ORACLE®

Oracle® Communications

Policy Management
Disaster Recovery Procedures

Release 9.4

E85223-01
March 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 Disaster Recovery Procedures

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose and Scope

This document describes the disaster recovery procedure in the case of a failed server (node) within a Configuration Management Platform (CMP), Multimedia Policy Engine Routing (MPE-R), Multimedia Policy Engine Serving (MPE-S), Bandwidth on Demand (BOD), Management Agent (MA) high availability (HA) cluster or a complete cluster failure for one of the cable policy components. In Policy Management, Release 9.4, georedundant architecture, three servers are deployed for BOD and MPE-S components in both geographic sites. For CMP, a cluster of 2 servers is deployed in each site forming four total servers in georedundant sites. Two servers are configured in an HA cluster in one site with one additional server in Active mode and one server in Standby mode. The third server is in spare mode in the secondary site. This document covers the preparation of a single replacement server (in the case of s single node failure) or the preparation of multiple replacement servers in the case of a complete cluster failure.

The following table lists the different network interfaces for the different H/W certified for the 9.4 cable release including the direct link (BP) used for the replication between nodes in same cluster:

Hardware Type	OAM	Sig-A	Sig-B	Backplane
HP DL360 G6	Bond2=eth13	Bond1=eth11+eth12	Bond3=eth14	Bond0=eth01+eth02
HP DL360 G7	Bond2=eth13	Bond1=eth11+eth12	Bond3=eth14	Bond0=eth01+eth02
HP DL360pGen8	Bond0=eth01+eth11	Bond1=eth02+eth12	Bond2=eth03+eth13	Bond3=eth04+eth14
HP DL380pGen8	Bond0=eth01+eth11	Bond1=eth02+eth12	Bond2=eth03+eth13	Bond3=eth04+eth14

1.2 References

- *General Installation Methods*, 910-6351-001
- *HP Solutions Firmware Upgrade Pack Release Notes Release Notes 2.2.4*, 910-6724-001
- *HP Solutions Firmware Upgrade Procedures 2.2*, 909-2234-001
- *TPD Initial Product Manufacture*, 909-2130-001
- *Platform Configuration User Guide*, 910-6732-001
- *Replacing a Failed Server in a Camiant Cluster Reference Guide*, 910-6114-001
- *HP iLO 4 User Guide*, c03334051
- *Oracle Communications Policy Management Bare Metal Installation Guide*, E85553-01

1.3 Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CMP	Configuration Management Platform
DVD	Digital Versatile Disc
FRU	Field Replaceable Unit
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MPE-R/S	Multimedia Policy Engine (Routing/Serving)
BOD	Bandwidth on Demand
MA	Management Agent
OS	Operating System (e.g. TPD)
PCRF	Policy and Charging Rules Function
TPD	Tekelec Platform Distribution
VSP	Virtual Serial Port

1.4 Software Release Numbering

This guide applies to Cable Policy Management Versions 9.4.x

1.5 Terminology

Term	Description
Base hardware	Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on and communicate on the network.
Base software	Base software includes installing the server’s operating system: Tekelec Platform Distribution (TPD).
Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.
Camiant initial configuration	The initial configuration put into the policy server through the platcfg utility that brings the server’s network interface online and allows management and configuration from the CMP
Node/Blade	In an HA cluster two servers, one active and one standby are required. In the case that a server within an HA cluster is referenced the term node will be used to describe each server within the HA cluster. The term blade may also be used in this context.

2 GENERAL DESCRIPTION

In the case that a production policy server or a cluster fails totally and need to be replaced. The following steps need to be performed to be ready for the policy software installation:

1. Verify the failed server is disconnected from the network
2. Equipment ordered by the customer, and installed by customer
3. Verify the hardware installation has been completed
4. Run cabling

The following are high level installation steps for replacement server(s):

1. Verify iLO Configuration
2. Verify Firmware Versions
3. Verify the BIOS settings
4. Install the TPD Platform Software
5. Install the Policy Management Application(CMP / MPE / MA / BOD)
6. Perform Camiant Initial Configuration or Restore Server Backup
7. Perform Topology Configuration from the CMP GUI
8. Synchronize the servers in an HA cluster
9. Configuring or Restoring node-specific information
10. Confirm Failover of Restored Cluster

2.1.1 Recovery of a Node Failure of the CMP Cluster

The complete failure of one node in the CMP cluster (either in site 1 or site 2 in case solution is georedundant) will require the use of a new server called the replacement server. Camiant initial configuration information needs to be restored either manually or from a server backup file, after which the cluster will reform, and database replication from the active server of the cluster will recover the cluster.

2.1.2 Recovery of a Node Failure of MPE/MA/BOD Cluster

The complete failure of one node in MPE or MA or BOD cluster in site 1 (or the spare node in site 2 in case the solution is georedundant) will require the use of a new server called the replacement server. Camiant initial configuration information needs to be restored either manually or from a server backup file, after which the cluster will reform, and database replication from the active server of the cluster will recover the cluster.

2.1.3 Complete Server Outage (Both Servers in CMP cluster)

In the event that both nodes in a CMP HA Cluster (either in site 1 or site 2 if solution is georedundant) have failed, the CMP cluster will require replacement of both servers. The servers are recovered using base recovery of hardware and software and then restoring a server backup (or Camiant Initial Configuration) followed by a restore of the system backup to the replacement CMP server. The system backup will be taken from customer offsite backup storage locations (assuming these were performed and stored off site prior to the outage). If no backup file is available, the only option is to rebuild the entire network from scratch. The networks data must be reconstructed from whatever sources are available, including entering all data manually.

2.1.4 Complete Server Outage (Both Servers in MPE/MA/BOD cluster)

In the event that both servers in a MPE or MA or BOD HA Cluster have failed, the cluster will require replacement of both servers. The servers are recovered using base recovery of hardware and software and then restoring a server backup to the active MPE/MA/BOD server. No system backup will be needed as the MPE/MA/BOD will update needed database information directly from the CMP.

2.1.5 Camiant initial configuration

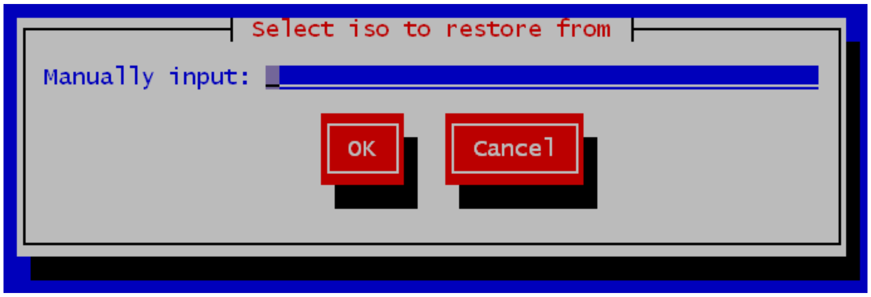
The information required for initial configuration is not extensive, and may be readily available from customer site documents, or from the CMP's topology configuration. In most cases it can be easier to manually input the initial configuration in platcfg than to try to load a server backup file into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

Needed initial configuration information:

- Hostname
- OAM real IP address and network mask
- OAM default router address
- NTP server
- DNS server A (optional)
- DNS Server B (optional)
- DNS search (optional)
- Device (use default)
- Backplane Device (use default)

2.1.6 Using the server backup file.

When asked to restore from serverbackup, the platcfg utility will look in `/var/camiant/backup/local-archive/serverbackup` directory. If no files are in that directory, the box below will be presented.



Select iso to restore from

Manually input:

You will have to 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.

3 PROCEDURE OVERVIEW

This section lists the materials required to perform disaster recovery procedures and a general overview (disaster recovery strategy) of the procedure Rund.

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. Disconnect failed servers from network
3. Evaluate the availability of server and system backup files for the servers that are to be restored.
4. Read and review the content in this document.
5. From the failure conditions, determine the Recovery Scenario and procedure to follow.
6. Run appropriate recovery procedures.

3.2 Required Materials

The following items are needed for disaster recovery:

1. A copy of this document and of all documents in the References list.
2. Customer provided network configuration of policy components (CMP/MPE/MA/BOD).
3. In case of CMP: Policy Management system backup file: electronic backup file (preferred) or hardcopy of all Policy system configuration and provisioning data.
4. The Firmware .ISO certified for the corresponding builds and servers.
5. Tekelec Platform Distribution (TPD) software
6. Policy Management Application software .ISO for the component(s) of the target release.

3.3 Policy Server Backup

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

- **Server Backup:** There is one Server Configuration backup for each server in the system. The server backup is a Back-up of the OS information unique to the server. Information such as: hostname, IP Addresses, NTP, DNS, Static Route configuration. This operation creates a Server Configuration Backup file, and should be Rund on each of the server in the customer's network.
- **System Backup:** There is one Application Configuration backup for the entire Policy Management system. The system backup will gather PCRF configuration information that is unique to this system. Information such as: topology, policy(s), feature configuration. The system backup should be Rund only on the Active CMP at the primary site.

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

4 PROCEDURE PREPARATION

4.1 Purpose and Scope

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. The first step is to evaluate the failure scenario and determine the procedure(s) that will be needed to restore operations. A series of procedures are included below that can be combined to recover one or more policy management nodes or clusters in the network.

NOTE: A failed server (node) in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.

The general steps recovering servers are:

1. Verify BIOS time is correct on servers
2. Verify Version of TPD installed
3. Load application for corresponding Server HW types
4. Check FW versions and upgraded if necessary
5. Check NTP status after recovery
6. Check Active Alarms from GUI and both syscheck, alarmMgr–alarmStatusfrom CLI

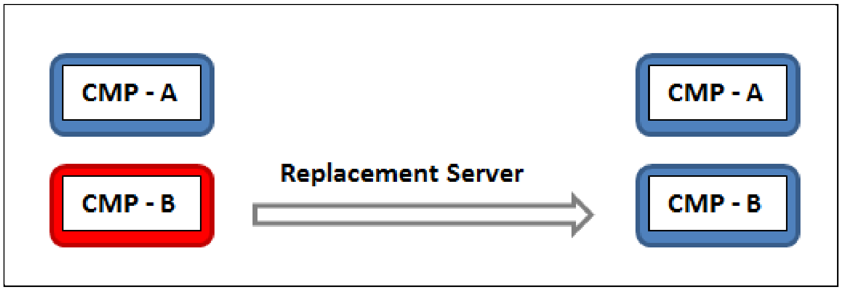
See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions on BIOS and iLO configuration as well as firmware loading and verification.

4.2 Recovery Scenarios

4.2.1 Recovery Scenario 1 (Single Node Failure in CMP HA Cluster)

For a partial outage with a CMP server available, only base recovery of hardware and software and initial Camiant configuration is needed. A single CMP server is capable of restoring the configuration database via replication to all MPE/MA/BOD servers, or to the other CMP node of a cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to Run the procedure. The steps are in the Restore Procedures section. The major activities are summarized as follows:

- Recover Failed CMP server (if necessary) by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
  - Initial Camiant configuration is re-installed. Either by hand or from server backup file
  - The database is intact at the active CMP server and will be replicated the standby CMP server.



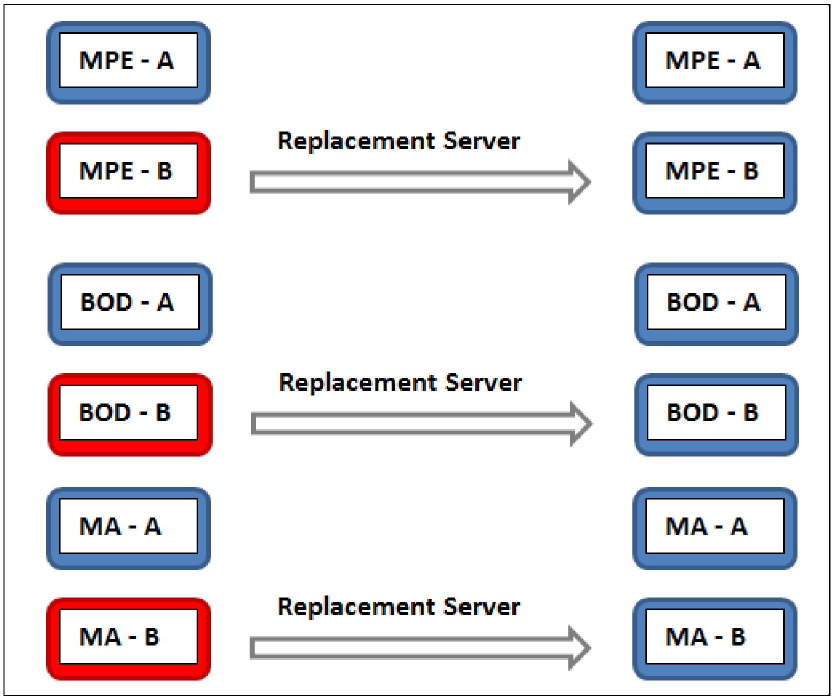
For complete details, refer to the following procedure in this document

- Procedure 1. Restoring Single Node Failure in CMP HA Cluster

4.2.2 Recovery Scenario 2 (Single Node Failure in MPE/MA/BOD HA Cluster)

For a partial outage with a MPE or Ma or BOD server available, only base recovery of hardware and software and initial Camiant configuration of the failed node is needed. The CMP server is capable of restoring the configuration database via replication to the replaced MPE or MA or BOD server. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to Run the procedure. The steps are in the Restore Procedures section. The major activities are summarized as follows:

- Recover any failed MPE or MA or BOD servers by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
  - Initial Camiant configuration is re-installed. Either by hand or from server backup file
  - The configuration database is available at the active MPE/MA/BOD server and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/MA/BOD replaced server using the re-apply configuration function.

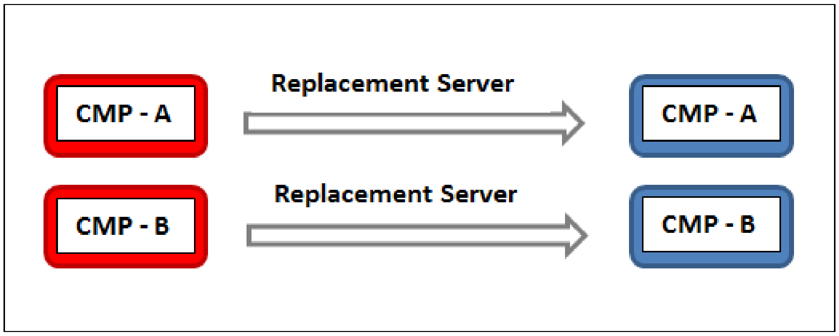


For complete details, refer to the following procedure in this document

- Procedure 2. Restoring Single Node Failure in MPE/MA/BOD HA Cluster

4.2.3 Recovery Scenario 3 (Complete Cluster Outage of the CMP)

For a full outage with a CMP server unavailable, base recovery of hardware and software is needed, then the recovery from system backup of the application configuration for the policy network. The first CMP server is built and restored with the configuration database from a system backup. Replication of the restored database to a second rebuilt CMP node will form a CMP cluster. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to Run the procedure. The steps are in the Restore Procedures section. The major activities are summarized as follows:



1. Recover the primary CMP server (if necessary) by recovering base hardware and software.
   - Recover the base hardware.
   - Recover the software.
   - Initial Camiant configuration is re-installed. Either by hand or from server backup file
   - The database of the CMP will be restored from a system backup provided by the customer.
   - If a system backup is not available, use customer provisioning systems to restore application level configuration to the CMP. It is possible to use the data at other policy solution components like MPEs, BODs, MAs (that should still be good) to verify that the re-entered data on the CMPs matches the previous configuration that was in-use. Also, check with engineering team for possible approach to verify if the data at the operational MPEs matches the data that has been re-entered at the CMP after re-entering the Policies and other application level data to the CMP.
2. Recover the secondary CMP server by recovering base hardware and software.
   - Recover the base hardware.
   - Recover the software.
   - Initial Camiant configuration is re-installed. Either by hand or from server backup file
   - The configuration database is available at the now active CMP server and does not require restoration on the second CMP node. Configuration will be replicated when the two new CMP nodes form a cluster.

For complete details, refer to the following procedure in this document

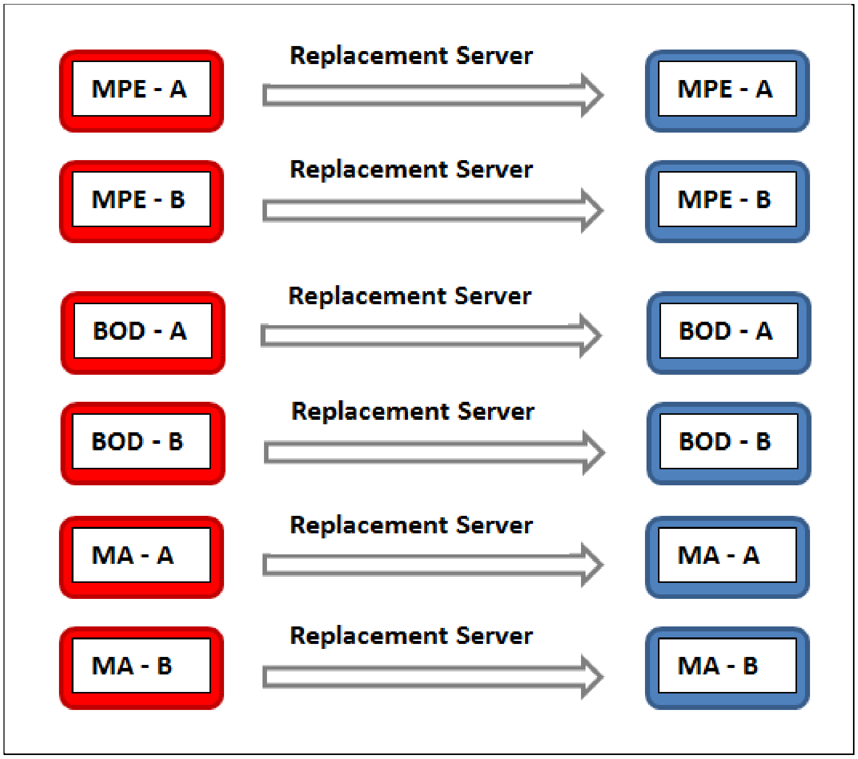
- Procedure 3. Restoring Complete Cluster Outage of the CMP

4.2.4 Recovery Scenario 4 (Complete Cluster Outage of MPE or BOD or MA)

For a full outage with no MPE/BOD/MA servers unavailable, a base recovery of hardware and software will be needed. Initial Camiant Configuration will then be performed on each replacement server. The CMP server is capable of restoring the configuration database for the replaced MPE or BOD or MA using Reapply Configuration to the active server in the MPE/BOD/MA HA Cluster. The active MPE/BOD/MA will then replicate the database via replication to its mate server.

The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to Run the procedure. The steps are in the Restore Procedures section. The major activities are summarized as follows:

1. Recover any failed MPE/BOD/MA servers by recovering base hardware and software.
   - Recover the base hardware.
   - Recover the software.
   - Initial Camiant configuration is re-installed. Either by hand or from server backup file
   - The configuration database is available at the now active CMP server and does not require restoration on the CMP. Configuration can be pushed from the CMP to the MPE/BOD/MA servers.



For complete details, refer to the following two procedures in this document

- Procedure 4. Restoring Complete Cluster Outage of the MPE/BOD/MA

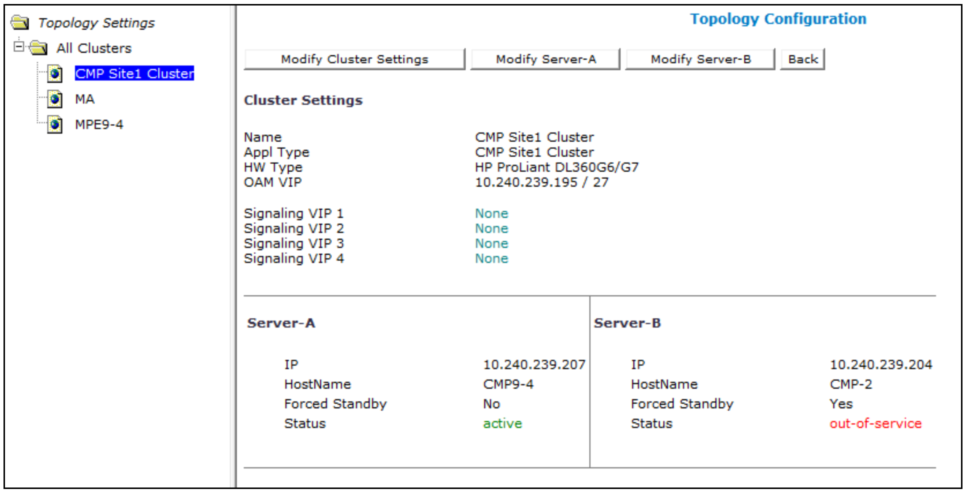
5 RESTORE PROCEDURES

5.1 Procedure 1. Restoring Single Node Failure in CMP HA Cluster

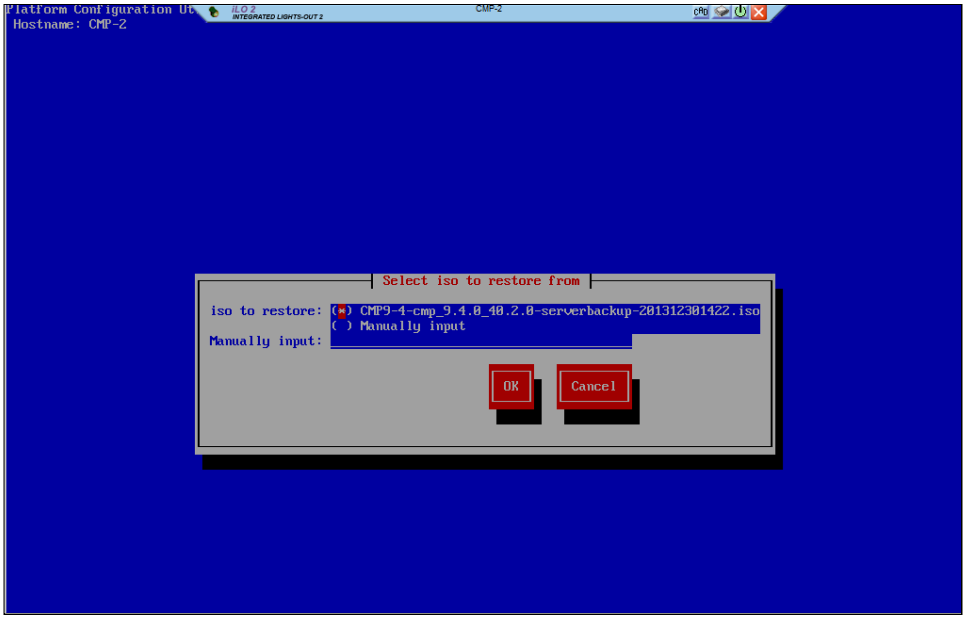
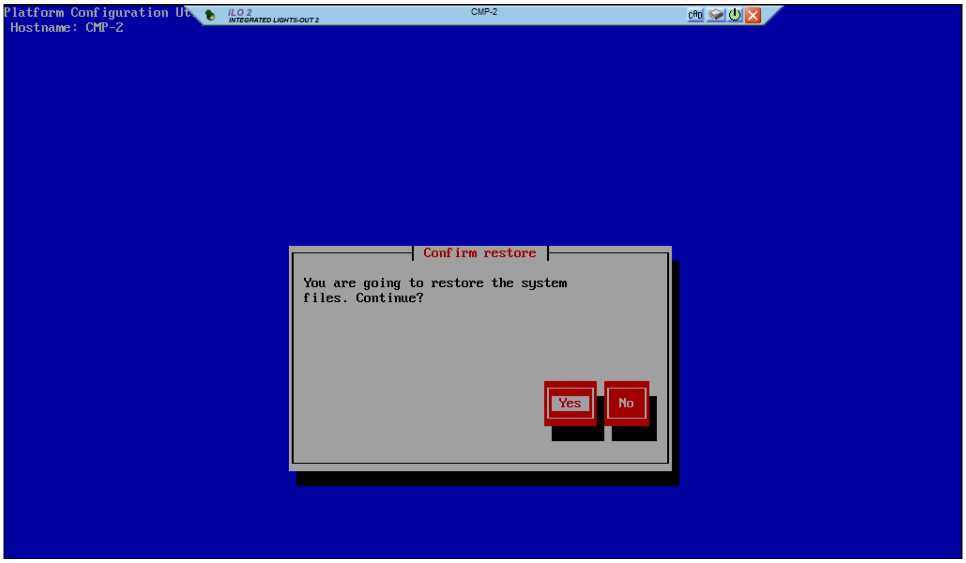
This Procedure restores the standby CMP node, when a server level backup is available or using Camiant Initial Configuration if no server level backup is available. .

