Oracle® Communications Policy and Charging Rules Function

PCRF Cable Disaster Recovery Procedure

Release 11.5

E61664-01

February 2015

ORACLE®

Oracle® Communications Policy and Charging Rules Function, Cable Disaster Recovery Procedure, Release 11.5

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*.

TABLE OF CONTENTS

List of Tables

1. Introduction

1.1 Purpose and Scope

This document describes the disaster recovery procedure in the case of a failed server (node) within a CMP, MPE-R, MPE-S, BOD, MA 'HA Cluster' or a complete cluster failure for one of the cable policy components. In Policy Release 11.5 geo-redundant architecture, three servers are deployed for BOD and MPE-S components in two different geographic sites. Optionally for CMP, a cluster of 2 servers can be deployed in each site forming four total servers in 2 sites however CMP component is not geo-redundant component. For BOD and MPE-S components, two servers are configured in a (HA) high availability cluster in one site with one 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 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
Netra X3-2	Bond0.x=eth01+eth02	Bond1.y=eth03+eth04	Bond1.z=eth03+eth04	Bond3=eth63+eth64

1.2 References

[1] *910-6351-001_General Installation Methods*
[2] *910-6929-001_HP Solutions Firmware Upgrade Pack 2.2.5*
[3] *909-2234-001_HP Solutions Firmware Upgrade Procedures 2.2.pdf*
[4] *909-2130-001_TPD Initial Product Manufacture*
[5] *E55083 _Platform Configuration User Guide*
[6] *910-6114-001_Replacing a Failed Server in a Camiant Cluster Reference Guide.pdf*
[7] *MO008416_Cable Policy 11.5 Installation Procedure*

1.3 Acronyms

An alphabetized list of acronyms used in the document:

Acronym	Definition
BIOS	Basic Input Output System
CMP	Policy Manager
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

Table 1: Acronyms

1.4 Software Release Numbering

This guide applies to Cable Policy Management Versions 11.5.x

1.5 Terminology

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.
Policy 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 in this document the term "node" will be used to describe the each server within the HA cluster. The term "blade" may also be used in this context.

Table 2. Terminology

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 Application(CMP / MPE / MA / BOD)
6. Perform 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

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 geo-redundant) will require the use of a new server called the "replacement server". "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.

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 of BOD or MPE in case the solution is geo-redundant) will require the use of a new server called the "replacement server". "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.

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 geo-redundant) 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 Performing 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.

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.

A note on 'Initial configuration':

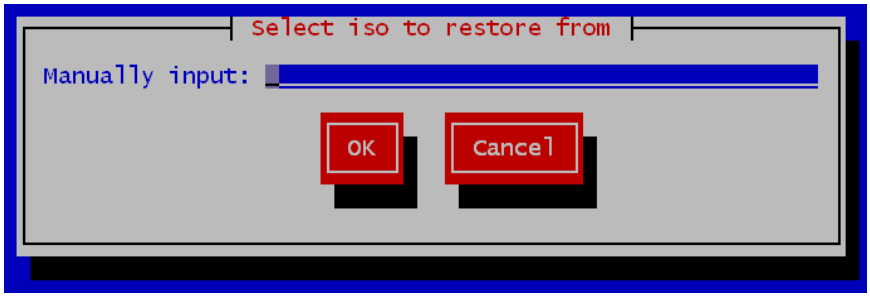
The information required for initial configuration is not extensive, and may be readily available from customer site documents, or from the CMP's topology configuration. In most cases it can be easier to manually input the 'initial configuration' in platcfg than to try to load a server backup file into 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)
- OAM Device (use default)
- Backplane Device (use default)
- Backplane IP Prefix (use default)

Using the server backup file.

When asked to restore from 'server backup', the platcfg utility will look in /var/camiant/backup/local_archive/serverbackup directory. If no files exist in that directory, the box below will be presented.



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 executed.

3.1 Disaster Recovery Strategy

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

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.

Disconnect failed server(s) from network

Evaluate the availability of server and system backup files for the servers that are to be restored.

Read and review the content in this document.

From the failure conditions, determine the Recovery Scenario and procedure to follow.

Execute 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 '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 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' and 'system backup':

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

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

4. Procedure Preparation

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 syscheck from CLI

***Reference [7] for detailed 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 Perform initial 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 execute the procedure. The actual procedures' detailed 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.
    - Perform initial configuration needs to be re-done 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.

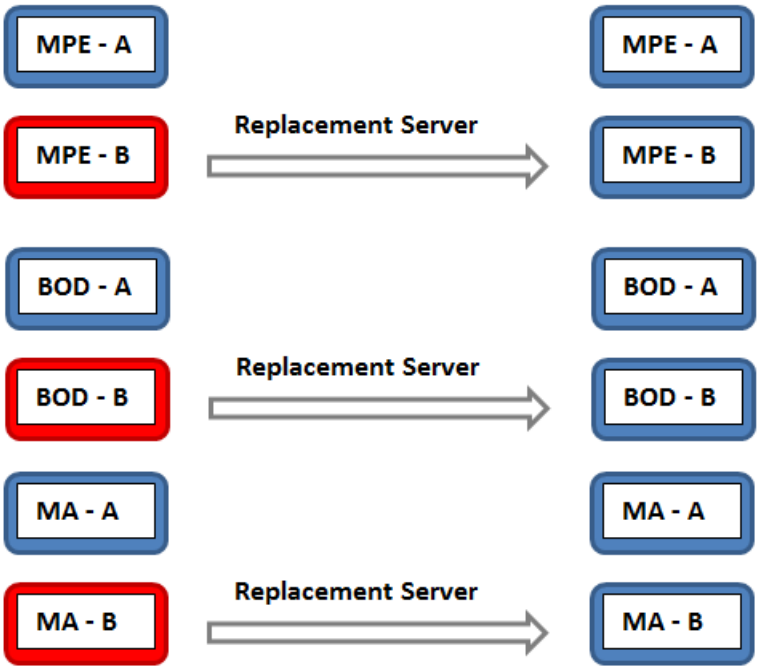
For complete details, refer to the following procedure in this document

- 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 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 execute the procedure. The actual procedures' detailed 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 configuration needs to be re-performed 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 're-apply configuration'



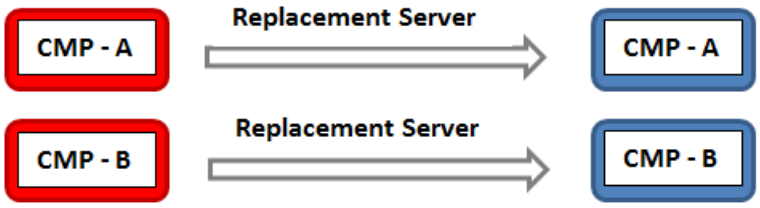
For complete details, refer to the following procedure in this document

- 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. Then the data will be replicated from the restored database to a second rebuilt CMP node which 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 execute the procedure. The actual procedures' detailed steps are in the Restore Procedures section. The major activities are summarized as follows:

- Recover Primary CMP server (if necessary) by recovering base hardware and software.
    - Recover the base hardware.
    - Recover the software.
    - Initial configuration is re-performed 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.
- Recover the second CMP server by recovering base hardware and software.
    - Recover the base hardware.
    - Recover the software.
    - Initial configuration is re-performed 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

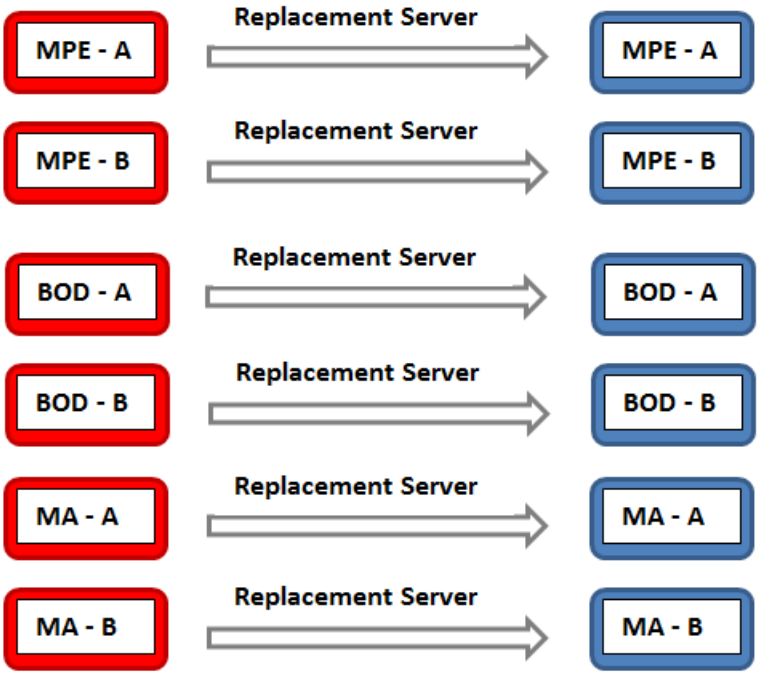
- Procedure 3. Restoring Complete Cluster Outage of the CMP

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 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 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 execute the procedure. The actual procedures' detailed steps are in the Restore Procedures section. The major activities are summarized as follows:

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



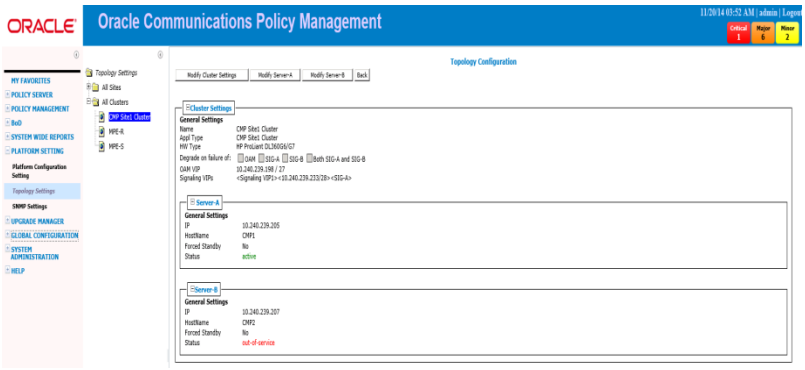
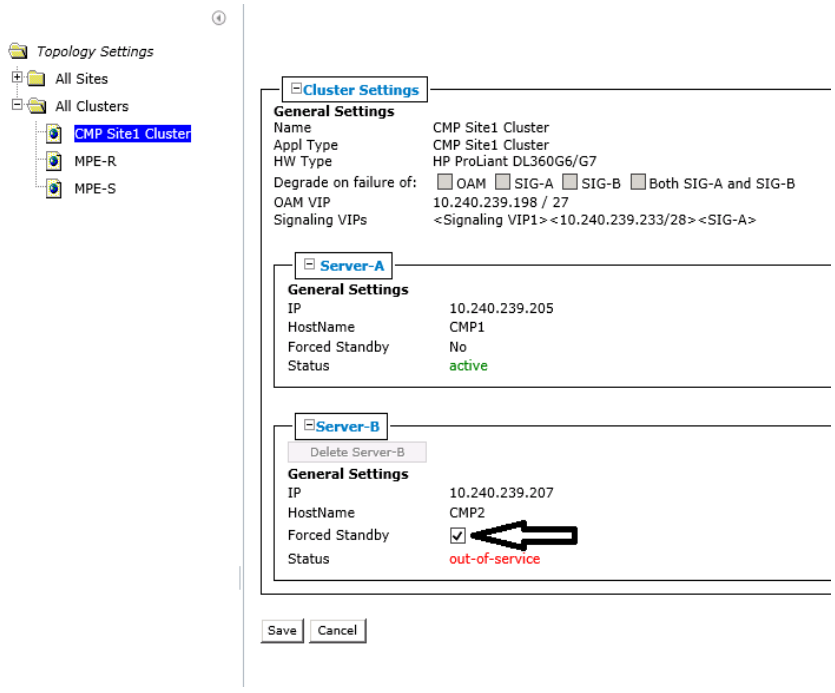
For complete details, refer to the following two procedures in this document

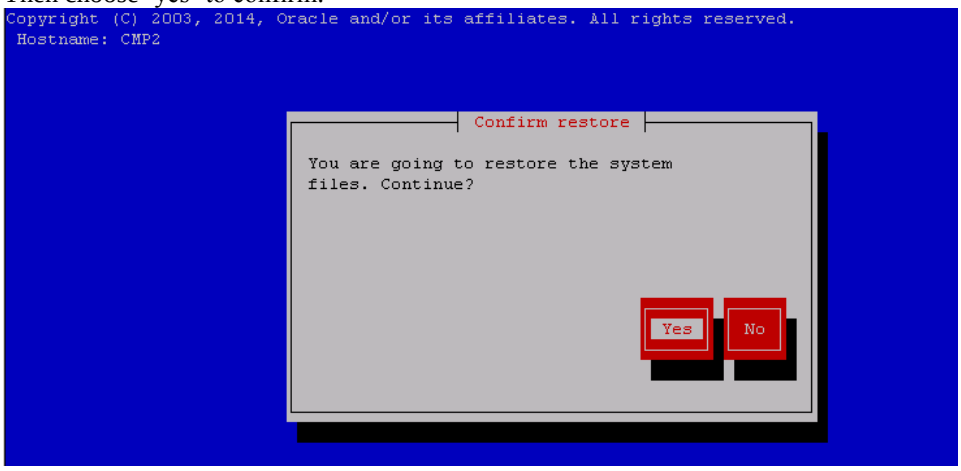
- Procedure 4. Restoring Complete Cluster Outage of the MPE/BOD/MA

