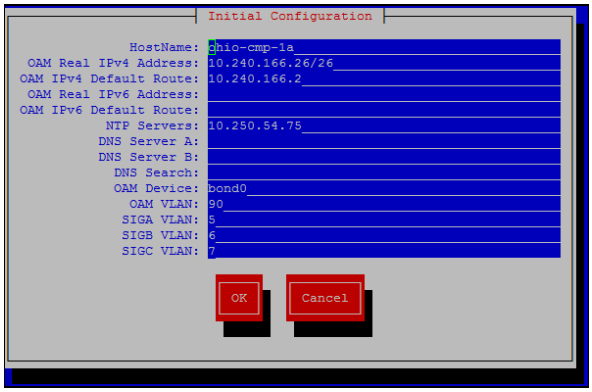
This Procedure performs Restoring CMP cluster with system backup available

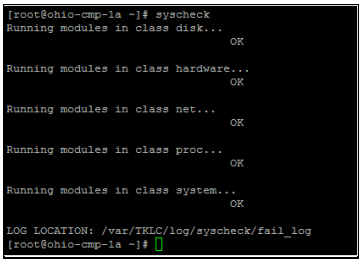
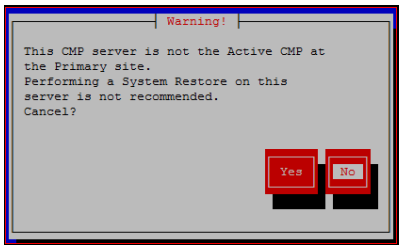
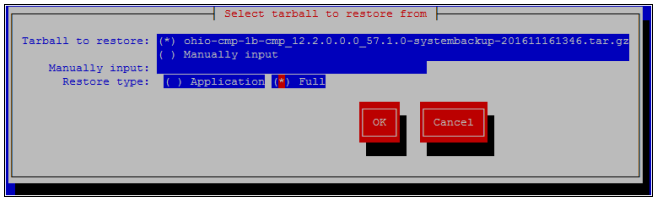
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

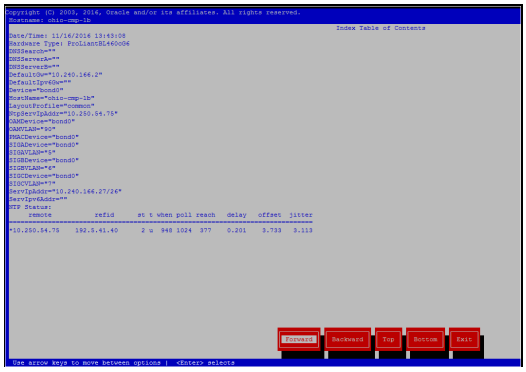
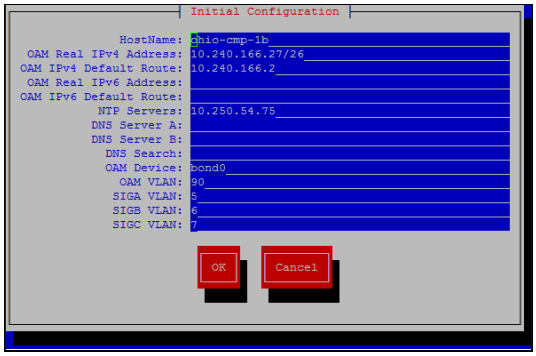
If this procedure fails, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

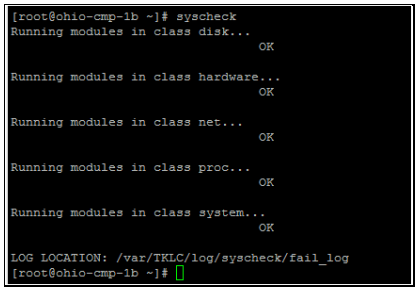
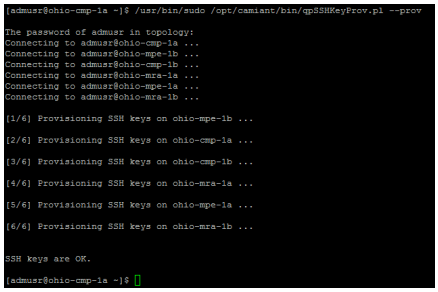
Step	Procedure	Details
1. ☐	Create the VM	Create the VM according to *Oracle Communications Policy Management Cloud Installation Guide* [1]

2. ☐	Login via SSH to new VM instance	SSH to the new VM instance:
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