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

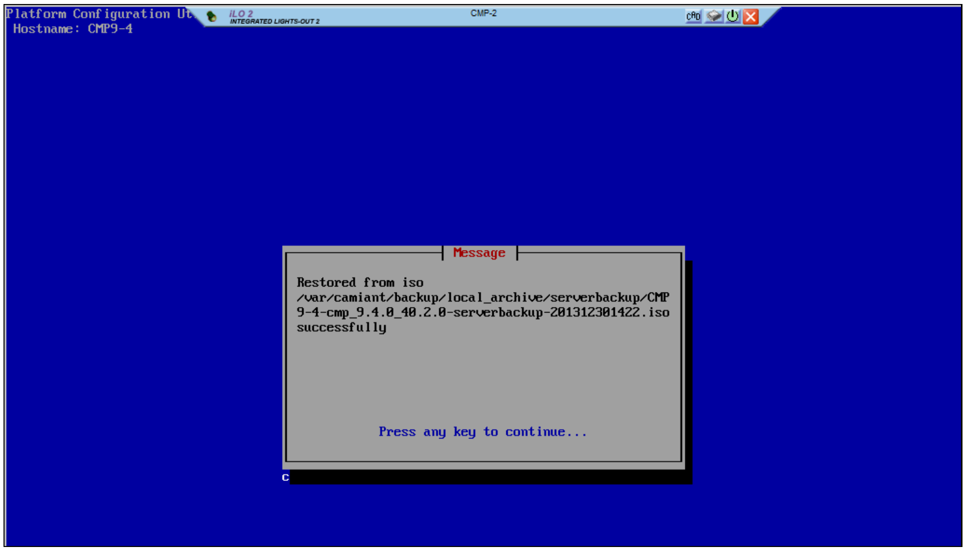
Should this procedure fail, contact the Oracle Customer Care Center and ask for assistance.

Step	Procedure	Instruction
1. □	Required resources / information	The purpose of this procedure is to replace one node of a CMP HA cluster. Base level software is confirmed. Camiant initial configuration is restored from a server backup file or manually. Then the new node is allowed to re-sync to the existing node to form a complete CMP cluster. Required resources: • Replacement node hardware • TPD installation ISO • CMP Policy Management Application installation ISO. • *serverbackup.ISO* of the node to be replaced (optional)
2. □	Prerequisites	1. Remove failed hardware and replace. 2. Verify that the node has TPD on it, or install TPD 3. Install the correct version of the application software – CMP 4. Cable as per network requirements See *Oracle Communications Policy Management Bare Metal Installation Guide* for directions on installing TPD and the CMP Application. This procedure can also be used to confirm Bios, Firmware and iLO settings.
3. □	Set the failed node to Forced Standby	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 1. Determine the cluster with the failed node 2. Determine the failed node 3. Click **Modify** for the failed node 4. Select the **Forced Standby**, then click **Save**  Topology Settings All Clusters CMP Site1 Cluster MA MPE9-4 Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.195 / 27 Signaling VIP 1 None Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None Server-A IP 10.240.239.207 HostName CMP9-4 Forced Standby No Status active Server-B IP 10.240.239.204 HostName CMP-2 Forced Standby Yes Status out-of-service

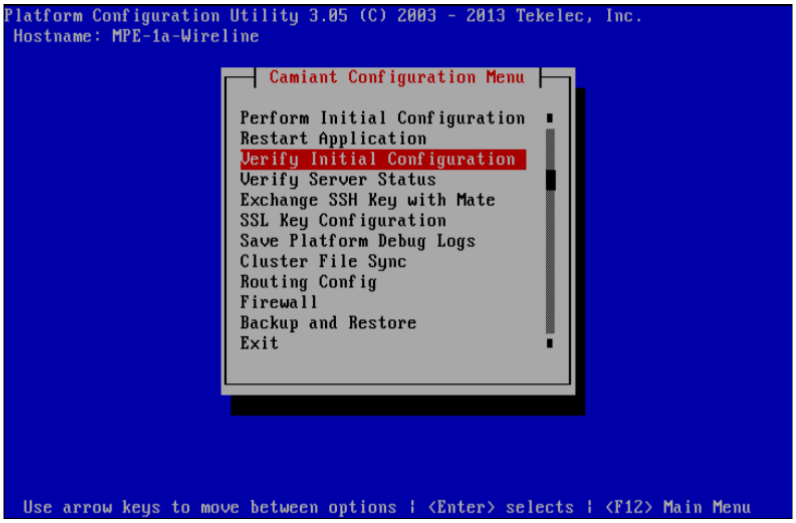
Step	Procedure	Instruction
4. □	Load the ISO for server restore	If a server backup is available proceed with this step. **If a server backup is not available skip to step 11.** Obtain the *serverbackup.iso* for the node to be restored. When the replacement node is available (TPD/App installation complete, cabled as per network requirements), the server backup file should be copied to the following directory: **`/var/camiant/backup/local_archive/serverbackup.`** **NOTE:** Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu. The platcfg utility also allows the user to manually enter any mounted path on the server. See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions accessing the iLO, launching the remote console.
5. □	Login via the iLO Interface	Access the iLO Interface and launch the remote console to gain root level access to the cli

Step	Procedure	Instruction
6. □	Perform platcfg restore from iLO session on replacement node	1. Run the following command `# su – platcfg` 2. From within the platcfg utility, navigate to: **Camiant Configuration → Backup and Restore → Server Restore** 3. Select the *serverbackup*.ISO that you just put on the system and click **OK**.  Platform Configuration Ut Hostname: CMP-2 Select iso to restore from iso to restore: (*) CMP9-4-cmp_9.4.0_40.2.0-serverbackup-201312301422.iso ( ) Manually input Manually input: 4. Click **Yes** to confirm:  Platform Configuration Ut Hostname: CMP-2 Confirm restore You are going to restore the system files. Continue? **NOTE:** This may take a couple of minutes.

Step	Procedure	Instruction

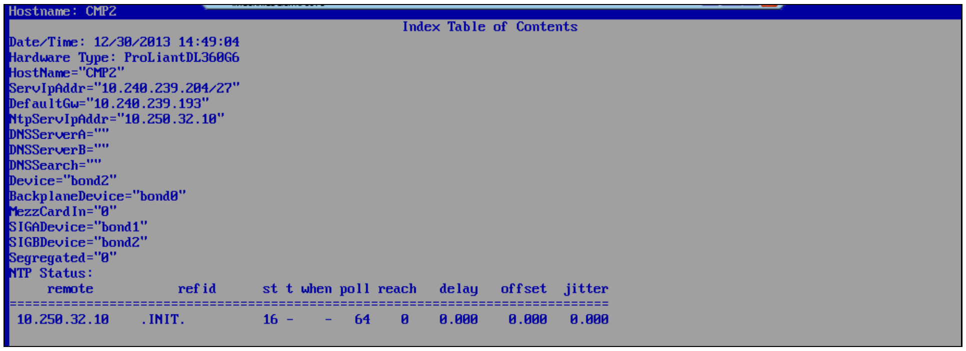
7. □	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding:
		
		`Platform Configuration Ut`
		`Hostname: CMP9-4`
		`Message`
		`Restored from iso /var/camiant/backup/local_archive/serverbackup/CMP9-4-cmp_9.4.0_40.2.0-serverbackup-201312301422.iso successfully`
		`Press any key to continue...`

8. □	Reboot the server	Exit form the platcfg menu and Reboot from the command line. **`shutdown -r now`**

9. □	Verify Config	After the server has been rebooted you should be returned to a login prompt via the iLO remote console. Verify the configuration by selecting **Camiant Configuration → Verify Initial Configuration** from within the platcfg utility.
		
		`Platform Configuration Utility 3.05 (C) 2003 - 2013 Tekelec, Inc.`
		`Hostname: MPE-1a-Wireline`
		 Camiant Configuration Menu
		Perform Initial Configuration
		Restart Application
		Verify Initial Configuration
		Verify Server Status
		Exchange SSH Key with Mate
		SSL Key Configuration
		Save Platform Debug Logs
		Cluster File Sync
		Routing Config
		Firewall
		Backup and Restore
		Exit
		`Use arrow keys to move between options ¦ <Enter> selects ¦ <F12> Main Menu`

<table>
<tr><th>Step</th><th>Procedure</th><th>Instruction</th></tr>
<tr><td><b>10.</b> □</td><td>Verify Config</td><td>

Confirm the configured Hostname, ServIpAddr, DefaultGw and NtpServIpAddr previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.



```
Hostname: CMP2
                                                 Index Table of Contents
Date/Time: 12/30/2013 14:49:04
Hardware Type: ProLiantDL360G6
HostName="CMP2"
ServIpAddr="10.240.239.204/27"
DefaultGw="10.240.239.193"
NtpServIpAddr="10.250.32.10"
DNSServerA=""
DNSServerB=""
DNSSearch=""
Device="bond2"
BackplaneDevice="bond0"
MezzCardIn="0"
SIGADevice="bond1"
SIGBDevice="bond2"
Segregated="0"
NTP Status:
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.250.32.10    .INIT.          16 -    -   64    0    0.000    0.000   0.000
```

Skip to step 21.

</td></tr>
<tr><td><b>11.</b> □</td><td>Perform Camiant Initial Configuration using platcfg</td><td>

If directed to this step because a server backup is not available, then the following steps can be used perform the Initial Configuration based on network information available and a cluster file sync.

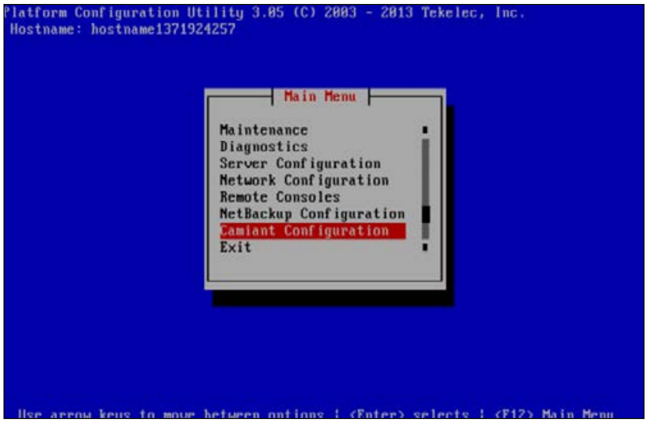
NOTE: Customer provided data is required to perform the Camaint Initial Configuration in step 15.

</td></tr>
<tr><td><b>12.</b> □</td><td>Run platcfg tool on the replacement server</td><td>

The failed sever in the HA cluster has already been placed in forced standby as per step 3. The replacement server is in place and has had the base software already installed. Launch the remote console using the iLO interface.

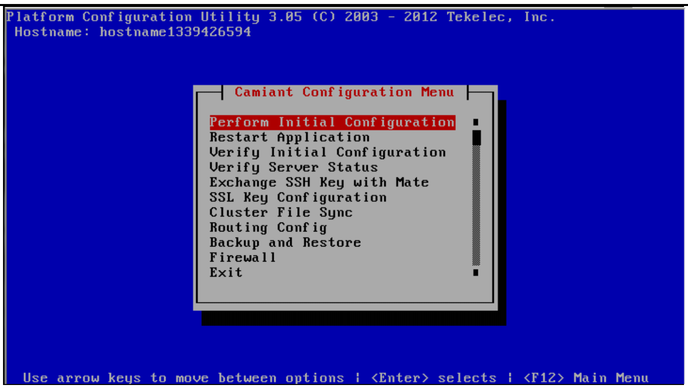
```
# su - platcfg
```

When presented with following screen select **Camiant Configuration**.



```
Platform Configuration Utility 3.05 (C) 2003 - 2013 Tekelec, Inc.
 Hostname: hostname1371924257
```

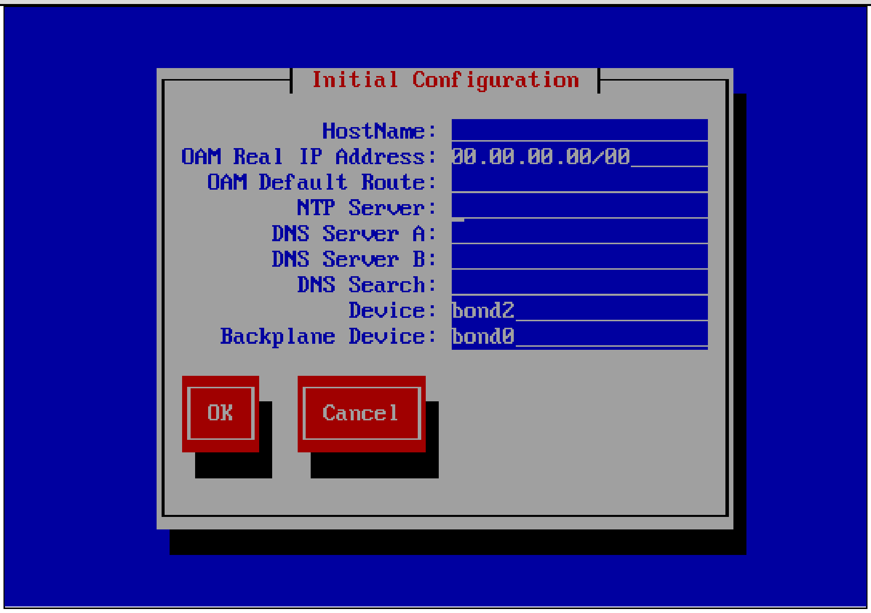
</td></tr>
<tr><td><b>13.</b> □</td><td>Select <b>Perform Initial Configuration</b></td><td>

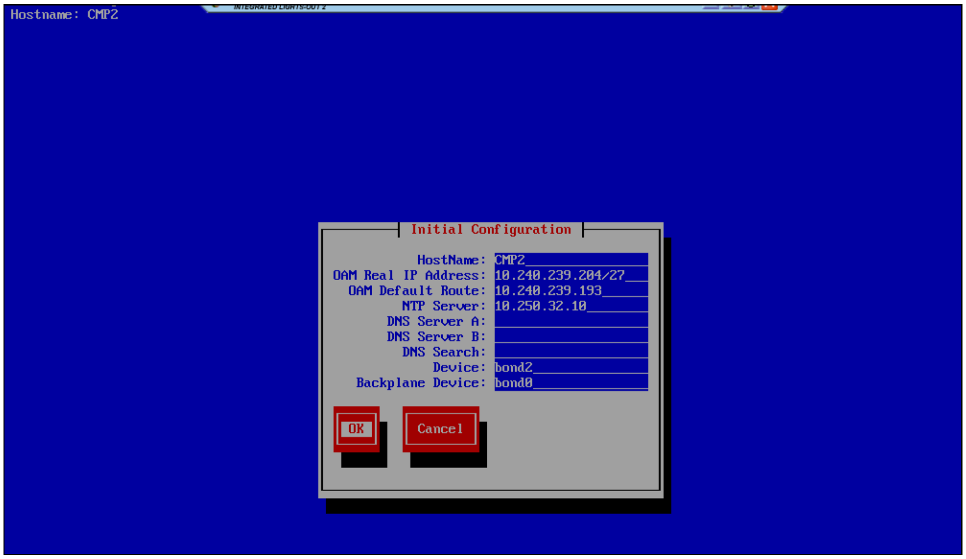


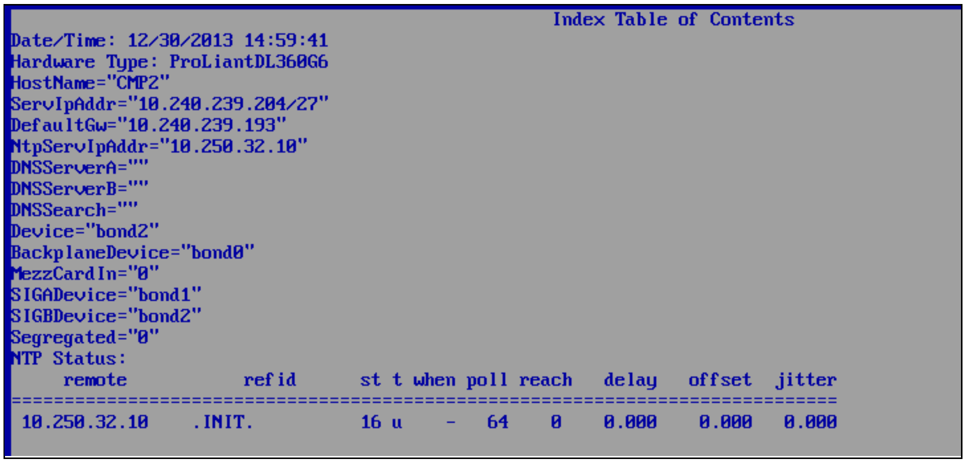
```
Platform Configuration Utility 3.05 (C) 2003 - 2012 Tekelec, Inc.
 Hostname: hostname1339426594
```

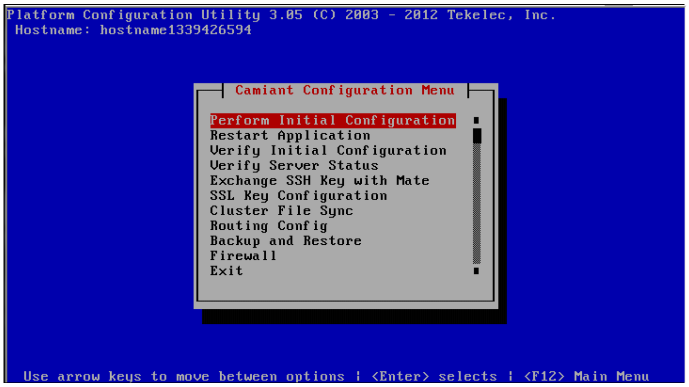
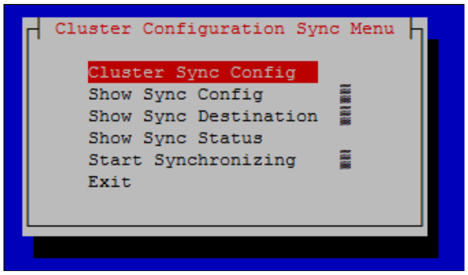
Camiant Configuration Menu
Perform Initial Configuration
Restart Application
Verify Initial Configuration
Verify Server Status
Exchange SSH Key with Mate
SSL Key Configuration
Cluster File Sync
Routing Config
Backup and Restore
Firewall
Exit
Use arrow keys to move between options | <Enter> selects | <F12> Main Menu

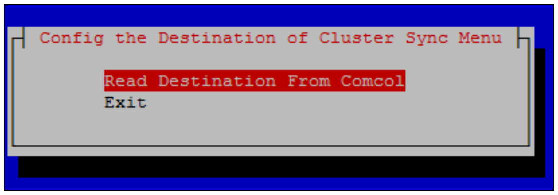
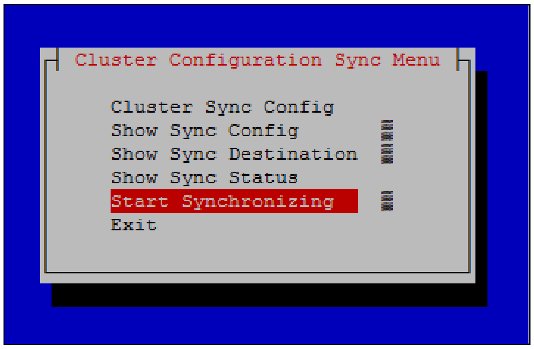
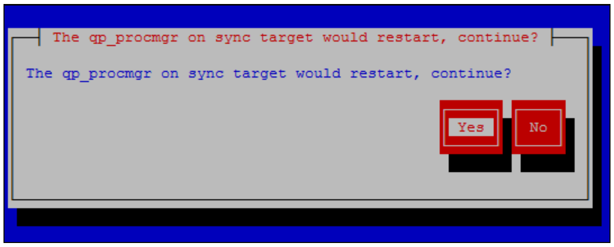
</td></tr>
</table>

Step	Procedure	Instruction
14. □	Complete Initial Configuration form	 Initial Configuration HostName: OAM Real IP Address: 00.00.00.00/00 OAM Default Route: NTP Server: DNS Server A: DNS Server B: DNS Search: Device: bond2 Backplane Device: bond0 • **Hostname** - the unique hostname for the device being configured. • **OAM Real IP Address** - the IP address that is permanently assigned to this device. (sometimes called Physical IP or Real IP). • **OAM Default Route** - the default route of the OAM network. • **NTP Server** - a reachable NTP (required) • **DNS Server A** - a reachable DNS server (optional) • **DNS Server B** - a reachable DNS server (optional) • **DNS Search** - is a directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out a DNS query. • **Device** - the bond interface of the OAM device. Note that the default value should be used, as changing this value is not supported. • **Backplane Device** – the bond interface of the backplane device Note that the default value should be used, as changing this value is not supported.