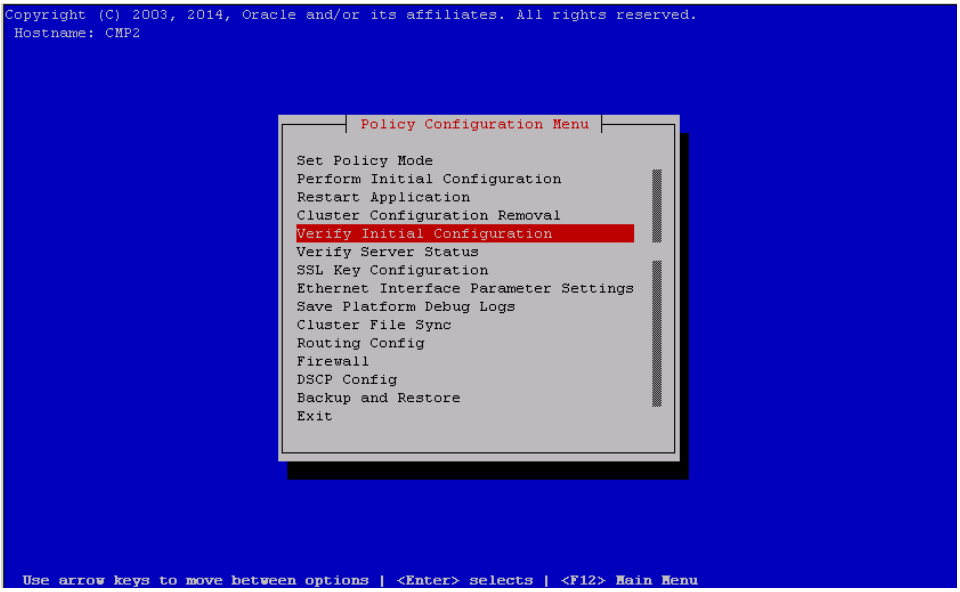
5. Restore Procedures

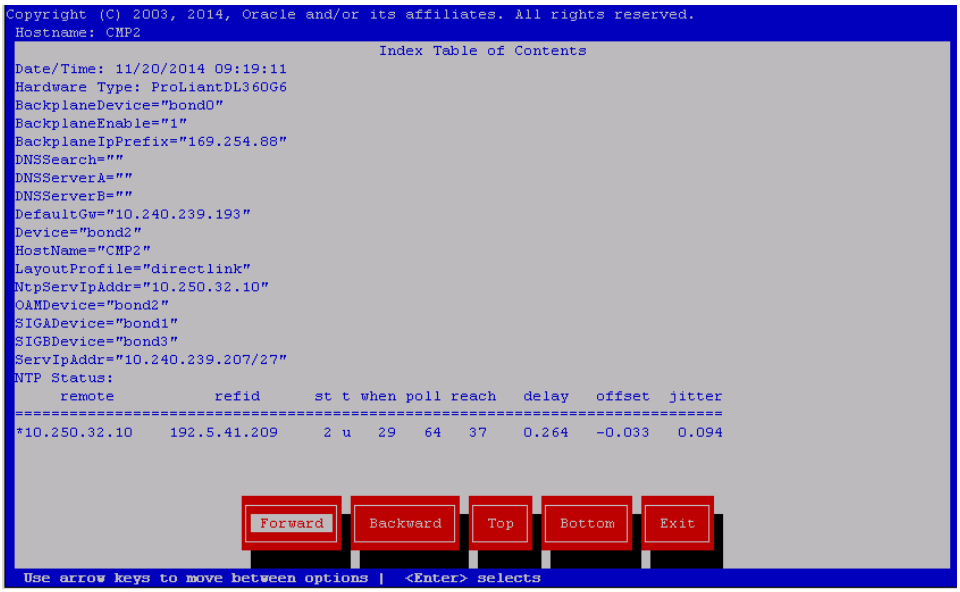
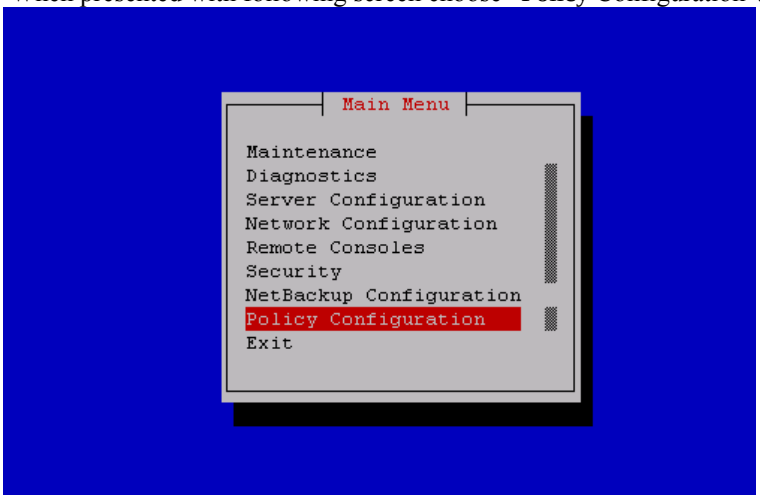
5.1 Procedure 1. Restoring Single Node Failure in CMP HA Cluster

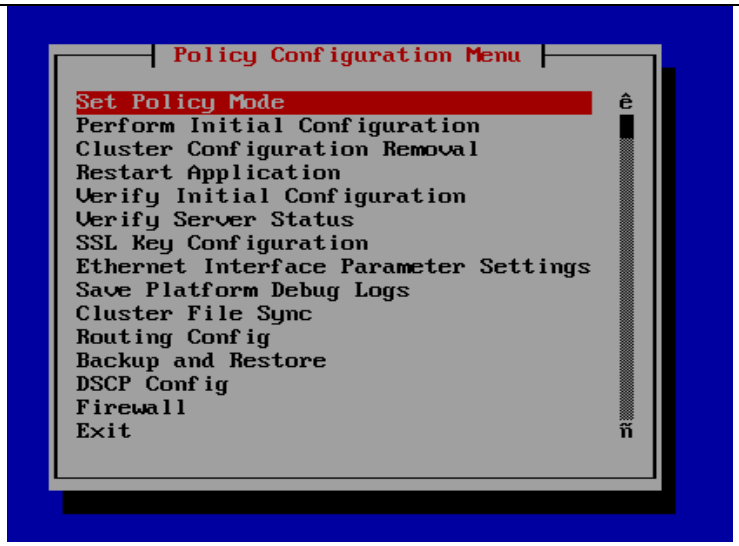
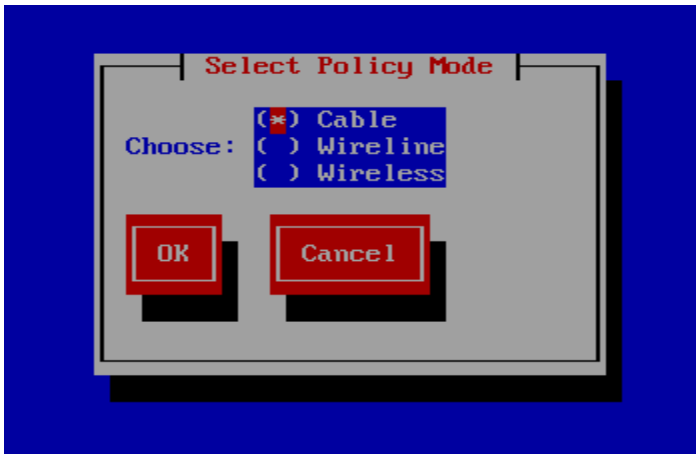
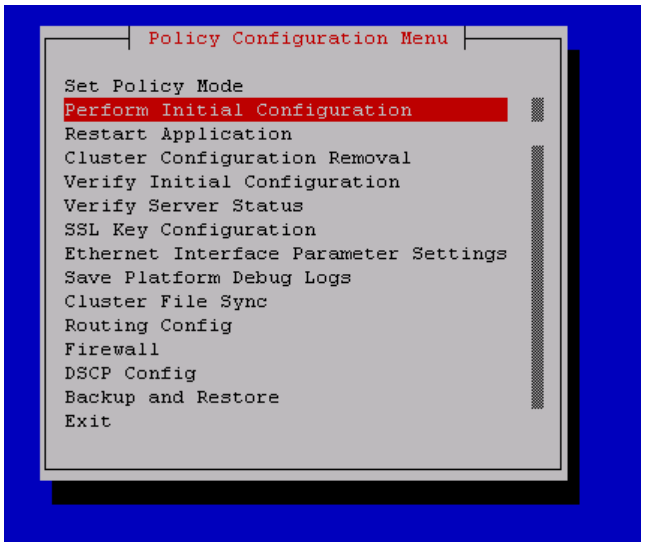
S T E P	This Procedure restores the standby CMP node, when a server level backup is available or using Initial Configuration if no server level backup is available. . Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec/Oracle Customer Care Center and ask for assistance.	
1. ☐	Required resources / information:	The purpose of this procedure is to replace one node of a CMP HA cluster. Base level software is confirmed. 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 Application installation ISO. • *serverbackup.ISO* of the node to be replaced (optional)
2. ☐	Prerequisites	- Remove failed hardware and replace. - Verify that the node has TPD on it, or install TPD - Install the correct version of the application software – CMP - Cable as per network requirements **Reference [7] for detailed directions on installing TPD and the CMP Application. This procedure can also be used to confirm Bios, Firmware and iLO settings.**

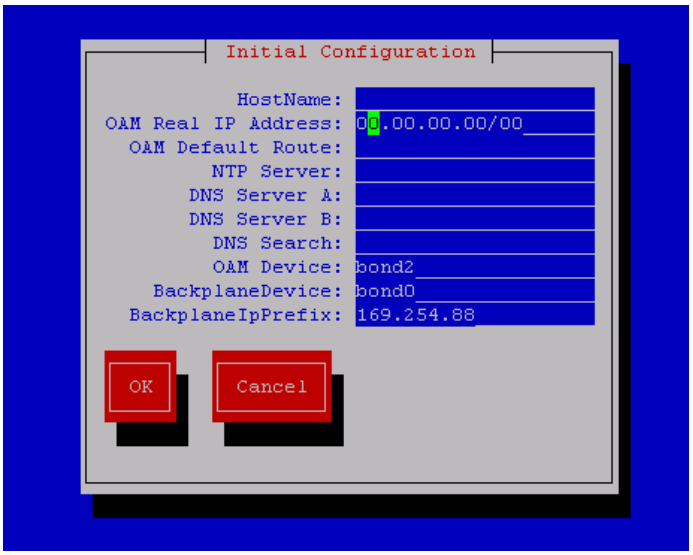
3. ☐	Set the failed node to 'Forced Standby'	In the CMP GUI: Navigate to: **Platform Setting → Topology Setting → All Clusters** 1) Determine the cluster with the failed node 2) Determine the failed node  3) Click the Modify button of the failed node  4) Click the Forced Standby checkbox so that it is checked, then click Save 

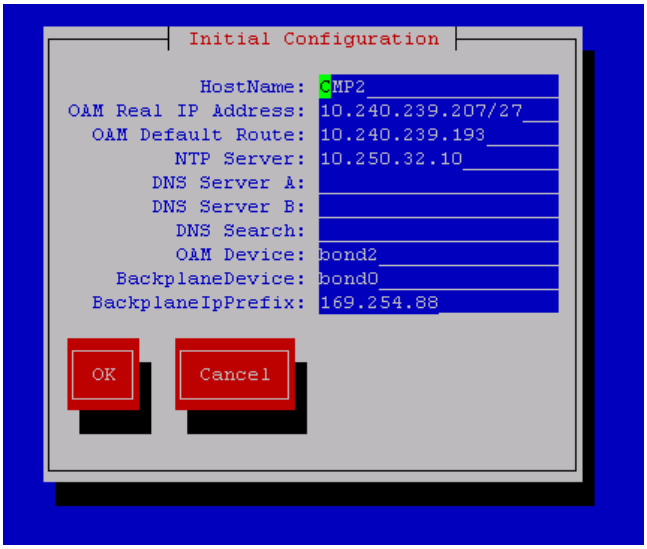
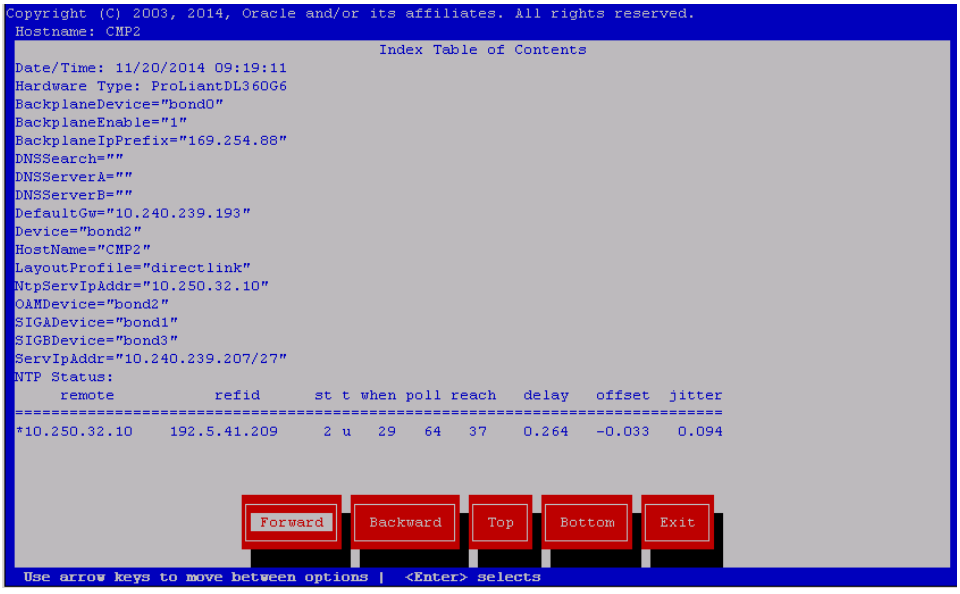
4. ☐	Load the ISO for server restore	If a 'server backup' is available proceed with this step. **If a 'server backup' is not available skip to step 11.** Obtain the *serverbackup.iso* for the node to be restored. When the replacement node is available (TPD/App installation complete, cabled as per network 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 to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.* **Reference [7]for detailed 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
6. ☐	Perform platcfg restore from iLO session on replacement node	Execute the following command **# su – platcfg** From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.ISO that you just put on the system and hit OK  Then choose 'yes' to confirm:  This may take a couple of minutes.

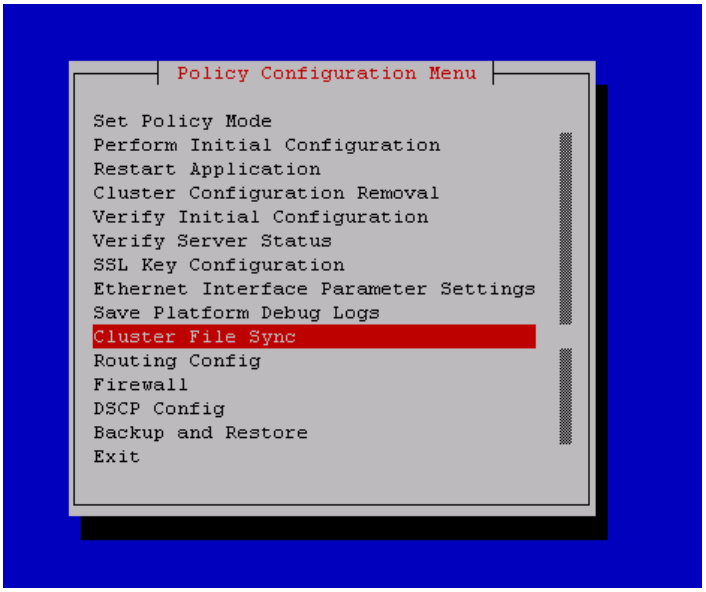
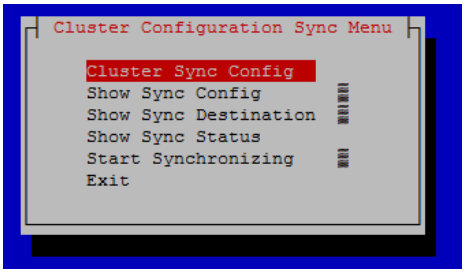
7. ☐	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding: 
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 **Policy Configuration** > **Verify Initial Configuration** from within the platcfg utility. 

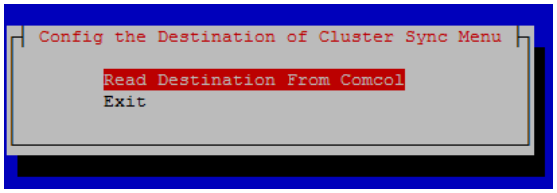
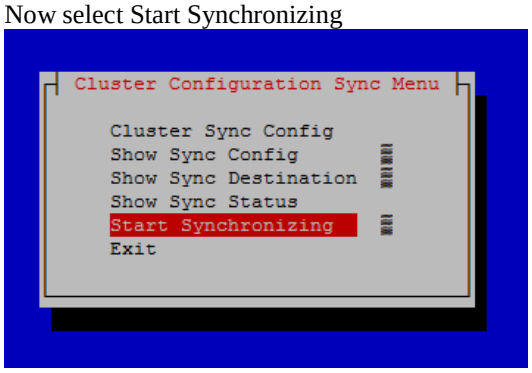
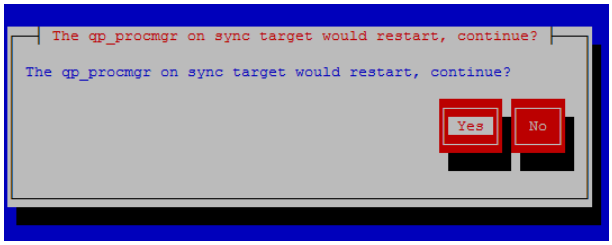
10. ☐	Verify Config	Confirm the configured "Hostname, ServIpAddr, DefaultGw and NtpServIpAddr" previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.  **Skip to step 22**
11. ☐	Perform Policy 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. 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 choose "Policy Configuration". 

