Oracle® Communications Diameter Signaling Router 7.1

Hardware and Software Installation Procedure 1/2

E53488 Revision 01

July 2015

ORACLE®

Oracle® Communications Diameter Signaling Router 7.1 Hardware and Software Installation Procedure

1/2

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This document provides the methods and procedures used to configure the DSR 7.1 Management Server TVOE and PM&C, initialize the system's aggregation switches and enclosure switches, and perform the initial configuration of the DSR system's RMS and HP c-Class enclosure.

Following the execution of the subject document the DSR user will follow a DSR application procedure document (*E58954-02*) to complete the DSR application specific configurations.

The procedures in this document should be executed in order. Skipping steps or procedures is not allowed unless explicitly stated.

Note: Before executing any procedures in this document, power must be available to each component, and all networking cabling must be in place. Switch uplinks to the customer network should remain disconnected until instructed otherwise.

The audience for this document includes Oracle customers and:

- Software System
- Product Verification
- Documentation
- Customer Service including Software Operations and First Office Applications
- Oracle Partners

1.1 References

For HP Blade and RMS firmware upgrades, Software Centric customers will need the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes on *http://docs.oracle.com* under Platform documentation. Beyond the minimum version specified for the Platform below, the application will dictate which Firmware Upgrade Packs to use.

1. *DSR 7.0/7.1 Software Installation and Configuration Procedure Part 2/2*, E58954:
2. *HP Solutions Firmware Upgrade Pack*, version 2.x.x (the latest is recommended if an upgrade is to be performed, otherwise version 2.2.8 is the minimum)
3. *HP Solutions Firmware Upgrade Pack, Software Centric Release Notes* (the latest version is recommended if an upgrade is performed, otherwise the minimum version is 2.2.8)
4. *Oracle Firmware Upgrade Pack Release Notes,* version 3.x.x (the latest version is recommended if an upgrade is performed, otherwise 3.1.3 is the minimum)
5. *Oracle Firmware Upgrade Pack Upgrade Guide*, version 3.x.x
6. *TPD Initial Product Manufacture Software Installation Procedure*, E53017

1.2 Acronyms

An alphabetized list of acronyms used in the document:

Table 1: Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CA	Certificate Authority
CSR	Certificate Signing Request
DNS	Domain Name System
DSCP	Differentiated Services Code Point, a form of QoS
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FMA	File Management Area
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
HP FUP	HP Firmware Upgrade Pack
iLO	Integrated Lights Out remote management port
ILOM	Integrated Lights Out Manager

Acronym	Definition
IE	Internet Explorer
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MSA	Modular Smart Array
NAPD	Network Architecture Planning Diagram
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
PM&C	Platform Management & Configuration
RMS	Rack Mount Server
QOS	Quality of Service
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSO	Single Sign On
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VSP	Virtual Serial Port

1.3 Terminology

Multiple server types may be involved with the procedures in this manual. Therefore, most steps in the written procedures begin with the name or type of server to which the step applies. For example:

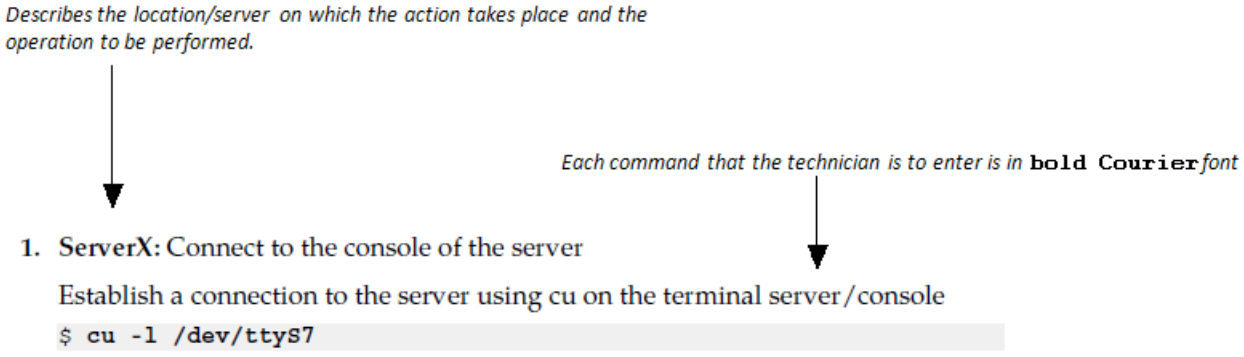


Figure 1: Example Of An Instruction That Indicates The Server To Which It Applies

Table 2: Terminology

Community String	An SNMP community string is a text string used to authenticate messages sent between a management station and a device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Domain Name System	A system for converting hostnames and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol
Management Server	An HP ProLiant DL 360/DL 380 that has physical connectivity required to configure switches and may host the PM&C application or serve other configuration purposes.
NetBackup Feature	Feature that provides support of the Symantec NetBackup client utility on an application server.
Non-Segregated Network	Network interconnect where the control and management, or customer, networks utilize the same physical network.
PM&C	An application that supports platform-level capability to manage and provision platform components of the system, so they can host applications.
Segregated Network	Network interconnect where the control and management, or customer, networks utilize separate physical networks.
Server	A generic term to refer to a server, regardless of underlying hardware, be it physical hardware or a virtual TVOE guest server.
Software Centric	A term used to differentiate between customers buying both hardware and software from Oracle, and customers buying only software.
Virtual PM&C	Additional term for PM&C - used in networking procedures to distinguish activities done on a PM&C guest and not the TVOE host running on the Management server.

1.4 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.

1.5 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.

1.6 Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

1.7 Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

Chapter 2

Acquiring Firmware

Topics:

2.1 Acquiring Firmware

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices that are part of the Platform 7.0.x configuration.

Platform 7.0.x servers and devices requiring possible firmware updates are:

- HP c7000 BladeSystem Enclosure Components:
  - Onboard Administrator
  - 1Gb Ethernet Pass-Thru Module
  - Cisco 3020 Enclosure Switches
  - HP6120XG Enclosure Switches
  - HP6125G Enclosure Switches
  - HP6125XLG Enclosure Switches
  - Brocade Fibre Channel Switches
  - Blade Servers (BL460/BL620)
- HP Rack Mount Servers (DL360 / DL380)
- HP External Storage Systems
  - MSA2012fc
  - D2200sb (Storage Blade)
  - D2220sb (Storage Blade)
  - D2700
  - P2000
- Cisco 4948/4948E/4948E-F Rack Mount Network Switches

2.1.1 HP

Software Centric Customers do not receive firmware upgrades through Oracle. Instead, refer to the *HP Solutions Firmware Upgrade Pack, Software Centric Release Notes* on *http://docs.oracle.com* under Platform documentation. The latest release is recommended if an upgrade is performed, otherwise release 2.2.8 is the minimum.

The required firmware and documentation for upgrading the firmware on HP hardware systems and related components are distributed as the HP *Solutions Firmware Upgrade Pack 2.x.x*. The minimum firmware release required for Platform 7.0.x is *HP Solutions Firmware Upgrade Pack 2.2.8*. However, if a firmware upgrade is needed, the current GA release of the *HP Solutions Firmware Upgrade Pack 2.x.x* should be used.

Each version of the *HP Solutions Firmware Upgrade Pack* [2] contains multiple items including media and documentation. If an HP FUP 2.x.x version newer than the Platform 7.0.x minimum of HP FUP 2.2.8 is used, then the *HP Solutions Firmware Upgrade Guide* [3] should be used to upgrade the firmware. Otherwise, the Upgrade Guide of the *HP Solutions Firmware Upgrade Pack* [2] is not used for new installs. Instead, this document provides its own upgrade procedures for firmware.

The three pieces of required firmware media provided in the *HP Solutions Firmware Upgrade Pack 2.x.x* releases are:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP Service Pack for ProLiant (SPP) firmware USB image
- HP MISC Firmware ISO image

Refer to the Release Notes of the *HP Solutions Firmware Upgrade Pack* [2] to determine specific firmware versions provided. Contact *1.4 My Oracle Support (MOS)* for more information on obtaining the HP Firmware Upgrade Pack.

Chapter 3

Install Overview

Topics:

This section contains the installation overview, and includes information about required materials, strategies, and SNMP configuration.

This section will configure the DSR base hardware systems (RMS and HP c-Class enclosure) (RMS and Blade IPM, Networking, Enclosure and PM&C Configuration). Following the execution of this document the DSR user will follow a DSR application procedure document (*E58954-02*) to complete the DSR application specific configurations.

Note that IPM refers to installing either TVOE or TPD on the target system. TVOE is used when virtualization is needed (e.g., for the PM&C and NO/SO). TPD is used for systems that do not require virtualization and for the Virtual Machines.

3.1 Required Materials

1. One (1) ISO of TPD 7.x, release specified by Release Notes.
2. One (1) ISO of PM&C 6.x, release specified by Release Notes.
3. One (1) USB of TVOE 3.0, release specified by Release Notes.
4. One (1) USB or ISO of DSR 7.1 and all configuration files and templates acquired via the DSR ISO.
5. Passwords for users on the local system.
6. Access to the iLO Terminal or direct access to the server VGA port.
7. *Oracle Firmware Upgrade Pack*, version 3.x.x (the latest version should be used if an upgrade is being performed, otherwise 3.1.3 is the miniumum).
8. *HP Solutions Firmware Upgrade Pack*, version 2.x.x (the latest version must be used if an upgrade is to be performed, otherwise version 2.2.8 is the minimum). A 4Gb or larger USB Flash Drive.
9. NAPD and all relevant configuration materials for ALL sites involved. This includes host IP addresses, site network element XML files, and netConfig configuration files.
10. Keyboard and monitor if configuring iLO addresses.

Note: Customers are required to download all software from the Oracle Software Delivery Cloud (OSDC). A readme file which provides instructions for the Customer to create required bootable USBs using the .usb file will be included with the software. Please obtain required bootable USBs from the customer representative.

3.2 Installation Strategy

To ensure a successful application installation, carefully plan and assess all configuration materials and installation variables. After a customer site survey has been conducted, an installer can use this section to plan the exact procedure list that should be executed at each site.

The following list summarizes this process.

1. An overall installation requirement is established. This data that should be collected:
   - The total number of sites
   - The number of servers at each site and their role(s)
   - Determine whether the application's networking interface terminates on a Layer 2 or Layer 3 boundary
   - Establish the number of enclosures at each site (if any)
   - Determine if the application uses rack-mount servers or server blades
   - What time zone should be used across the entire collection of application sites
   - Will SNMP traps be viewed at the application level, or will an external NMS be used (or both)
2. A site survey is conducted to determine exact networking and site details. Additionally, IP networking options must be well understood, and IP address allocations collected from the customer, in order to complete switch configurations

3.3 SNMP Configuration

The network-wide plan for SNMP configuration should be decided upon before DSR installation proceeds. This section provides some recommendations for these decisions.

SNMP traps can originate from the following entities in a DSR installation:

- DSR Application Servers (NOAMP, SOAM, MPs of all types)
- DSR Auxiliary Components (OA, Switches, TVOE hosts, PMAC)

DSR application servers can be configured to:

Application server SNMP configuration is done from the NOAMP GUI, near the end of DSR installation. See the procedure list for details.

DSR Auxiliary components must have their SNMP trap destinations set explicitly. Trap destinations can be the NOAMP VIP, the SOAMP VIP, or an external (customer) NMS. The recommended configuration is as follows:

The following components:

- TVOE for PMAC server
- PMAC (App)
- OAs
- All Switch types (4948, 3020, 6120, 6125)
- TVOE for DSR Servers

Should have their SNMP trap destinations set to:

1. The local SOAM VIP
2. The customer NMS, if available

Note: All the entities **MUST** use the same Community String during configuration of the NMS server.

Note: SNMP community strings i.e. (Read Only or Read Write SNMP community strings) should be same for all the components like OAM/MP servers, PMACs, TVOEs and external NMS.

Note: Default SNMP Trap port used to receive traps is 162. Customer can provide the port number from the SNMP configuration screen

3.4 NTP Strategy

The following set of general principals capture the recommendations for NTP configuration of DSR.

Principle 1 - Virtual guests should not be used as NTP servers

Avoid specifying virtual guests as NTP references for other servers. Guest emulated clocks have been shown to result in poor NTP server behavior

Principle 2 - Virtual guests should synchronize to their virtual hosts

When virtualization is used in the product deployment, virtual guests should use their TVOE hosts as their NTP references.

Principle 3 - Follow a topology based approach

MP servers should use their topology parents (SOAMs in a three tier topology), or if those parents are virtual guests, the enclosing virtual hosts should be used instead. The PM&C TVOE host should be used as a third NTP source. See *Figure 2: Per Site NTP Topology* for clarification.

Similarly SOAM servers should use their topology parents (NOAMs), or if those parents are virtual guests, the enclosing virtual hosts should be used instead. See *Figure 2: Per Site NTP Topology* for clarification.

NOAMP and other A-Level servers should use a pool of reliable, customer provided references if the NOAMPs are implemented in hardware, otherwise they should sync to their virtual hosts.

Principle 4 - Provide a robust pool of sources

The pool of customer NTP server references should be of stratum 3 or above, accurate and highly reliable. If possible both local site server and backup remote site servers should be provided. Three or more customer NTP sources are required.

Principle 5 - Prefer local references

When references from multiple sites or networks are used on one server, the "prefer" keyword should be applied to the local references.

Principle 6 - Ensure connectivity

Care should be taken to ensure that all NTP references are reachable through the appropriate networking configuration. In particular firewall rules must be correctly specified to allow NTP clients to connect to their specified references.