Step	Procedure	Instruction
15. □	Save configuration	Enter the configuration (example data fill below) and then select **OK** Hostname: CMP2 Initial Configuration HostName: CMP2 OAM Real IP Address: 10.240.239.204/27 OAM Default Route: 10.240.239.193 NTP Server: 10.250.32.10 DNS Server A: DNS Server B: DNS Search: Device: bond2 Backplane Device: bond0 The platcfg form will pause for a minute while the server is configured, and then return to the platcfg menu.
16. □	Reboot the server	1. Exit from the platcfg menu 2. Reboot from the command line. `‘shutdown -r now ‘`
17. □	Verify Config	1. After the server has been rebooted you should be returned to a login prompt via the iLO remote console. 2. From within the platcfg utility, verify the configuration by selecting: **Camiant Configuration → Verify Initial Configuration**

18. □	Verify Config	Confirm the configured Hostname, ServIpAddr, DefaultGw and NtpServIpAddr previously configured are present. A display similar to the following is shown.
		Index Table of Contents
		Date/Time: 12/30/2013 14:59:41
		Hardware Type: ProLiantDL360G6
		HostName="CMP2"
		ServIpAddr="10.240.239.204/27"
		DefaultGw="10.240.239.193"
		NtpServIpAddr="10.250.32.10"
		DNSServerA=""
		DNSServerB=""
		DNSSearch=""
		Device="bond2"
		BackplaneDevice="bond0"
		MezzCardIn="0"
		SIGADevice="bond1"
		SIGBDevice="bond2"
		Segregated="0"
		NTP Status:
		remote refid st t when poll reach delay offset jitter
		==
		10.250.32.10 .INIT. 16 u - 64 0 0.000 0.000 0.000

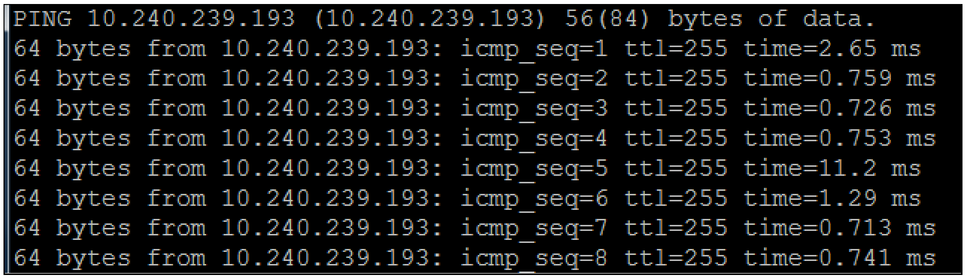
Step	Procedure	Instruction
19. □	Perform Cluster sync from the active server to the replacement server	Cluster file sync will copy over any firewall rules, static routes and security certificates that may have been configured manually on the active node and need to copied to the replacement server. 1. From the platcfg menu naviagte to **Camiant Configuration → Cluster File Sync**.  Platform Configuration Utility 3.05 (C) 2003 - 2012 Tekelec, Inc. Hostname: hostname1339426594 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Cluster File Sync Routing Config Backup and Restore Firewall Exit Use arrow keys to move between options | <Enter> selects | <F12> Main Menu 2. Select **Cluster Sync Config**.  Cluster Configuration Sync Menu Cluster Sync Config Show Sync Config Show Sync Destination Show Sync Status Start Synchronizing Exit

Step	Procedure	Instruction
20. □	Perform Cluster sync from the active server to the replacement server	1. Select **Read Destination From Comcol**  Config the Destination of Cluster Sync Menu Read Destination From Comcol Exit **NOTE:** You may need to provide the root password to proceed 2. Select **Start Synchronizing**  Cluster Configuration Sync Menu Cluster Sync Config Show Sync Config Show Sync Destination Show Sync Status Start Synchronizing Exit  The qp_procmgr on sync target would restart, continue? 3. Click through the synchronizing screens until you are returned to Cluster Configuration Sync menu. You can now log into the replacement server and confirm the files have synced to the replacement server. You may check the ssl keystore for example.

<table>
<tr><th>Step</th><th>Procedure</th><th>Instruction</th></tr>
<tr>
<td><b>21.</b> □</td>
<td>Verify basic network connectivity and server health <b>on the replacement server</b></td>
<td>

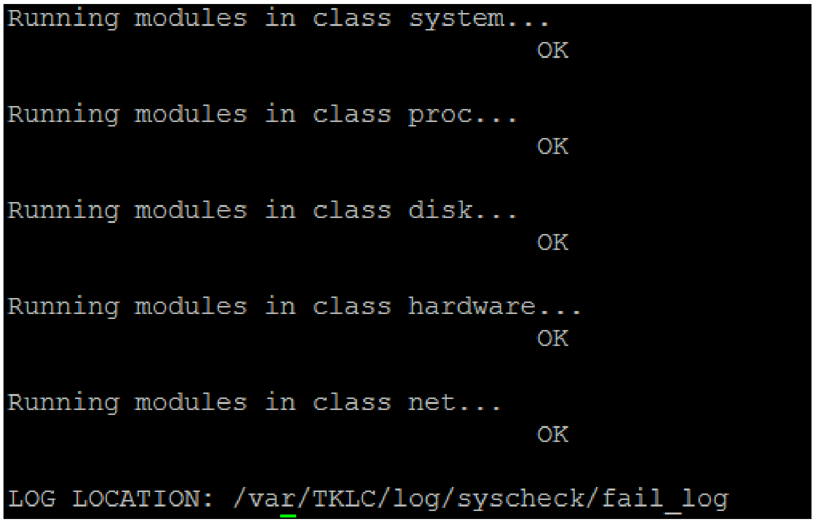
1. From the newly installed server, ping the OAM gateway.

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



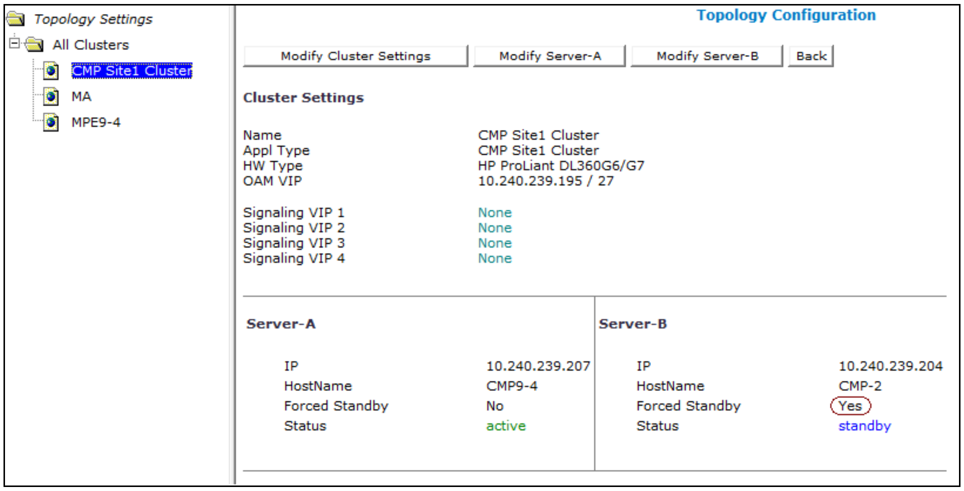
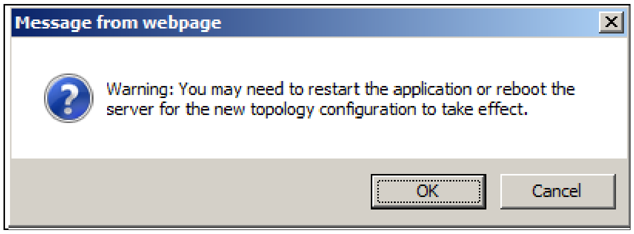
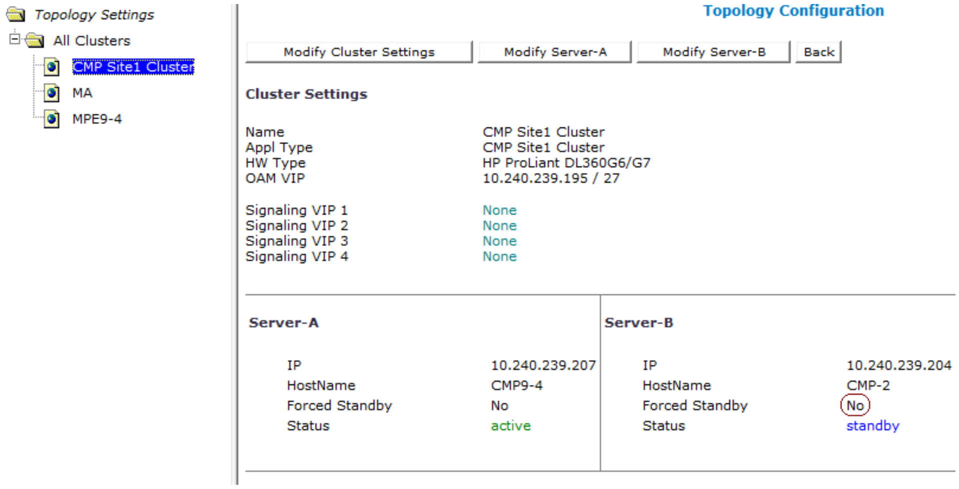
```
PING 10.240.239.193 (10.240.239.193) 56(84) bytes of data.
64 bytes from 10.240.239.193: icmp_seq=1 ttl=255 time=2.65 ms
64 bytes from 10.240.239.193: icmp_seq=2 ttl=255 time=0.759 ms
64 bytes from 10.240.239.193: icmp_seq=3 ttl=255 time=0.726 ms
64 bytes from 10.240.239.193: icmp_seq=4 ttl=255 time=0.753 ms
64 bytes from 10.240.239.193: icmp_seq=5 ttl=255 time=11.2 ms
64 bytes from 10.240.239.193: icmp_seq=6 ttl=255 time=1.29 ms
64 bytes from 10.240.239.193: icmp_seq=7 ttl=255 time=0.713 ms
64 bytes from 10.240.239.193: icmp_seq=8 ttl=255 time=0.741 ms
```

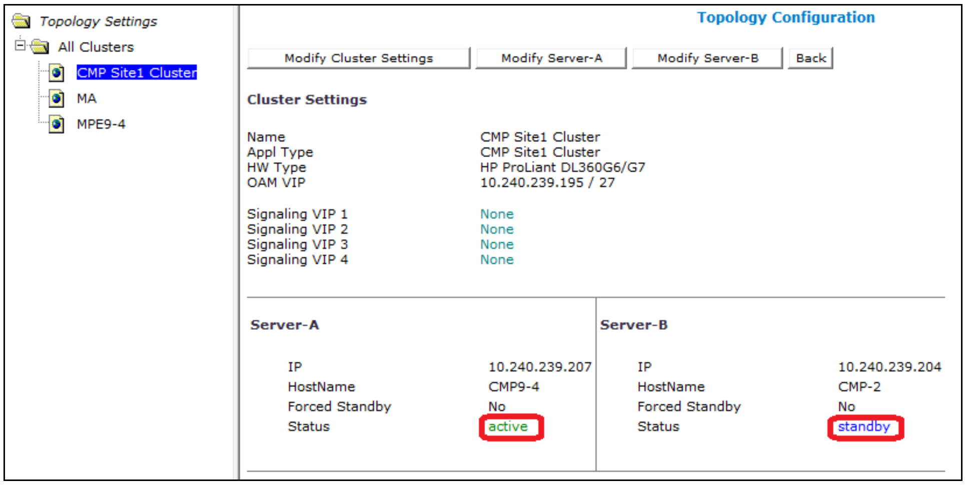
2. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed.
3. Contact Oracle support before proceeding if network ping tests still fail.
4. Run the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Oracle support.