13.	Set Policy mode	 Then set the mode to “Cable” and click “OK” 
14. ☐	Select Perform Initial Configuration	

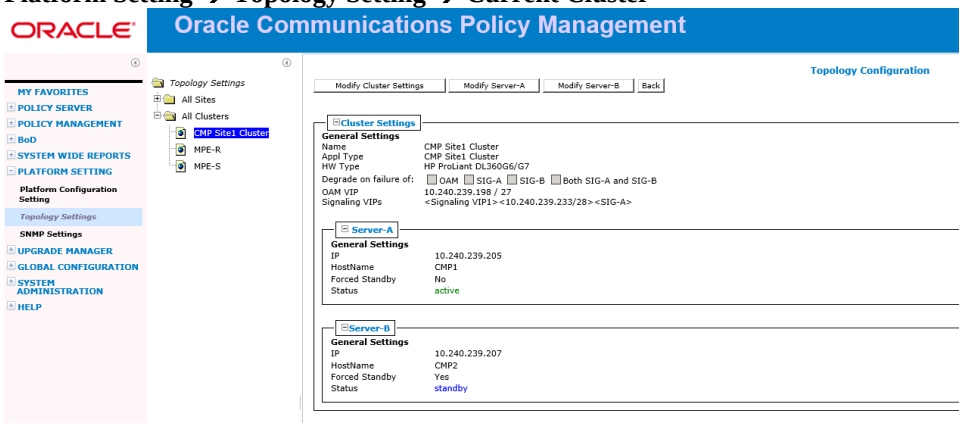
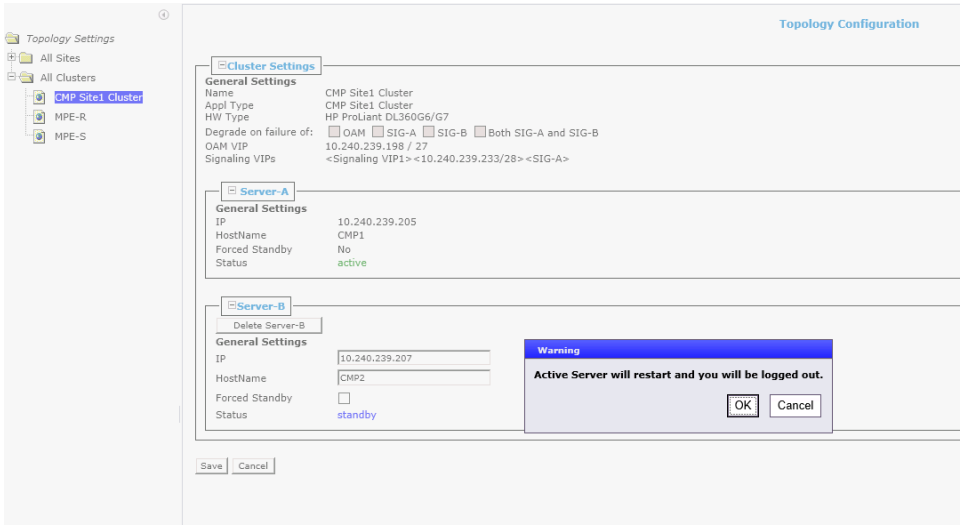
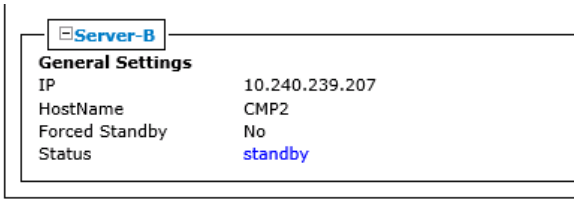
15. ☐	Complete Initial Configuration form	 • Hostname - the unique hostname for the device being configured. • OAM Real IP Address - the IP address that is permanently assigned to this device. (sometimes called “Physical IP” or “Real IP). • OAM Default Route - the default route of the OAM network. • 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. • Backplane IP Prefix – the IP prefix assigned to the backplane device. Note that the default value should be used, as changing this value is not supported.

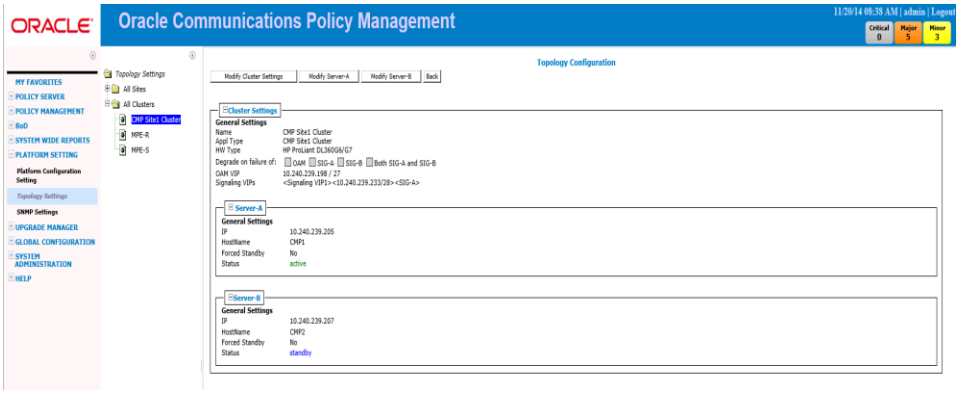
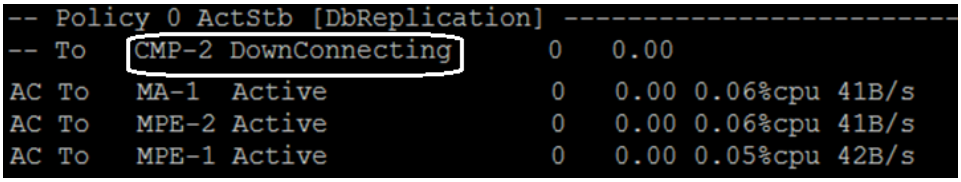
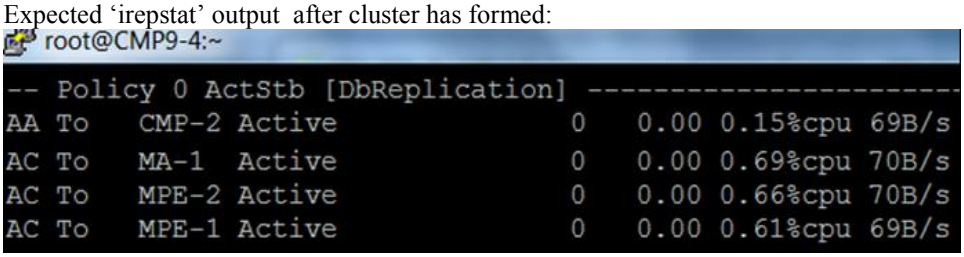
16. ☐	Save configuration	Enter the configuration (example data fill below) and then select **OK**  The platcfg form will pause for a minute while the server is configured, and then return to the platcfg menu.
17. ☐	Reboot the server	Exit from the platcfg menu and Reboot from the command line. 'shutdown –r now '
18. ☐	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 **Policy Configuration** -> **Verify Initial Configuration** from within the platcfg utility.
19. ☐	Verify Config	Confirm the configured "Hostname, ServIpAddr , DefaultGw and NtpServIpAddr" previously configured are present. A display similar to the following is shown. 

20. ☐	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. From the platcfg menu naviagte to Policy Configuration>Cluster File Sync  You will need to select Cluster Sync Config 

21. ☐	Perform Cluster sync from **the active server to the replacement server**	Read Destination From Comcol  You may need to provide the root password to proceed Now select Start Synchronizing   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.

22. ☐	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 Tekelec/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`
		Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Tekelec/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`

23. ☐	Remove 'Forced Standby' designation on current node.	In the CMP GUI: Navigate to: **Platform Setting → Topology Setting → Current Cluster**  - Modify for the server that has 'forced standby' - Ensure server status is "***standby***" - Clear the Forced Standby checkbox - Accept the resulting pop-up by clicking OK:  - Validate that force standby flag is off (set to "No") 

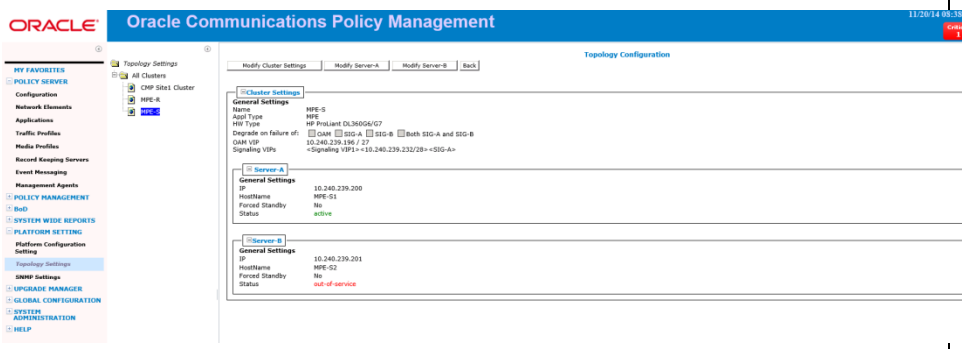
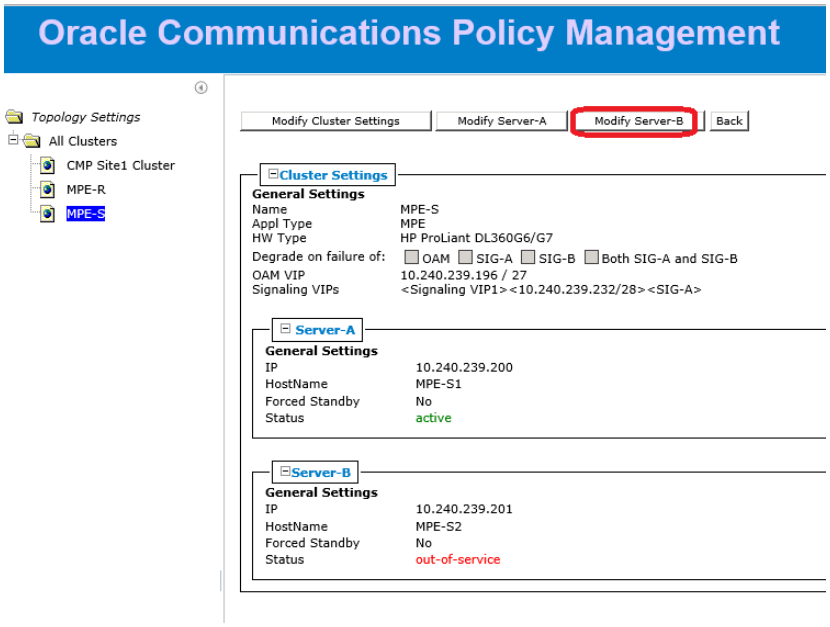
24. ☐	Verify cluster status	In the CMP GUI: Navigate to: **Platform Setting → Topology Setting → All → Current CMP Cluster** Monitor clustering of the new node to its peer, do not proceed until both nodes have a status of either 'active' or 'standby', and that there are no CMP related 'Active Alarms' (except for the "Accept new upgrade" alarm which will be cleared at the end of this procedure. 
25. ☐	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'. To do so, SSH to the Active node of the current cluster and execute the irepstat command: **# irepstat** Expected 'irepstat' output while waiting reconnection:  Expected 'irepstat' output after cluster has formed: 

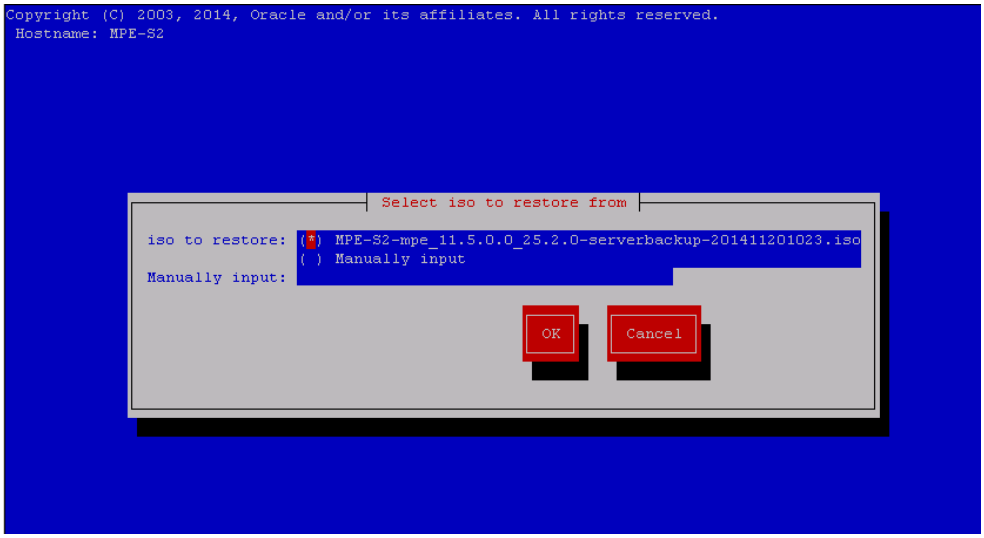
26.	**Active CMP CLI:**
	Sync SSH keys to all servers in topology
		Run the following command to sync the SSH keys of the new CMP server with all servers in the topology:
		
		qpSSHKeyProv.pl --prov --user=root
		
		`[root@CMP1 bin]# qpSSHKeyProv.pl --prov --user=root`
		
		`The password of root in topology:`
		
		`Connecting to root@MPE-R2 (10.240.238.97) ...`
		`Connecting to root@MPE-S1 (10.240.238.98) ...`
		`Connecting to root@MPE-R1 (10.240.238.96) ...`
		`Connecting to root@MPE-S2 (10.240.238.99) ...`
		`Connecting to root@CMP1 (10.240.238.90) ...`
		`Connecting to root@CMP2 (10.240.238.91) ...`
		