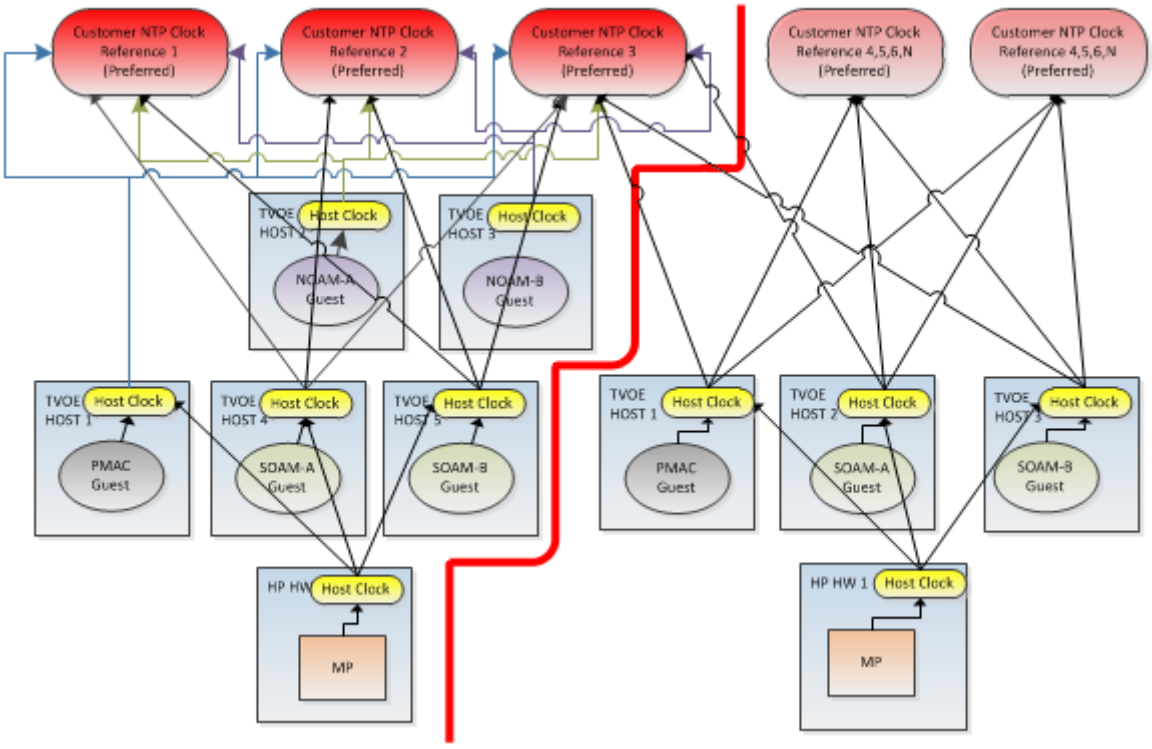


Figure 2: Per Site NTP Topology

3.5 Overview of DSR Networks

This table presents an overview of the networks configured and used by DSR at a site. Based on the deployment type/requirements, the networks could be physically or logically separated via VLANs.

Network Name	Default VLAN ID*	Routable	Description
Control	1	No	Network used by PM&C to IPM the servers/blades/VMs. Refer to the NAPD for site-specific IP information. (IPs are assigned via by the PM&C using DHCP)
Management	2	Yes	Network used for iLO interfaces, OAs, and enclosure switches. Also used to provide remote access to the TVOE and PM&C servers

Network Name	Default VLAN ID*	Routable	Description
XMI	3	Yes	Network used to provide access to the DSR entities (GUI, ssh), and for inter-site communication
IMI	4	No	Network used for intra-site communication
XSI-1	5	Yes	Network used for DSR signaling Traffic
XSI-2**	6	Yes	Network used for DSR signaling Traffic
XSI-3**	7	Yes	Network used for DSR signaling Traffic
XSI-4**	8	Yes	Network used for DSR signaling Traffic

* The VLAN ID assignments are site and deployment specific.

** Optional

Chapter 4

Software Installation Procedures

Topics:

This section contains the software installation procedures, including preparation and configuration information for a site.

The procedures in this section are expected to be executed in the order presented in this section.

If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

Sudo

Platform 6.7 introduced a new non-root user 'admusr'. As a non-root user, many commands --when run as admusr-- now require the use of 'sudo'. Using sudo will require a password with the first command, as well as intermittently over a period of time. Therefore, if a prompt for the "`[sudo] password:`" appears, the user should re-enter the admusr login password.

Example:

```
[admusr@hostname ~]$ sudo <command>
[sudo] password for admusr: <ENTER
 PASSWORD HERE>
<command output omitted>
[admusr@hostname ~]$
```

4.1 Configure and IPM Management Server

Note: The Management Server is installed as a Virtual Host environment, and will host the PM&C application, and may host other DSR applications (as defined by the deployment configuration for the customer site).

Note: Depending on the deployment plan, a server may be IPM'ed with either TVOE (if virtualization is needed) or TPD (if no virtualization is needed)

4.1.1 Installing TVOE on the Management Server

Install the TVOE Hypervisor platform on the Management Server

The PM&C is not available to do an IPM of the TVOE management server. It is necessary to physically provide the TVOE media via a bootable USB. Refer to section *3.1 Required Materials* for more information.

1. For more information about configuring the iLO IP address, refer to Appendix F in *Initial Product Manufacture*, E53017[6].
2. Install TVOE onto the Management Server

   Follow *4.1.1.1 IPM DL360 or DL380 Server* to IPM the management server with TVOE.

4.1.1.1 IPM DL360 or DL380 Server

This procedure provides instructions for configuring and IPMing the DL360 or DL380 server.

Needed material:

- TPD or TVOE installation media to be used for IPM.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

Configure and IPM the DL360 or DL380 server

Follow Appendix C *Initial Product Manufacture of Server* to configure and IPM the management server.

For a DL360 G6/G7 or DL380 G6/Gen8/Gen9 server, the correct options to use for the IPM of the management server are:

```
TPDnoraid console=tty0 diskconfig=HWRAID,force
```

Note: Do not use the remote serial console for installation.

4.1.2 Upgrade Management Server Firmware

Software Centric Customers: If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer

(including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP."

Note: This procedure uses a custom SPP version that cannot be obtained from the customer and therefore cannot be used for a Software Centric Customer. Software Centric Customers must ensure their firmware versions match those detailed in the *HP Solutions Firmware Upgrade Pack, Software Centric Release Notes* document.

4.1.2.1 DL360/DL380 Server

This procedure will upgrade the DL360 or DL380 server firmware. All servers should have SNMP disabled. Refer to Appendix *Changing SNMP Configuration Settings for iLO*.

The service Pack for ProLiant (SPP) installer automatically detects the firmware components available on the target server and will only upgrade those components with firmware older than what is provided by the SPP in the HP FUP version being used.

Procedure Reference Tables:

Variable	Value
<ilo_IP>	Fill in the IP address of the iLO for the server being upgraded _____
<ilo_admin_user>	Fill in the username of the iLO's Administrator User _____
<ilo_admin_password>	Fill in the password for the iLO's Administrator User _____
<local_HPSPP_image_path>	Fill in the filename for the HP Support Pack for ProLiant ISO _____
<admusr_password>	Fill in the password for the admusr user for the server being upgraded _____

Needed Material:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]
- Upgrade Guide of the *HP Solutions Firmware Upgrade Pack, Upgrade Guide* [2]
- 4GB or larger USB stick with the HP Service Pack for ProLiant (SPP) USB image previously written to it per directions in the *HP Solutions Firmware Upgrade Pack, Upgrade Guide*

Important Notes for this Procedure: The following procedure has some instructions meant for a production system in the field and you should be aware of the following notes regarding this procedure:

- Ignore references to the "Copy the ISO Images to the Workstation" procedure. Know that you must have the ISO files listed in the "Needed Material" section above.
- Ignore the <local_HPSPP_image_path> variable.
- For the "Update Firmware Errata" step check the Release Notes of the *HP Solutions Firmware Upgrade Pack* [2] to see if there are any firmware errata items that apply to the server being upgraded. If

there is, there will be a directory matching the errata's ID in the /errata directory of the HP MISC firmware ISO image. The errata directories contain the errata firmware and a README file detailing the installation steps.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **Local Workstation:** Insert the USB Flash Drive.
   If starting with the Oracle USB media, insert the SPP USB media into a USB port on the server. See Section 3.3.1.1 of the *HP Solutions Firmware Upgrade Pack, Upgrade Guide* for steps on creating bootable SPP USB media.
2. **Local Workstation:** Access the iLO Web GUI.
   Access the ProLiant Server iLO Web Login Page from an Internet Explorer ® session using the following URL:

```
https://<ilo_IP>/
```

3. **iLO Web GUI:** Login to iLO as an "administrator" user.

   Username = **<ilo_admin_user>**

   Password = **<ilo_admin_password>**

4. **Determine which iLO steps to take**
   a) If you are upgrading a G6 (iLO 2) server, continue at the next step.
   b) If you are upgrading a G7/Gen8 (iLO3/iLO4) server, continue at step 13.
5. **iLO 2 Web GUI:**

   If using SPP USB media plugged into the server, skip to step 10

   Select Virtual Media page.

   Click the **Virtual Media** tab from the System Summary page.

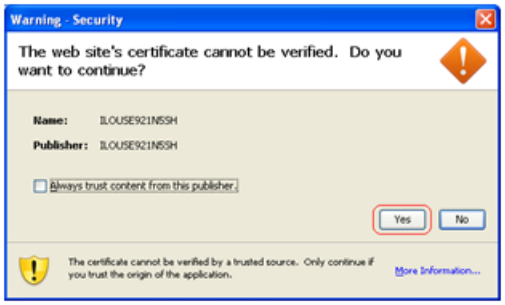
6. **iLO 2 Web GUI:**

   Open the Virtual Media Applet .

   Click on the **Virtual Media Applet** link to launch the Virtual Media application

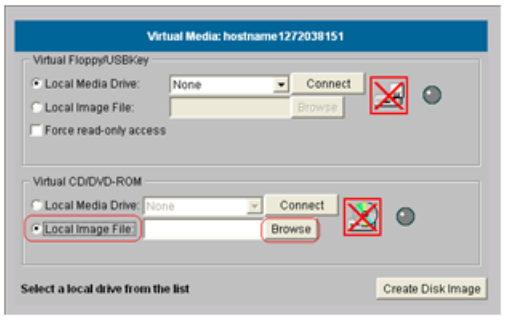
   The iLO GUI should open to the **Virtual Media** page.

7. **iLO 2 Web GUI:** Acknowledge Security Warning.
   If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed.



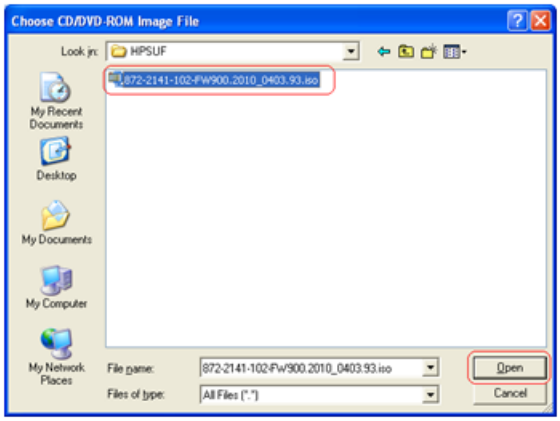
   If other warning dialogs are presented you may also acknowledge them as well to proceed to the Virtual Media applet.

8. **iLO 2 VM Applet:** Select the HP Support Pack for ProLiant ISO.
   In the Virtual CD/DVD-ROM Panel, select the **Local Image File** option and click the **Browse** button. Navigate to the *HP Service Pack for ProLiant (SPP)* ISO file copied to the workstation in the Copy the ISO images to the workstation procedure.

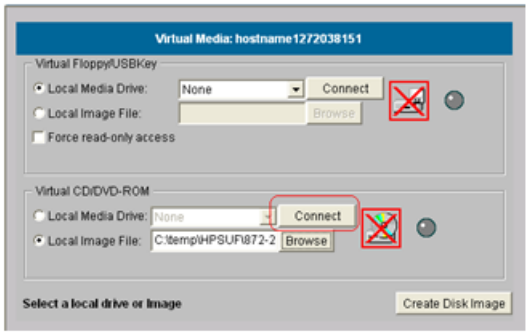


Select ISO image file and click **Open**.

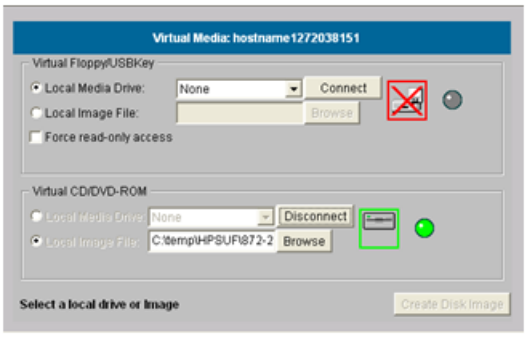
Image File Name: <local_HPSPP_image_path> (See Copy the ISO images to the workstation)



9. **iLO 2 VM Applet:** Create Virtual Drive Connection.
   Click the **Connect** button to create a virtual DVD-ROM connection to the ISO image file.



When created the LED Light icon should be green.



At this point, **DO NOT** close the applet but rather go back to the browser window containing the iLO Web GUI.

10. **iLO 2 Web GUI:** Access the Remote Console Page.
    At the ILO2 Web GUI, click on the **Remote Console** tab.

11. **iLO 2 Web GUI:** Launch the Remote Console Applet.
    On the Remote Console page, click on the **Remote Console** link to launch the console applet.