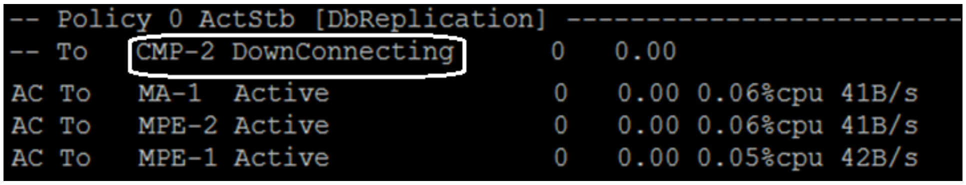
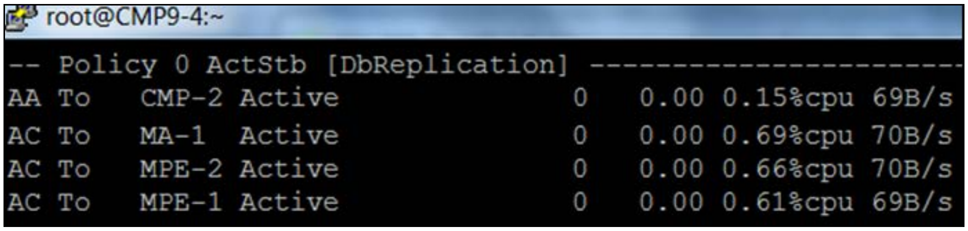


```
Running modules in class system...
                                OK

Running modules in class proc...
                                OK

Running modules in class disk...
                                OK

Running modules in class hardware...
                                OK

Running modules in class net...
                                OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

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

Step	Procedure	Instruction
22. □	Remove Forced Standby designation on current node.	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → Current Cluster**  Topology Settings All Clusters CMP Site1 Cluster MA MPE9-4 Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back **Cluster Settings** Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.195 / 27 Signaling VIP 1 None Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None **Server-A** IP 10.240.239.207 HostName CMP9-4 Forced Standby No Status active **Server-B** IP 10.240.239.204 HostName CMP-2 Forced Standby Yes Status standby 1. Modify for the server that has forced standby 2. Ensure server status is **standby**. 3. Clear the Forced Standby checkbox 4. Accept the resulting pop-up by clicking **OK**.  Message from webpage Warning: You may need to restart the application or reboot the server for the new topology configuration to take effect. 5. Click **Save**  Topology Settings All Clusters CMP Site1 Cluster MA MPE9-4 Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back **Cluster Settings** Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.195 / 27 Signaling VIP 1 None Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None **Server-A** IP 10.240.239.207 HostName CMP9-4 Forced Standby No Status active **Server-B** IP 10.240.239.204 HostName CMP-2 Forced Standby No Status standby

Step	Procedure	Instruction
23. □	Verify cluster status	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All → Current CMP Cluster** Monitor clustering of the new node to its peer, do not proceed until both nodes have a status of either active or standby, and that there are no CMP related Active Alarms (except for the Accept new upgrade alarm which will be cleared at the end of this procedure.  Topology Settings All Clusters CMP Site1 Cluster MA MPE9-4 Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.195 / 27 Signaling VIP 1 None Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None Server-A IP 10.240.239.207 HostName CMP9-4 Forced Standby No Status active Server-B IP 10.240.239.204 HostName CMP-2 Forced Standby No Status standby

24. □	Alternative method to check status	You can also monitor the clustering of the new node from within the shell on the active server node with `irepstat`.
		1. SSH to the Active node of the current cluster and Run the `irepstat` command:
		`# irepstat`
		Expected `irepstat` output while waiting reconnection:
		
		`-- Policy 0 ActStb [DbReplication] -------------------------`
		`-- To   CMP-2 DownConnecting        0   0.00`
		`AC To   MA-1  Active                0   0.00 0.06%cpu 41B/s`
		`AC To   MPE-2 Active                0   0.00 0.06%cpu 41B/s`
		`AC To   MPE-1 Active                0   0.00 0.05%cpu 42B/s`
		Expected `irepstat` output after cluster has formed:
		
		`-- Policy 0 ActStb [DbReplication] ----------------------`
		`AA To   CMP-2 Active              0   0.00 0.15%cpu 69B/s`
		`AC To   MA-1  Active              0   0.00 0.69%cpu 70B/s`
		`AC To   MPE-2 Active              0   0.00 0.66%cpu 70B/s`
		`AC To   MPE-1 Active              0   0.00 0.61%cpu 69B/s`

		THIS PROCEDURE HAS BEEN COMPLETED

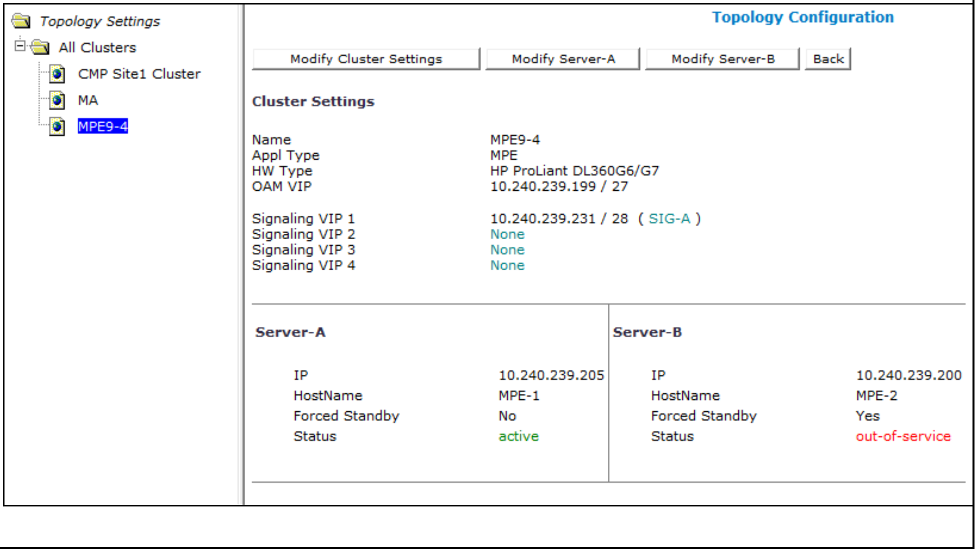
5.2 Procedure 2. Restoring Single Node Failure in MPE/BOD/MA HA Cluster

This Procedure restores the standby MPE/BOD/MA node, when a server level backup is available or using Camiant Initial Configuration if no server level backup is available. .

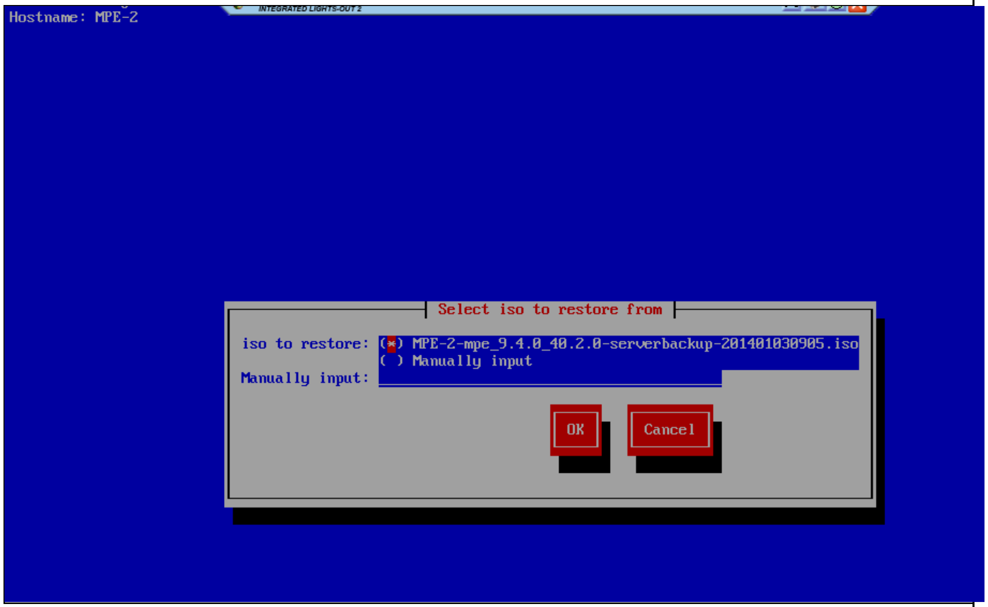
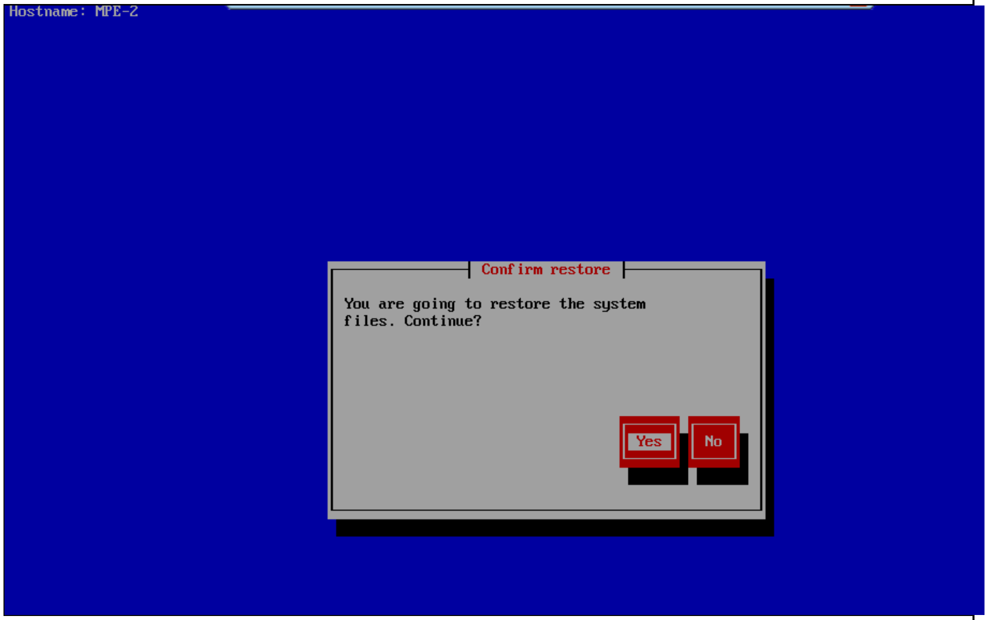
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

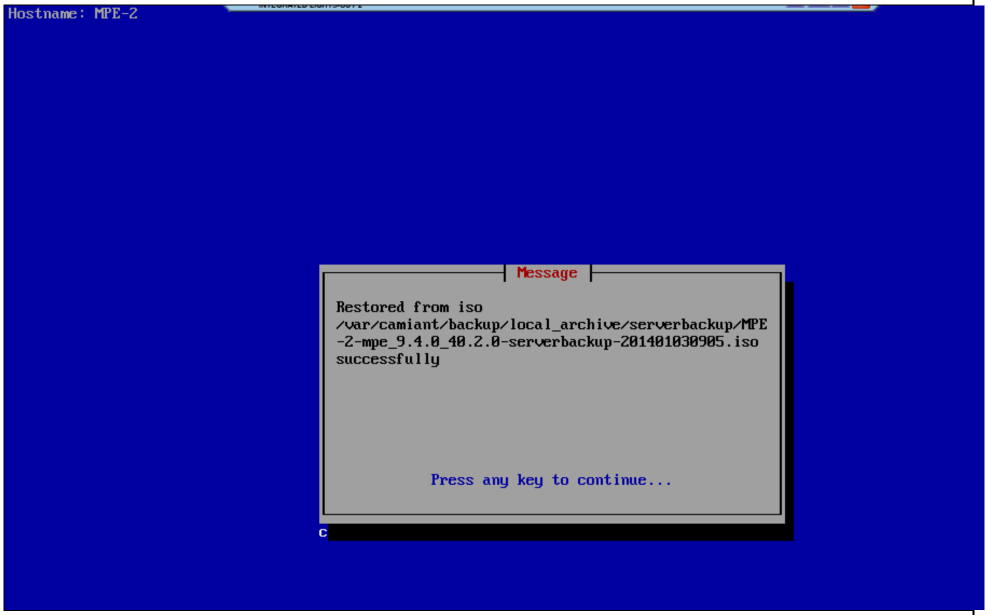
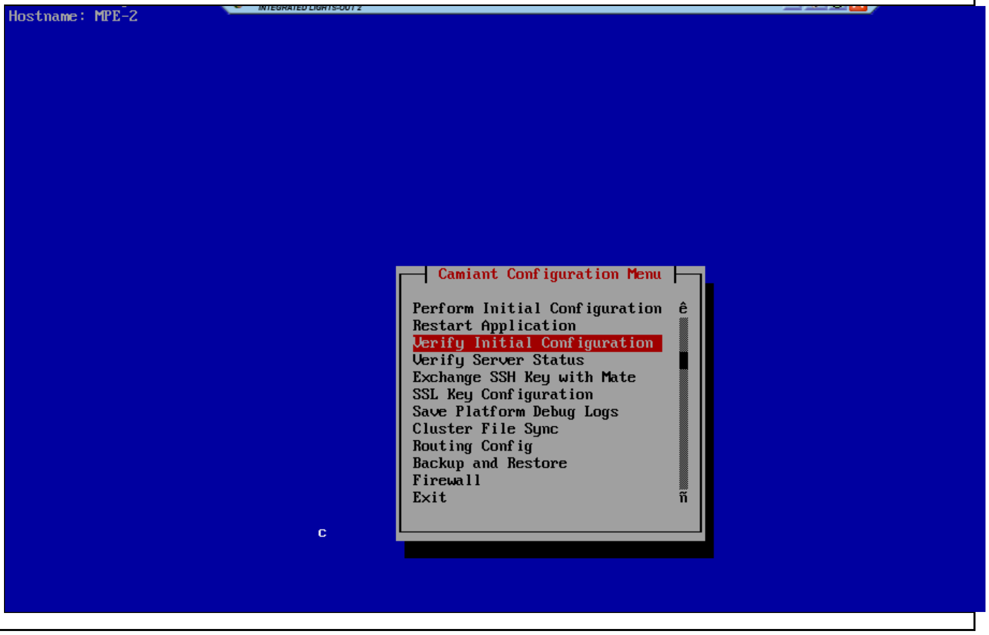
Should this procedure fail, contact the Oracle Customer Care Center and ask for assistance.

NOTE: We will cover the procedures for MPE, however the same procedures could be followed for BOD and/or MA if any or both need recovery.

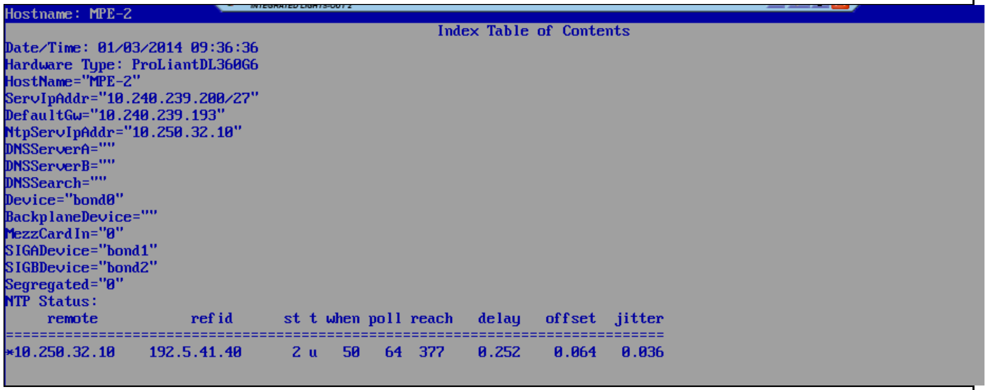
Step	Procedure	Instructions
1. □	Required resources / information	The purpose of this procedure is to replace one node of MPE HA cluster. Base level software is confirmed. Camiant initial configuration is restored from a server backup file or manually. Then the new node is allowed to re-sync to the existing node to form a complete MPE cluster. Required resources: - Replacement node hardware - TPD installation ISO - MPE Policy Management Application installation ISO. - *serverbackup.ISO* of the node to be replaced (optional)
2. □	Prerequisites	1. Remove failed hardware and replace. 2. Verify that the node has TPD on it, or install TPD 3. Install the correct version of the application software – CMP 4. Cable as per network requirements See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions on installing TPD and the MPE Application. This procedure can also be used to confirm Bios, Firmware and iLO settings.
3. □	Set the failed node to Forced Standby	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → All Clusters** 1. Determine the cluster with the failed node 2. Determine the failed node and make sure it is on standBy state 3. Click **Modify** for the failed node 4. Select **Forced Standby**, then click **Save**.  Topology Settings All Clusters CMP Site1 Cluster MA MPE9-4 Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings Name MPE9-4 Appl Type MPE HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.199 / 27 Signaling VIP 1 10.240.239.231 / 28 (SIG-A) Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None Server-A IP 10.240.239.205 HostName MPE-1 Forced Standby No Status active Server-B IP 10.240.239.200 HostName MPE-2 Forced Standby Yes Status out-of-service

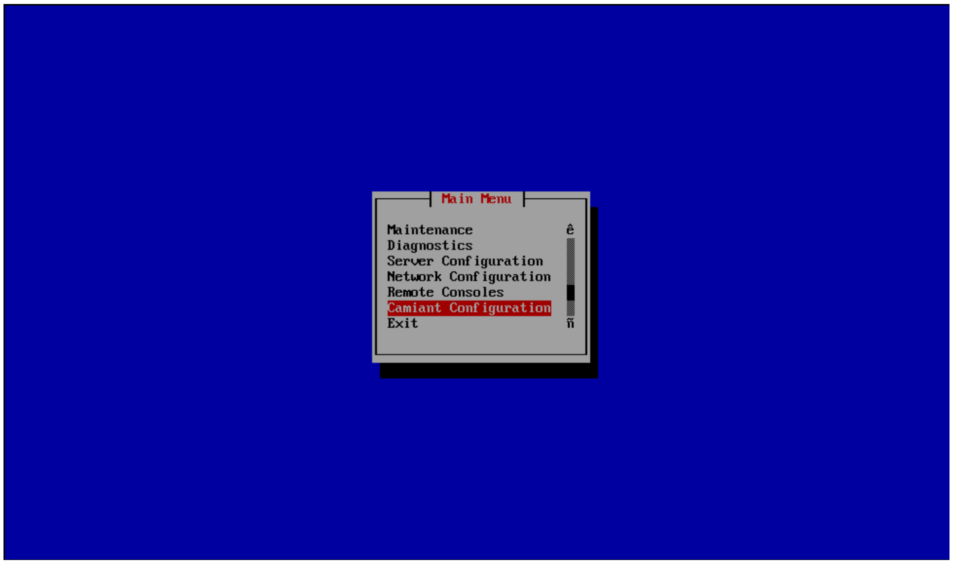
Step	Procedure	Instructions
4. □	Load the ISO for server restore	If a server backup is available proceed with this step. **If a server backup is not available skip to step 11.** Obtain the *serverbackup.iso* for the node to be restored. When the replacement node is available (TPD/App installation complete, cabled as per network requirements), the server backup file should be copied to the following directory: `/var/camiant/backup/local_archive/serverbackup.` **NOTE:** Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu. The platcfg utility also allows the user to manually enter any mounted path on the server. See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions accessing the iLO, launching the remote console.
5. □	Login via the iLO Interface	Access the iLO Interface and launch the remote console to gain root level access to the cli

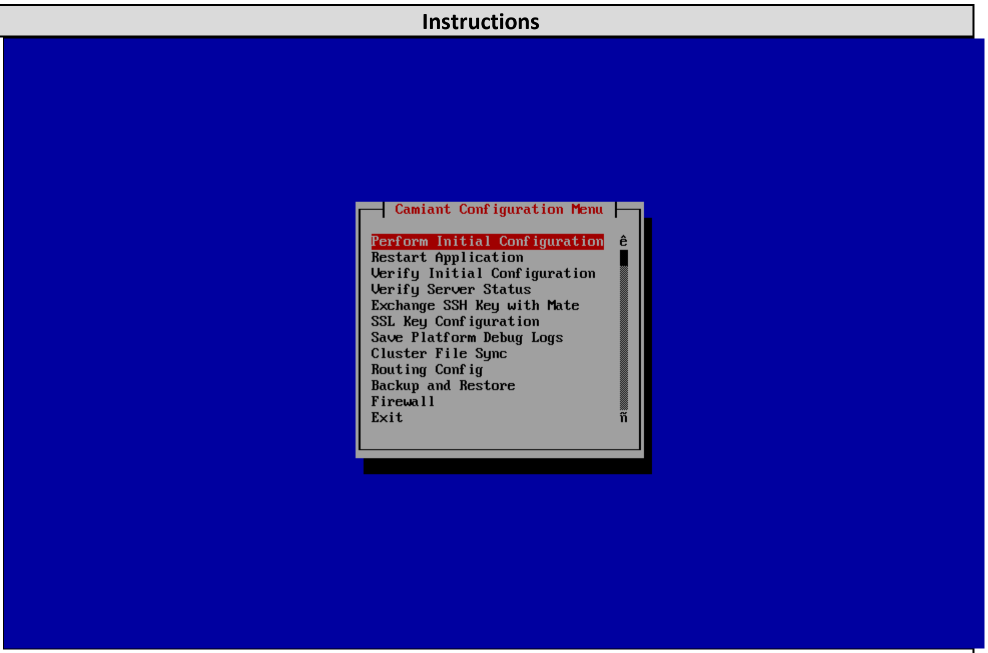
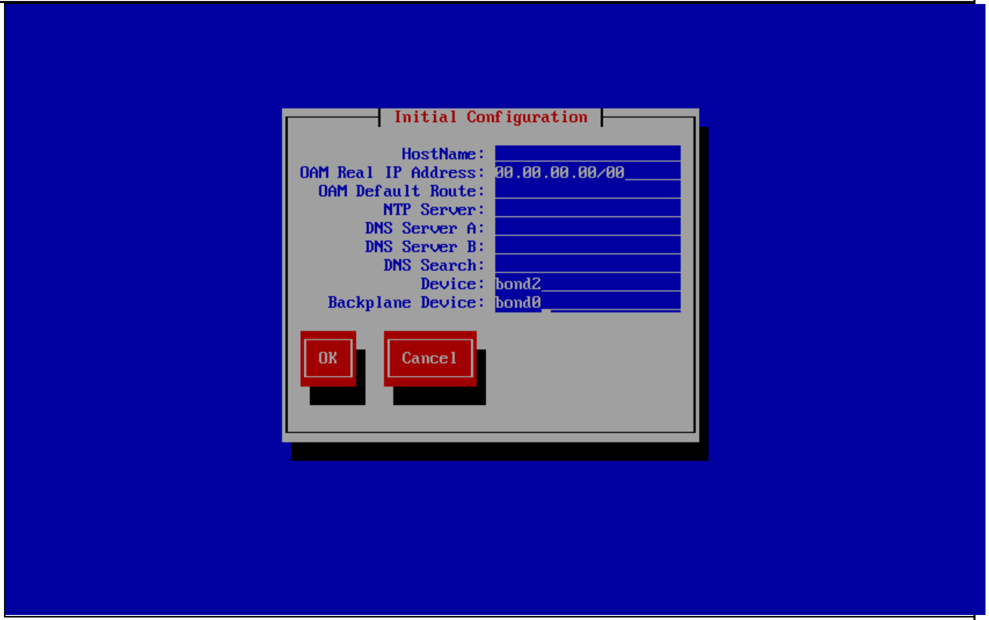
Step	Procedure	Instructions
6. □	Perform platcfg restore from iLO remote console	1. Run the following command `# su – platcfg` 2. From within the platcfg utility, navigate to: **Camiant Configuration → Backup and Restore → Server Restore** 3. Select the *serverbackup*.ISO that you just put on the system and click **OK**  Hostname: MPE-2 Select iso to restore from iso to restore: (*) MPE-2-mpe_9.4.0_40.2.0-serverbackup-201401030905.iso ( ) Manually input Manually input: 4. Click **Yes** to confirm.  Hostname: MPE-2 Confirm restore You are going to restore the system files. Continue? **NOTE:** This may take a couple of minutes.

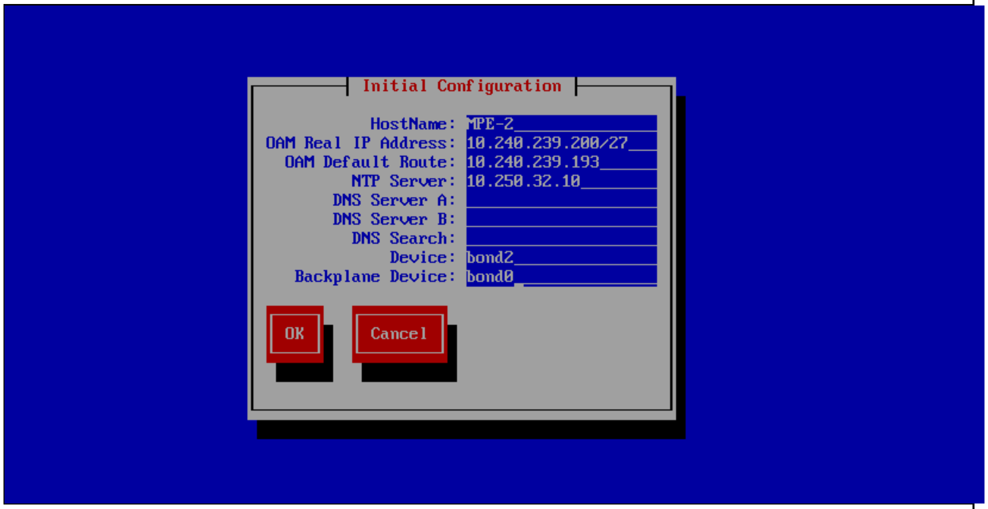
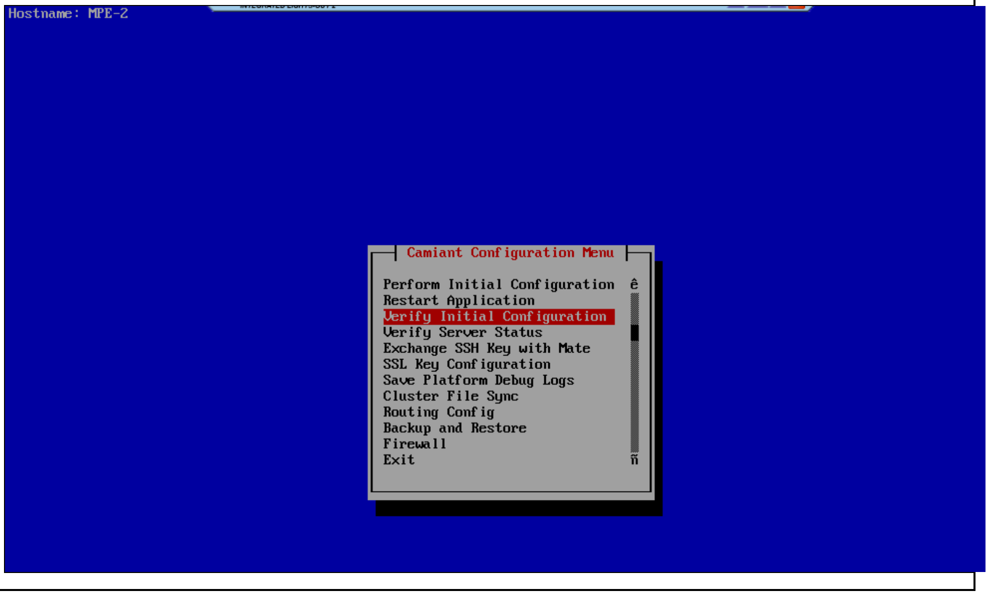
Step	Procedure	Instructions
7. □	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding:  Hostname: MPE-2 Message Restored from iso /var/camiant/backup/local_archive/serverbackup/MPE-2-mpe_9.4.0_40.2.0-serverbackup-201401030905.iso successfully Press any key to continue...
8. □	Reboot the server	Exit form the platcfg menu and reboot from the command line. `‘shutdown -r now’`
9. □	Verify Config	After the server has been rebooted you are returned to a login prompt via the iLO remote console. Verify the configuration by selecting **Camiant Configuration → Verify Initial Configuration** from within the platcfg utility.  Hostname: MPE-2 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Save Platform Debug Logs Cluster File Sync Routing Config Backup and Restore Firewall Exit

Step	Procedure	Instructions

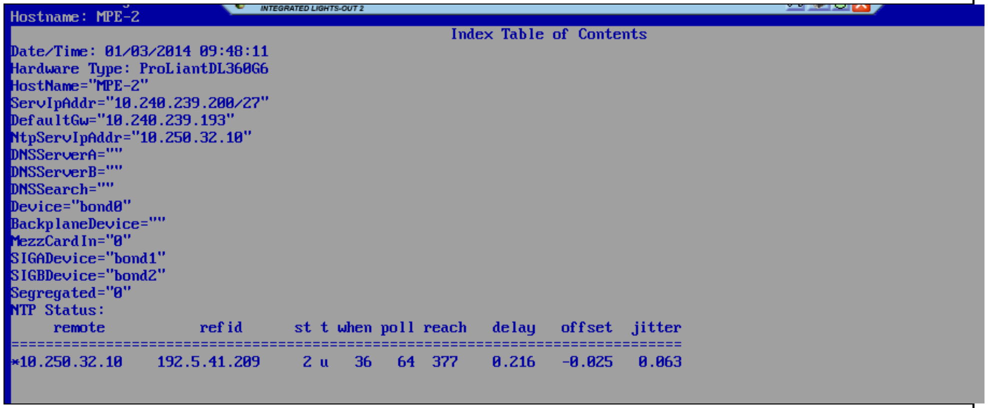
10. □	Verify Config	Confirm the configured Hostname, ServIpAddr, DefaultGw and NtpServIpAddr previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.
		
		`Hostname: MPE-2`
		`Index Table of Contents`
		`Date/Time: 01/03/2014 09:36:36`
		`Hardware Type: ProLiantDL360G6`
		`HostName="MPE-2"`
		`ServIpAddr="10.240.239.200/27"`
		`DefaultGw="10.240.239.193"`
		`NtpServIpAddr="10.250.32.10"`
		`DNSServerA=""`
		`DNSServerB=""`
		`DNSSearch=""`
		`Device="bond0"`
		`BackplaneDevice=""`
		`MezzCardIn="0"`
		`SIGADevice="bond1"`
		`SIGBDevice="bond2"`
		`Segregated="0"`
		`NTP Status:`
		`     remote           refid      st t when poll reach   delay   offset  jitter`
		`==============================================================================`
		`*10.250.32.10    192.5.41.40      2 u   50   64  377    0.252    0.064   0.036`
		Skip to step 21

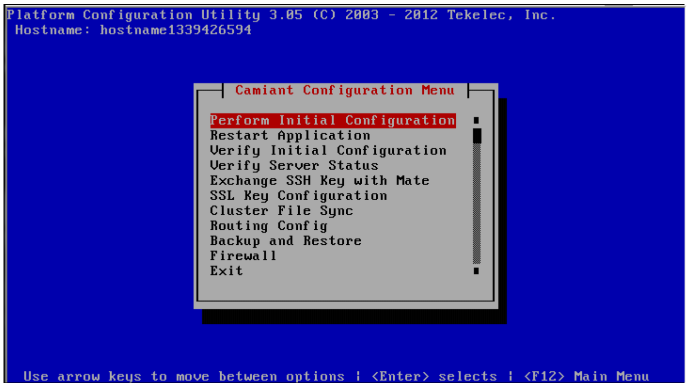
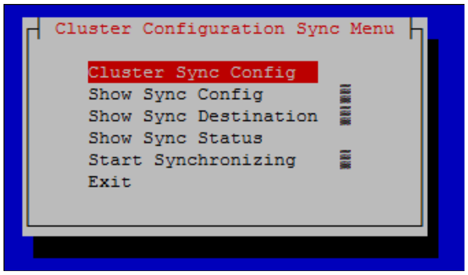
11. □	Perform Camiant Initial Configuration using platcfg	If directed to this step because a server backup is not available, then the following steps can be used perform the Initial Configuration based on network information available and a cluster file sync. The following steps can also be found in *Oracle Communications Policy Management Bare Metal Installation Guide.* **NOTE:** Customer provided data is required to perform the Camaint Initial Configuration in step 15.
12. □	Run platcfg tool on the replacement server	The failed sever in the HA cluster has already been placed in forced standby as per step 3. The replacement server is in place and has had the base software already installed. Launch the remote console using the iLO interface. `# su - platcfg` When presented with following screen select **Camiant Configuration**.  Main Menu Maintenance Diagnostics Server Configuration Network Configuration Remote Consoles Camiant Configuration Exit

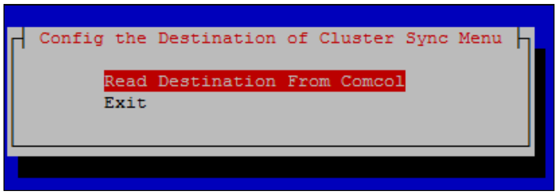
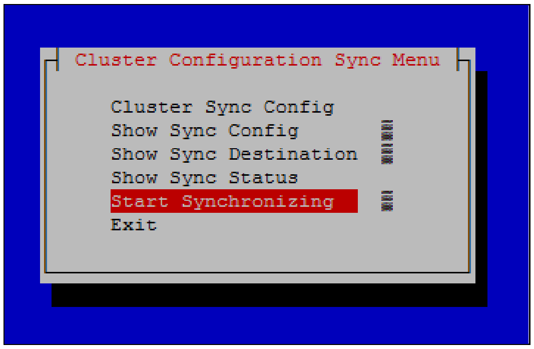
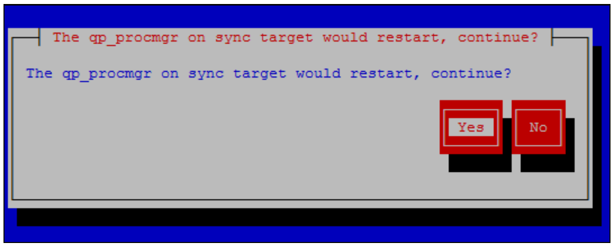
Step	Procedure	Instructions
13. □	Select **Perform Initial Configuration**	 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Save Platform Debug Logs Cluster File Sync Routing Config Backup and Restore Firewall Exit
14. □	Complete Initial Configuration form	Initial Configuration HostName: OAM Real IP Address: 00.00.00.00/00 OAM Default Route: NTP Server: DNS Server A: DNS Server B: DNS Search: Device: bond2 Backplane Device: bond0 • **Hostname** - the unique hostname for the device being configured. • **OAM Real IP Address** - the IP address that is permanently assigned to this device (sometimes called Physical IP or Real IP). • **OAM Default Route** - the default route of the OAM network. • **NTP Server** - a reachable NTP (required) • **DNS Server A** - a reachable DNS server (optional) • **DNS Server** B - a reachable DNS server (optional) • **DNS Search** - is a directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out a DNS query. • **Device** - the bond interface of the OAM device. Note that the default value should be used, as changing this value is not supported. • **Backplane Device** – the bond interface of the backplane device Note that the default value should be used, as changing this value is not supported.

Step	Procedure	Instructions
15. □	Save configuration	Enter the configuration (example data fill below) and then click **OK**.  Initial Configuration HostName: MPE-2 OAM Real IP Address: 10.240.239.200/27 OAM Default Route: 10.240.239.193 NTP Server: 10.250.32.10 DNS Server A: DNS Server B: DNS Search: Device: bond2 Backplane Device: bond0 The platcfg form will pause for a minute while the server is configured, and then return to the platcfg menu.
16. □	Verify Config	After the server has been rebooted you should be returned to a login prompt via the iLO remote console. Verify the configuration by selecting **Camiant Configuration → Verify Initial Configuration** from within the platcfg utility.  Hostname: MPE-2 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Save Platform Debug Logs Cluster File Sync Routing Config Backup and Restore Firewall Exit

Step	Procedure	Instructions

17. □	Verify Config	Confirm the configured Hostname, ServIpAddr, DefaultGw, and NtpServIpAddr previously configured are present. A display similar to the following is shown.
		
		Hostname: MPE-2
		INTEGRATED LIGHTS-OUT 2
		Index Table of Contents
		Date/Time: 01/03/2014 09:48:11
		Hardware Type: ProLiantDL360G6
		HostName="MPE-2"
		ServIpAddr="10.240.239.200/27"
		DefaultGw="10.240.239.193"
		NtpServIpAddr="10.250.32.10"
		DNSServerA=""
		DNSServerB=""
		DNSSearch=""
		Device="bond0"
		BackplaneDevice=""
		MezzCardIn="0"
		SIGADevice="bond1"
		SIGBDevice="bond2"
		Segregated="0"
		NTP Status:
		remote refid st t when poll reach delay offset jitter
		==
		*10.250.32.10 192.5.41.209 2 u 36 64 377 0.216 -0.025 0.063

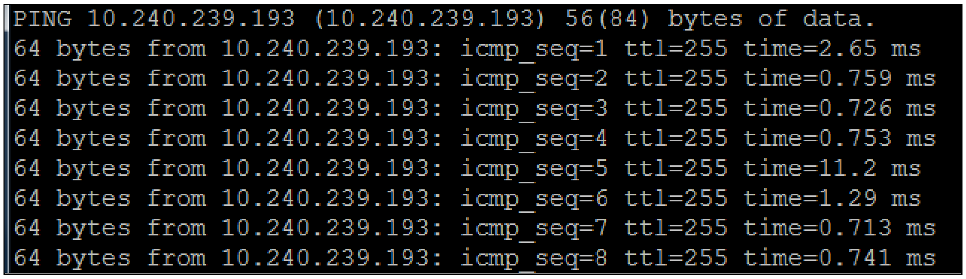
18. □	Reboot the server	Exit from the platcfg menu and Reboot from the command line. **'shutdown –r now '**
19. □	Perform Cluster sync from **the active server to the replacement server**	Cluster file sync will copy over any firewall rules, static routes and scecurity certificates that may have been configured manually on the active node and need to copied to the replacement server. 1. From the platcfg menu naviagte to **Camiant Configuration → Cluster File**.  Platform Configuration Utility 3.05 (C) 2003 - 2012 Tekelec, Inc. Hostname: hostname1339426594 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Cluster File Sync Routing Config Backup and Restore Firewall Exit Use arrow keys to move between options ¦ <Enter> selects ¦ <F12> Main Menu 2. Select **Cluster Sync Config**  Cluster Configuration Sync Menu Cluster Sync Config Show Sync Config Show Sync Destination Show Sync Status Start Synchronizing Exit

Step	Procedure	Instructions
20. □	Perform Cluster sync from the active server to the replacement server	1. Select **Read Destination From Comcol**.  Config the Destination of Cluster Sync Menu Read Destination From Comcol Exit You may need to provide the root password to proceed 2. Select **Start Synchronizong**  Cluster Configuration Sync Menu Cluster Sync Config Show Sync Config Show Sync Destination Show Sync Status Start Synchronizing Exit  The qp_procmgr on sync target would restart, continue? The qp_procmgr on sync target would restart, continue? 3. Click through the synchronizing screens until you are returned to Cluster Configuration Sync menu. 4. You can now log into the replacement server and confirm the files have synced to the replacement server. You may check the ssl keystore for example.

<table>
<tr><th>Step</th><th>Procedure</th><th>Instructions</th></tr>
<tr><td>**21.** □</td><td>Verify basic network connectivity and server health on the replacement server</td><td>

1. From the newly installed server, ping the OAM gateway.

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

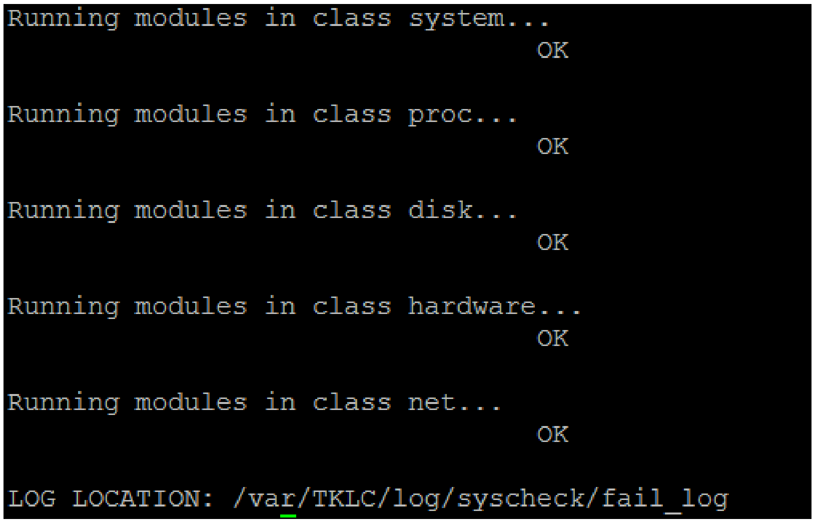