		`[2/10] Provisioning SSH keys on MPE-R2 (10.240.238.97) ...`
		
		`[5/10] Provisioning SSH keys on MPE-S1 (10.240.238.98) ...`
		
		`[6/10] Provisioning SSH keys on MPE-R1 (10.240.238.96) ...`
		
		`[7/10] Provisioning SSH keys on MPE-S2 (10.240.238.99) ...`
		
		`[8/10] Provisioning SSH keys on CMP1 (10.240.238.90) ...`
		
		`[10/10] Provisioning SSH keys on CMP2 (10.240.238.91) ...`
		
		`SSH keys are OK.`
		
		`[root@CMP1 bin]#`

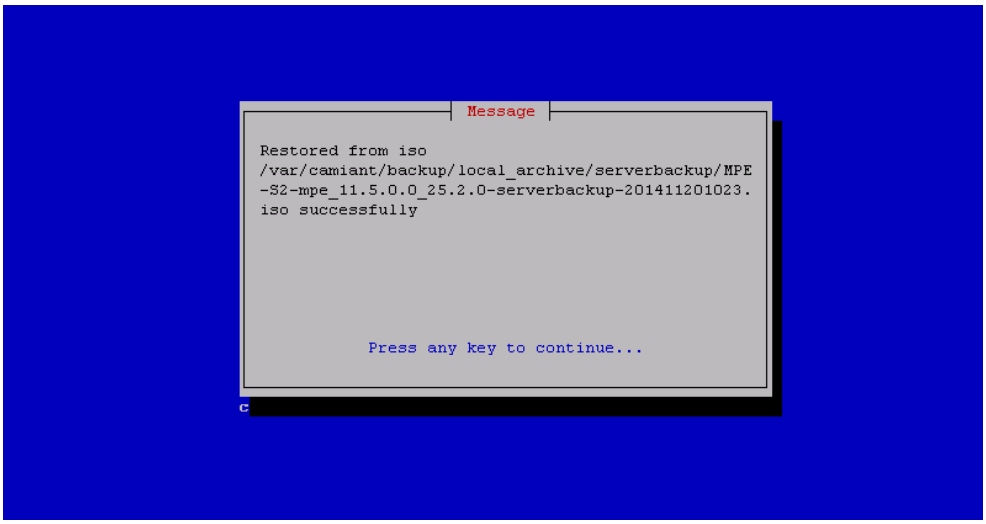
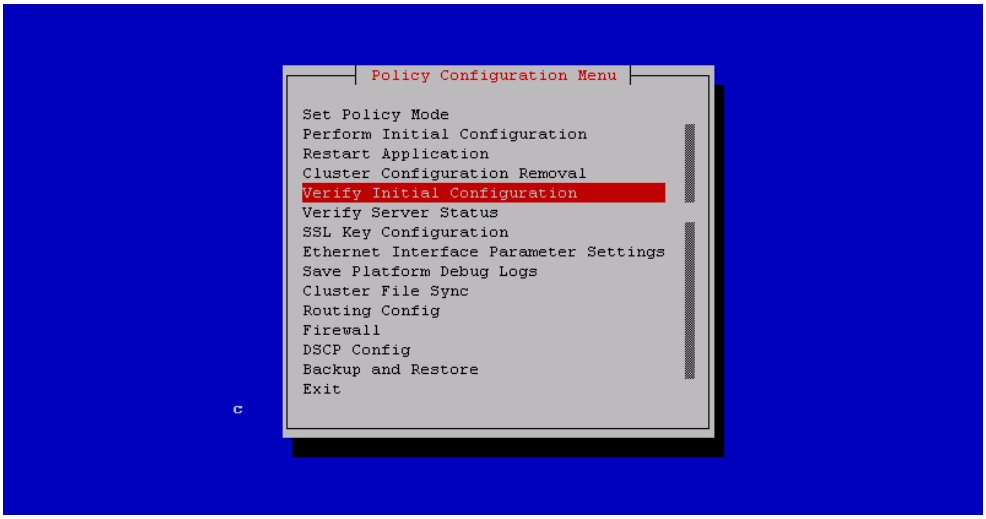
27. ☐	End of procedure	This procedure is completed

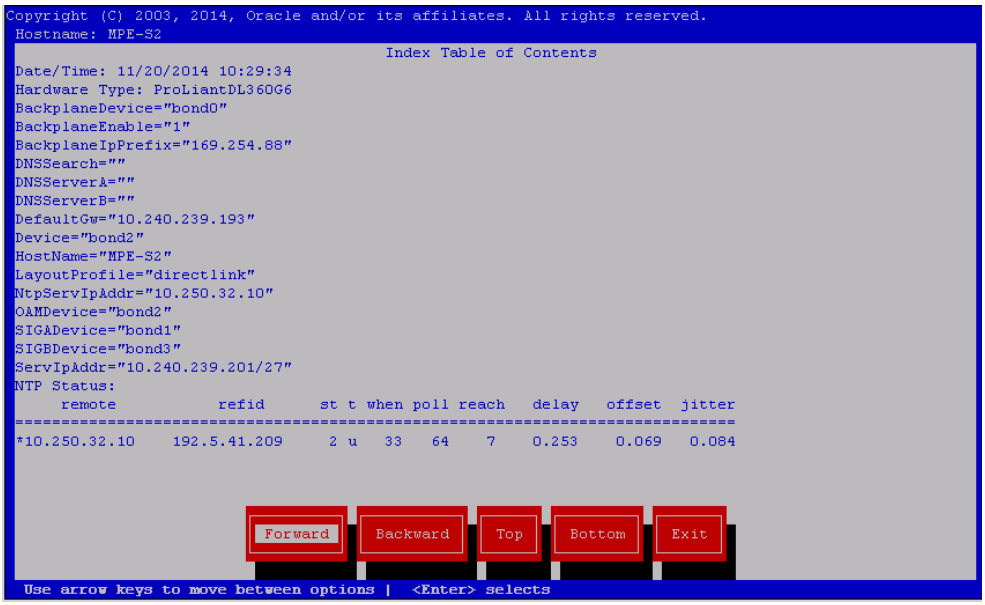
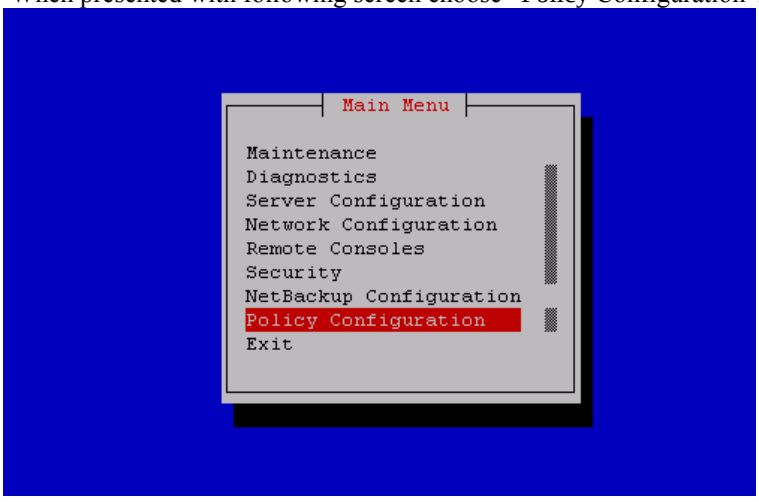
5.2 Procedure 2. Restoring Single Node Failure in MPE-R/MPE-S/BOD/MA HA Cluster

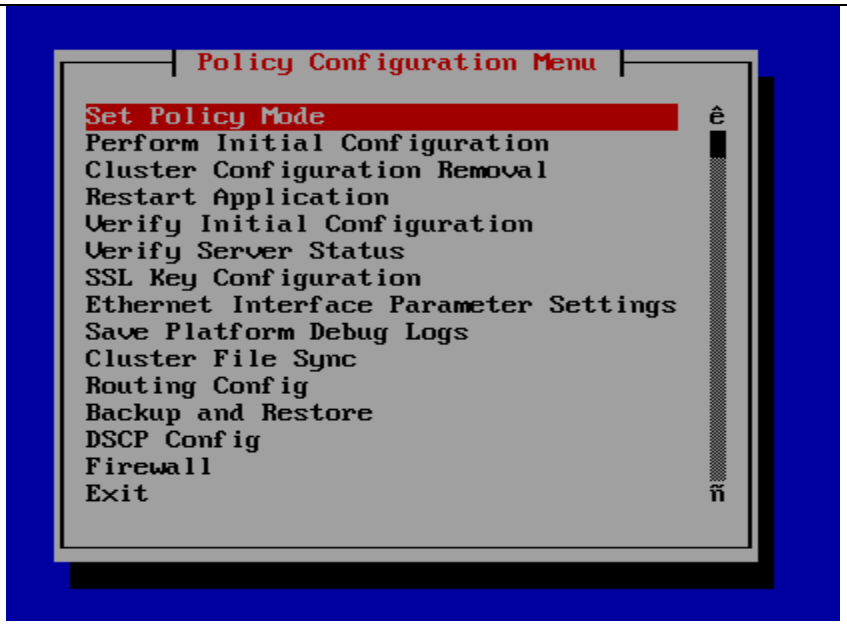
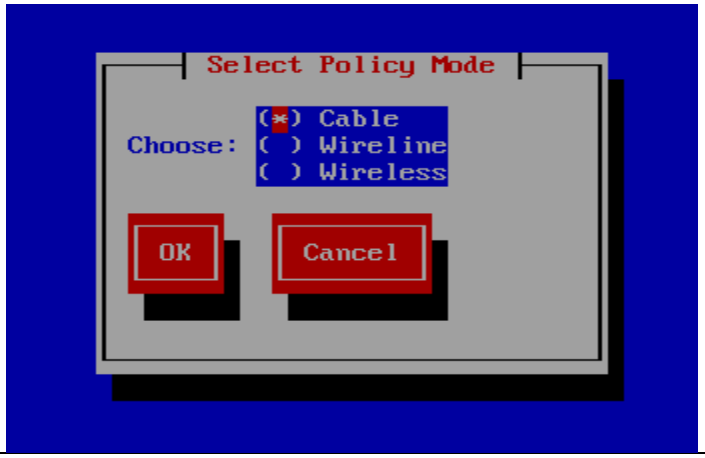
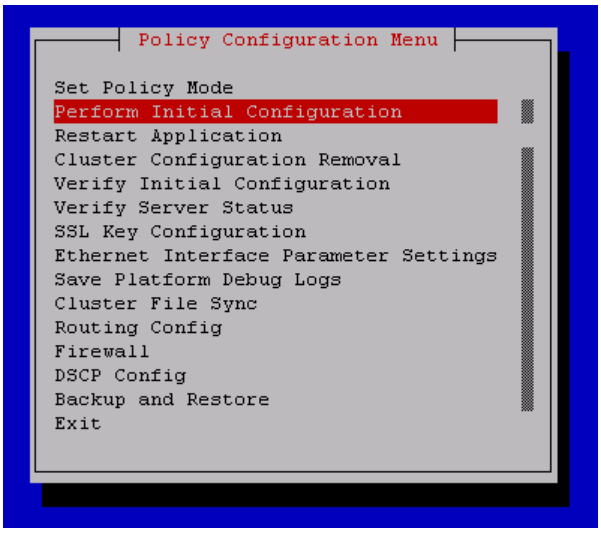
S T E P		
	This Procedure restores the standby MPE/BOD/MA node, when a server level backup is available or using Initial Configuration if no server level backup is available. . Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec/Oracle Customer Care Center and ask for assistance. **Note: We will cover the procedures for MPE-S, however the same procedures could be followed for BOD, MPE-R and MA if any need recovery.**	
1. ☐	Required resources / information:	The purpose of this procedure is to replace one node of MPE HA cluster. Base level software is confirmed. 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 Application installation ISO. • *serverbackup.ISO* of the node to be replaced (optional)
2. ☐	Prerequisites	- Remove failed hardware and replace. - Verify that the node has TPD on it, or install TPD - Install the correct version of the application software – CMP - Cable as per network requirements **Reference [7] for detailed 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 Out of Service state  3) Click the Modify button of the failed node  4) Click the Forced Standby checkbox so that it is checked, then click Save 

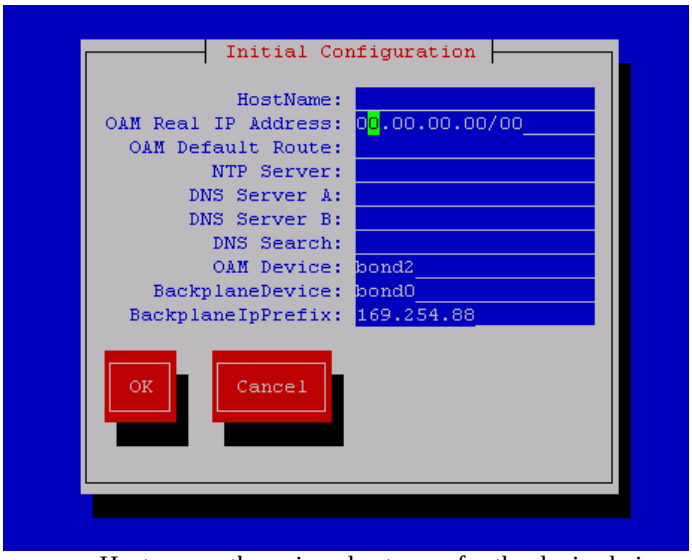
4. ☐	Load the ISO for server restore	If a 'server backup' is available proceed with this step. **If a 'server backup' is not available skip to step 11.** Obtain the *serverbackup.iso* for the node to be restored. When the replacement node is available (TPD/App installation complete, cabled as per network 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 to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.* **Reference [7]**for **detailed 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
6. ☐	Perform platcfg restore from iLO remote console	Execute the following command **# su – platcfg** From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.ISO that you just put on the system and hit OK – then 'yes' to confirm.  This may take a couple of minutes.

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: 
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 **Policy Configuration** > **Verify Initial Configuration** from within the platcfg utility. 

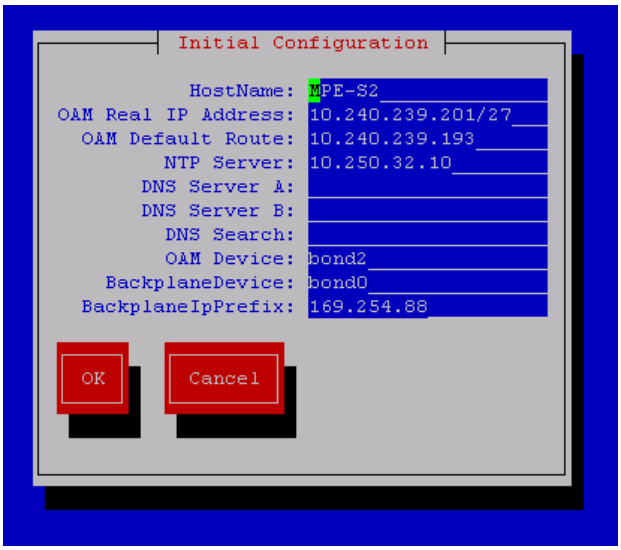
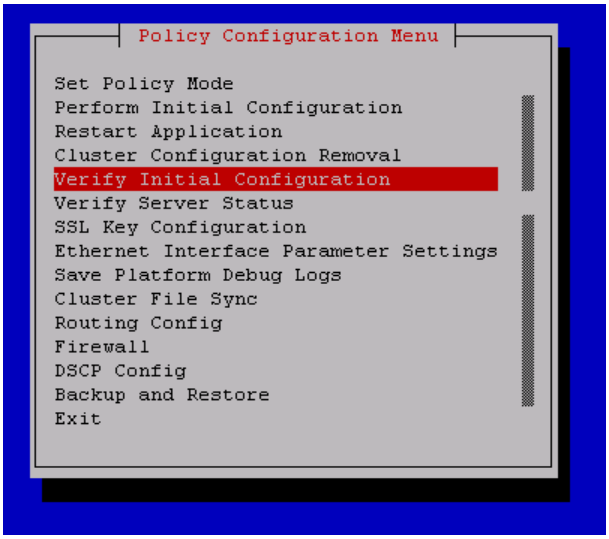
10. ☐	Verify Config	Confirm the configured "Hostname, ServIpAddr, DefaultGw and NtpServIpAddr" previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.  **Skip to step 22**
11. ☐	Perform Initial 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 reference [7] 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 choose "Policy Configuration". 