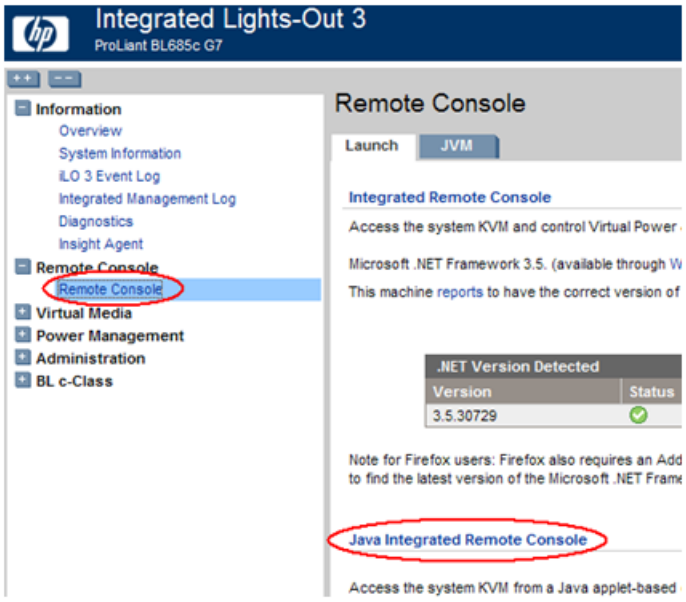
12. **iLO 2 - Java Security Prompt:** Acknowledge Security Warning

If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed.

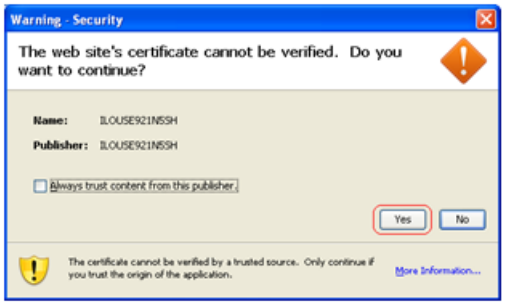
Then skip to step 16.

If other warning dialogs are presented you may also acknowledge them as well to proceed to the Java Integrated Remote Console applet.

13. **iLO3/iLO4 Web GUI:** Launch the Java Integrated Remote Console applet.
    On the menu to the left navigate to the Remote Console page. Click on the Java Integrated Remote Console to open it.



14. **iLO3/iLO4 - Java Security Prompt:** Acknowledge Security Warning.
    If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed.

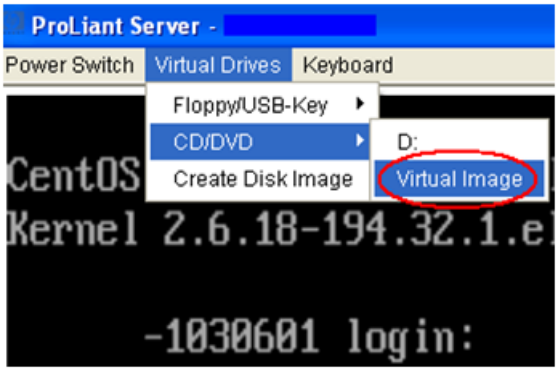


If other warning dialogs are presented you may also acknowledge them as well to proceed to the Java Integrated Remote Console applet.

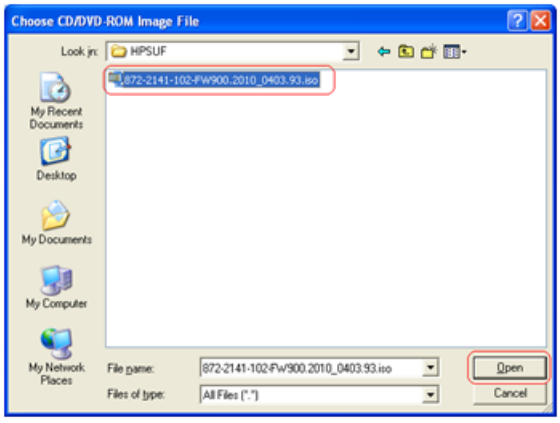
15. **iLO3/iLO4 - Remote Console:** Create Virtual Drive Connection

    If using SPP USB media plugged into the server, skip to step 17

    Click on the Virtual Drives drop down menu. Go to CD/DVD then click on Virtual Image.



    Navigate to the *HP Support Pack for ProLiant ISO* ISO file copied to the workstation from the Copy the ISO images to the workstation procedure.



    Select the ISO image file and click **Open**.

16. **iLO3/iLO4 - Remote Console:** Verify Virtual Image connection.
    At the bottom of the remote console window you should now see a green highlighted drive icon and "VirtualM" written next to it.

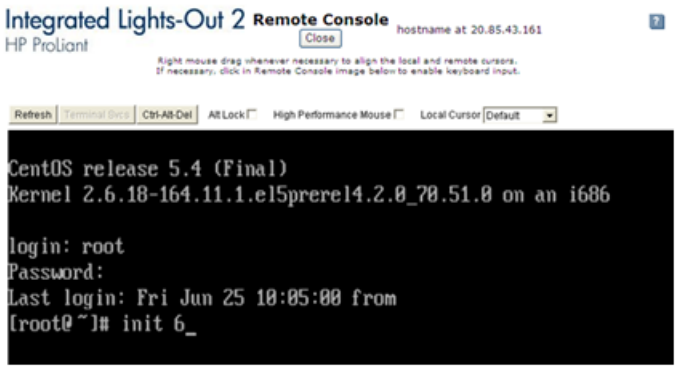
17. **Remote Console:** Reboot the server.

Once the remote console application opens to the login prompt, login to the server as admusr.

```
localhost login: admusr
Password: <admusr_password>
```

Next, initiate server reboot by executing the following command:

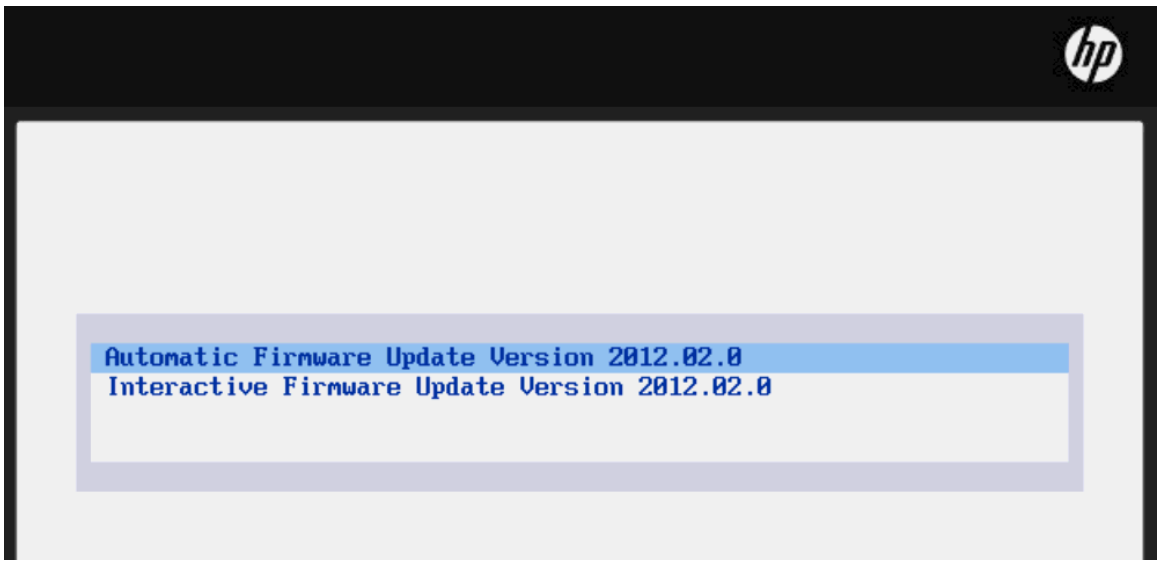
```
$ sudo init 6
```



18. **Remote Console:** Perform an unattended firmware upgrade.

    The server will reboot into the *HP Support Pack for ProLiant* ISO and present the following boot prompt.

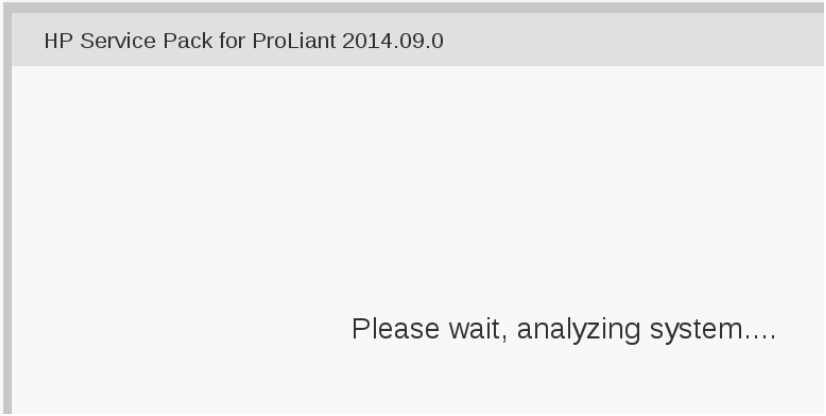
    Press **[Enter]** to select the **Automatic Firmware Update** procedure.



    If no key is pressed in 30 seconds the system will automatically perform an Automatic Firmware Update.

19. **Remote Console:** Monitor Installation.
    Important: Do not click inside the remote console during the rest of the firmware upgrade process. The firmware install will stay at the EULA acceptance screen for a short period of time. The time

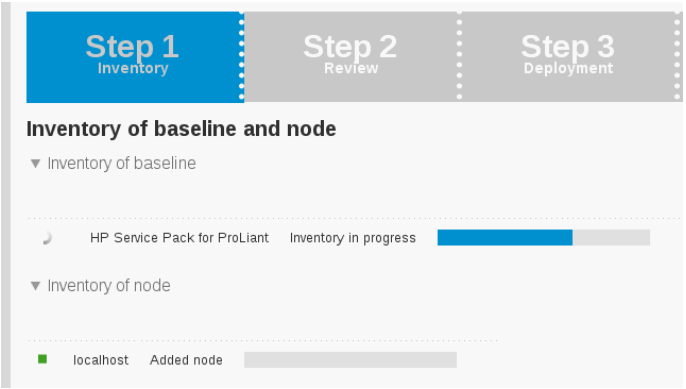
it takes this process to complete will vary by server and network connection speed and will take several minutes. During that time, the following screen is displayed on the console.



Note: No progress indication is displayed during the system scan and analysis stage. In about 10 minutes, the installation will automatically proceed to the next step.No progress indication is displayed. The installation will proceed automatically to the next step.

20. **Remote Console:** Monitor Installation.
    Once analysis is complete, the installer will begin to inventory and deploy the eligible firmware components. A progress indicator is displayed at this time, as shown below.

    If iLO firmware is applied, the Remote Console will disconnect, but will continue upgrading. If the Remote Console closes due to the iLO upgrading, wait 3-5 minutes and log back in to the iLO Web GUI and re-connect to the Remote Console. The server might already be done upgrading and might have rebooted.



Note: If the iLO firmware is to be upgraded, the iLO2 session will be terminated and you will lose the remote console, virtual media and Web GUI connections to the server. This is expected and will not impact the firmware upgrade process.

21. **Local Workstation:** Clean up.
    Once the firmware updates have been completed the server will automatically be rebooted.

    - If you are upgrading a **G6 (iLO 2)** server; at this time you may close the remote console and virtual media applet windows and the iLO2 Web GUI browser session.
    - If you are upgrading a **G7/Gen8 (iLO3/iLO4)** server; closing the remote console window will disconnect the Virtual Image and you can close the iLO3/iLO4 Web GUI browser session.

- If you are using SPP USB media plugged into the server you can now remove it.

22. **Local Workstation:** Verify server availability
    Wait 3 to 5 minutes and verify the server has rebooted and is available by gaining access to the login prompt.
23. **Update Firmware Errata:**
    Refer to the ProLiant Server Firmware Errata section to determine if this HP Solutions Firmware Update Pack contains additional firmware errata updates that should be applied to the server at this time.
24. **Repeat for all remaining RMSs:**
    Repeat this procedure for all remaining RMSs, if any.

4.1.3 Deploying Virtualized PM&C Overview

Deployment Procedure

Deploying a VM guest in the absence of a PM&C is complicated. To facilitate this, the PM&C media will include a guest archive and a script that will deploy the running PMAC into a state where the Initialization process can begin.

- Install TVOE 3.0 on the management server via the ILO.
- Create and configure the management bridge.
- Attach PM&C media to the TVOE (USB).
- Mount the media.
- Use the <mount-point>/upgrade/pmac-deploy script to create the VM and configure the guest on the first boot.
- Navigate browser to the management IP address of the deployed PM&C.
- Perform Initial Configuration.

What You Will Need -- Worksheet

Use the completed NAPD information to fill in the appropriate data in this Procedure's Reference tables. The following are provided to aid with the data collection for the TVOE management server and the PM&C Application hosted on the Management Server TVOE.

- Determine if the network configuration of this management server is Non-Segregated or Segregated.

  Note: The term "segregated networks" refers to the separation of the Management Server's control and plat-management networks onto separate physical NICs. If either of the following scenarios exists the networks are considered segregated.

  1. Devices eth01 and eth02 of the Management Server are physically connected to the first pair of the c7000 enclosure switches.
  2. Devices eth01 and eth02 of two RMS servers are directly connected to each other (e.g. eth01 > eth01 and eth02 > eth02

- Determine the TVOE management server's required network interface, bond, and Ethernet device, and route data.

- Determine if the control network on the TVOE management server is to be tagged. If appropriate, fill in the <control VLAN ID> value in the table, otherwise the control network is not tagged.

- Determine if the management network on the TVOE management Server is to be tagged. If appropriate, fill in the <management_VLAN_ID> value in the table, otherwise the management network is not tagged.
- Determine the bridge name to be used on the TVOE management server for the management network. Fill in the <TVOE_Management_Bridge> value in the table.
- Determine if the NetBackup feature is enabled
  - Determine the NetBackup network on the TVOE management server is to be tagged. If appropriate, fill in the <NetBackup_VLAN_ID> value in the table, otherwise the NetBackup network is not tagged.
  - Determine the bridge name to be used on the TVOE management server for the NetBackup network. Fill in the <TVOE_NetBackup_Bridge> value in the table.
  - Determine if the NetBackup network is to be configured with jumbo frames. If appropriate, fill in the <NetBackup_MTU_size> value in the table, otherwise the NetBackup network will use the default MTU size.
  - If the PM&C NetBackup feature is enabled, and the backup service will be routed, with a source interface different than the management interface where the default route is applied, then define the route during PM&C initialization as a host route to the NetBackup server.
- The PM&C initialization profiles have been designed to configure the PM&C's networks and features. Profiles must identify interfaces. Existing profiles provided by PM&C use standard named interfaces (control, management). No vlan tagging is expected on the PM&C's interfaces, all tagging should be handled on the TVOE management server configuration.