3. ☐	Perform Initial Policy Configuration from within platcfg utility on the installed VM instance	1. Run the following command `# su - platcfg` 2. From the platcfg utility, navigate to: **Policy Configuration → Perform Initial Configuration.** 3. Enter the relevant details from the blade being replaced:  4. Aftr the server details are entered and verified for correctness click **OK**. A menu displays asking if the new settings should be applied, click **Yes** and allow the operation to complete. No specific message is 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 again. If all appears as expected, contact My Oracle Support before proceeding. 5. Exit platcfg by selecting Exit from each platcfg menu until you are returned to the shell. **NOTE:** The above snapshot is for Cable mode, for Wireless mode the Backplane Device and Backplane IP Prefix parameters do not exist.
4. ☐	Reboot the server	Reboot: `# init 6` Allow the server time to reboot;

Step	Procedure	Details
5. ☐	Verify basic network connectivity and server health.	From the installed VM, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old blade configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
6. ☐	Load the system backup file for server restore	The system backup file contains the database information that makes up the application level configuration of the policy network. Without that backup, the application configuration must be restored either through the platcfg menu, or from the server backup file from site documentation. If the system backup file is available, put a copy of the file on the constructed CMP VM instance into the: via secure copy (pscp scp, or WinSCP). /var/camiant/backup/local_archive/systembackup/
7. ☐	Perform platcfg restore from SSH session to replacement VM instance	1. Run the following command `# su - platcfg` 2. From the platcfg utility, 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 behavior is expected, continue by clicking **No**.  4. A window opens asking to select the file to use for the restore. If the file was copied correctly in the previous step, it is shown here as an option, otherwise select **Manually Input**, and select **Full** and then click **OK** to proceed.  **NOTE: Full** also restores Comcol data, but **Application** excludes Comcol.

Step	Procedure	Details
8. ☐	Verify the status	A window opens indicating that the restore operation was successful and ask 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.
9. ☐	Verify Initial configuration	1. Click Exit repeatedly until back to the Main Menu of the platcfg utility. 2. While in the platcfg utility, navigate to **Policy Configuration → Verify Initial Configuration**.  3. Ensure that your data is correct, if configuration is not there, then navigate to **Perform Initial Configuration** and enter the information as shown below:  4. Click **OK** and then click **Yes** to save and apply 5. After the server details are entered and verified, click OK 6. A window opens asking if the new settings should be applied, click **Yes** and allow the operation to complete. No specific message is 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 again, if all appears as expected, contact My Oracle Support before proceeding. 7. Exit platcfg by clicking **Exit** from each platcfg menu until you are returned to the shell. **NOTE:** The above snapshot is for Cable mode, for Wireless mode the Backplane Device and Backplane IP Prefix parameters do not exist.
10. ☐	Reboot the server	Reboot. `# init 6` Allow the server time to reboot.

Step	Procedure	Details
11. ☐	Verify basic network connectivity and server health.	From the installed VM, ping the OAM/XMI gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **syscheck** command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact My Oracle Support. 
12. ☐	Exchange keys with cluster mate (This step must be run from the 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** 
13. ☐	Check status	In the CMP GUI, navigate to: Platform Setting → Topology Setting → All Clusters When the server has returned to online status, log into the GUI on the OAM virtual IP address • Verify to the best of your abilities that the new manager has configuration for the MPE clusters in the network (whether those clusters are online or not) • Verify other application configuration properties as you are able. After one CMP is in place, the other node of the CMP cluster can replaced with the procedures above, and any other clusters or individual nodes that require replacement can be handled with the above procedures (Follow procedure 3 or 4 for MPE/MRA clusters).
---End of Procedure---		

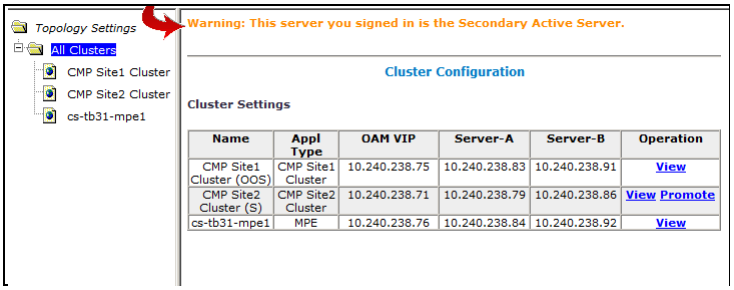
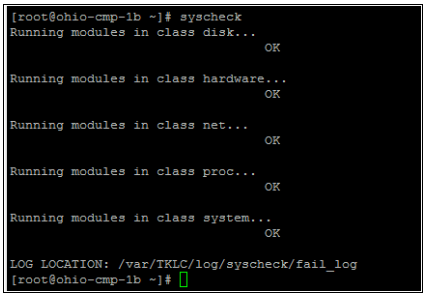
5.8 Procedure 8: Promoting Georedundant CMP Cluster