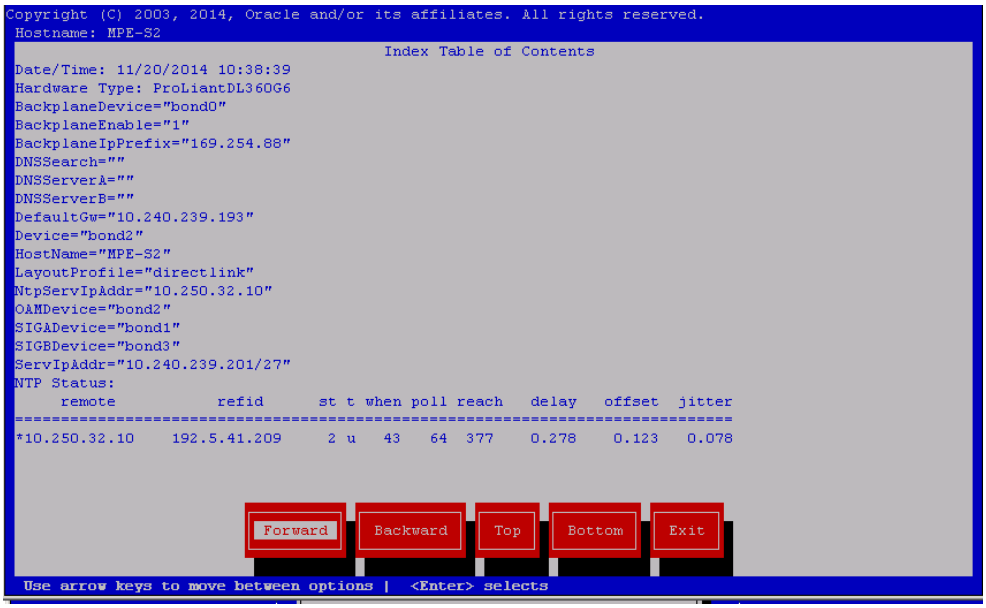
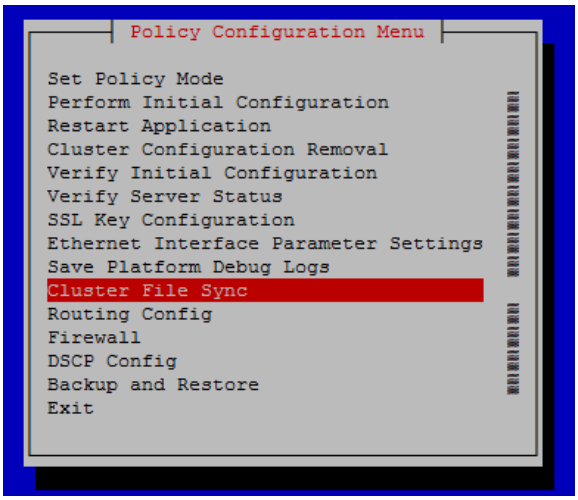
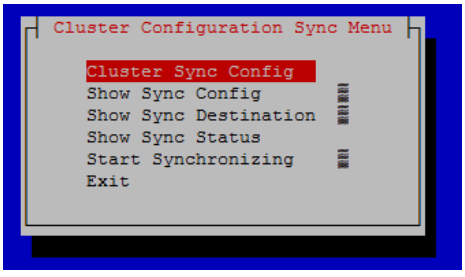
13.	Set Policy Mode	 Then set the mode to “Cable” and click “OK” 
14. ☐	Select Perform Initial Configuration	

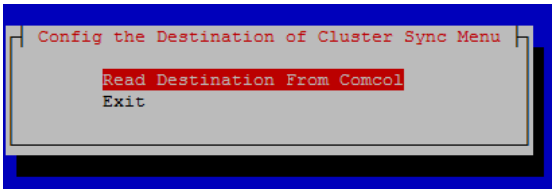
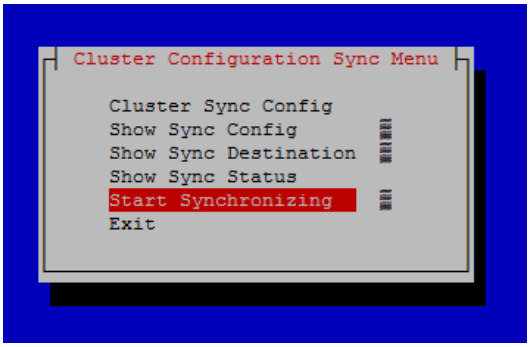
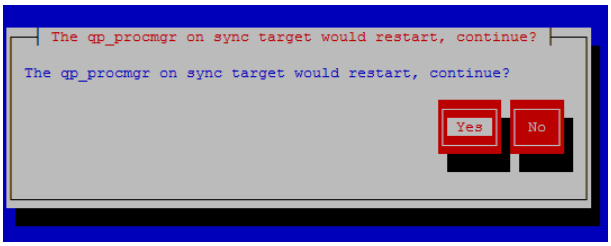
15. ☐ Complete Initial Configuration form



- 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.
- Backplane IP Prefix – the IP prefix assigned to the backplane device. Note that the default value should be used, as changing this value is not supported.

16. ☐	Save configuration	Enter the configuration (example data fill below) and then select **OK**  The platcfg form will pause for a minute while the server is configured, and then return to the platcfg menu.
17. ☐	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 **Policy Configuration** -> **Verify Initial Configuration** from within the platcfg utility. 

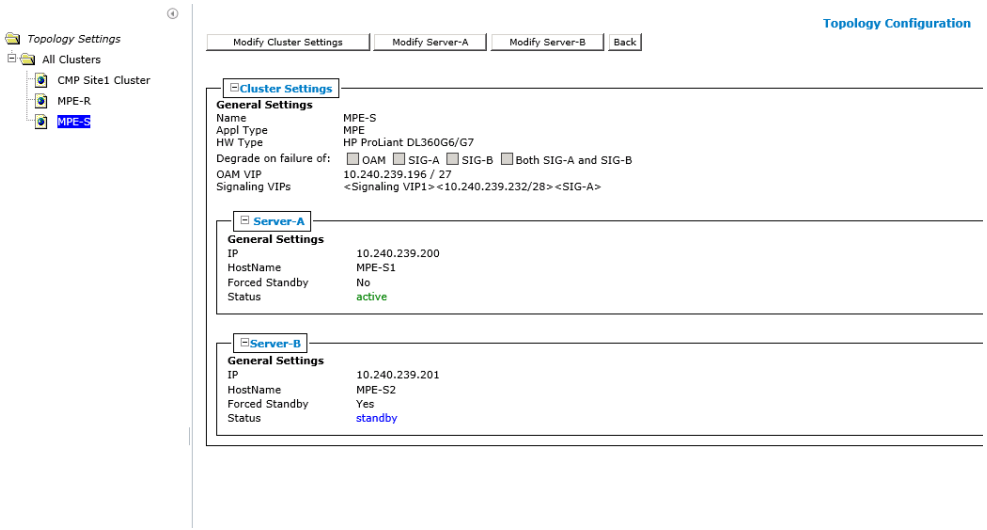
18. ☐	Verify Config	Confirm the configured "Hostname, ServIpAddr , DefaultGw and NtpServIpAddr" previously configured are present. A display similar to the following is shown. 
19. ☐	Reboot the server	Exit from the platcfg menu and Reboot from the command line. 'shutdown –r now '
20. ☐	Perform Cluster 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. From the platcfg menu naviagte to Policy Configuration>Cluster File Sync  You will need to select Cluster Sync Config 

21. ☐	Perform Cluster sync from **the active server to the replacement server**	Read Destination From Comcol  You may need to provide the root password to proceed Now select Start Synchronizong   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.

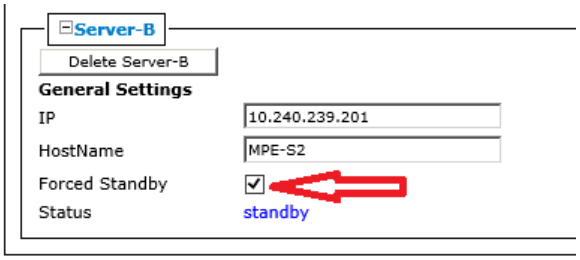
22. ☐	Verify basic network connectivity and server health **on the replacement server**	From the newly installed server, ping the OAM gateway. If the ping is not successful, verify all network settings match the old hardware configuration and reconfigure if needed. Contact Tekelec/Oracle support before 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`
		Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Tekelec/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`

23. ☐ Remove 'Forced Standby' designation on current node.

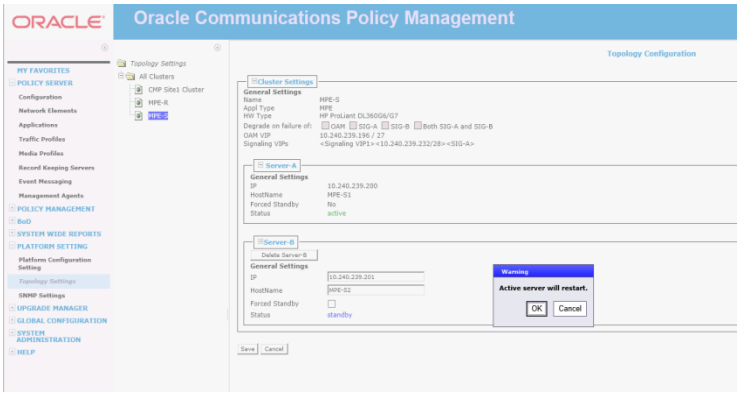
In the CMP GUI:
Navigate to: **Platform Setting → Topology Setting → Current Cluster**



- Modify for the server that has 'forced standby'
- Ensure server status is "***standby***"
- Clear the Forced Standby checkbox



- Accept the resulting pop-up by clicking OK:



24. ☐	Verify cluster status	In the CMP GUI: Navigate to: **Platform Setting → Topology Setting → All → Current MPE-S 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 MPE related 'Active Alarms' (except for the "Accept new upgrade" alarm which will be cleared at the end of this procedure. 

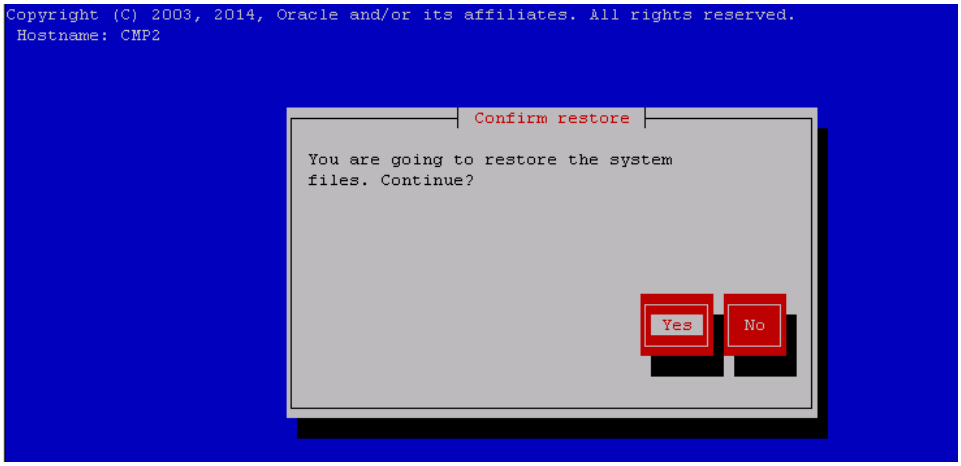
25. ☐	Check DataBase Replication status	You can also monitor the clustering of the new node from within the shell on the active server node with 'irepstat'. To do so, SSH to the Active node of the current cluster and execute the irepstat command:
		
		# irepstat
		
		Expected 'irepstat' output while waiting reconnection:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To CMP2 Active 0 0.00 1%R 0.04%cpu 76B/s`
		`AC To MPE-S1 Active 0 0.00 1%R 0.03%cpu 83B/s`
		`AC To MPE-S2 DownConnecting 0 0.42 1%R 0.04%cpu 84B/s`
		`AC To BOD2 Active 0 0.35 1%R 0.03%cpu 72B/s`
		`AC To BOD1 Active 0 0.00 1%R 0.03%cpu 90B/s`
		
		Expected 'irepstat' output after cluster has formed:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To CMP2 Active 0 0.00 1%R 0.04%cpu 76B/s`
		`AC To MPE-S1 Active 0 0.00 1%R 0.03%cpu 83B/s`
		`AC To MPE-S2 Active 0 0.42 1%R 0.04%cpu 84B/s`
		`AC To BOD2 Active 0 0.35 1%R 0.03%cpu 72B/s`
		`AC To BOD1 Active 0 0.00 1%R 0.03%cpu 90B/s`

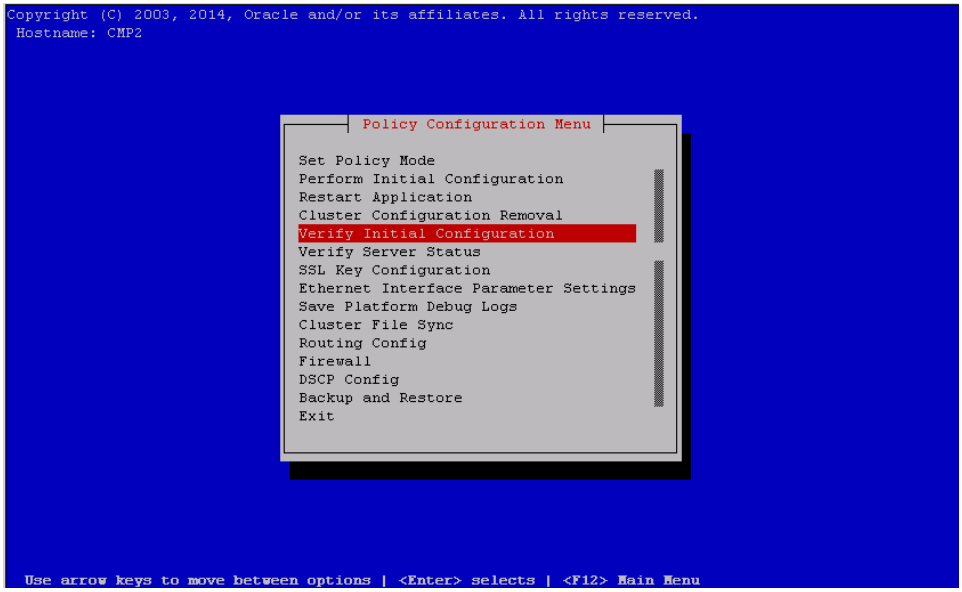
26.	**Active CMP CLI:** Sync SSH keys to all servers in topology	Run the following command to sync the SSH keys of the new MPE server with all servers in the topology:
		
		qpSSHKeyProv.pl --prov --user=root
		
		`[root@CMP1 bin]# qpSSHKeyProv.pl --prov --user=root`
		
		`The password of root in topology:`
		
		`Connecting to root@MPE-R2 (10.240.238.97) ...`
		`Connecting to root@MPE-S1 (10.240.238.98) ...`
		`Connecting to root@MPE-R1 (10.240.238.96) ...`
		`Connecting to root@MPE-S2 (10.240.238.99) ...`
		`Connecting to root@CMP1 (10.240.238.90) ...`
		`Connecting to root@CMP2 (10.240.238.91) ...`
		
		`[2/10] Provisioning SSH keys on MPE-R2 (10.240.238.97) ...`
		
		`[5/10] Provisioning SSH keys on MPE-S1 (10.240.238.98) ...`
		
		`[6/10] Provisioning SSH keys on MPE-R1 (10.240.238.96) ...`
		
		`[7/10] Provisioning SSH keys on MPE-S2 (10.240.238.99) ...`
		
		`[8/10] Provisioning SSH keys on CMP1 (10.240.238.90) ...`
		
		`[10/10] Provisioning SSH keys on CMP2 (10.240.238.91) ...`
		
		`SSH keys are OK.`
		
		`[root@CMP1 bin]#`

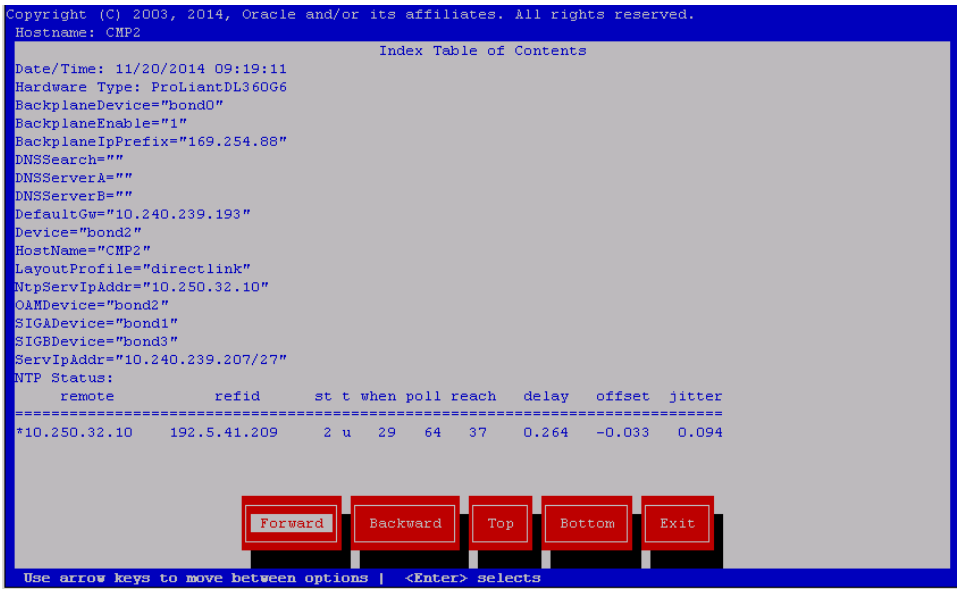
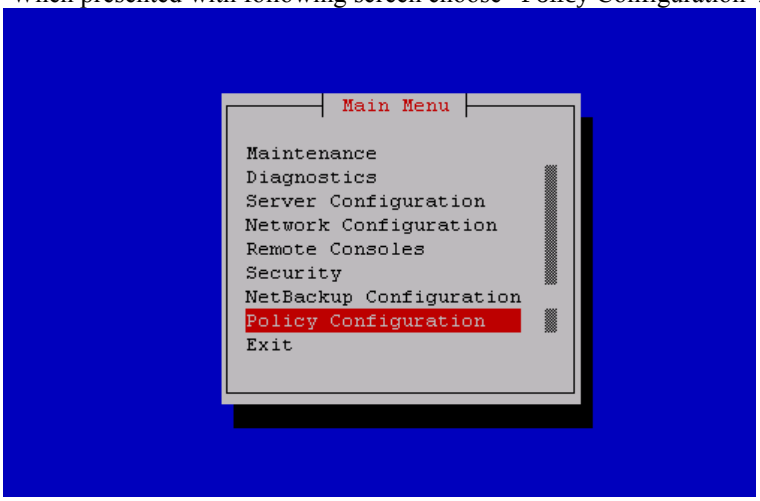
27. ☐	End of procedure	This procedure is completed