Network Interface	**DL360 (without HP NC364T 4pt Gigabit)**	**DL360 (with HP NC364T 4pt Gigabit in PCI Slot 2)**	**DL380 (with only LOM 4pt NICs) (G6)**	**DL380 (with HP 4pt Gigabit in PCI Slot 1) (Gen8, 9)**	**DL380 (with HP 4pt Gigabit in PCI Slot 3) (G6)**	**DL380 (with HP 1Gb 4pt 331FLR Adapter)**
<ethernet_interface_1>	eth01	eth01	eth01	eth01	eth01	eth01
<ethernet_interface_2>	eth02	eth02	eth02	eth02	eth02	eth02
<ethernet_interface_3>		eth21		eth11	eth31	eth03
<ethernet_interface_4>		eth22		eth12	eth32	eth04
<ethernet_interface_5>		eth23		eth04	eth04	eth05

PM&C Interface Alias	**TVOE Bridge Name**	**TVOE Bridge Interface**
control	control	Fill in the appropriate value for this site (default is bond0): _____ <TVOE_Control_Bridge_Interface>

PM&C Interface Alias	TVOE Bridge Name	TVOE Bridge Interface
management	Fill in the appropriate value for this site: _____ <TVOE_Management_Bridge>	Fill in the appropriate value for this site: _____ <TVOE_Management_Bridge_Interface>
NetBackup	Fill in the appropriate value for this site: _____ <TVOE_NetBackup_Bridge>	Fill in the appropriate value for this site: _____ <TVOE_NetBackup_Bridge_Interface>

Fill in the appropriate value for this site:

Variable	Value	Description
<control_VLAN_ID>		For non-segregated networks, the control network may have a VLAN id assigned. In most cases, there is none.
<base_device_hosting_control_network>		If <control_VLAN_ID> has a value, then the device used for the control network <TVOE_Control_Bridge_Interface> will have a tagged interface name. The base device for the control network is the untagged interface name. (For example, if the device interface is bond1.2 then the base device is bond1).
<management_VLAN_ID>		For non-segregated networks, the management network will be on a tagged VLAN coming in on bond0
<mgmtVLAN_gateway_address>		Gateway address used for routing on the management network.
<NetBackup_server_IP>		The IP address of the remote NetBackup Server.
<NetBackup_VLAN_ID>		For non-segregated networks, the NetBackup network will be on a tagged VLAN coming in on bond0
<NetBackup_gateway_address>		Gateway address used for routing on the NetBackup network.

Variable	Value	Description
<NetBackup_network_ip>		The Network IP for the NetBackup network
<PMAC_NetBackup_netmask _or_prefix>		The IPv4 netmask or IPv6 prefix assigned to the PM&C for participation in the NetBackup network
<PMAC_NetBackup_ip_address>		The IP Address assigned to the PM&C for participation in the NetBackup network
<NetBackup_MTU_size>		If desired, the MTU size can be set to tune the NetBackup network traffic.
<management_server_mgmt_ip_address>		The TVOE Management Server's IP address on the management network.
<PMAC_mgmt_ip_address>		The PM&C Application's IP address on the management network.
<mgmt_netmask_or_prefix>		The IPv4 netmask or IPv6 prefix for the management network.
<PMAC_control_ip_address>		The PM&C Application's IP address on the control network.
<control_netmask>		The IP netmask for the control network.

Fill in the appropriate value for this site:

Network Bond Interface	Enslaved Interface 1	Enslaved Interface 2
bond0		
For Segregated Networks Only		
bond1		
bond2		Bonding used for abstraction only, not multiple interfaces

4.1.4 TVOE Network Configuration

1. **TVOE Management Server iLO:** Log into the management server on the remote console
   Login to iLo using application provided passwords via *L.1 How to Access a Server Console Remotely*.
   Login to iLO in IE using password provided by application:

```
http://<management_server_iLO_ip>
```

Click in the Remote Console tab and launch the Integrated Remote Console on the server.

Click Yes if the Security Alert pops up.

2. **TVOE Management Server:** Verify the control network bond

   Note: The output below is for illustrative purposes only. It shows the control bond configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_Control_Bridge_Interface>

   Protocol: none
    On Boot: yes
 IP Address:
    Netmask:
Bonded Mode: active-backup
  Enslaving: <ethernet_interface_1> <ethernet_interface_2>
```

   If the bond has not been configured, skip to the next step.

   If the RMS servers connect back-to-back for their control network, execute this step to recreate the bond0 interface with a primary interface of <ethernet_interface_1>. If the RMS servers do not fit this configuration, move onto the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces (network devices, bonds, and bond enslaved devices) to configure.

   Remove existing bond:

```
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control
--delBridgeInt=<TVOE_Control_Bridge_Interface>
Interface <TVOE_Control_Bridge_Interface> updated
Bridge control updated

$ sudo /usr/TKLC/plat/bin/netAdm delete --device=<TVOE_Control_Bridge_Interface>
Interface bond0 removed
```

   Re-create control bond (<TVOE_Control_Bridge_Interface>) with primary interface set to <ethernet_interface_1>:

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=bond0 --onboot=yes --type=Bonding
 --mode=active-backup --miimon=100 --primary=<ethernet_interface_1>
Interface <TVOE_Control_Bridge_Interface> added

$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_1>
--type=Ethernet --master=<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes
Interface <ethernet_interface_1> updated

$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_2>
--type=Ethernet --master=<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes
Interface <ethernet_interface_2> updated
```

   Add <TVOE_Control_Bridge_Interface> back to existing control bridge:

```
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control
--bridgeInterfaces=<TVOE_Control_Interface>
```

3. **TVOE Management Server:** Verify the control network bridge

Note: The output below is for illustrative purposes only. It shows the control bridge configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=control
Bridge Name: control
    On Boot: yes
   Protocol: dhcp
 Persistent: yes
Promiscuous: no
     Hwaddr: 00:24:81:fb:29:52
        MTU:
Bridge Interface: bond0
```

If the bridge has been configured, skip to the next step.

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. Create control bridge (<TVOE_Control_Bridge>).

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_Control_Bridge>
 --bootproto=dhcp --onboot=yes --bridgeInterfaces=<TVOE_Control_Bridge_Interface>
```

4. **TVOE iLO:** Create tagged control interface and bridge (optional)

   If you are using a tagged control network interface on this PM&C, then complete this step using values for the control interface on bond0 from the preceding tables. Otherwise, proceed to the next step now.

```
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control
--delBridgeInt=bond0
Interface bond0 updated
Bridge control updated
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Control_Bridge_Interface>
--onboot=yes
Interface <TVOE_Control_Bridge_Interface> created
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Enslaved Interface 1> --onboot=yes
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Enslaved Interface 2> --onboot=yes
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control
--bridgeInterfaces=<TVOE_Control_Bridge_Interface>
```

5. **TVOE Management Server** Verify the tagged/non-segregated management network

   Note: A Segregated Management Network can be either "tagged" or "untagged." In most cases the network will be tagged when the TVOE Host is used to host DSR guests in addition to the PM&C guest. In this scenario, both the "Management" and "XMI" networks are required and will be tagged on the same bond. In scenarios where only the PM&C is hosted by the TVOE and only the "Management" network is required, untagged can be used. The switch configuration of the connected switches must match the server configuration "tagged" or "untagged".

   Note: This step only applies if the management network is tagged (non-segregated).

   Note: The output below is for illustrative purposes only. It shows the management bridge configured on a non-segregated network setup.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --device=bond0.2
      Protocol:  none
       On Boot:  yes
    IP Address:
```

```
       Netmask:
        Bridge:  Member of bridge management
```

If the device has been configured, skip to the next step.

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

Note: The example below illustrates a PM&C management server configuration in a Non-Segregated network, an un-tagged control network, and a tagged management network.

For this example created tagged device for management device.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface>
 --onboot=yes
Interface <TVOE_Management_Bridge_Interface> added
```

6. **TVOE Management Server:** Verify the untagged/segregated management network

   Note: This step only applies if the management network is untagged (segregated).

   Note: The output below is for illustrative purposes only. It shows the management bond configured on a segregated network setup.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_Management_Bridge_Interface>

      Protocol:  none
       On Boot:  yes
    IP Address:
       Netmask:
   Bonded Mode:  active-backup
     Enslaving:  <ethernet_interface_3> <ethernet_interface_4>
```

   If the bond has been configured, skip to the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface>
 --onboot=yes --type=Bonding --mode=active-backup --miimon=100
--bondInterfaces="<ethernet_interface_3>,<ethernet_interface_4>"
Interface <TVOE_Management_Bridge_Interface> added
```

7. **TVOE Management Server:** Verify the management bridge

   Note: The output below is for illustrative purposes only. It shows the management bridge configured on a non-segregated network setup.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=management
Bridge Name: management
    On Boot: yes
   Protocol: none
 IP Address: 10.240.4.86
    Netmask: 255.255.255.0
Promiscuous: no
     Hwaddr: 00:24:81:fb:29:52
        MTU:
Bridge Interface: bond0.2
```

If the bridge has been configured, skip to the next step.

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

For this example, created a tagged device for management bridge.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_Management_Bridge>
 --address=<management_server_mgmtVLAN_IP> --netmask=<mgmtVLAN_netmask_or_prefix>
 --onboot=yes --bridgeInterfaces=<TVOE_Management_Bridge_Interface>
```

8. **TVOE Management Server:** Verify the NetBackup network (if needed)

   If the NetBackup feature is not needed, skip to the next step.

   Note: The output below is for illustrative purposes only. It shows the**NetBackup** bridge is configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=netbackup
     Bridge Name: netbackup
         On Boot: yes
        Protocol: none
      IP Address: 10.240.6.2
         Netmask: 255.255.255.0
     Promiscuous: no
          Hwaddr: 00:24:81:fb:29:58
             MTU:
Bridge Interface: bond2
```

   If the bridge has been configured, skip to the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

   Note: The example below illustrates a TVOE management server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size.

   Note: The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.

   Select**only one** of the following configurations:

   - Option 1: Create NetBackup bridge using an untagged native interface.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>
 --bootproto=none --onboot=yes --MTU=<NetBackup_MTU_size>
--bridgeInterfaces=<Ethernet_interface_5> --address=<TVOE_NetBackup_IP>
--netmask=<TVOE_NetBackup_Netmask_or_prefix>
```

   - Option 2: Create NetBackup bridge using a tagged device.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface>
 --onboot=yes
Interface <TVOE_NetBackup_Bridge_Interface> added
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>
 --onboot=yes --MTU=<NetBackup_MTU_size>
--bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP>
 --netmask=<TVOE_NetBackup_Netmask_or_prefix>
```

9. **TVOE Management Server:** Setup syscheck

syscheck must be configured to monitor bond interfaces. Replace "**bondedInterfaces**" with "**bond0**" or "**bond0,bond1**" if segregated networks are used:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES
--val=<bondedInterfaces>
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond –enable
$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond
```

Note: The following is an example of the setup of syscheck with a single bond, bond0:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=bond0
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable
$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond
```

Note: The following is an example of the setup of syscheck with multiple bonds, bond0 and bond1:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES
--val=bond0,bond1
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable
$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond
```

10. **TVOE Management Server:** Verify the default route

    Note: The output below is for illustrative purposes only. It shows the default route on the management bridge is configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --route=default --device=management
Routes for TABLE: main and DEVICE: management
* NETWORK: default
  GATEWAY: 10.240.4.1
```

    If the route has been configured, skip to the next step.

    Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

    For this example add default route on management network.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=default
--device=<TVOE_Management_Bridge> --gateway=<mgmt_gateway_address>
Route to <TVOE_Management_Bridge> added
```

11. **TVOE Management Server:** Verify the NetBackup route (optional)

    If the NetBackup network is a unique network for NetBackup data, verify the existence of the appropriate NetBackup route.

    Note: The output below is for illustrative purposes only. It shows the route on the NetBackup bridge is configured.

    If the NetBackup route is to be a network route, then:

```
$ sudo /usr/TKLC/plat/bin/netAdm query --route=net
--device=<TVOE_NetBackup_Bridge>
Routes for TABLE: main and DEVICE: netbackup
* NETWORK: net
GATEWAY: 169.254.253.1
```

If the NetBackup route is to be a host route then:

```
$ sudo /usr/TKLC/plat/bin/netAdm query --route=host
--device=<TVOE_NetBackup_Bridge>
Routes for TABLE: main and DEVICE: netbackup
* NETWORK: host
GATEWAY: 169.254.253.1
```

If the route has been configured, skip to the next step.

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces (network devices, bonds, and bond enslaved devices) to configure.

For this example add network route on management network.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=<TVOE_Management_Bridge>
 --gateway=<NetBackup_gateway_address> --address=<NetBackup_network_IP>
--netmask=<TVOE_NetBackup_Netmask_or_prefix>
Route to <TVOE_NetBackup_Bridge> added
```

For this example, add host route on management network.

Note: For the configuration of a host route, the <TVOE_NetBackup_Netmask> will be set to "255.255.255.255".

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=host
--device=<TVOE_Management_Bridge> --gateway=<NetBackup_Server_IP>
--address=<NetBackup_Server_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix>
Route to <TVOE_NetBackup_Bridge> added
```

12. **TVOE Management Server:** Set hostname

```
$ sudo /bin/su - platcfg
```

1. Navigate to **Server Configuration** > **Hostname** and set the hostname.
2. Set TVOE Management Server hostname
3. Press OK.
4. Navigate out of Hostname

13. **TVOE Management Server:** Set time zone and/or hardware clock

1. Navigate to **Server Configuration** > **Time Zone.**
2. Select Edit.
3. Set the time zone and/or hardware clock to GMT (Greenwich Mean Time).
4. Press OK.
5. Navigate out of Server Configuration.