```
PING 10.240.239.193 (10.240.239.193) 56(84) bytes of data.
64 bytes from 10.240.239.193: icmp_seq=1 ttl=255 time=2.65 ms
64 bytes from 10.240.239.193: icmp_seq=2 ttl=255 time=0.759 ms
64 bytes from 10.240.239.193: icmp_seq=3 ttl=255 time=0.726 ms
64 bytes from 10.240.239.193: icmp_seq=4 ttl=255 time=0.753 ms
64 bytes from 10.240.239.193: icmp_seq=5 ttl=255 time=11.2 ms
64 bytes from 10.240.239.193: icmp_seq=6 ttl=255 time=1.29 ms
64 bytes from 10.240.239.193: icmp_seq=7 ttl=255 time=0.713 ms
64 bytes from 10.240.239.193: icmp_seq=8 ttl=255 time=0.741 ms
```

If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact Oracle support before proceeding if network ping tests still fail.

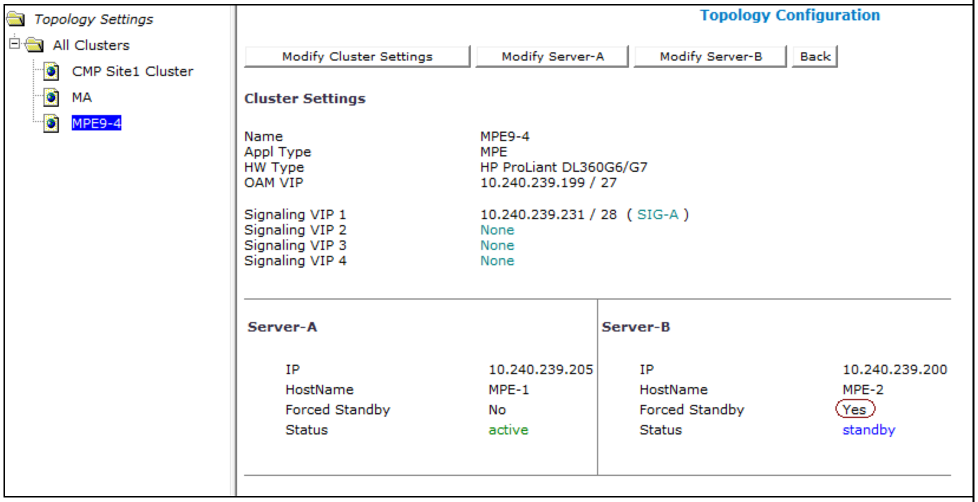
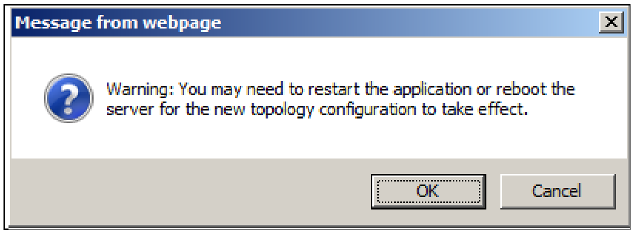
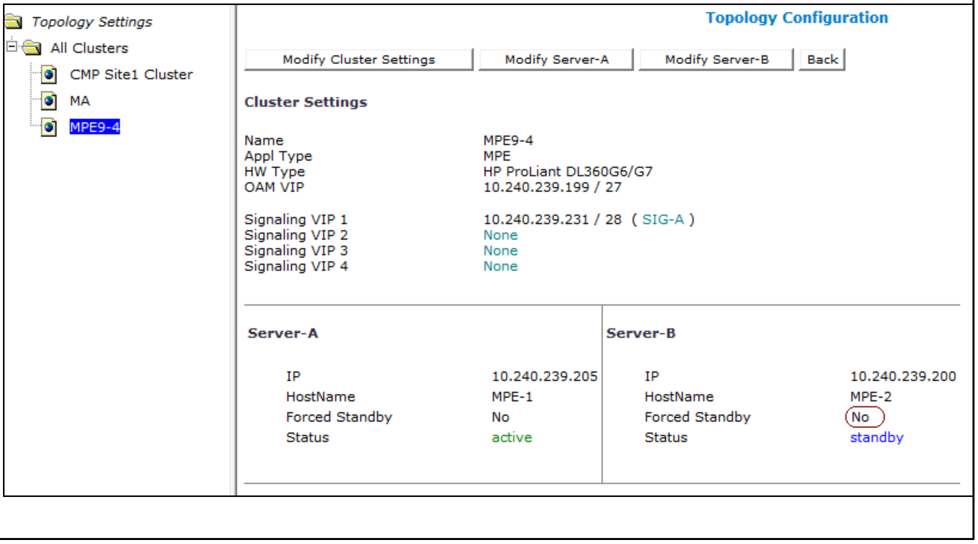
2. Run the syscheck command, ensuring that all tests return successfully.

If errors are found, discontinue this procedure and contact Oracle support.



```
Running modules in class system...
                                 OK

Running modules in class proc...
                                 OK

Running modules in class disk...
                                 OK

Running modules in class hardware...
                                 OK

Running modules in class net...
                                 OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

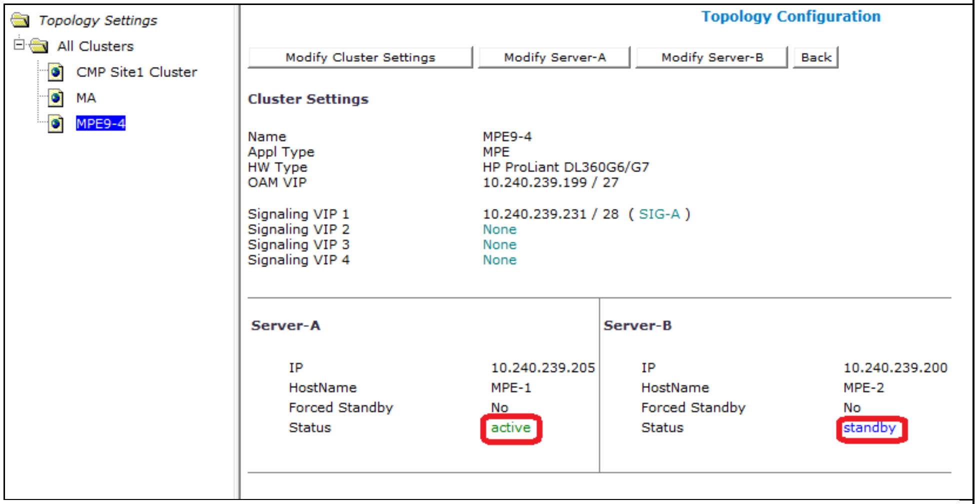
</td></tr>
</table>

Step	Procedure	Instructions
22. □	Remove Forced Standby designation on current node.	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → Current Cluster**  Topology Settings All Clusters CMP Site1 Cluster MA MPE9-4 Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back **Cluster Settings** Name MPE9-4 Appl Type MPE HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.199 / 27 Signaling VIP 1 10.240.239.231 / 28 (SIG-A) Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None **Server-A** IP 10.240.239.205 HostName MPE-1 Forced Standby No Status active **Server-B** IP 10.240.239.200 HostName MPE-2 Forced Standby Yes Status standby 1. Modify for the server that has forced standby. 2. Ensure server status is standby. 3. Clear the Forced Standby checkbox 4. Accept the resulting pop-up by clicking **OK**.  **Message from webpage** Warning: You may need to restart the application or reboot the server for the new topology configuration to take effect. 5. Click **Save**  Topology Settings All Clusters CMP Site1 Cluster MA MPE9-4 Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back **Cluster Settings** Name MPE9-4 Appl Type MPE HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.199 / 27 Signaling VIP 1 10.240.239.231 / 28 (SIG-A) Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None **Server-A** IP 10.240.239.205 HostName MPE-1 Forced Standby No Status active **Server-B** IP 10.240.239.200 HostName MPE-2 Forced Standby No Status standby

<table>
<tr><th>Step</th><th>Procedure</th><th>Instructions</th></tr>
<tr><td><b>23.</b> □</td><td>Verify cluster status</td><td>In the CMP GUI, navigate to:

<b>Platform Setting → Topology Setting → All → Current CMP Cluster</b>

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 (except for the Accept new upgrade alarm which will be cleared at the end of this procedure.



<b>Cluster Settings</b>

Name MPE9-4
Appl Type MPE
HW Type HP ProLiant DL360G6/G7
OAM VIP 10.240.239.199 / 27

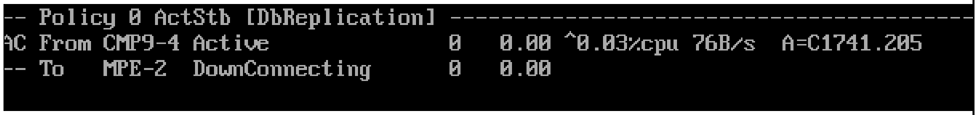
Signaling VIP 1 10.240.239.231 / 28 (SIG-A)
Signaling VIP 2 None
Signaling VIP 3 None
Signaling VIP 4 None

<b>Server-A</b>
IP 10.240.239.205
HostName MPE-1
Forced Standby No
Status active

<b>Server-B</b>
IP 10.240.239.200
HostName MPE-2
Forced Standby No
Status standby</td></tr>
<tr><td><b>24.</b> □</td><td>Alternative method to check status</td><td>You can also monitor the clustering of the new node from within the shell on the active server node with <code>irepstat</code>. To do so, SSH to the Active node of the current cluster and Run the <code>irepstat</code> command:

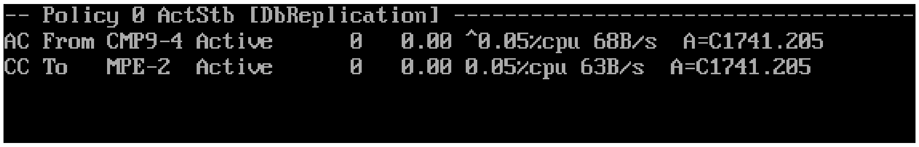
<pre>
# irepstat
</pre>

Expected <code>irepstat</code> output while waiting reconnection:



<pre>
-- Policy 0 ActStb [DbReplication] --
AC From CMP9-4 Active   0   0.00 ^0.03%cpu 76B/s A=C1741.205
-- To   MPE-2 DownConnecting   0   0.00
</pre>

Expected <code>irepstat</code> output after cluster has formed:



<pre>
-- Policy 0 ActStb [DbReplication] -----------------------------------
AC From CMP9-4 Active   0   0.00 ^0.05%cpu 68B/s A=C1741.205
CC To   MPE-2 Active   0   0.00 0.05%cpu 63B/s A=C1741.205
</pre></td></tr>
<tr><td colspan="3"><b>THIS PROCEDURE HAS BEEN COMPLETED</b></td></tr>
</table>

5.3 Procedure 3. Restoring Complete Cluster Outage of the CMP

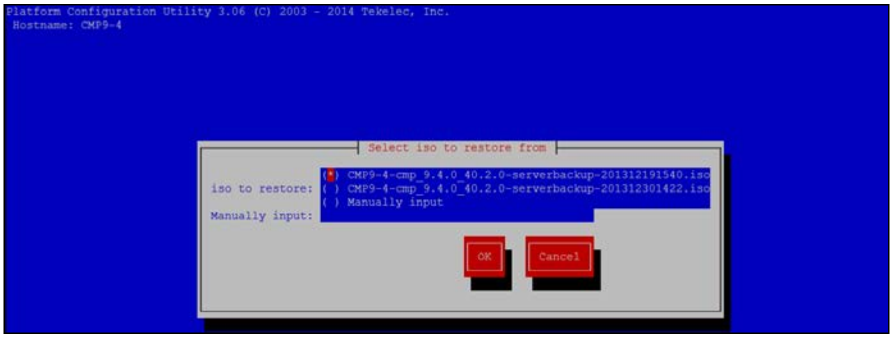
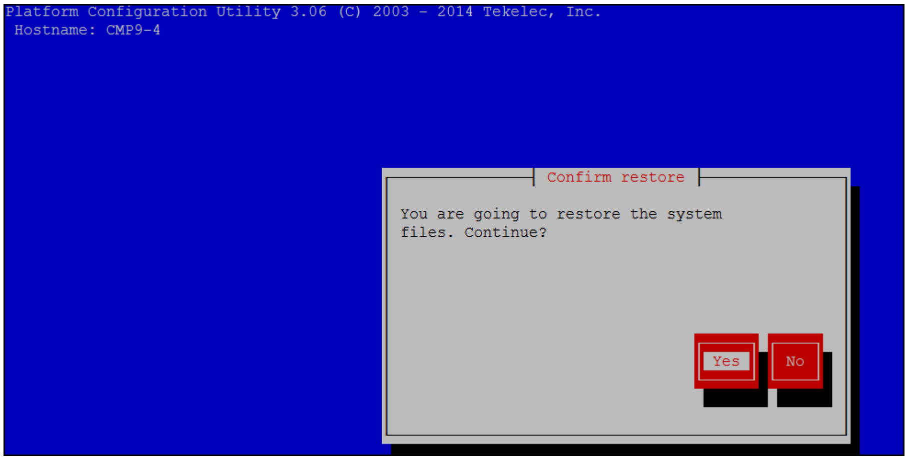
This Procedure performs Restoring CMP cluster with system backup available

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

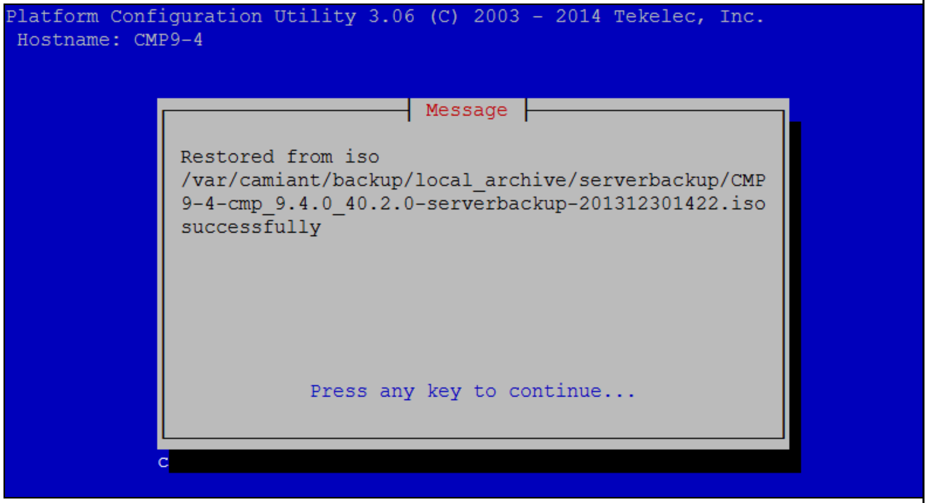
Should this procedure fail, contact the Oracle Customer Care Center and ask for assistance.