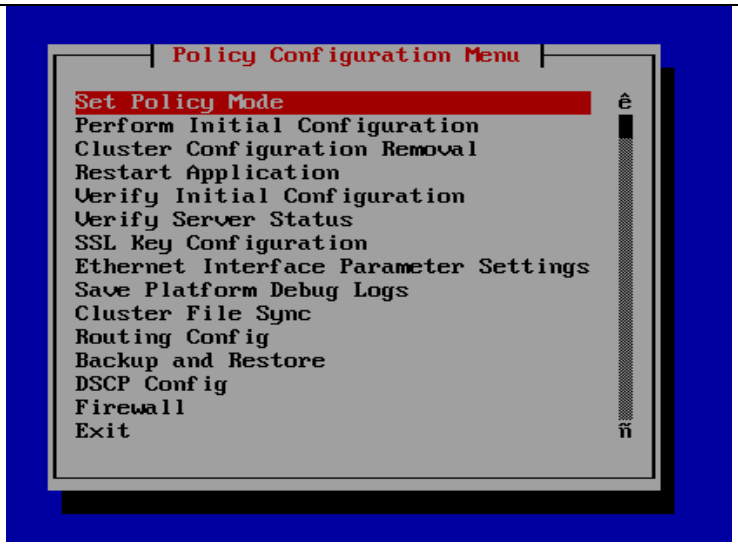
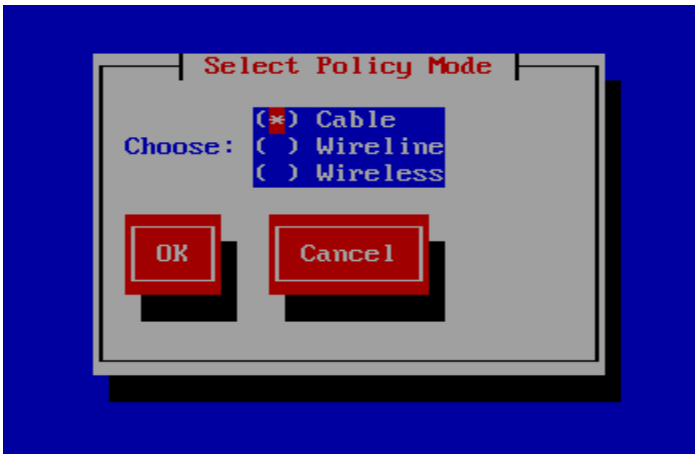
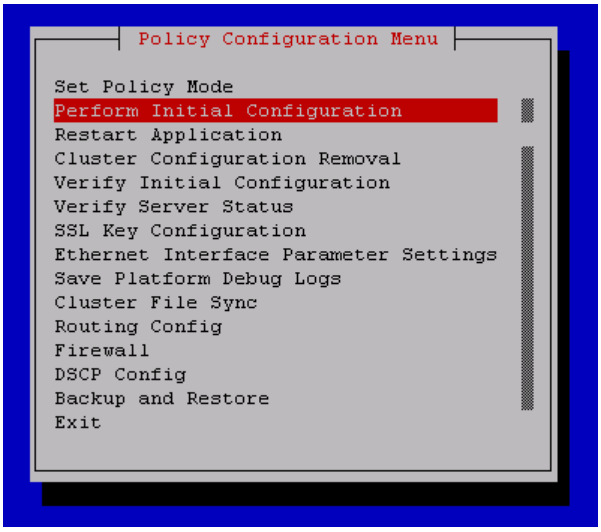
5.3 Procedure 3. Restoring Complete Cluster Outage of the CMP

S T E P #		
	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 Tekelec/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 [7]	
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*.ISO of Active CMP Intial Configuration Information: • OAM IP address, default gateway, NTP & SNMP server IP addresses • Hostname and any static routes required
2. ☐	Prerequisites	- Remove failed hardware and replace. - Verify that that each node has TPD on it, or install TPD - Install the correct version of the application software – CMP - Cable as per network requirements **Reference [7]for detailed 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 to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.* **Reference [7]**for **detailed 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

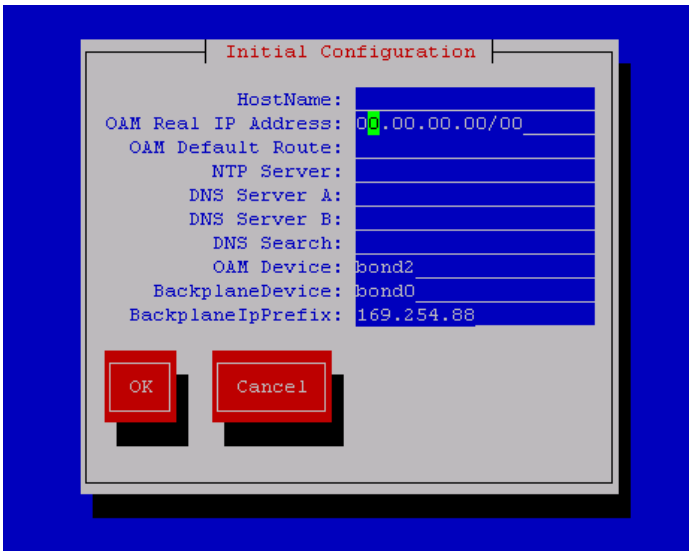
5. ☐	Perform platcfg restore from iLO session to replacement node	Execute the following command **# su – platcfg** From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.ISO that you just put on the system and hit OK – then 'yes' to confirm.  Then choose "Yes" to confirm restore in next message:  This may take a couple of minutes.

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: 
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 **Policy Configuration** > **Verify Initial Configuration** from within the platcfg utility. 

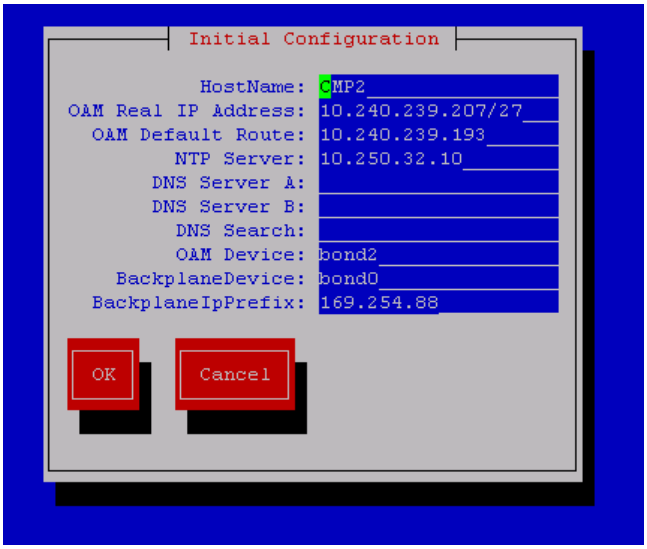
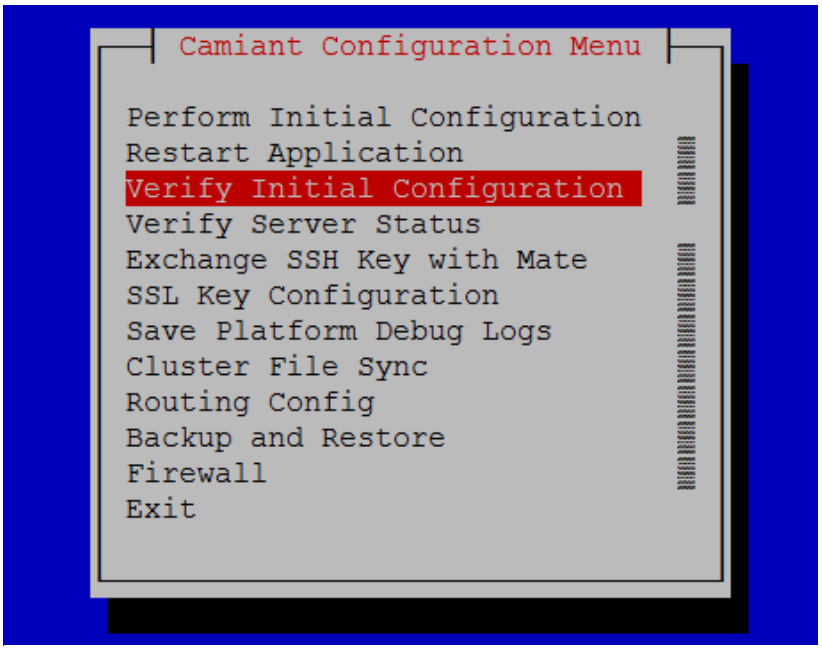
9. ☐	Verify Config	Confirm the configured "Hostname, ServIpAddr, DefaultGw and NtpServIpAddr" previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are.  **Skip to step 19**
10. ☐	Perform Policy 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 reference [7] Note: Customer provided data is required to perform the Policy 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 choose "Policy Configuration". 

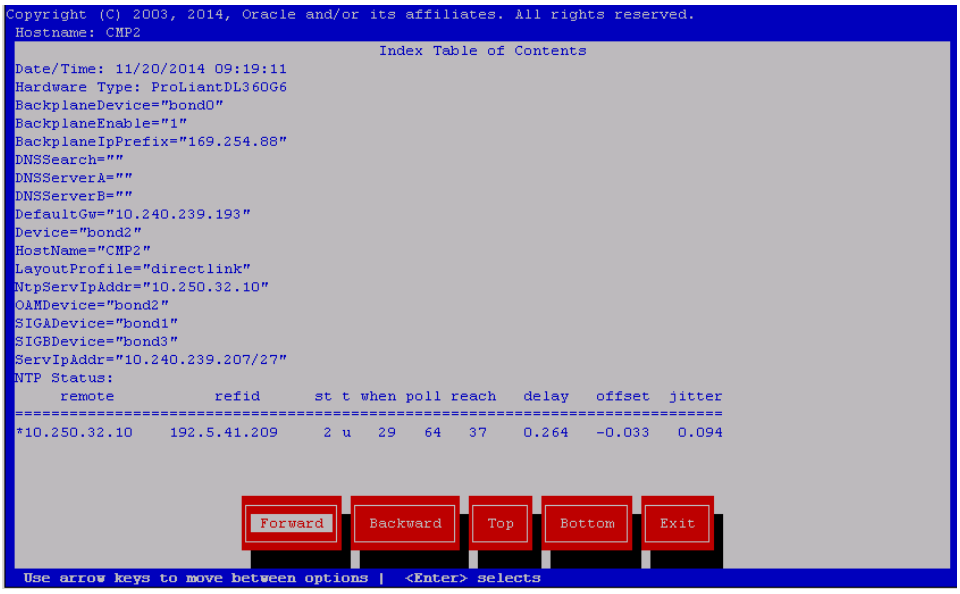
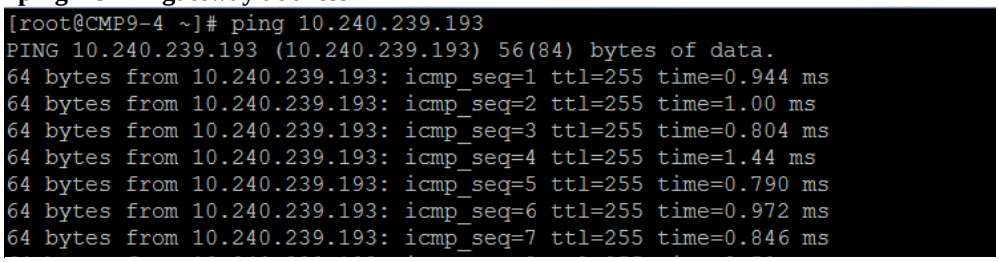
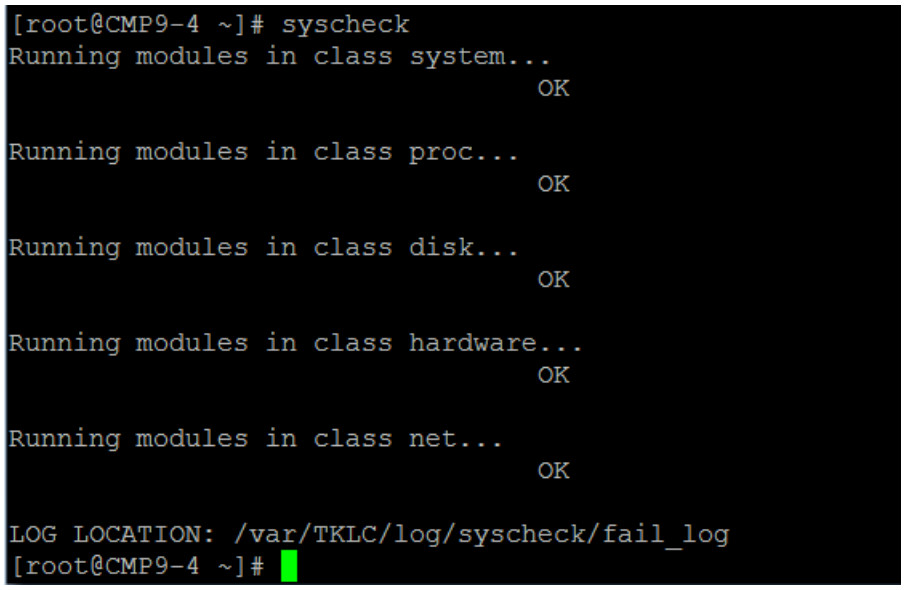
12.	Set Policy mode	 Then set the mode to “Cable” and click “OK” 
13. ☐	Select Perform Initial Configuration	

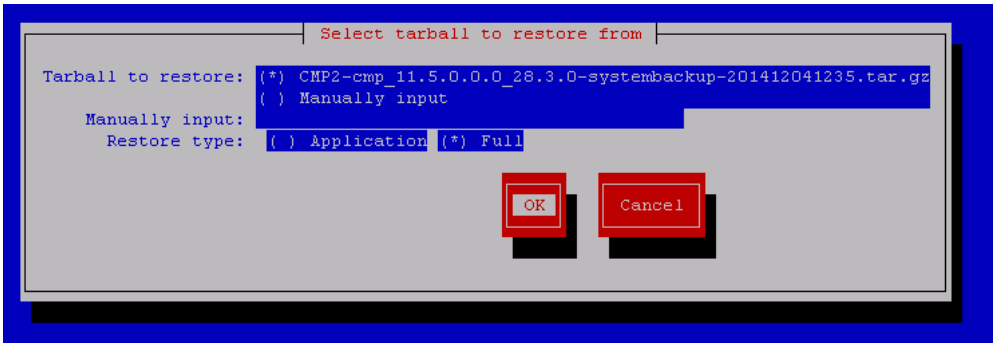
14. ☐ Complete Initial Configuration form

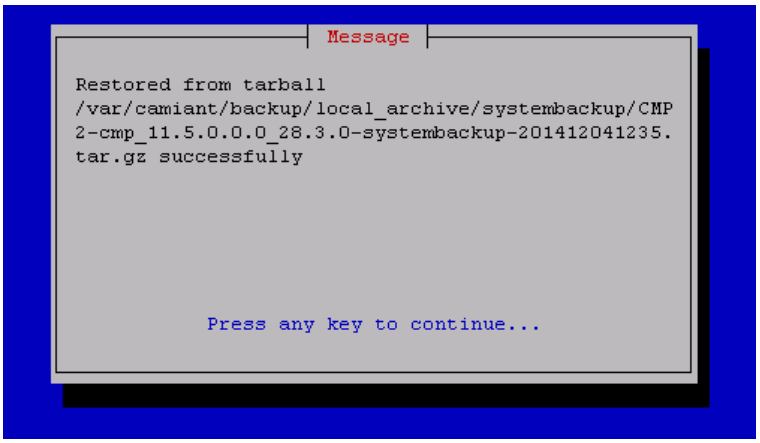


- Hostname - the unique hostname for the device being configured.
- OAM Real IP Address - the IP address that is permanently assigned to this device. (Sometimes called “Physical IP” or “Real IP).
- OAM Default Route - the default route of the OAM network.
- NTP Server - a reachable NTP (required)
- DNS 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.
- Backplane IP Prefix – the IP prefix assigned to the backplane device. Note that the default value should be used, as changing this value is not supported.