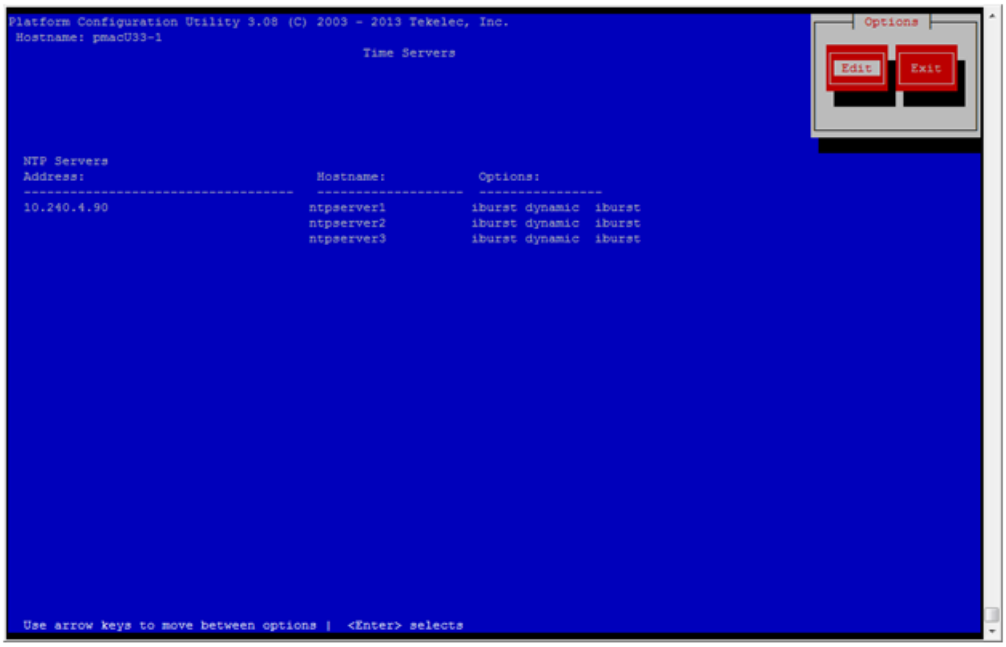
14. This step will configure NTP servers for a server based on TPD.

Note: 3 NTP Sources will be configured in this step. Refer to*3.4 NTP Strategy*.

a) **Server:** Login as platcfg

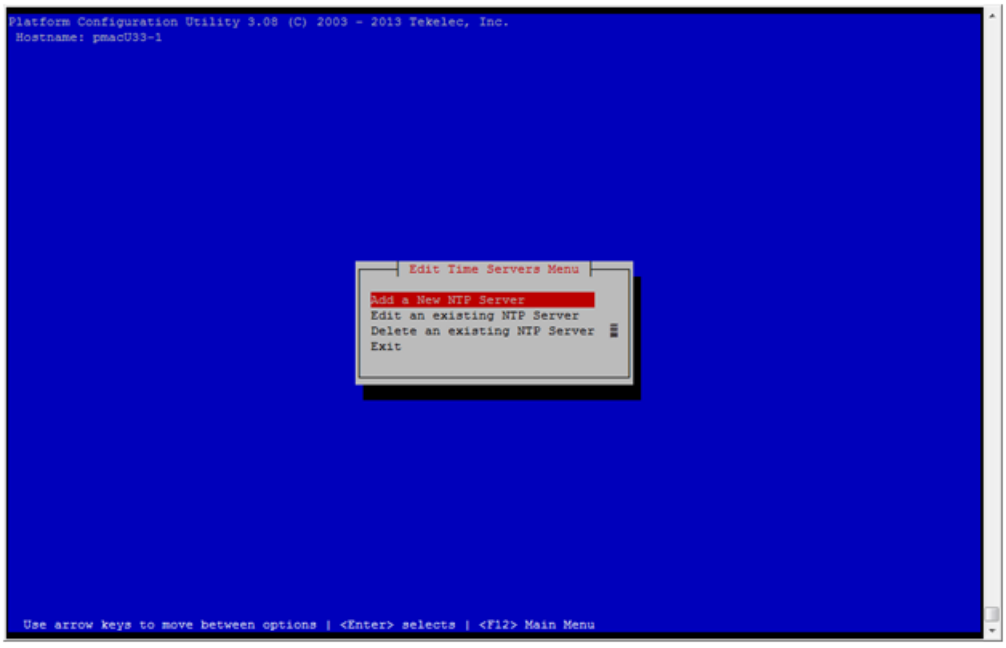
Login as platcfg user on the server. The platcfg main menu will be shown.

b) **Server:** Navigate to Time Servers configuration page. Select the following menu options sequentially: **Network Configuration** > **NTP**. The 'Time Servers' page will now be shown, which shows the configured NTP servers and peers.



c) **Server:** Update NTP Information

Select **Edit**. The **Edit Time Servers Menu** is displayed.



d) **Server:** Edit NTP Information

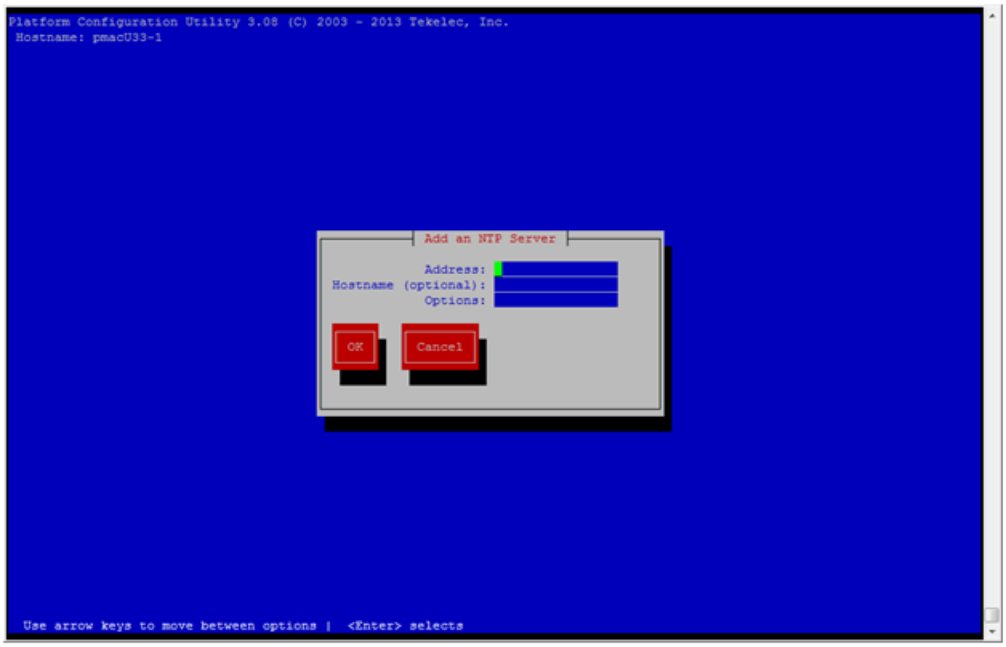
Select the appropriate **Edit Time Servers Menu** option. When all Time Server actions are complete exit the **Edit Time Servers Menu**. Remember that 3 (or more) NTP sources are required.

Note: You can move directly to Substep 2 *Editing an NTP Server* to edit the existing NTP servers (if they exist) instead of adding new NTP servers.

1. **Adding an NTP Server**

   a. **Server:** If adding a new NTP server select **Add a New NTP Server**.

   The **Add an NTP Server** window is displayed.



   b. **Server:** Enter Appropriate data, and select **OK**

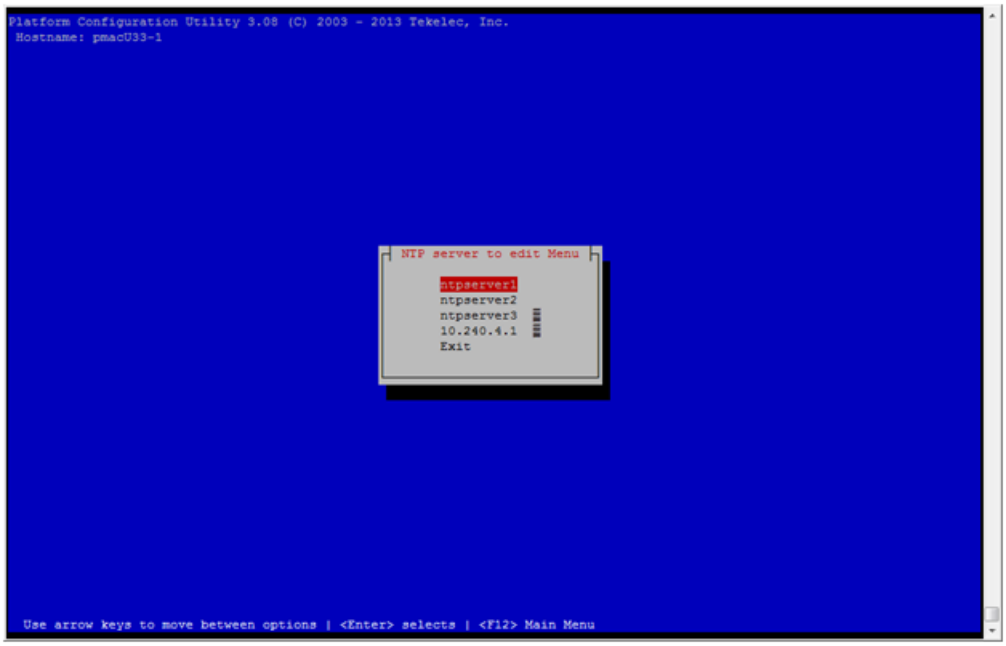
   The NTP server is added. The **Edit Time Servers Menu** is displayed.

   Note: The default NTP option is iburst. Additional NTP options are listed in the ntp.conf man page, some of the valid options are: burst, minpoll, and maxpoll.

2. **Editing an NTP Server**

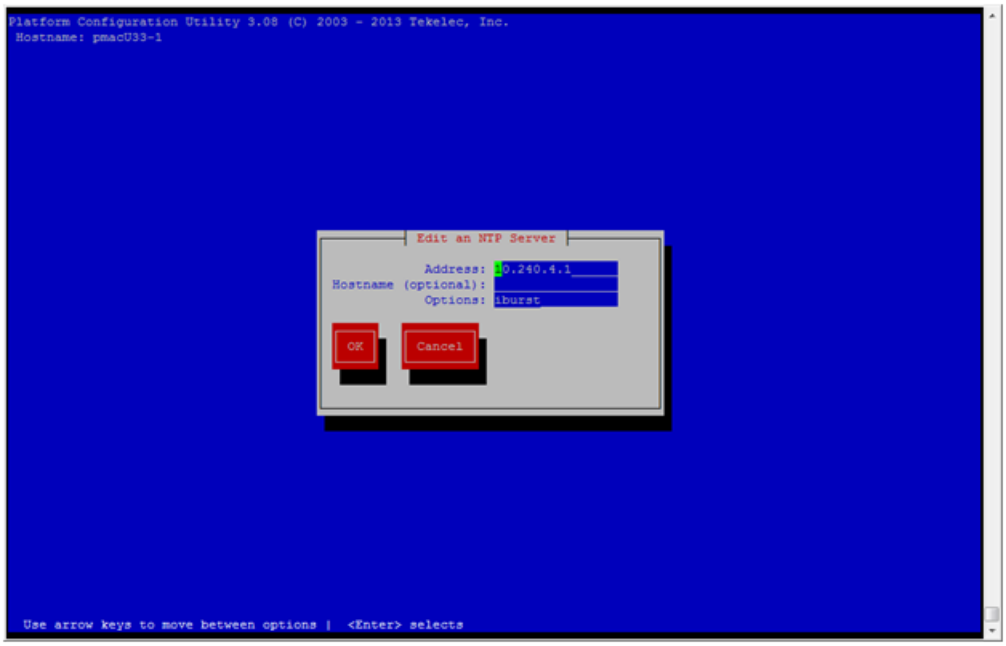
   a. **Server:** If editing an existing NTP server select **Edit an existing NTP Server**.

   The **NTP Server to edit Menu** window is displayed.



b. **Server:** Select appropriate NTP server.

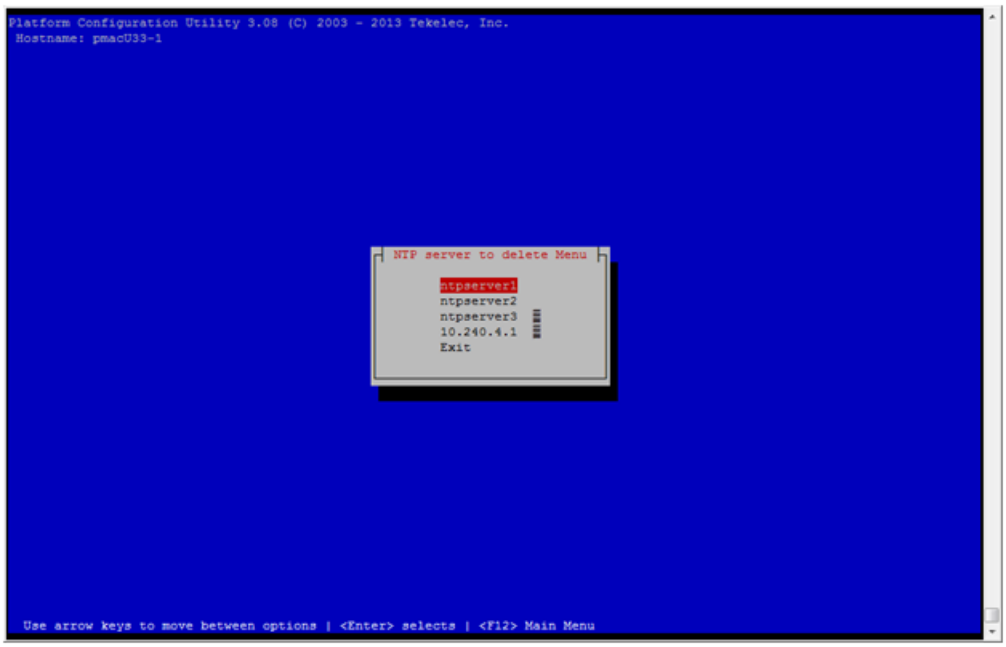
   The **Edit an NTP Server** window is displayed.