If no backup files are available, the only option is to rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually. In this case the replacements servers will be considered as new installs. To review the procedures required for new installs refer to document *Policy 9.4 Installation Procedure*.

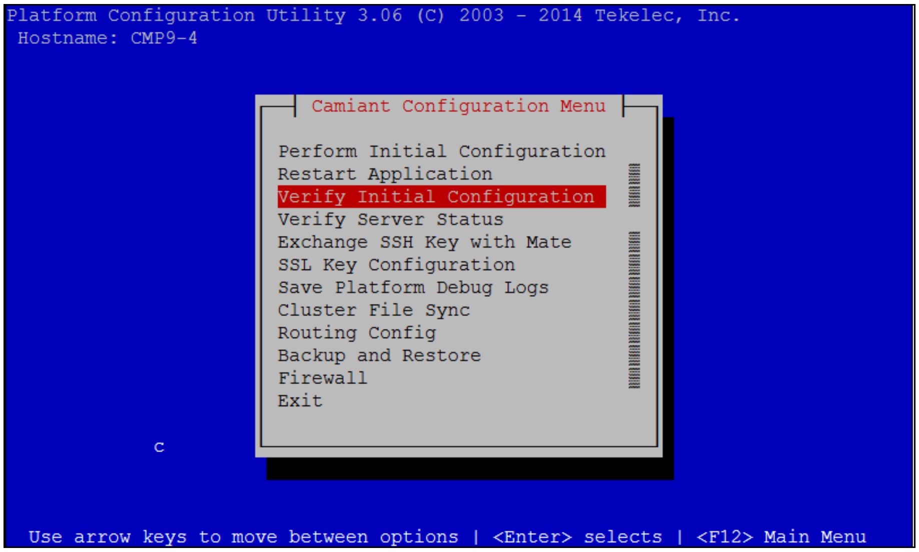
STEP	Procedure	Instructions
1. □	Required resources / information	The purpose of this procedure is to re-create a CMP cluster with the application level configuration of the policy network (**System Backup**) that can be used to re-create the policy network that is to be recovered. Once a CMP is online, all other servers of the policy network can be re-created using the procedures described in this document and will have their application level configuration restored from this CMP. In the case of a massive outage that has resulted in a failure of the entire CMP cluster, at least one of the CMP nodes should be restored first. Required resources: • Replacement node hardware • TPD installation ISO • CMP Policy Application installation ISO. • *serverbackup.ISO* of both nodes in the CMP HA cluster to be replaced or Initial configuration information about the node to be restored • * systembackup* in case server backup is not available Intial Configuration Information: • OAM IP address, default gateway, NTP & SNMP server IP addresses • Hostname and any static routes required
2. □	Prerequisites	1. Remove failed hardware and replace. 2. Verify that that each node has TPD on it, or install TPD 3. Install the correct version of the application software – CMP 4. Cable as per network requirements See the *Oracle Communications Policy Management Bare Metal Installation Guide e* for directions on installing TPD and the CMP Application. This procedure can also be used to confirm Bios, Firmware and iLO settings
3. □	Load the ISO for server restore	If a server backup is available proceed with this step. **If a server backup is not available skip to step 10.** Obtain the *serverbackup.iso* for the first node to be restored. When the replacement node is available (TPD/App installation complete, cabled as per network requirements), the server backup file should be copied to the following directory: `/var/camiant/backup/local_archive/serverbackup.` **NOTE:** Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu. The platcfg utility also allows the user to manually enter any mounted path on the server. See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions accessing the iLO, launching the remote console.
4. □	Login via the iLO Interface	Access the iLO Interface and launch the remote console to gain root level access to the cli

STEP	Procedure	Instructions
5. □	Perform platcfg restore from iLO session to replacement node	1. Run the following command `# su – platcfg` 2. From within the platcfg utility, navigate to: **Camiant Configuration → Backup and Restore → Server Restore** 3. Select the *serverbackup*.ISO that you just put on the system. 4. Click **OK.** Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc. Hostname: CMP9-4 Select iso to restore from iso to restore: (*) CMP9-4-cmp_9.4.0_40.2.0-serverbackup-201312191540.iso ( ) CMP9-4-cmp_9.4.0_40.2.0-serverbackup-201312301422.iso ( ) Manually input Manually input: 5. Click **Yes** to confirm. Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc. Hostname: CMP9-4 Confirm restore You are going to restore the system files. Continue? **NOTE:** This may take a couple of minutes.

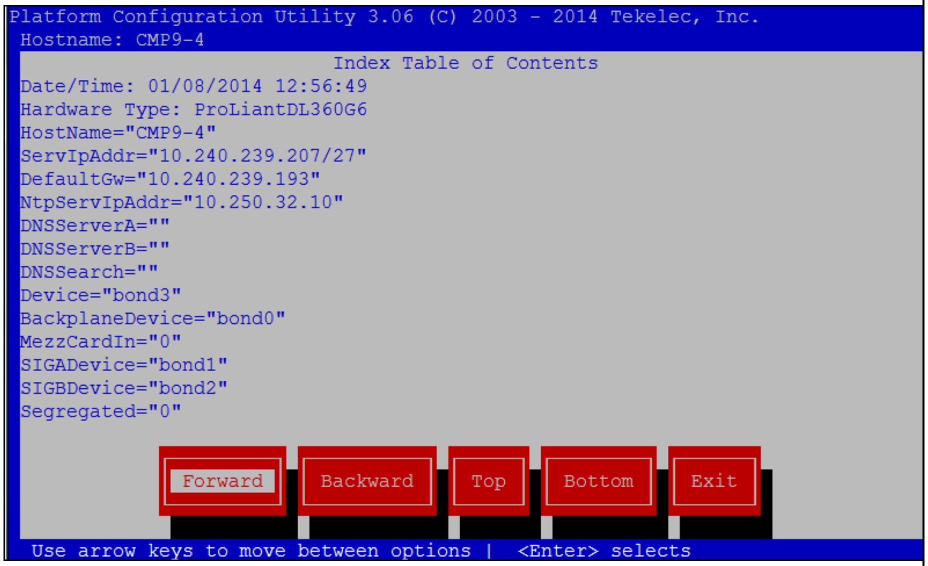
STEP	Procedure	Instructions

6. □	Verify the status	If the restore is successful, then exit from the backup and restore menu.
		If it is not successful, retry the restore.
		If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding:
		
		`Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc.`
		`Hostname: CMP9-4`
		`Message`
		`Restored from iso /var/camiant/backup/local_archive/serverbackup/CMP9-4-cmp_9.4.0_40.2.0-serverbackup-201312301422.iso successfully`
		`Press any key to continue...`
		`c`

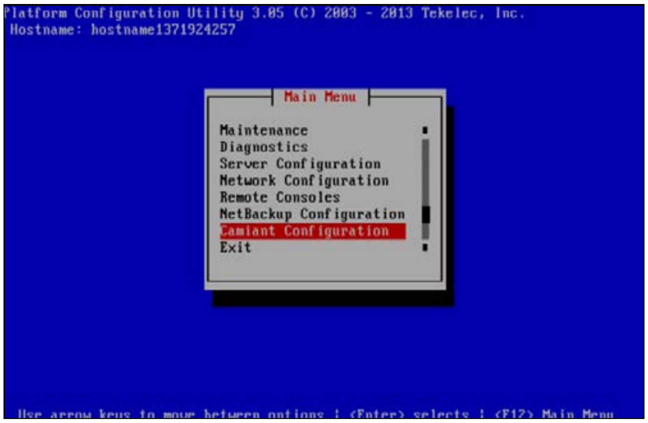
7. □	Reboot the server	Exit form the platcfg menu and Reboot from the command line. **`shutdown -r now`**

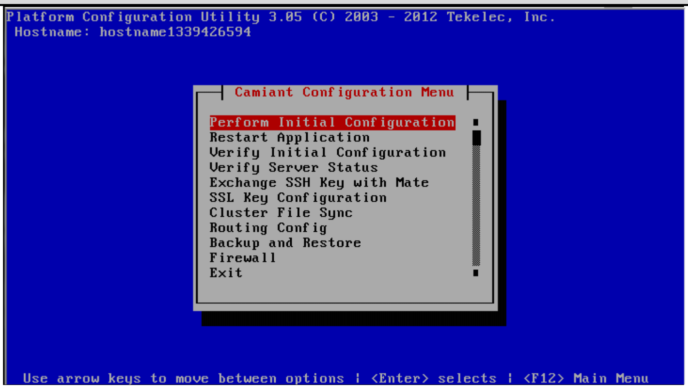
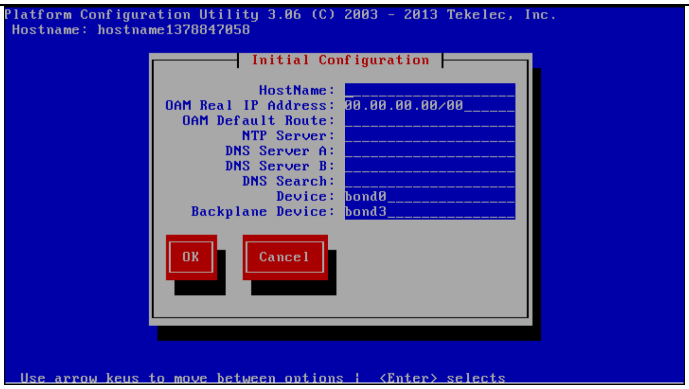
8. □	Verify Config	After the server has been rebooted you should be returned to a login prompt via the iLO remote console. Verify the configuration by selecting **Camiant Configuration → Verify Initial Configuration** from within the platcfg utility.
		
		`Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc.`
		`Hostname: CMP9-4`
		 Camiant Configuration Menu
		Perform Initial Configuration
		Restart Application
		Verify Initial Configuration
		Verify Server Status
		Exchange SSH Key with Mate
		SSL Key Configuration
		Save Platform Debug Logs
		Cluster File Sync
		Routing Config
		Backup and Restore
		Firewall
		Exit
		`c`
		`Use arrow keys to move between options | <Enter> selects | <F12> Main Menu`

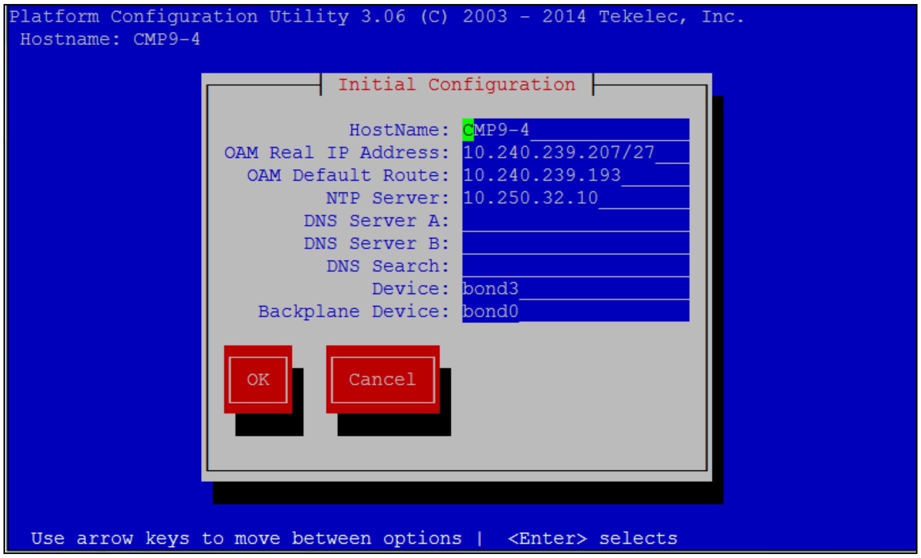
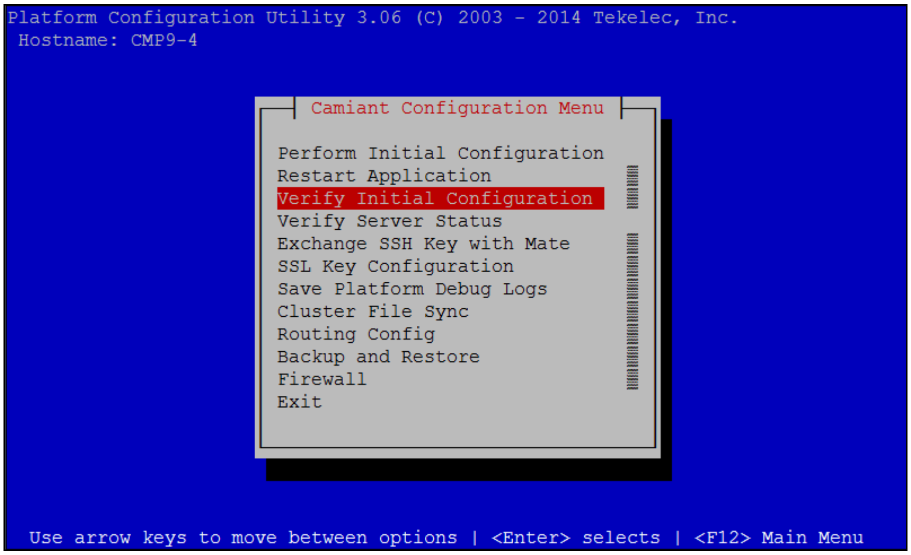
STEP	Procedure	Instructions

9. □	Verify Config	Confirm the configured Hostname, ServIpAddr, DefaultGw, and NtpServIpAddr previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.
		
		`Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc.`
		`Hostname: CMP9-4`
		`Index Table of Contents`
		`Date/Time: 01/08/2014 12:56:49`
		`Hardware Type: ProLiantDL360G6`
		`HostName="CMP9-4"`
		`ServIpAddr="10.240.239.207/27"`
		`DefaultGw="10.240.239.193"`
		`NtpServIpAddr="10.250.32.10"`
		`DNSServerA=""`
		`DNSServerB=""`
		`DNSSearch=""`
		`Device="bond3"`
		`BackplaneDevice="bond0"`
		`MezzCardIn="0"`
		`SIGADevice="bond1"`
		`SIGBDevice="bond2"`
		`Segregated="0"`
		
		`Use arrow keys to move between options | <Enter> selects`
		Skip to step 18

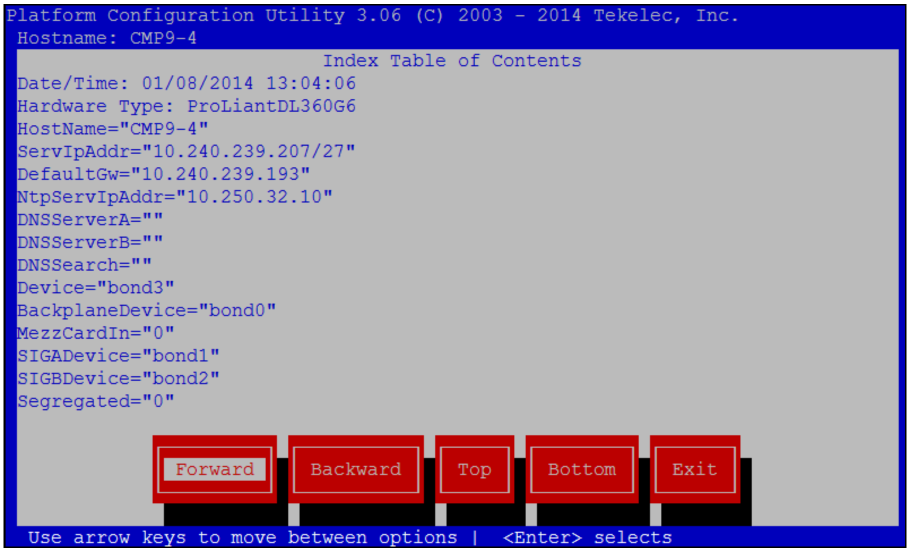
10. □	Perform Camiant Initial Configuration using platcfg	If directed to this step because a server backup is not available, then the following steps can be used perform the Initial Configuration based on network information available. The following steps can also be found in the *Oracle Communications Policy Management Bare Metal Installation Guide.* **NOTE:** Customer provided data is required to perform the Camaint Initial Configuration in step 14.

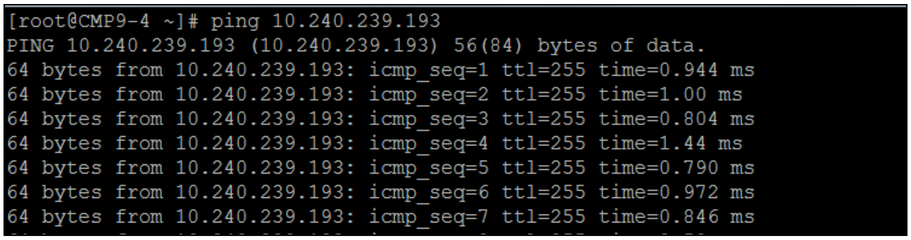
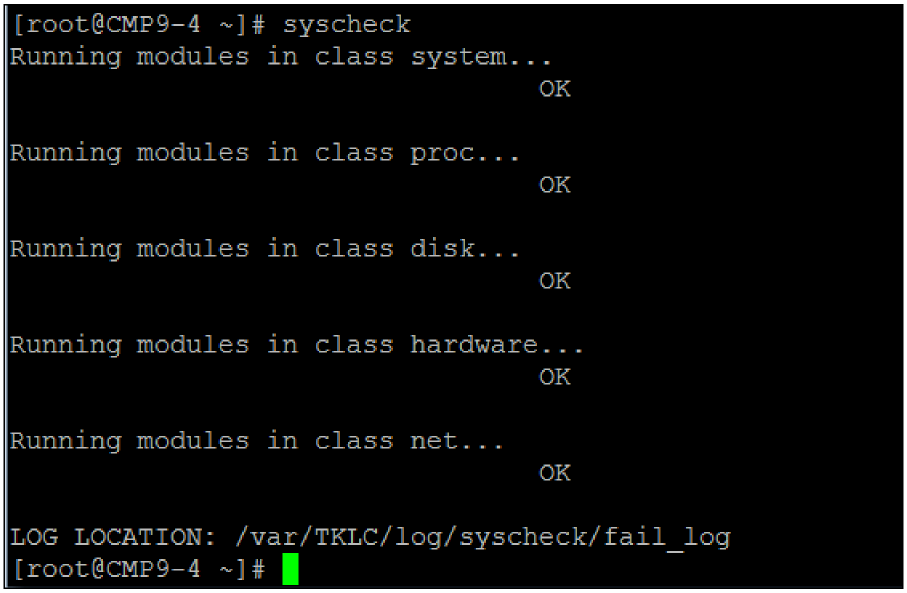
11. □	Run platcfg tool on the first replacement server	The replacement server is in place and has had the base software already installed. Launch the remote console using the iLO interface.
		`# su - platcfg`
		When presented with following screen select **Camiant Configuration**.
		
		`Platform Configuration Utility 3.05 (C) 2003 - 2013 Tekelec, Inc.`
		`Hostname: hostname1371924257`
		 Main Menu
		Maintenance
		Diagnostics
		Server Configuration
		Network Configuration
		Remote Consoles
		NetBackup Configuration
		Camiant Configuration
		Exit
		`Use arrow keys to move between options | <Enter> selects | <F12> Main Menu`

STEP	Procedure	Instructions
12. □	Select **Perform Initial Configuration**	 Platform Configuration Utility 3.05 (C) 2003 - 2012 Tekelec, Inc. Hostname: hostname1339426594 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Cluster File Sync Routing Config Backup and Restore Firewall Exit Use arrow keys to move between options | <Enter> selects | <F12> Main Menu
13. □	Complete Initial Configuration form	 Platform Configuration Utility 3.06 (C) 2003 - 2013 Tekelec, Inc. Hostname: hostname1378847058 Initial Configuration HostName: OAM Real IP Address: 00.00.00.00/00 OAM Default Route: NTP Server: DNS Server A: DNS Server B: DNS Search: Device: bond0 Backplane Device: bond3 Use arrow keys to move between options | <Enter> selects • **Hostname** - the unique hostname for the device being configured. • **OAM Real IP Address** - the IP address that is permanently assigned to this device. (Sometimes called Physical IP or Real IP). • **OAM Default Route** - the default route of the OAM network. • **NTP Server** - a reachable NTP (required) • **DNS Server A** - a reachable DNS server (optional) • **DNS Server B** - a reachable DNS server (optional) • **DNS Search** - is a directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out a DNS query. • **Device** - the bond interface of the OAM device. Note that the default value should be used, as changing this value is not supported. • **Backplane Device** – the bond interface of the backplane device Note that the default value should be used, as changing this value is not supported.

STEP	Procedure	Instructions
14. □	Save configuration	Enter the configuration (example data fill below) and then select **OK**  Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc. Hostname: CMP9-4 Initial Configuration HostName: CMP9-4 OAM Real IP Address: 10.240.239.207/27 OAM Default Route: 10.240.239.193 NTP Server: 10.250.32.10 DNS Server A: DNS Server B: DNS Search: Device: bond3 Backplane Device: bond0 Use arrow keys to move between options | <Enter> selects The platcfg form will pause for a minute while the server is configured, and then return to the platcfg menu.
15. □	Reboot the server	Exit from the platcfg menu and Reboot from the command line. `‘shutdown –r now ‘`
16. □	Verify Config	After the server has been rebooted you should be returned to a login prompt via the iLO remote console Verify the configuration by selecting **Camiant Configuration → Verify Initial Configuration** from within the platcfg utility.  Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc. Hostname: CMP9-4 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Save Platform Debug Logs Cluster File Sync Routing Config Backup and Restore Firewall Exit Use arrow keys to move between options | <Enter> selects | <F12> Main Menu

STEP	Procedure	Instructions

17. □	Verify Config	Confirm the configured Hostname, ServIpAddr', DefaultGw and NtpServIpAddr previously configured are present. A display similar to the following is shown.
		
		Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc.
		Hostname: CMP9-4
		Index Table of Contents
		Date/Time: 01/08/2014 13:04:06
		Hardware Type: ProLiantDL360G6
		HostName="CMP9-4"
		ServIpAddr="10.240.239.207/27"
		DefaultGw="10.240.239.193"
		NtpServIpAddr="10.250.32.10"
		DNSServerA=""
		DNSServerB=""
		DNSSearch=""
		Device="bond3"
		BackplaneDevice="bond0"
		MezzCardIn="0"
		SIGADevice="bond1"
		SIGBDevice="bond2"
		Segregated="0"
		
		Use arrow keys to move between options | <Enter> selects

18. □	Verify basic network connectivity and server health **on the replacement server**	From the newly installed server, ping the OAM gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact Oracle support before proceeding if network ping tests still fail. `#ping <OAM gateway address>`  [root@CMP9-4 ~]# ping 10.240.239.193 PING 10.240.239.193 (10.240.239.193) 56(84) bytes of data. 64 bytes from 10.240.239.193: icmp_seq=1 ttl=255 time=0.944 ms 64 bytes from 10.240.239.193: icmp_seq=2 ttl=255 time=1.00 ms 64 bytes from 10.240.239.193: icmp_seq=3 ttl=255 time=0.804 ms 64 bytes from 10.240.239.193: icmp_seq=4 ttl=255 time=1.44 ms 64 bytes from 10.240.239.193: icmp_seq=5 ttl=255 time=0.790 ms 64 bytes from 10.240.239.193: icmp_seq=6 ttl=255 time=0.972 ms 64 bytes from 10.240.239.193: icmp_seq=7 ttl=255 time=0.846 ms Run the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Oracle support.  [root@CMP9-4 ~]# syscheck Running modules in class system... OK Running modules in class proc... OK Running modules in class disk... OK Running modules in class hardware... OK Running modules in class net... OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log [root@CMP9-4 ~]#

<table>
<tr><th>STEP</th><th>Procedure</th><th>Instructions</th></tr>
<tr><td>19. □</td><td>Proceed with System Restore</td><td>The initial configuration of the server should be restored at this point, either automatically using a Server Restore backup (as described in steps 3 through 9) or manually using platcfg Initial Configuration (as described in steps 10 through 19).</td></tr>
<tr><td>20. □</td><td>Load the tarball for <b>system restore</b></td><td>

Locate the most recent system backup to proceed with this step. The format of the system back up restore file will look something like this.

```
CMP9-4-cmp_9.4.0_40.2.0-systembackup-201401101139.tar.gz
```

The system backup file should be copied to the following directory:

```
/var/camiant/backup/local_archive/systembackup.
```

NOTE: Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu. The platcfg utility also allows the user to manually enter any mounted path on the server.

See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions accessing the iLO, launching the remote console.

</td></tr>
<tr><td>21. □</td><td>Perform platcfg - restore from SSH session to replacement server</td><td>

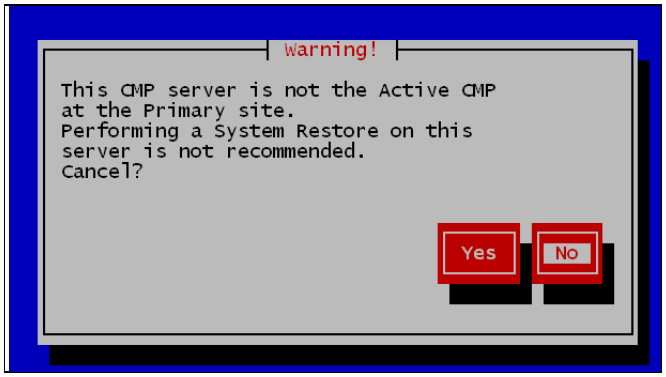
1. Run the following command

```
# su – platcfg
```

2. From within the platcfg utility, navigate to:

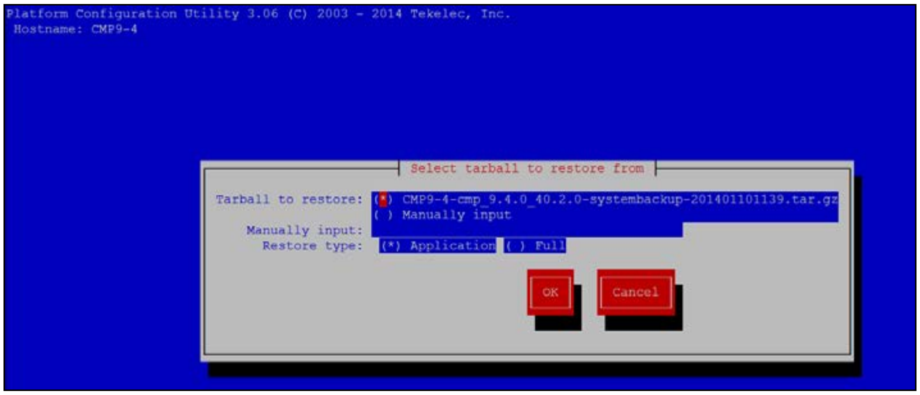
Camiant Configuration → Backup and Restore → System Restore

A message will appear prompting confirmation to restore even though this node is not recognized as the active member. This behavior is expected, continue by clicking **NO**.



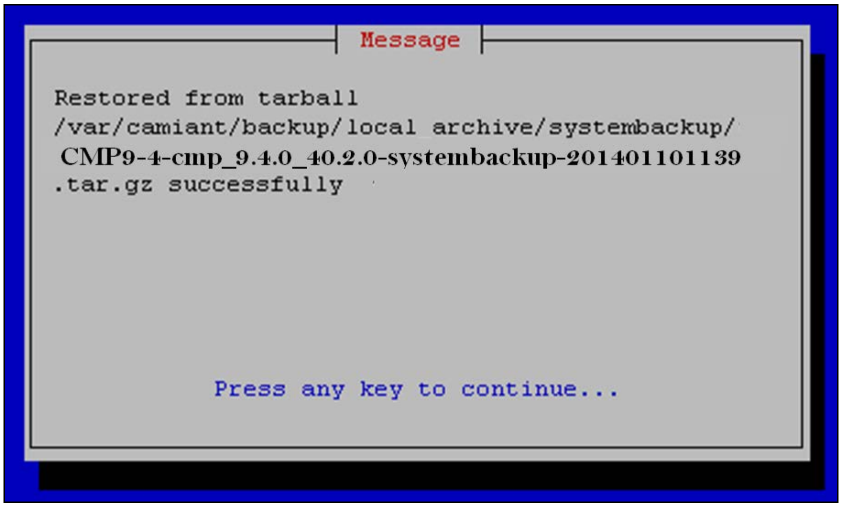
```
Warning!
This CMP server is not the Active CMP
at the Primary site.
Performing a System Restore on this
server is not recommended.
Cancel?
```

A screen appears asking you to select the file for the restore. If the file was copied correctly in the previous step, it will be shown here as an option, otherwise select **Manually input**, and then select **Full** for the Restore type and then click **OK** to proceed.



```
Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc.
 Hostname: CMP9-4

Select tarball to restore from

Tarball to restore: (*) CMP9-4-cmp_9.4.0_40.2.0-systembackup-201401101139.tar.gz
                    ( ) Manually input
   Manually input:
     Restore type:  (*) Application ( ) Full
```

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

STEP	Procedure	Instructions
22. □	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding:  Message Restored from tarball /var/camiant/backup/local archive/systembackup/ CMP9-4-cmp_9.4.0_40.2.0-systembackup-201401101139 .tar.gz successfully Press any key to continue...
23.	Reboot the server	Reboot. Allow the server time to reboot, then reconnect via SSH `#shutdown -r now`
24. □	Connect to the newly loaded replacement server with a browser	Using the OAM network ip address assigned during Camiant Intial Configuration (or from the server back file) connect with a browser to confirm the application configuration has been restored.
25. □	Restore the second replacement server	At this point, to recover the second server in the CMP HA cluster, it is only necessary to perform the steps to recover a single node failure as described in Section 5.1 Procedure 1. Restoring Single Node Failure in CMP HA Cluster Proceed to section 5.1 Procedure 1.
THIS PROCEDURE HAS BEEN COMPLETED		

5.4 Procedure 4. Restoring Complete Cluster Outage of the MPE

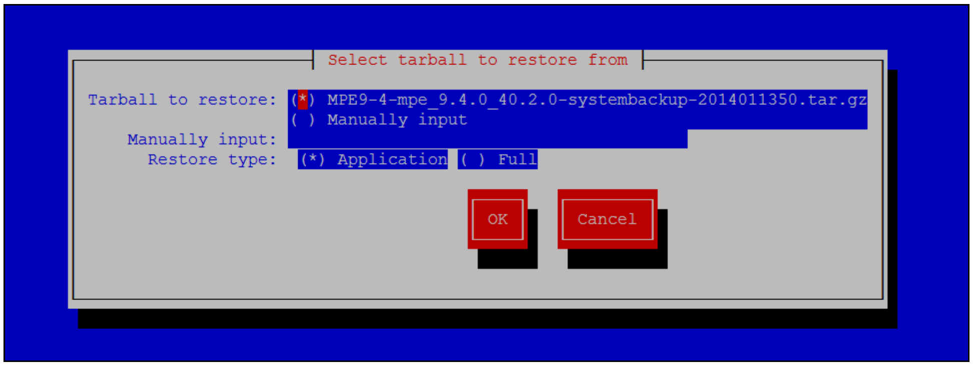
This Procedure performs Restoring a complete MPE cluster

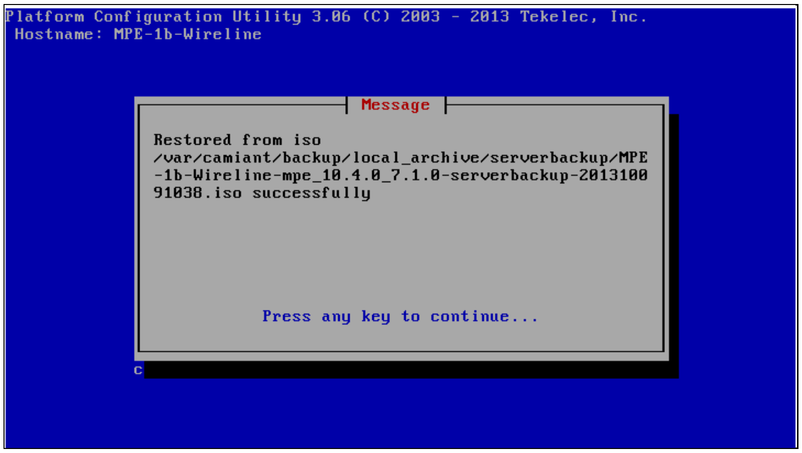
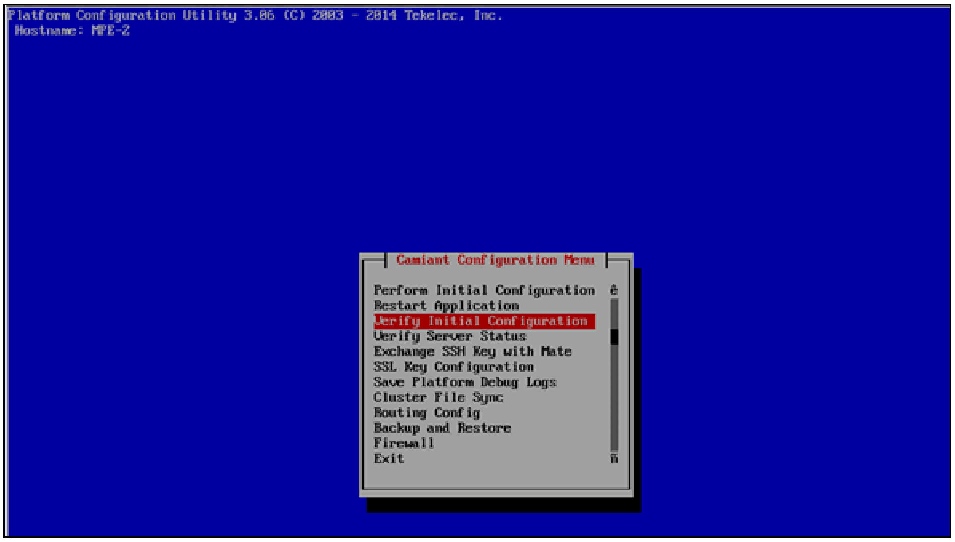
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Should this procedure fail, contact the Oracle Customer Care Center and ask for assistance.

NOTE: We will cover the procedures for MPE, however the same procedures could be followed for BOD and/or MA if any or both need recovery.

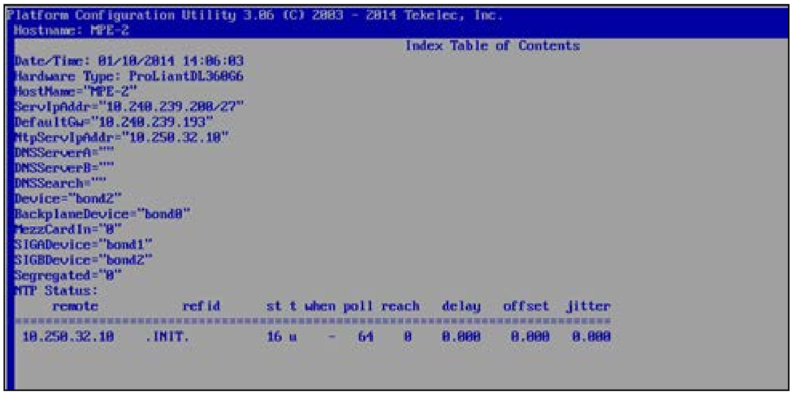
Step	Procedure	Instructions
1. □	Required resources / information	The purpose of this procedure is to create the MPE cluster from replacement hardware and software, then restore application level configuration by pushing that configuration from the active CMP. In this example, initial Camiant configuration is restored to the replacement server through the use of server backup files for each server to be restored. Required resources: • Replacement servers • TPD installation ISO • MPE Policy Management Application installation ISO. • *serverbackup*.ISO of the node to be replaced

Step		Procedure	Instructions
2.	□	Prerequisites	1. Remove and replace both nodes 2. IPM both nodes (fresh install of TPD software) 3. Install MPE application on both nodes
3.	□	Load the ISO for server restore on the replacement server	**NOTE 1:** The following steps will be performed on the 1st replacement server, and then the same steps will be performed on the 2nd replacement server. **NOTE 2:** It is assumed that both nodes of the MPE cluster that has failed, have already been placed in force standby from the CMP GUI. At the end of this procedure there are steps to remove force standby when the MPE cluster is ready to resume service. Obtain the *serverbackup.iso* for the node to be restored. When the replacement node is available (TPD/App installation complete, cabled as per network requirements), the server backup file should be copied to the following directory: `/var/camiant/backup/local_archive/serverbackup` **NOTE 3:** Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu. The platcfg utility also allows the user to manually enter any mounted path on the server. See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions accessing the iLO, launching the remote console.
4.	□	Login via the iLO Interface	Access the iLO Interface and launch the remote console of the first replacement server to gain root level access to the server CLI
5.	□	Perform platcfg restore from iLO remote console	1. Run the following command `# su – platcfg` 2. From within the platcfg utility, navigate to: **Camiant Configuration → Backup and Restore → Server Restore** 3. Select the *serverbackup*.ISO that you just put on the system. 4. Click **OK** 5. Click **Yes** to confirm.  Select tarball to restore from Tarball to restore: (*) MPE9-4-mpe_9.4.0_40.2.0-systembackup-2014011350.tar.gz ( ) Manually input Manually input: Restore type: (*) Application ( ) Full **NOTE:** This may take a couple of minutes.

Step	Procedure	Instructions
6. □	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding:  Platform Configuration Utility 3.06 (C) 2003 - 2013 Tekelec, Inc. Hostname: MPE-1b-Wireline Message Restored from iso /var/camiant/backup/local_archive/serverbackup/MPE-1b-Wireline-mpe_10.4.0_7.1.0-serverbackup-201310091038.iso successfully Press any key to continue...
7. □	Reboot the server	Exit form the platcfg menu and Reboot from the command line. `'shutdown -r now'`
8. □	Verify Config	After the server has been rebooted you should be returned to a login prompt via the iLO remote console. Verify the configuration by selecting **Camiant Configuration → Verify Initial Configuration** from within the platcfg utility.  Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc. Hostname: MPE-2 Camiant Configuration Menu Perform Initial Configuration Restart Application Verify Initial Configuration Verify Server Status Exchange SSH Key with Mate SSL Key Configuration Save Platform Debug Logs Cluster File Sync Routing Config Backup and Restore Firewall Exit

<table>
<tr><th>Step</th><th>Procedure</th><th>Instructions</th></tr>
<tr><td><b>9.</b> □</td><td>Verify Config</td><td>

Confirm the configured Hostname, ServIpAddr, DefaultGw and NtpServIpAddr previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.

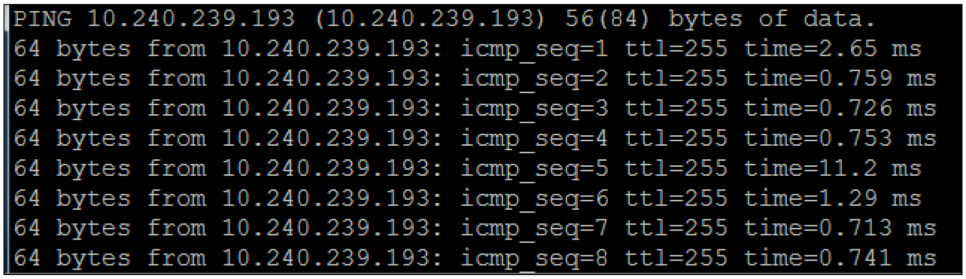


```
Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc.
 Hostname: MPE-2
                                                  Index Table of Contents
Date/Time: 01/10/2014 14:06:03
Hardware Type: ProLiantDL360G6
HostName="MPE-2"
ServIpAddr="10.240.239.200/27"
DefaultGw="10.240.239.193"
NtpServIpAddr="10.250.32.10"
DNSServerA=""
DNSServerB=""
DNSSearch=""
Device="bond2"
BackplaneDevice="bond0"
MezzCardIn="0"
SIGADevice="bond1"
SIGBDevice="bond2"
Segregated="0"
NTP Status:
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.250.32.10    .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

</td></tr>
<tr><td><b>10.</b> □</td><td>Verify basic network connectivity and server health <b>on the replacement server</b></td><td>

1. From the newly installed server, ping the OAM gateway.

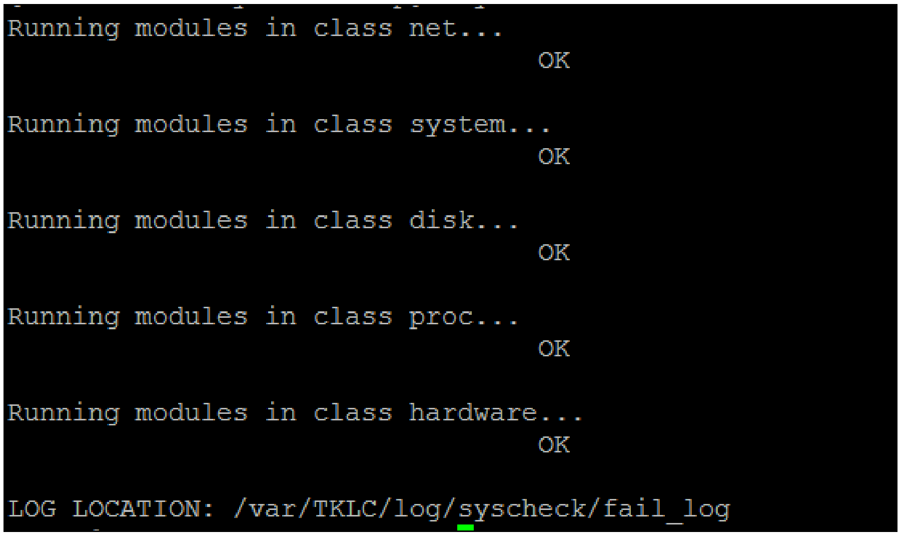
```
#ping <OAM gateway address>
```



```
PING 10.240.239.193 (10.240.239.193) 56(84) bytes of data.
64 bytes from 10.240.239.193: icmp_seq=1 ttl=255 time=2.65 ms
64 bytes from 10.240.239.193: icmp_seq=2 ttl=255 time=0.759 ms
64 bytes from 10.240.239.193: icmp_seq=3 ttl=255 time=0.726 ms
64 bytes from 10.240.239.193: icmp_seq=4 ttl=255 time=0.753 ms
64 bytes from 10.240.239.193: icmp_seq=5 ttl=255 time=11.2 ms
64 bytes from 10.240.239.193: icmp_seq=6 ttl=255 time=1.29 ms
64 bytes from 10.240.239.193: icmp_seq=7 ttl=255 time=0.713 ms
64 bytes from 10.240.239.193: icmp_seq=8 ttl=255 time=0.741 ms
```

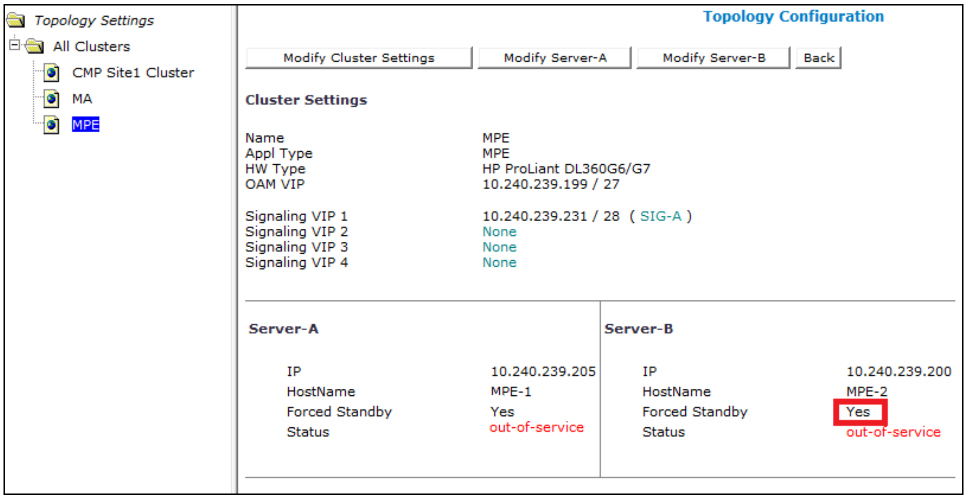
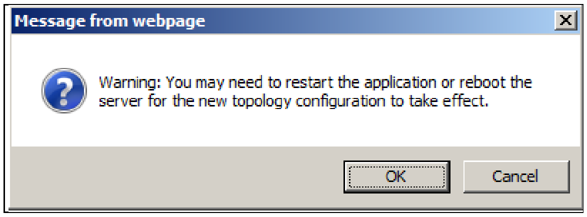
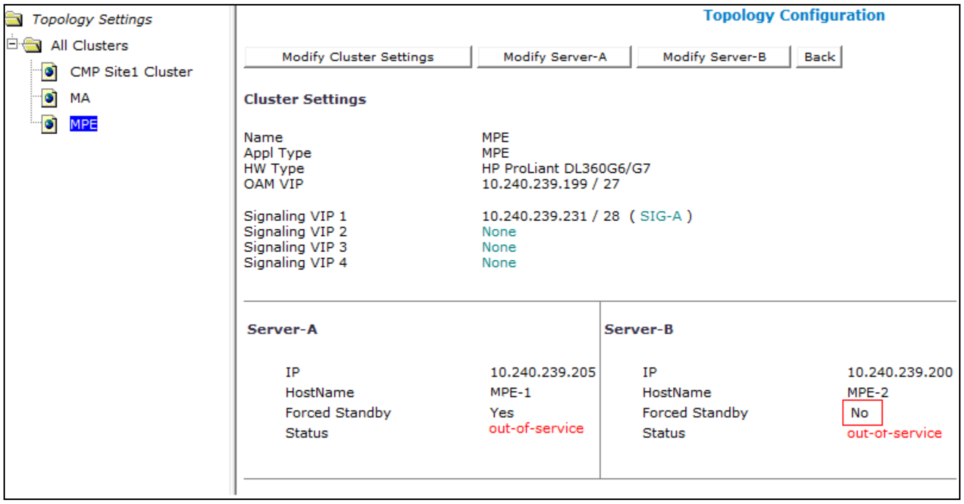
If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact Oracle support before proceeding if network ping tests still fail.

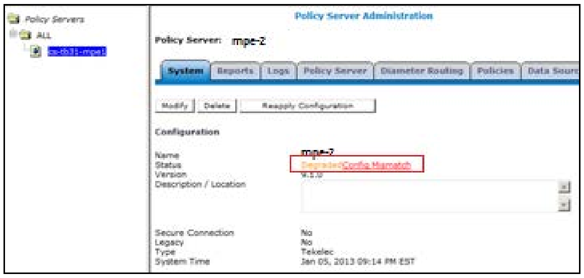
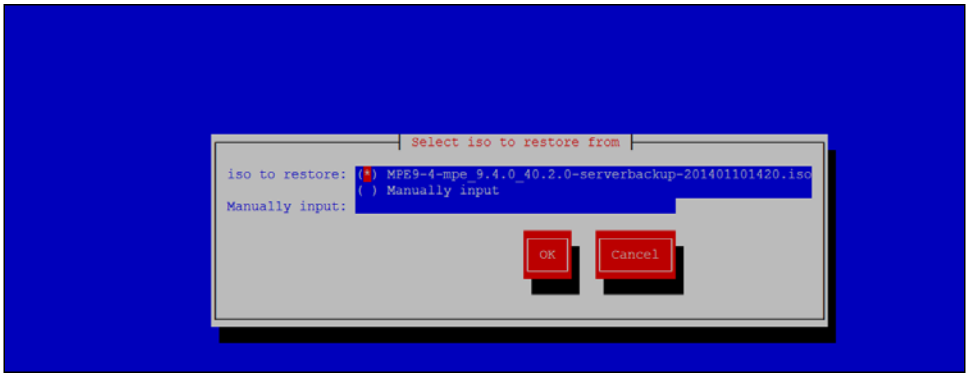
2. Run the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Oracle support.