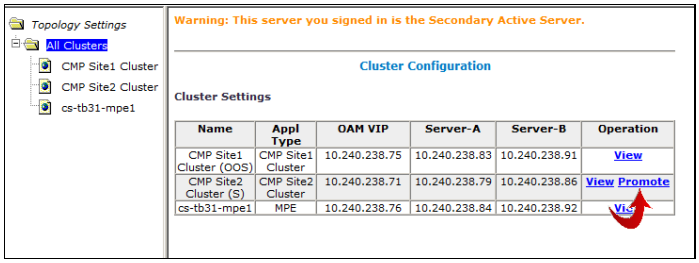
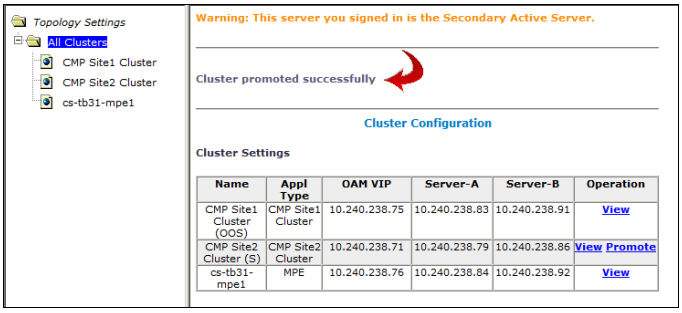
This procedure is used to bring a georedundant secondary active CMP online before beginning restoration of other policy clusters in the network. After a CMP is online, all other servers (MPE/MRA) of the policy network can be re-created using the above procedures and then their application level configuration restored from this CMP.

This Procedure performs Promoting georedundant CMP cluster

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

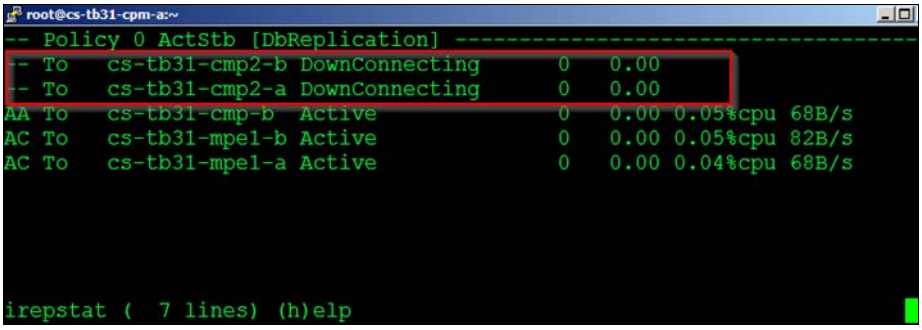
If this procedure fails, contact the My Oracle Support (MOS) Customer Care Center and ask for assistance.

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.	From the active VM 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. Contact My Oracle Support before proceeding if network ping tests still fail. `# ping <XMI or OAM gateway address>` Run the **`syscheck`** command, ensuring 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** for the secondary server. Click **OK** on the confirmation dialog.  You should see a message appear above the Cluster Configuration header indicating the successful promotion (see example below). 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** 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 procedures listed in this document to bring other failed servers/clusters back online.

7. ☐	SSH to active node of promoted cluster	SSH to the active node of the promoted cluster
		`# ssh admusr@<node_IP_Address>`
		`$ sudo su -`

Step	Procedure	Details

8. ☐	Verify irepstat output shows expected status	Run the irepstat command to verify that cluster replication is Active. If not Active after 5 minutes, check the CMP GUI for any active alarms.
		`# irepstat`
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To  Site1-nw-cmp-a Active  0  0.25 1%R 0.04%cpu 65B/s`
		`AA To  Site2-nw-cmp-a Active  0  0.50 1%R 0.04%cpu 65B/s`
		The status of all clusters except known failed servers should have a status of Active as in the above snapshot.
		Otherwise if any of the replication paths show DownConnecting as in the snapshot below contact My Oracle Support.
		The example below shows an installation with servers cs-tb31-cmp2-a and cs-tb31-cmp2-b failed, while all other cluster replication is working properly.
		 

9. ☐	Rebuild failed CMP cluster	Refer to Procedure 6: Restoring Complete Cluster without Server Backup File to rebuild failed CMP cluster.
---End of Procedure---		

APPENDIX A. CONTACTING ORACLE

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

A.1 My Oracle Support (MOS)

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

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

  Make the following selections on the Support telephone menu:

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

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

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

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

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

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

A.2 Emergency Response

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

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

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

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