3. **Deleting an existing NTP Server**

   a. **Server:** If deleting an existing NTP server, select **Delete an existing NTP Server**.

      The **NTP server to delete Menu** is displayed.



b. Server: Select appropriate NTP server.

The NTP server is deleted. The **Edit Time Servers Menu** is displayed.

e) **Server:** Restart the NTP server

f) **Server:** Exit platcfg.

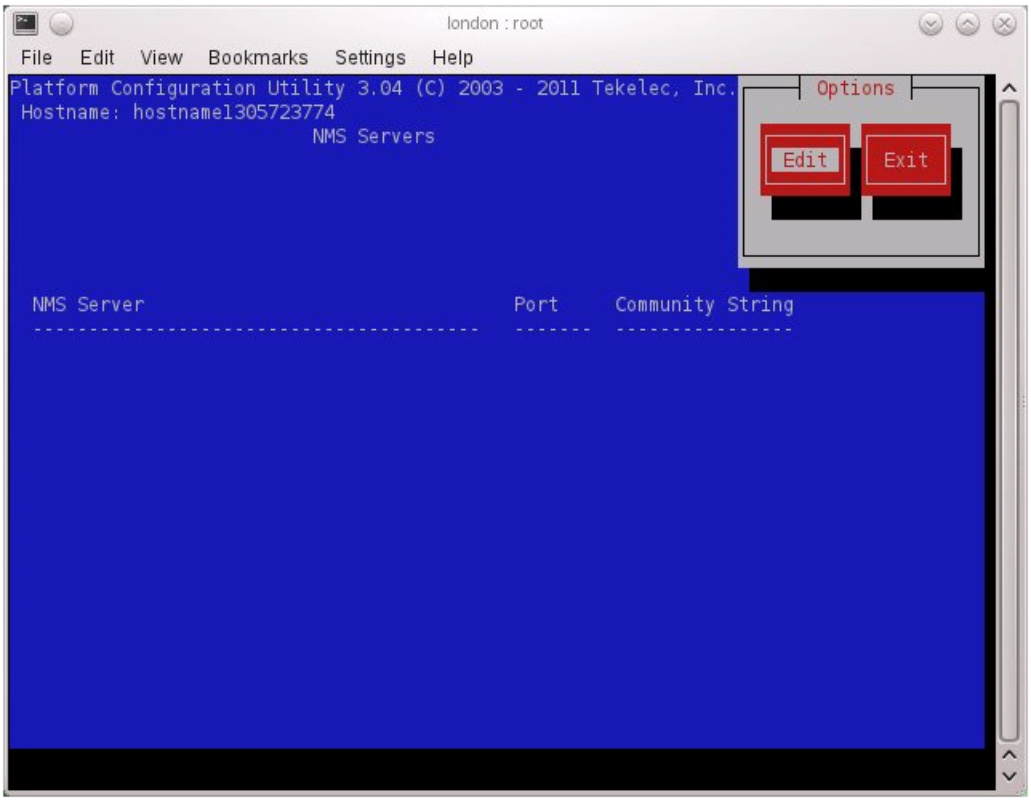
Select **Exit** on each menu until platcfg has been exited.

15. This step will add an SNMP trap destination to a server based on TPD. All alarm information will then be sent to the NMS located at the destination.

a) **Server:** Login as platcfg user on the server. The platcfg main menu will be shown.

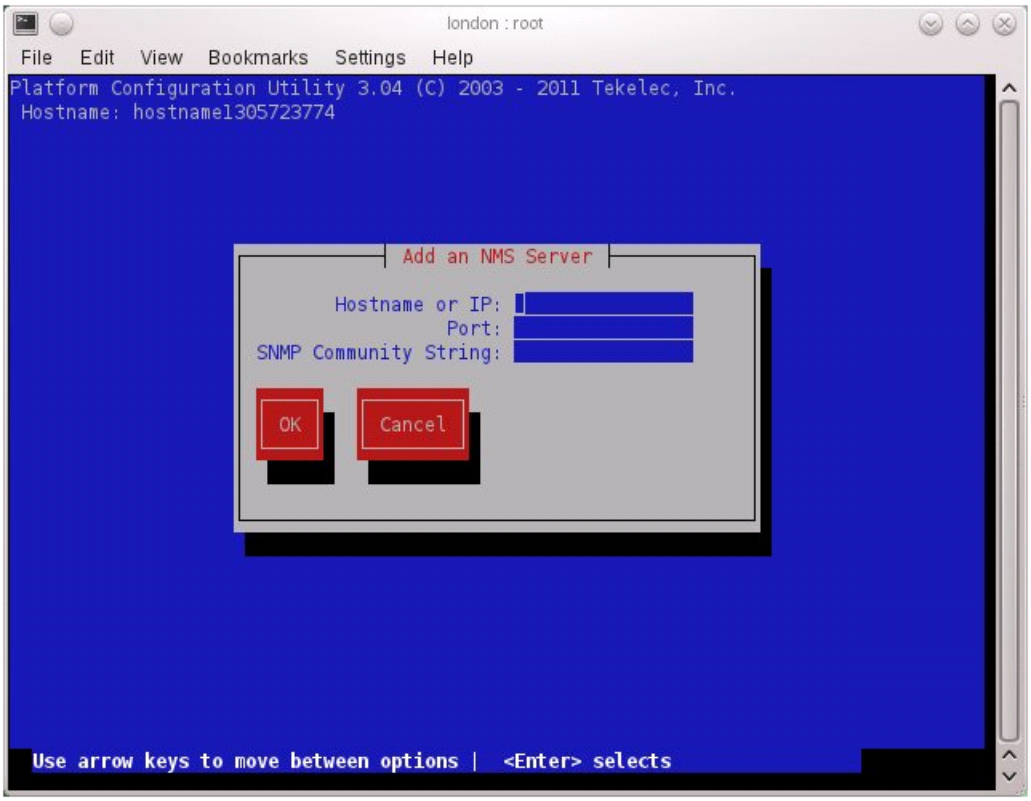
b) **Server:** Navigate to NMS server configuration page.

Select the following menu options sequentially: **Network Configuration** > **SNMP Configuration** > **NMS Configuration**. The 'NMS Servers' page will be shown, which displays all configured NMS servers for the server.



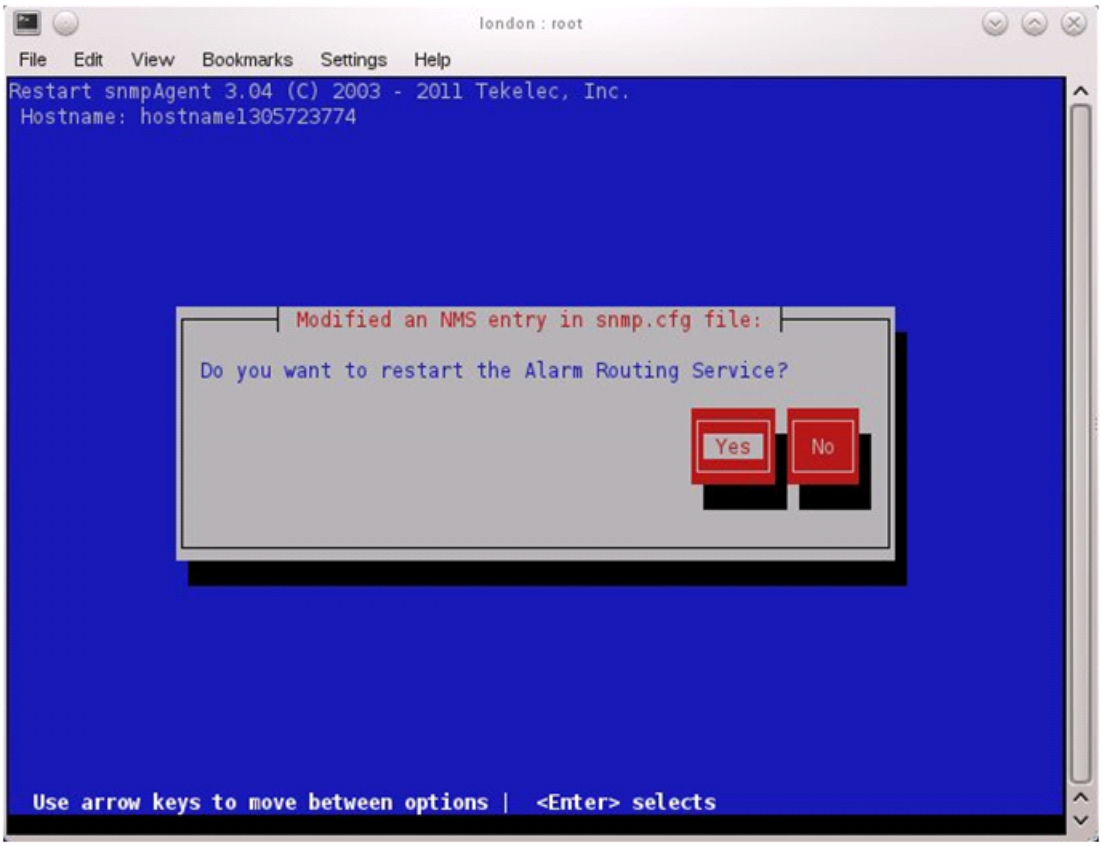
c) **Server:** Add the SNMP trap destination.

Select **Edit** and then choose **Add a New NMS Server**. The 'Add an NMS Server' page will be displayed.



Complete the form by entering in all information about the SNMP trap destination. Refer to *3.3 SNMP Configuration*. Select **OK** to finalize the configuration.

The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialogue will then be presented.



Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented.

d) Select **Exit** on each menu until platcfg has been exited.

Note: If NetBackup is to be configured on the TVOE host, please follow the steps in Appendix*Install NetBackup Client on TVOE Server (optional)*. The steps in Appendix*Install NetBackup Client on TVOE Server (optional)*can only be performed after the Aggregation Switches in*4.3 Configure Aggregation Switches*have been properly configured.

16. **TVOE Management Server:** Verify server health

```
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
```

Alarms may be observed if network connectivity has not been established.

17. **TVOE Management Server:** Ensure time set correctly.

a) Set time based on NTP Server

```
$ sudo /sbin/service ntpd stop
$ sudo /usr/sbin/ntpdate ntpserver1
$ sudo /sbin/service ntpd start
```

b) Reboot the server

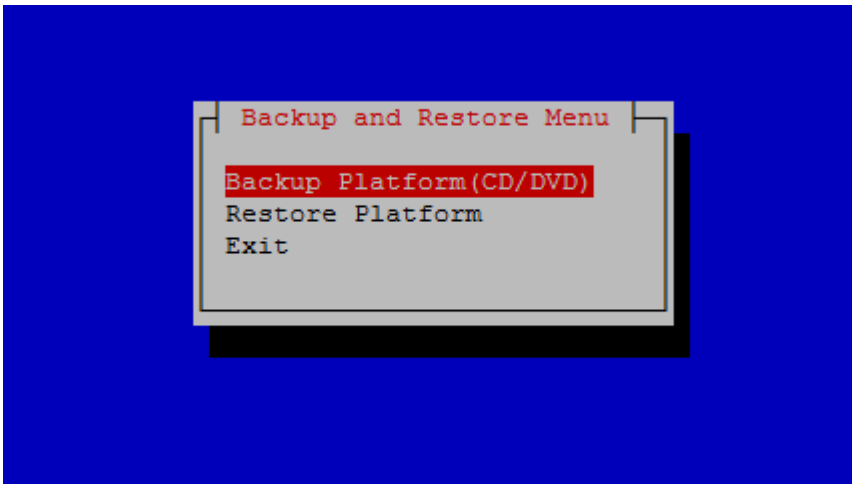
```
$ sudo /sbin/init 6
```

18. This step will backup system files which can be used at a later time to restore a failed system.

Note: The backup image is to be stored on a customer provided medium.