15. ☐	Save configuration	Enter the configuration (example data fill below) and then select **OK**  The platcfg form will pause for a minute while the server is configured, and then return to the platcfg menu.
16. ☐	Reboot the server	Exit from the platcfg menu and Reboot from the command line. 'shutdown –r now '
17. ☐	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 **Policy Configuration** -> **Verify Initial Configuration** from within the platcfg utility. 

18. ☐	Verify Config	Confirm the configured "Hostname, ServIpAddr , DefaultGw and NtpServIpAddr" previously configured are present. A display similar to the following is shown. 
19. ☐	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 Tekelec/Oracle support before proceeding if network ping tests still fail. **#ping <OAM gateway address>**  Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Tekelec/Oracle support. 

20. ☐	Proceed with System Restore	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).
21. ☐	Load the 'tarball' for **system restore**	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. • CMP2-cmp_11.5.0.0.0_28.3.0-systembackup-201412041231.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 to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.* **Refer to Reference [7]for detailed directions accessing the iLO, launching the remote console.**
22. ☐	Perform platcfg - restore from SSH session to replacement server	Execute the following command **# su – platcfg** From within the platcfg utility, navigate to: **Policy 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 selecting 'NO'.  Then a screen will appear asking to select the file to restore from. If the file was copied correctly in the previous step, it will be shown here as an option, otherwise select 'Manually Input', mark **'Full'** for the Restore type and then select OK to proceed. 

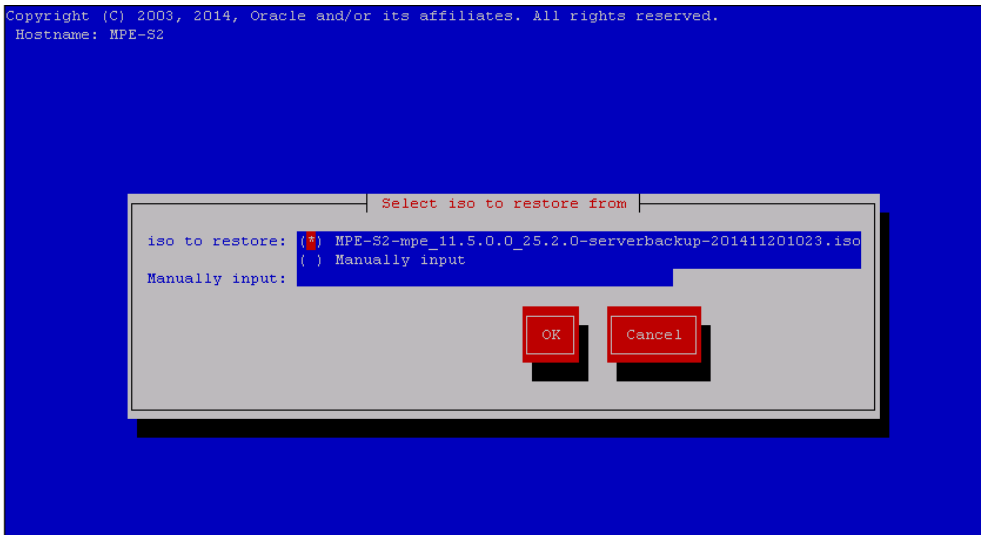
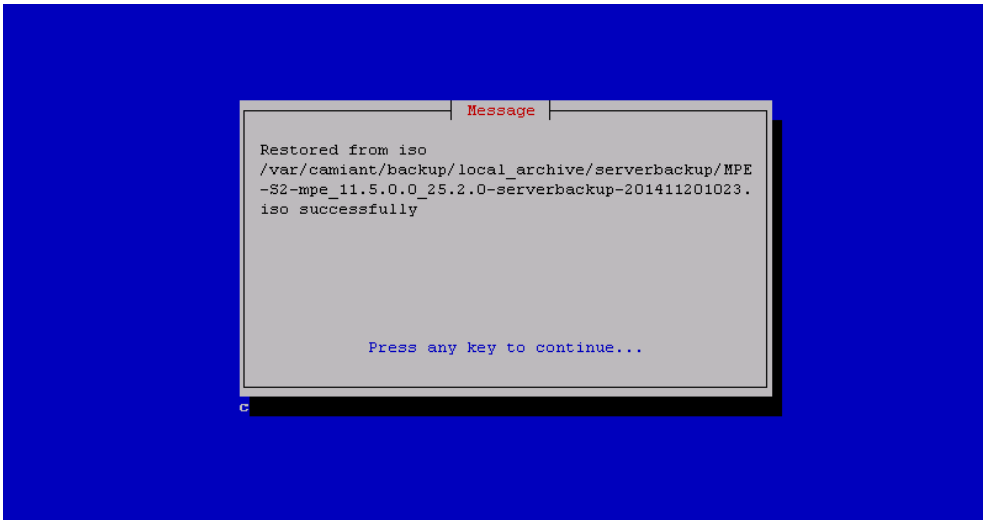
23. ☐	Verify the status	If the restore is successful, then exit from the backup and restore menu. If it is not successful, retry the restore. If the second restore is not successful, stop and contact support team or engineering team for assistance. Be sure that results of restore operation indicate success as in the example below before proceeding: 
24. ☐	Reboot the server	Reboot. Allow the server time to reboot, then reconnect via SSH **#shutdown –r now**
25. ☐	Connect to the newly loaded replacement server with a browser	Using the OAM network ip address assigned during Policy Intial Configuration (or from the server back file) connect with a browser to confirm the application configuration has been restored.
26. ☐	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

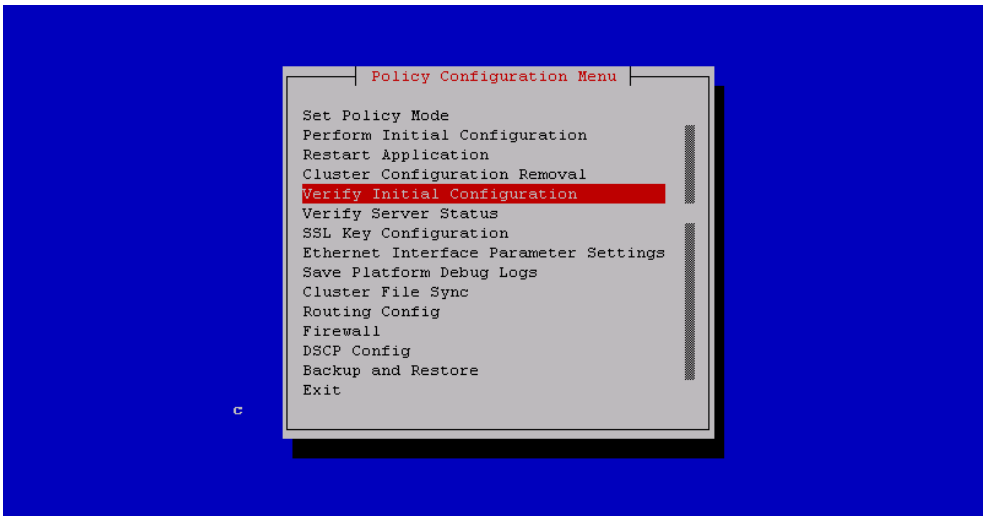
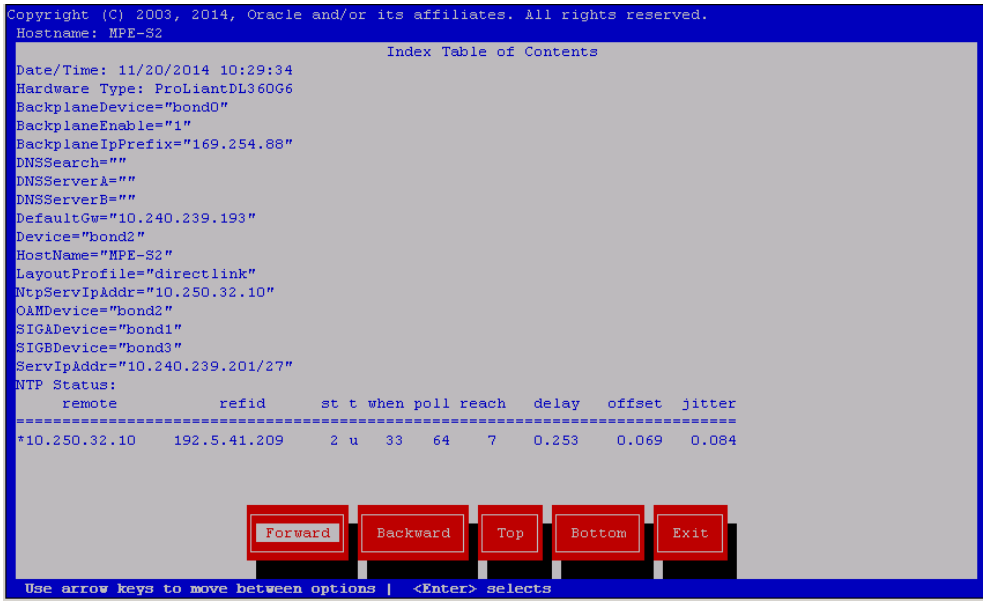
27.	**Active CMP CLI:** Sync SSH keys to all servers in topology	Run the following command to sync the SSH keys of the new CMP server with all servers in the topology:
		
		qpSSHKeyProv.pl --prov --user=root
		
		`[root@CMP1 bin]# qpSSHKeyProv.pl --prov --user=root`
		
		`The password of root in topology:`
		
		`Connecting to root@MPE-R2 (10.240.238.97) ...`
		`Connecting to root@MPE-S1 (10.240.238.98) ...`
		`Connecting to root@MPE-R1 (10.240.238.96) ...`
		`Connecting to root@MPE-S2 (10.240.238.99) ...`
		`Connecting to root@CMP1 (10.240.238.90) ...`
		`Connecting to root@CMP2 (10.240.238.91) ...`
		
		`[2/10] Provisioning SSH keys on MPE-R2 (10.240.238.97) ...`
		
		`[5/10] Provisioning SSH keys on MPE-S1 (10.240.238.98) ...`
		
		`[6/10] Provisioning SSH keys on MPE-R1 (10.240.238.96) ...`
		
		`[7/10] Provisioning SSH keys on MPE-S2 (10.240.238.99) ...`
		
		`[8/10] Provisioning SSH keys on CMP1 (10.240.238.90) ...`
		
		`[10/10] Provisioning SSH keys on CMP2 (10.240.238.91) ...`
		
		`SSH keys are OK.`
		
		`[root@CMP1 bin]#`

28. ☐	End of procedure	This procedure is completed

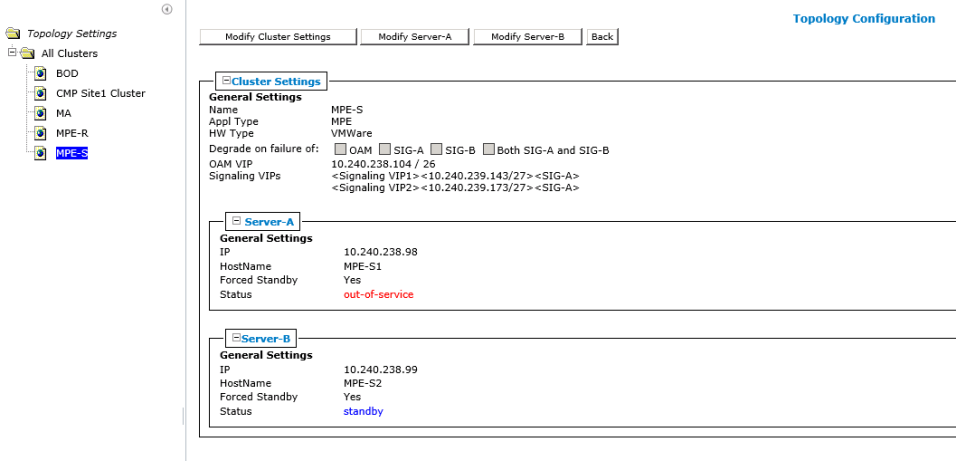
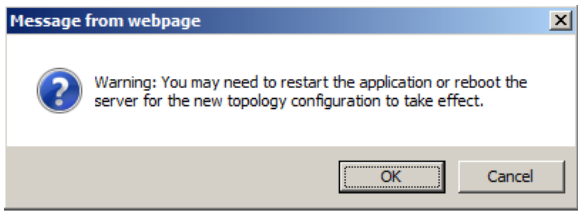
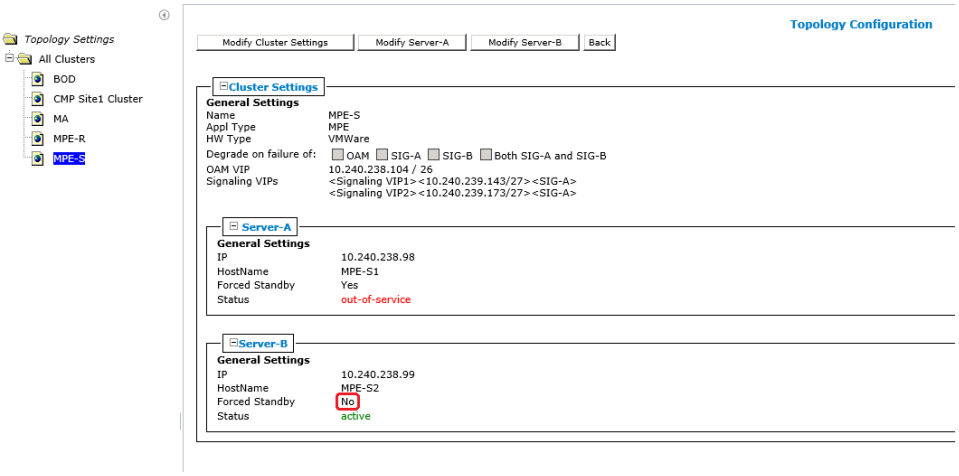
5.4 Procedure 4. Restoring Complete Cluster Outage of the MPE