```
Running modules in class net...
                                OK

Running modules in class system...
                                OK

Running modules in class disk...
                                OK

Running modules in class proc...
                                OK

Running modules in class hardware...
                                OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

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

Step	Procedure	Instructions
11. □	Set Forced Standby designation on cluster node that is still out-of-service.	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → Current Cluster**  Topology Settings All Clusters CMP Site1 Cluster MA MPE Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings Name MPE Appl Type MPE HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.199 / 27 Signaling VIP 1 10.240.239.231 / 28 (SIG-A) Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None Server-A IP 10.240.239.205 HostName MPE-1 Forced Standby Yes Status out-of-service Server-B IP 10.240.239.200 HostName MPE-2 Forced Standby Yes Status out-of-service 1. Modify the server that has been restored 2. Uncheck the **Forced Standby** checkbox 3. Accept the resulting pop-up by clicking **OK**.  Message from webpage Warning: You may need to restart the application or reboot the server for the new topology configuration to take effect. 4. Click **Save**.  Topology Settings All Clusters CMP Site1 Cluster MA MPE Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings Name MPE Appl Type MPE HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.199 / 27 Signaling VIP 1 10.240.239.231 / 28 (SIG-A) Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None Server-A IP 10.240.239.205 HostName MPE-1 Forced Standby Yes Status out-of-service Server-B IP 10.240.239.200 HostName MPE-2 Forced Standby No Status out-of-service

Step	Procedure	Instructions
12. ☐	Check status	In the CMP GUI, navigate to: **PolicyServer → Configuration →Cluster System tab** Check system tab for the MPE cluster being recovered. If the Status field indicates Config Mismatch, click **Reapply Configuration** and wait for the Config Mismatch designation to disappear. If it does not, contact Oracle support before proceeding.  Policy Servers ALL Policy Server Administration System Reports Logs Policy Server Diameter Routing Policies Data Sourc Modify Delete Reapply Configuration Policy Server: mpe-2 Configuration Name mpe-2 Status Degraded/Config Mismatch Version 9.1.0 Description / Location Secure Connection No Legacy No Type Tekelec System Time Jan 05, 2013 09:14 PM EST
13. ☐	Load the ISO for server restore on the 2nd replacement server	Obtain the *serverbackup.iso* for the node to be restored. When the replacement node is available (TPD/App installation complete, cabled as per network requirements), the server backup file should be copied to the following directory: `/var/camiant/backup/local_archive/serverbackup.` **NOTES:** • If there are ISO files in the `/var/TKLC/upgrade` directory, you can remove • Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu. The platcfg utility also allows the user to manually enter any mounted path on the server. See the *Oracle Communications Policy Management Bare Metal Installation Guide* for directions accessing the iLO, launching the remote console.
14. ☐	Login via the iLO Interface	Access the iLO Interface and launch the remote console of the **second** replacement server to gain root level access to the cli
15. ☐	Perform platcfg restore from iLO remote console	1. Run the following command: `# su – platcfg` 2. From within the platcfg utility, navigate to: **Camiant Configuration → Backup and Restore → Server Restore** 3. Select the *serverbackup*.ISO that you just put on the system and click **OK**. 4. Click **Yes** to confirm.  Select iso to restore from iso to restore: (*) MPE9-4-mpe_9.4.0_40.2.0-serverbackup-201401101420.iso ( ) Manually input Manually input: **NOTE:** This may take a couple of minutes.
16. ☐	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success.

<table>
<tr><th>Step</th><th>Procedure</th><th>Instructions</th></tr>
<tr><td><b>17.</b> □</td><td>Reboot the server</td><td>

Exit form the platcfg menu and Reboot from the command line.

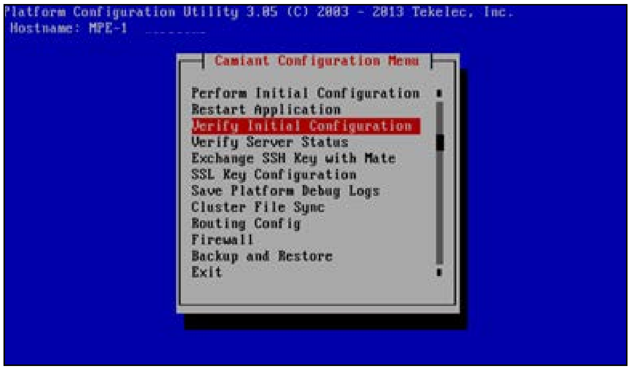
```
'shutdown –r now'
```

</td></tr>
<tr><td><b>18.</b> □</td><td>Verify Config</td><td>

After the server has been rebooted you should be returned to a login prompt via the iLO remote console.

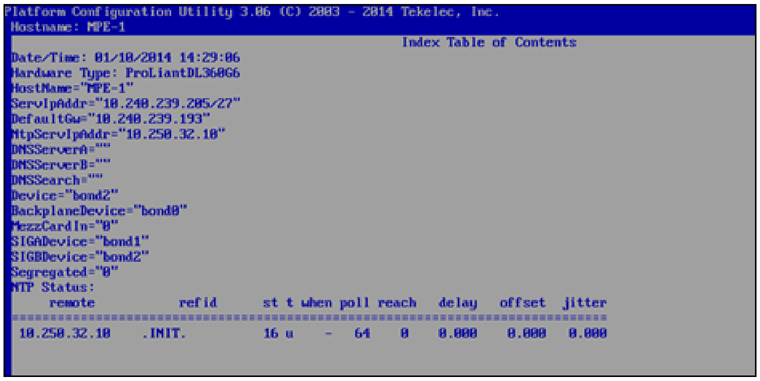
From within the platcfg utility, verify the configuration by selecting:

Camiant Configuration → Verify Initial Configuration


Platform Configuration Utility 3.05 (C) 2003 - 2013 Tekelec, Inc.
Hostname: MPE-1
Camiant Configuration Menu
Perform Initial Configuration
Restart Application
Verify Initial Configuration
Verify Server Status
Exchange SSH Key with Mate
SSL Key Configuration
Save Platform Debug Logs
Cluster File Sync
Routing Config
Firewall
Backup and Restore
Exit

</td></tr>
<tr><td><b>19.</b> □</td><td>Verify Config</td><td>

Confirm the configured Hostname, ServIpAddr, DefaultGw, and NtpServIpAddr previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.



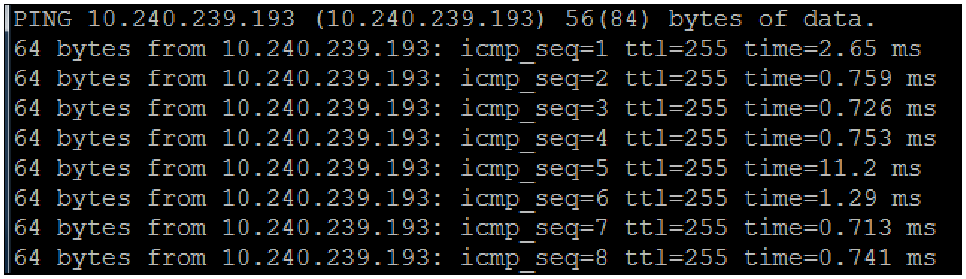
```
Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, Inc.
 Hostname: MPE-1
                                                   Index Table of Contents
Date/Time: 01/10/2014 14:29:06
Hardware Type: ProLiantDL360G6
HostName="MPE-1"
ServIpAddr="10.240.239.205/27"
DefaultGw="10.240.239.193"
NtpServIpAddr="10.250.32.10"
DNSServerA=""
DNSServerB=""
DNSSearch=""
Device="bond2"
BackplaneDevice="bond0"
MezzCardIn="0"
SIGADevice="bond1"
SIGBDevice="bond2"
Segregated="0"
NTP Status:
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.250.32.10    .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

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

<table>
<tr><th>Step</th><th>Procedure</th><th>Instructions</th></tr>
<tr><td>20. □</td><td>Verify basic network connectivity and server health <b>on the replacement server</b></td><td>

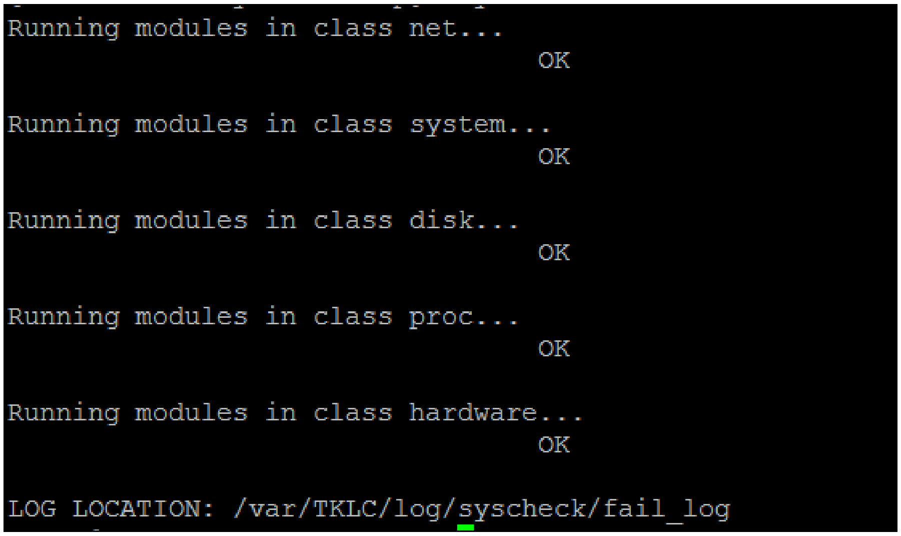
From the newly installed server, ping the OAM gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact Oracle support before proceeding if network ping tests still fail.

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



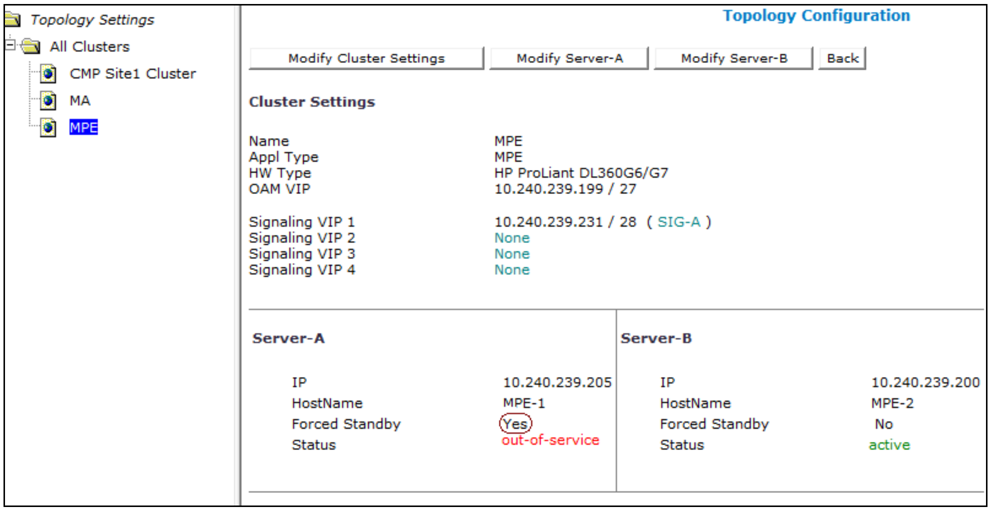
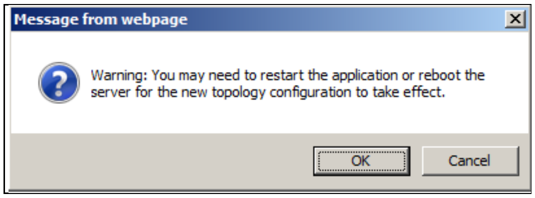
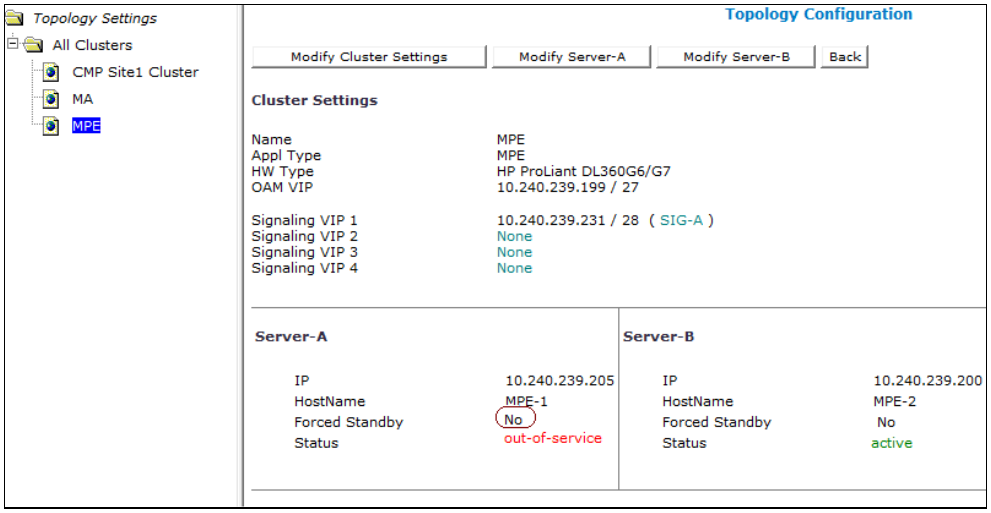
```
PING 10.240.239.193 (10.240.239.193) 56(84) bytes of data.
64 bytes from 10.240.239.193: icmp_seq=1 ttl=255 time=2.65 ms
64 bytes from 10.240.239.193: icmp_seq=2 ttl=255 time=0.759 ms
64 bytes from 10.240.239.193: icmp_seq=3 ttl=255 time=0.726 ms
64 bytes from 10.240.239.193: icmp_seq=4 ttl=255 time=0.753 ms
64 bytes from 10.240.239.193: icmp_seq=5 ttl=255 time=11.2 ms
64 bytes from 10.240.239.193: icmp_seq=6 ttl=255 time=1.29 ms
64 bytes from 10.240.239.193: icmp_seq=7 ttl=255 time=0.713 ms
64 bytes from 10.240.239.193: icmp_seq=8 ttl=255 time=0.741 ms
```

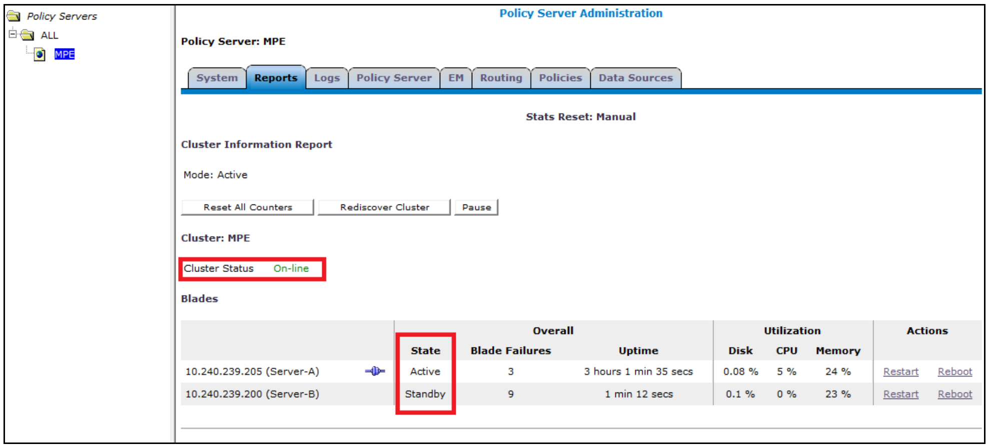
Run the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Oracle support.

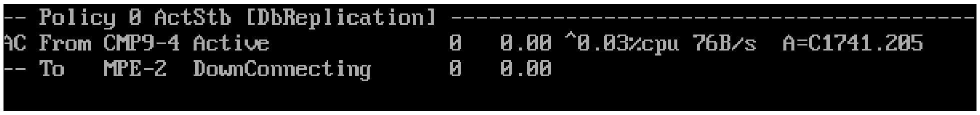
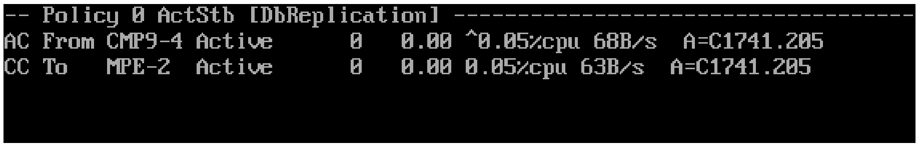


```
Running modules in class net...
                                 OK

Running modules in class system...
                                 OK

Running modules in class disk...
                                 OK

Running modules in class proc...
                                 OK

Running modules in class hardware...
                                 OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

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

Step	Procedure	Instructions
21. □	Remove Forced Standby designation on current node.	In the CMP GUI, navigate to: **Platform Setting → Topology Setting → Current Cluster**  Topology Settings All Clusters CMP Site1 Cluster MA MPE Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings Name MPE Appl Type MPE HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.199 / 27 Signaling VIP 1 10.240.239.231 / 28 (SIG-A) Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None Server-A IP 10.240.239.205 HostName MPE-1 Forced Standby Yes Status out-of-service Server-B IP 10.240.239.200 HostName MPE-2 Forced Standby No Status active 1. Modify for the server that has forced standby 2. Clear the Forced Standby checkbox 3. Accept the resulting pop-up by clicking **OK**.  Message from webpage Warning: You may need to restart the application or reboot the server for the new topology configuration to take effect. 4. Click **Save**  Topology Settings All Clusters CMP Site1 Cluster MA MPE Topology Configuration Modify Cluster Settings Modify Server-A Modify Server-B Back Cluster Settings Name MPE Appl Type MPE HW Type HP ProLiant DL360G6/G7 OAM VIP 10.240.239.199 / 27 Signaling VIP 1 10.240.239.231 / 28 (SIG-A) Signaling VIP 2 None Signaling VIP 3 None Signaling VIP 4 None Server-A IP 10.240.239.205 HostName MPE-1 Forced Standby No Status out-of-service Server-B IP 10.240.239.200 HostName MPE-2 Forced Standby No Status active

Step	Procedure	Instructions
22. □	Check status	In the CMP GUI, navigate to: **Policy Server → Configuration → All → Reports Tab** Monitor clustering of the replacement node to its peer, do not proceed until the Cluster Status changes from Degraded to On-line.  Policy Server Administration Policy Server: MPE Stats Reset: Manual Cluster Information Report Mode: Active Cluster: MPE Cluster Status On-line Blades Overall: State, Blade Failures, Uptime; Utilization: Disk, CPU, Memory; Actions 10.240.239.205 (Server-A) Active 3 3 hours 1 min 35 secs 0.08 % 5 % 24 % Restart Reboot 10.240.239.200 (Server-B) Standby 9 1 min 12 secs 0.1 % 0 % 23 % Restart Reboot Policy Servers ALL MPE System Reports Logs Policy Server EM Routing Policies Data Sources Reset All Counters Rediscover Cluster Pause

23. □	Alternative method to check status	You can also monitor the clustering of the replacement node from within the shell on the primary node with `irepstat`. To do so, SSH to the Active node of the current cluster and Run the `irepstat` command:
		`# irepstat`
		Expected `irepstat` output while waiting reconnection:
		
		`-- Policy 0 ActStb [DbReplication] ----------------------------------------`
		`AC From CMP9-4 Active              0   0.00 ^0.03%cpu 76B/s   A=C1741.205`
		`-- To   MPE-2  DownConnecting      0   0.00`
		Expected `irepstat` output after cluster has formed:
		
		`-- Policy 0 ActStb [DbReplication] -----------------------------------`
		`AC From CMP9-4 Active      0   0.00 ^0.05%cpu 68B/s   A=C1741.205`
		`CC To   MPE-2  Active      0   0.00 0.05%cpu 63B/s  A=C1741.205`

		THIS PROCEDURE HAS BEEN COMPLETED

6 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.