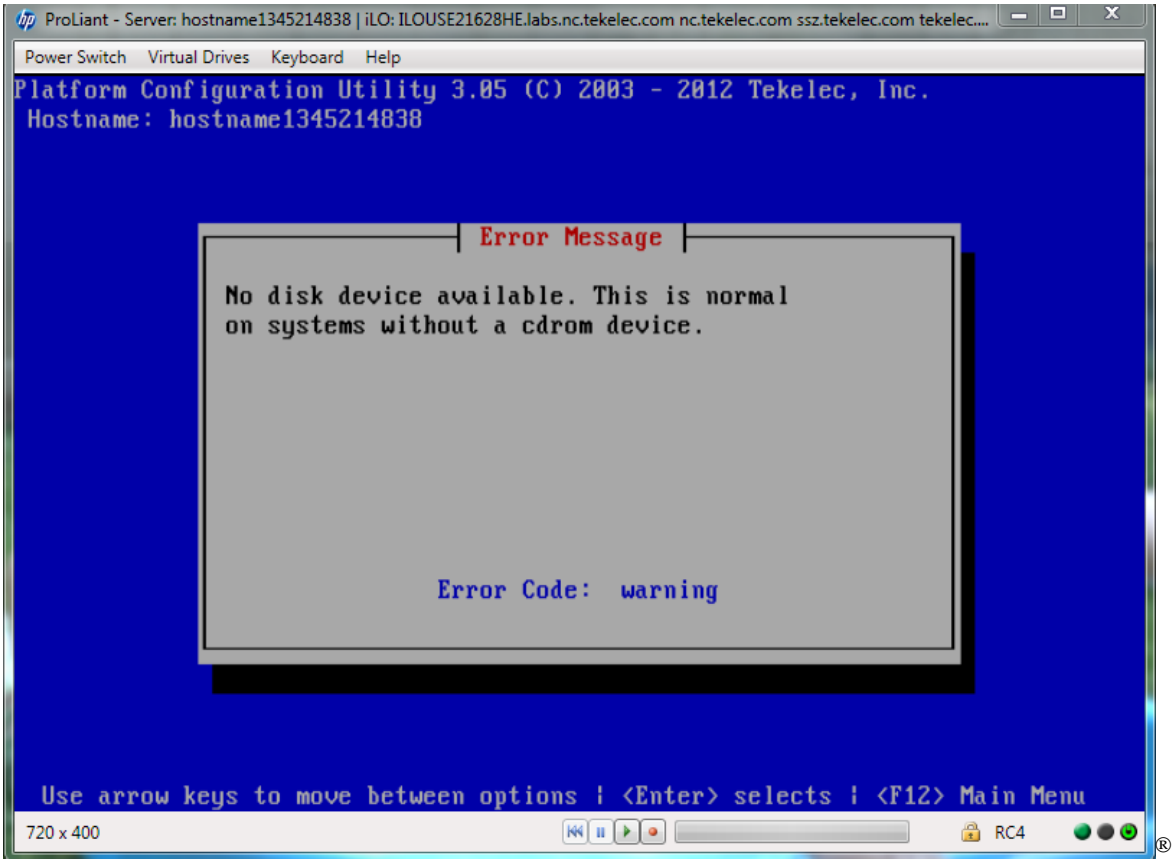
a) **TVOE Host:** Login as platcfg user.

Select the following menu options sequentially: **Maintenance** > **Backup and Restore** > **Backup Platform**. The 'Backup and Restore Menu' will now be shown.



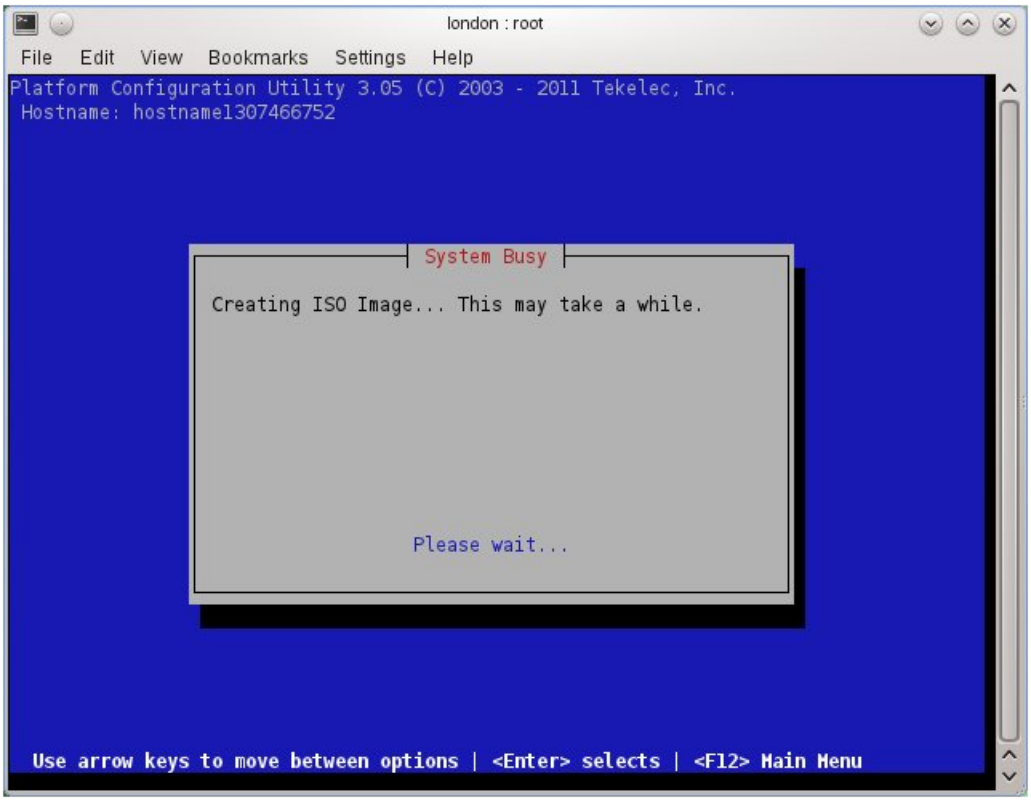
Select the menu 'Backup Platform (CD/DVD)'.

Note: If this operation is attempted on a system without media, the following message will appear:



b) **TVOE Host:** Build the backup ISO image. Select **Build ISO file only**. The following screen will display:

Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant.



After the ISO is created, platcfg will return to the Backup TekServer Menu as shown in step 2. The ISO has now been created and is located in the `/var/TKLC/bkp/` directory. An example filename of a backup file that was created is: "hostname1307466752-plat-app-201104171705.iso"

c) **TVOE Host:** Exit platcfg

Select **Exit** on each menu until platcfg has been exited. The SSH connection to the TVOE server will be terminated.

d) **Customer Server:** Login to the customer server and copy backup image to the customer server where it can be safely stored.

If the customer system is a Linux system, execute the following command to copy the backup image to the customer system.

```
# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/
```

When prompted, enter the tvoexfer user password and press **Enter**.

An example of the output looks like:

```
# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/
tvoexfer@10.24.34.73's password:
hostname1301859532-plat-app-301104171705.iso     100% 134MB 26.9MB/s 00:05
```

If the Customer System is a Windows system refer to *D.1 Using WinSCP* to copy the backup image to the customer system.

The TVOE backup file has now been successfully placed on the Customer System.

4.2 Install PM&C

4.2.1 Deploy PM&C Guest

The **pmac-deploy** script is responsible for deploying a PM&C guest in the absence of a PM&C to create the guest and install the OS and application. This is all done at build-time and the system disk image is kept on the PM&C media, along with this script. Once the PM&C media is mounted, the **pmac-deploy** script can be found in the upgrade directory of the media.

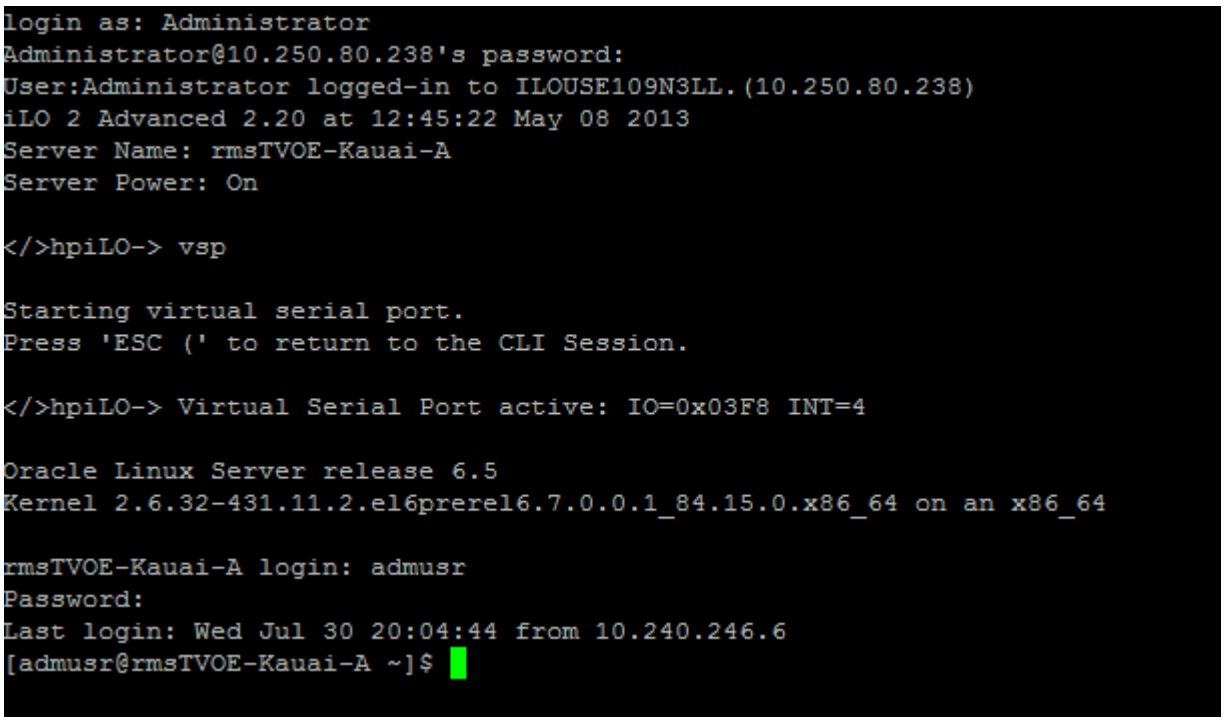
1. **TVOE Management Server iLO:** Login to the management server on the remote console

   Login to iLo using application provided passwords via *L.1 How to Access a Server Console Remotely*.

   ```
   http://<management_server_iLO_ip>
   ```

   Click in the Remote Console tab and launch the Integrated Remote Console on the server.

   Click Yes if the Security Alert pops up.

2. **TVOE Management Server:** Mount the PM&C media to the TVOE Management server.

   Alternatively, user can login to the management console through PuTTY.

   For a sample of mounting a USB media

   ```
   $ sudo /bin/ls /media/*/*.iso
   /media/usb/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso
   $ sudo /bin/mount -o loop /media/usb/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso
   /mnt/upgrade
   ```

3. **TVOE Management Server:** Validate the PM&C media.

   Execute the self-validating media script:

```
$ cd /mnt/upgrade/upgrade
$ sudo .validate/validate_cd
Validating cdrom...

UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012
Validating <device or ISO>
Date&Time: 2012-10-25 10:07:01
Volume ID: tklc_872-2441-106_Rev_A_50.11.0
Part Number: 872-2441-106_Rev_A
Version: 50.11.0
Disc Label: PMAC
Disc description: PMAC
The media validation is complete, the result is: PASS

CDROM is Valid
```

   If the media validation fails, the media is not valid and should not be used.

4. **TVOE Management Server:** Using the pmac-deploy script, deploy the PM&C instance using the configuration detailed by the completed NAPD.

   For this example, deploy a PM&C without NetBackup feature

```
$ cd /mnt/upgrade/upgrade
$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name>
--controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address>
--controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge>
--managementIP=<PMAC_Management_ip_address>
--managementNM=<PMAC_Management_netmask_or_prefix>
--routeGW=<PMAC_Management_gateway_address>
--ntpserver=<TVOE_Management_server_ip_address> --isoimagesVolSizeGB=20
```

   Deploying a PM&C with the NetBackup feature requires the "--netbackupVol" option, which creates a separate NetBackup logical volume on the TVOE host of PM&C. If the NetBackup feature's source interface is different from the management interface include the "--bridge" and the "--nic" as in the example below.

```
$ cd /mnt/upgrade/upgrade
$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name>
--controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address>
--controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge>
--managementIP=<PMAC_Management_ip_address>
--managementNM=<PMAC_Management_netmask_or_prefix>
--routeGW=<PMAC_Management_gateway_address>
--ntpserver=<TVOE_Management_server_ip_address>
--netbackupVol
--bridge=<TVOE_NetBackup_Bridge>
--nic=netbackup
```

   Note: If a mistake in the pmac-deploy is identified during this step the operator under the advisement of customer service can remove the guest with the following command:

```
$ sudo /usr/TKLC/plat/bin/guestMgr --remove <PMAC_Name>
```

5. The PM&C will deploy and boot. The management and control network will come up based on the settings that were provided to the pmac-deploy script.

6. **TVOE Management Server:** Unmount the media and remove.

```
$ cd /
$ sudo /bin/umount /mnt/upgrade
```

7. **TVOE Management Server:** Remove the PM&C Media

4.2.2 Setup PM&C

The steps in this section configure the PM&C application guest environment on the Management Server TVOE host. It also initializes the PM&C application. At the conclusion of this section, the PM&C application environment is sufficiently configured to allow configuration of system network assets associated with the Management Server.

1. **TVOE Management Server iLO:** Login to the management server on the remote console

   Log in to iLo using application provided passwords via *L.1 How to Access a Server Console Remotely*.

```
http://<management_server_iLO_ip>
```

   Click in the Remote Console tab and launch the Integrated Remote Console on the server.

   Click Yes if the Security Alert pops up.

2. Log in with PM&C admusr credentials

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **sudo /usr/bin/virsh console X**" or from the virsh utility "virsh # **console X"** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**ps -ef |grep virsh**", then kill the existing process "**kill -9 <PID>**". Then execute the "virsh console X" command. Your console session should now run as expected.

   Login using **virsh**, and wait until you see the login prompt. If a login prompt does not appear after the guest is finished booting, press **ENTER** to make one appear:

```
$ sudo /usr/bin/virsh
virsh # list

 Id    Name                           State
----------------------------------------------------
 4     pmacU17-1                      running

virsh # console pmacU17-1

[Output Removed]

####################
1371236760: Upstart Job readahead-collector: stopping
1371236767: Upstart Job readahead-collector: stopped
####################

CentOS release 6.4 (Final)
Kernel 2.6.32-358.6.1.el6prerel6.5.0_82.16.0.x86_64 on an x86_64

pmacU17-1 login:
```

3. Verify the PM&C configured correctly on first boot.

Run the following command (there should be no output):

```
$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/
$
```

4. Determine the TimeZone to be used for the PM&C

   Note: Valid time zones can be found on the server in the directory "/usr/share/zoneinfo". Only the time zones within the sub-directories (i.e. America, Africa, Pacific, Mexico, etc…..) are valid with platcfg.