S T E P #		
	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 Tekelec/Oracle Customer Care Center and ask for assistance. **Note: We will cover the procedures for MPE, however the same procedures could be applied for BOD and/or MA if any or both need recovery.**	
1. ☐	Required resources / information:	The purpose of this procedure is to create the MPE policy cluster from replacement hardware and software, then restore application level configuration by pushing that configuration from the active CMP. In this example, initial Policy 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 Application inssalltion ISO. - *serverbackup*.ISO of the node to be replaced
2. ☐	Prerequisites	- Remove and replace both nodes - IPM both nodes (fresh install of TPD software) - 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: Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.* **Reference [7]for detailed 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

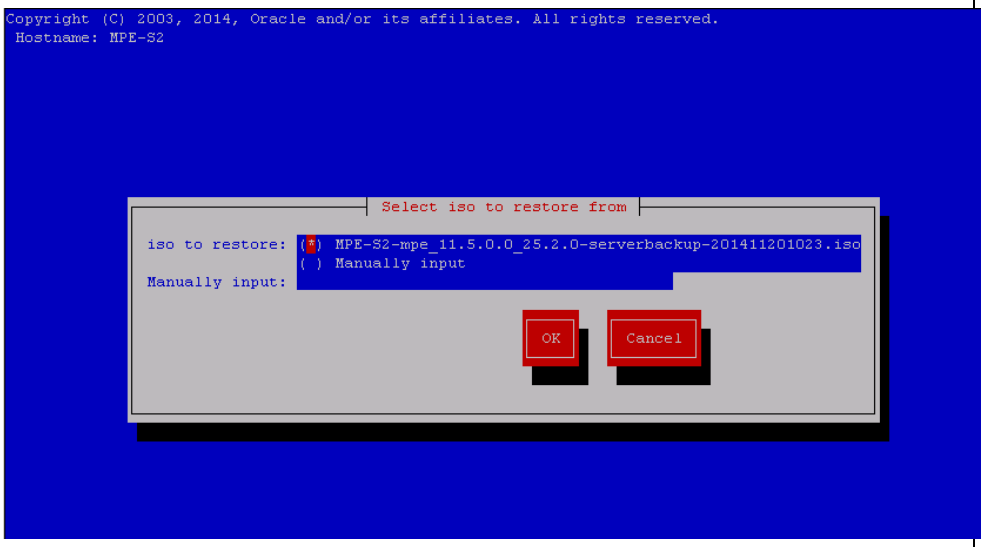
5. ☐	Perform platcfg restore from iLO remote console	Execute the following command **# su – platcfg** From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.ISO that you just put on the system and hit OK – then 'yes' to confirm.  This may take a couple of minutes.
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: 
7. ☐	Reboot the server	Exit form the platcfg menu and Reboot from the command line. 'shutdown –r now'

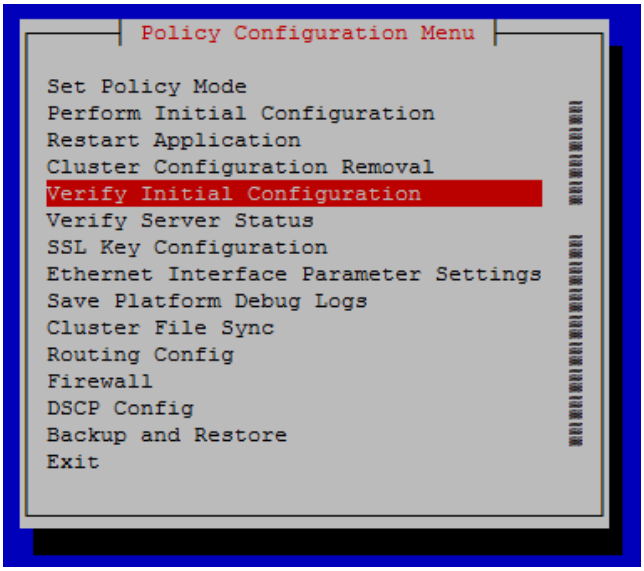
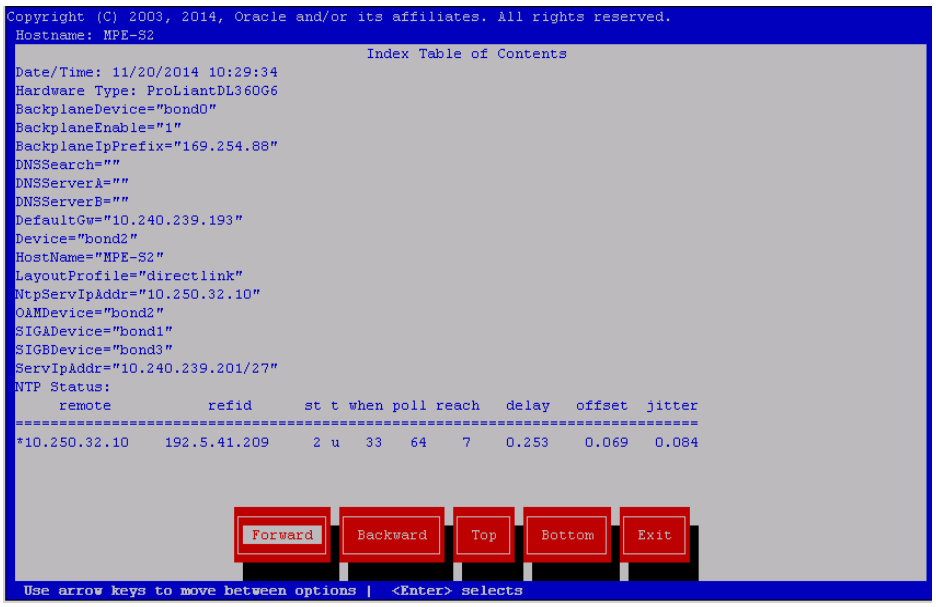
8. ☐	Verify Config	After the server has been rebooted you should be returned to a login prompt via the iLO remote console. Verify the configuration by selecting **Policy Configuration** > **Verify Initial Configuration** from within the platcfg utility. 
9. ☐	Verify Config	Confirm the configured "Hostname, 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. 

10. ☐	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 Tekelec/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`
		Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Tekelec/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`

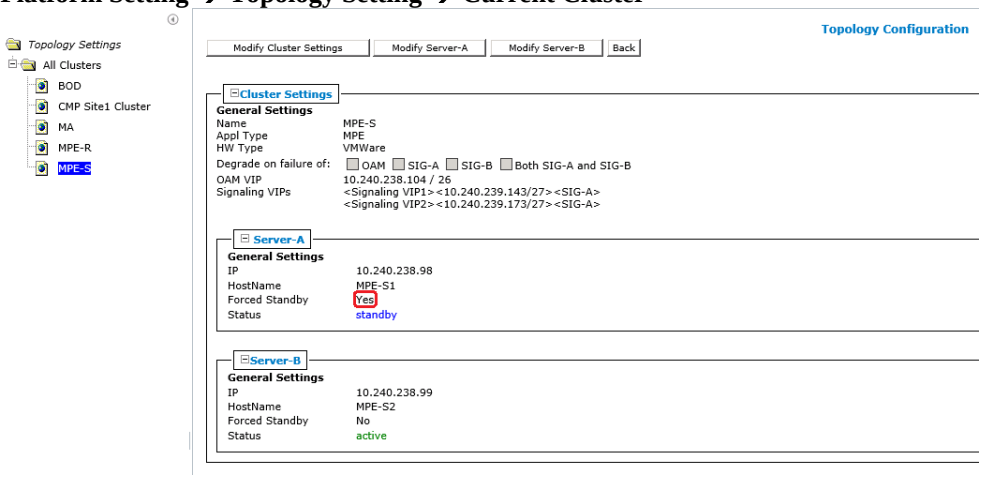
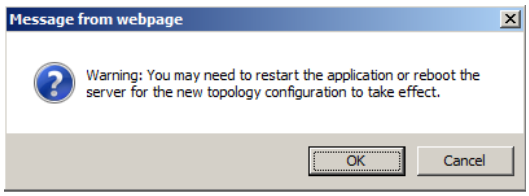
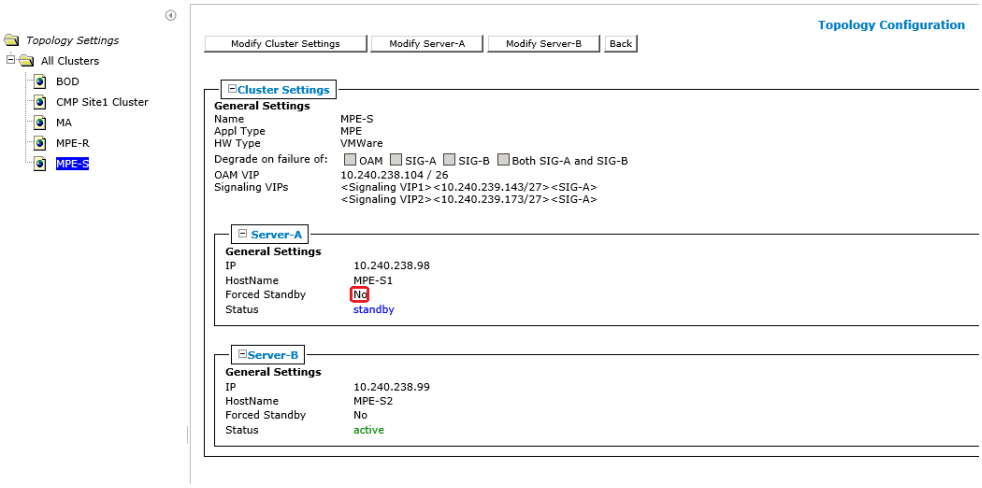
11. ☐	Set 'Forced Standby' designation on cluster node that is still 'out-of-service'.	In the CMP GUI: Navigate to: **Platform Setting → Topology Setting → Current Cluster**  - Modify the server that has been restored - Uncheck the Forced Standby checkbox - Accept the resulting pop-up by clicking OK:  - Click Save 

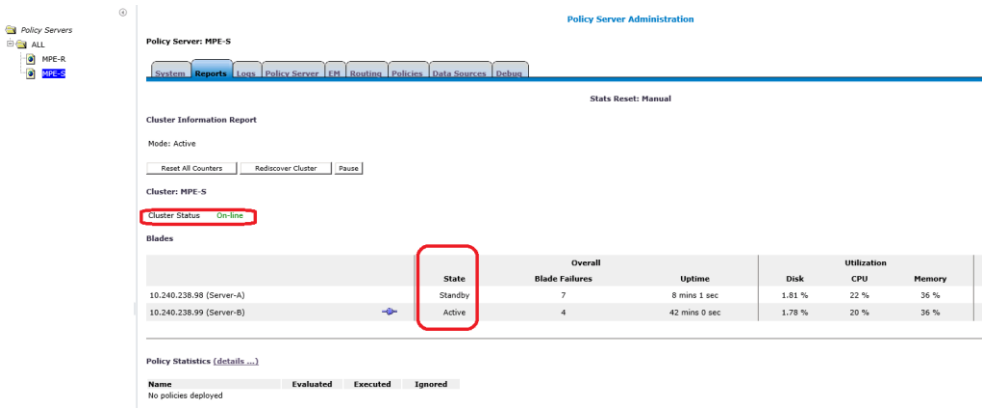
12. ☐	Check status	In the CMP GUI: Navigate to: **Policy Server → Configuration →Cluster System tab** Check system tab for the MPE cluster being recovered. If the Status field indicates 'Config Mismatch', click the 'Reapply Configuration' button and wait for the 'Config Mismatch' designation to disappear. If it does not, contact Tekelec/Oracle support before proceeding. 
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.** *Note: Later in this procedure, the platcfg restore function checks this directory and offers the user a convenient menu to choose from. The platcfg utility also allows the user to manually enter any mounted path on the server.* **Reference [7]**for **detailed 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	Execute the following command **# su – platcfg** From within the platcfg utility, navigate to: **Policy Configuration → Backup and Restore → Server Restore** Select the *serverbackup*.ISO that you just put on the system and hit OK – then 'yes' to confirm.  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.
17. ☐	Reboot the server	Exit form the platcfg menu and Reboot from the command line. 'shutdown –r now'

18. ☐	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 **Policy Configuration** > **Verify Initial Configuration** from within the platcfg utility. 
19. ☐	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. 

20. ☐	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 Tekelec/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`
		Execute the syscheck command, ensuring that all tests return successfully. If errors are found, discontinue this procedure and contact Tekelec/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`

21. ☐	Remove 'Forced Standby' designation on current node.	In the CMP GUI: Navigate to: **Platform Setting → Topology Setting → Current Cluster**  - Modify for the server that has 'forced standby' - Clear the Forced Standby checkbox - Accept the resulting pop-up by clicking OK:  - Click Save 

22. ☐	Check status	In the CMP GUI: o Navigate to: **Policy Server → Configuration → All → Reports Tab** Monitor clustering of the replacement node to its peer, do not proceed until the Cluster Status returns from 'Degraded' to 'On-line' 

23. ☐	Check DataBase Replication 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 execute the irepstat command:
		# irepstat
		
		Expected 'irepstat' output while waiting reconnection:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To CMP2 Active 0 0.00 1%R 0.04%cpu 76B/s`
		`AC To MPE-S1 Active 0 0.00 1%R 0.03%cpu 83B/s`
		`AC To MPE-S2 DownConnecting 0 0.42 1%R 0.04%cpu 84B/s`
		`AC To BOD2 Active 0 0.35 1%R 0.03%cpu 72B/s`
		`AC To BOD1 Active 0 0.00 1%R 0.03%cpu 90B/s`
		
		Expected 'irepstat' output after cluster has formed:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`AA To CMP2 Active 0 0.00 1%R 0.04%cpu 76B/s`
		`AC To MPE-S1 Active 0 0.00 1%R 0.03%cpu 83B/s`
		`AC To MPE-S2 Active 0 0.42 1%R 0.04%cpu 84B/s`
		`AC To BOD2 Active 0 0.35 1%R 0.03%cpu 72B/s`
		`AC To BOD1 Active 0 0.00 1%R 0.03%cpu 90B/s`

24.	**Active CMP CLI:** Sync SSH keys to all servers in topology	Run the following command to sync the SSH keys of the new MPE server with all servers in the topology:
		
		qpSSHKeyProv.pl --prov --user=root
		
		`[root@CMP1 bin]# qpSSHKeyProv.pl --prov --user=root`
		
		`The password of root in topology:`
		
		`Connecting to root@MPE-R2 (10.240.238.97) ...`
		`Connecting to root@MPE-S1 (10.240.238.98) ...`
		`Connecting to root@MPE-R1 (10.240.238.96) ...`
		`Connecting to root@MPE-S2 (10.240.238.99) ...`
		`Connecting to root@CMP1 (10.240.238.90) ...`
		`Connecting to root@CMP2 (10.240.238.91) ...`
		
		`[2/10] Provisioning SSH keys on MPE-R2 (10.240.238.97) ...`
		
		`[5/10] Provisioning SSH keys on MPE-S1 (10.240.238.98) ...`
		
		`[6/10] Provisioning SSH keys on MPE-R1 (10.240.238.96) ...`
		
		`[7/10] Provisioning SSH keys on MPE-S2 (10.240.238.99) ...`
		
		`[8/10] Provisioning SSH keys on CMP1 (10.240.238.90) ...`
		
		`[10/10] Provisioning SSH keys on CMP2 (10.240.238.91) ...`
		
		`SSH keys are OK.`
		
		`[root@CMP1 bin]#`

25. ☐	End of procedure	This procedure is completed

Appendix A: Contacting Oracle

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

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration. Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*

When calling,make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
• For Technical issues such as creating a new Service Request (SR), Select **1**
• For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

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

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.