5. Set the TimeZone

   Run:

   ```
   $ sudo /usr/TKLC/smac/bin/set_pmac_tz.pl <timezone>
   ```

   For Example:

   ```
   $ sudo set_pmac_tz.pl America/New_York
   ```

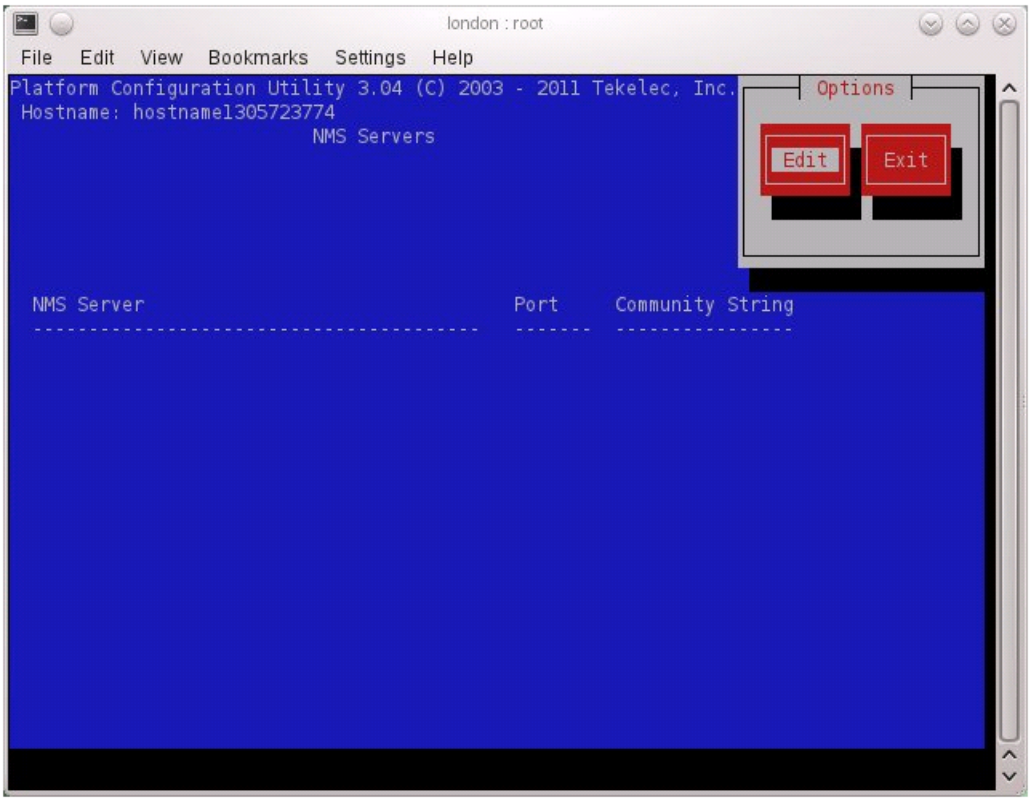
6. Verify the TimeZone has been updated

   Run:

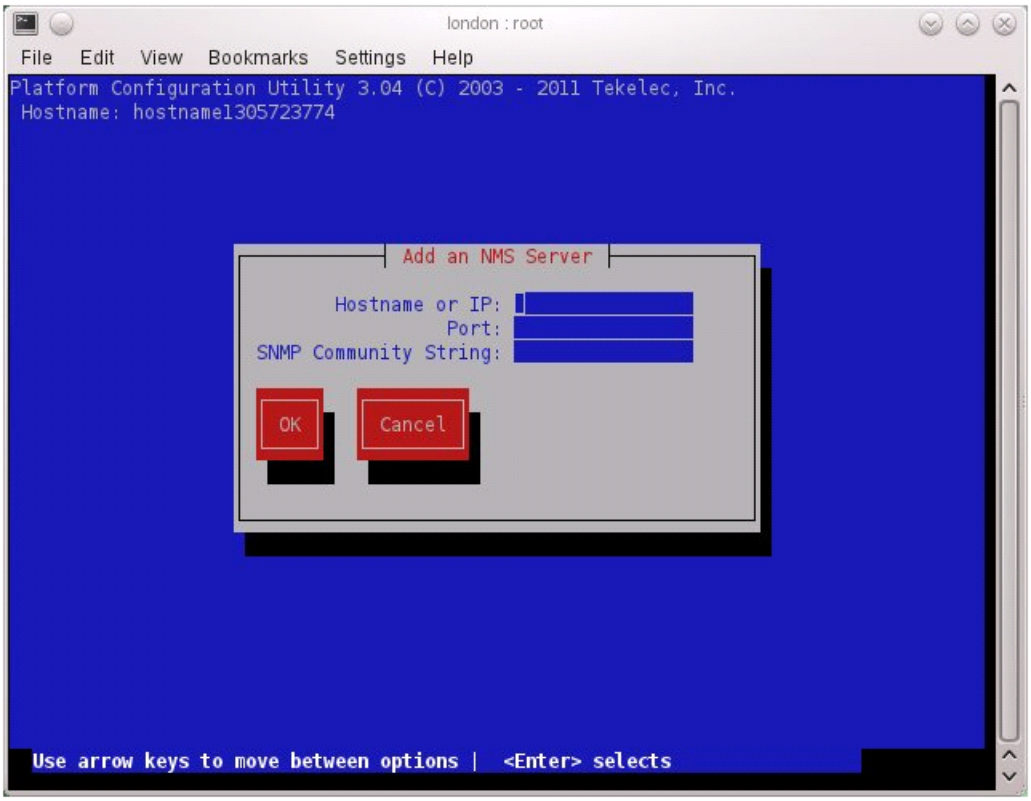
   ```
   $ sudo /bin/date
   ```

7. This step will add an SNMP trap destination to a server based on TPD. All alarm information will then be sent to the NMS located at the destination.

   1. **Server:** Login as platcfg user. Log in as platcfg user on the server. The platcfg main menu will be shown.
   2. **Server:** Navigate to NMS server configuration page. Select the following menu options sequentially: **Network Configuration** > **SNMP Configuration** > **NMS Configuration**. The 'NMS Servers' page will be shown, which displays all configured NMS servers for the server.

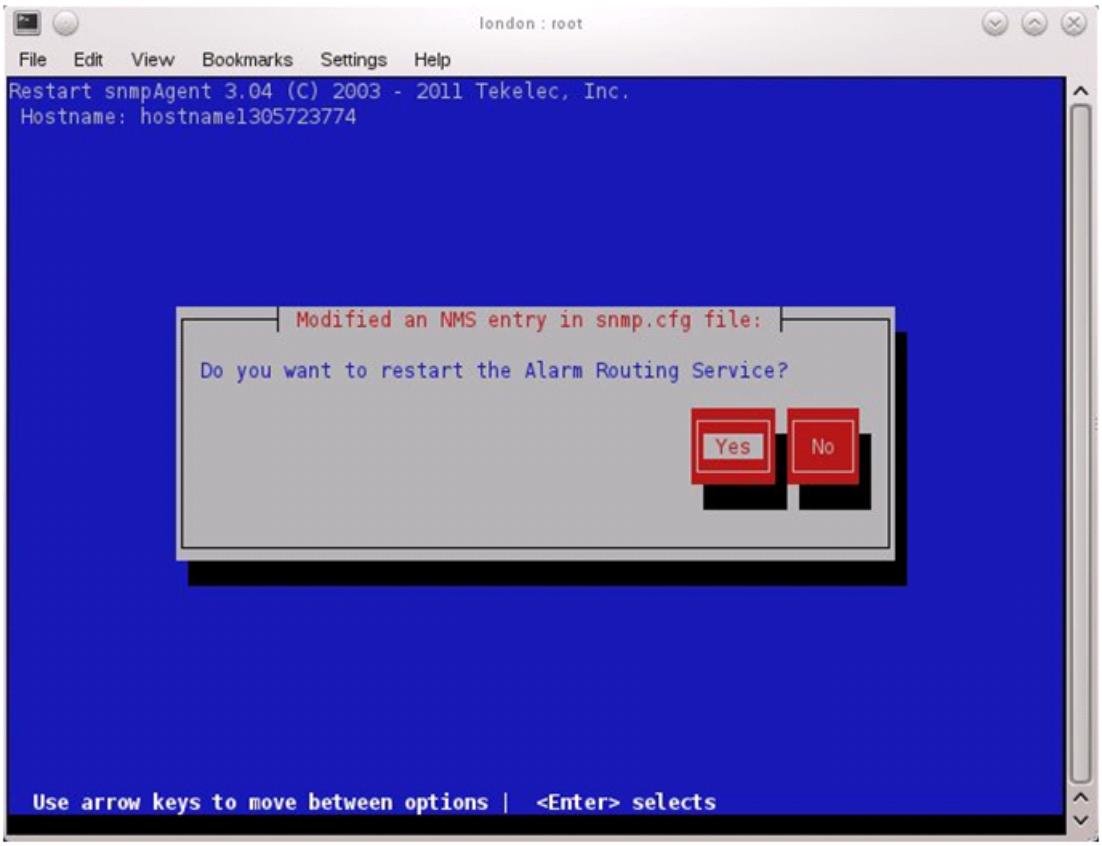


3. **Server:** Add the SNMP trap destination. Select **Edit** and then choose **Add a New NMS Server**. The 'Add an NMS Server' page will be displayed.



Complete the form by entering in all information about the SNMP trap destination. Refer to *3.3 SNMP Configuration*. Select **OK** to finalize the configuration.

The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialogue will then be presented.



Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented.

4. **Server:** Exit platcfg. Select **Exit** on each menu until platcfg has been exited.

8. Reboot the server to ensure all processes are started with the new TimeZone.

   Run:

```
$ sudo /sbin/init 6
```

9. Use this procedure to gather and prepare configuration files that are required to proceed with the DSR 7.1 installation.

   Needed Material:

   - HP Misc. Firmware DVD
   - Upgrade Pack of the *HP Solutions Firmware Upgrade Pack Notes* [2]

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

   Gather and prepare configuration files that must be resident on the PM&C. These might be required to proceed with the Application installation after the PM&C has been deployed but before it has been initialized. These files are usually located within a given ISO on physical media.

   a) Once the PM&C has completed rebooting, but prior to initializing, log into the PM&C as admusr using virsh on the management server iLO.

b) Create any necessary destination subdirectories in the PM&C **`/usr/TKLC/smac/etc`** directory if not using an existing directory to transfer files.

c) Make the media available to the TVOE Host server. Mount the media on the TVOE Host using the following method:

1. Insert the USB into an available USB slot on the TVOE Host server and execute the following command to determine its location and the ISO to be mounted:

```
$ sudo /bin/ls /media/*/*.iso
```

Example: `/media/sdd1/872-2507-111-4.1.0_41.16.2-DSR-x86_64.iso`

Note: The USB device is immediately added to the list of media devices once it is inserted into a USB slot on the TVOE Host server.

2. Note the device directory name under the media directory. This could be sdb1, sdc1, sdd1, or sde1, depending on the USB slot into which the media was inserted.
3. Loop mount the ISO to the standard TVOE Host mount point (if it is not already in use):

```
$ sudo /bin/mount -o loop /media/<device directory>/<ISO Name>.iso /mnt/upgrade
```

d) Execute the following commands on the PM&C guest to copy the required files from the TVOE host to the PM&C guest.

Wildcards can be used as necessary.

```
$ sudo /usr/bin/scp -r
admusr@<TVOE_management_ip_address>:/mnt/upgrade/upgrade/overlay/*
/usr/TKLC/smac/etc/
```

e) Change the permission of TVOEclean.sh and TVOEcfg.sh file

```
$ sudo chmod 555 /usr/TKLC/smac/etc/TVOEclean.sh
$ sudo chmod 555 /usr/TKLC/smac/etc/TVOEcfg.sh
```

f) Remove the application media from the TVOE host:

```
$ sudo /bin/umount /mnt/upgrade
```

g) **Management server:** Copy IOS images into place (this will copy both the 4948E and 3020 IOS images into place).

1. Insert the *Misc. Firmware* media into the CD or USB drive of the management server. For this step, be sure to use the correct IOS version specified by the Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]. Copy each IOS image called out by the release notes [2].
2. Execute the following commands to copy the required files. Note that the **<PMAC Management_IP Address>** is the one used to deploy PM&C in *4.1.3 Deploying Virtualized PM&C Overview*.

```
$ sudo /usr/bin/scp –p /media/cdrom/files/<4948E_IOS_image_filename> admusr@<PMAC
 Management_IP Address>:/var/TKLC/smac/image
$ sudo /usr/bin/scp –p /media/cdrom/files/<3020(6120)_IOS_image_filename>
admusr@<PMAC Management_IP Address>:/var/TKLC/smac/image
```

Make sure you copy the images for all type of enclosure switches present by re-running the previous command.

3. If using a CDROM drive, unmount it using the following command:

```
# umount /media/cdrom
```

4. Remove the *Misc. Firmware* media from the drive.

10. Initialize the PM&C Application; run the following commands:

Note: If performing the setup on a Redundant PM&C do not initialize, skip this step and continue to *Step 14*.

If using IPv4:

```
$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE
Profile successfully applied.
$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState
PMAC Feature State = InProgress
$ sudo /usr/TKLC/smac/bin/pmacadm addRoute --gateway=<mgmt_IPv4gateway_address>
 --ip=0.0.0.0 --mask=0.0.0.0 --device=management
Successful add of Admin Route
$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig
Initialization has been started as a background task
```

If using IPv6:

```
$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE
Profile successfully applied.
$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState
PMAC Feature State = InProgress
$ sudo /usr/TKLC/smac/bin/pmacadm addRoute --gateway=<IPv6mgmt_gateway_address>
 --ip=:: --mask=0 --device=management
Successful add of Admin Route
$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig
Initialization has been started as a background task
```

11. Wait for the background task to successfully complete.

The command will show "IN_PROGRESS" for a short time.

Run the following command until a "COMPETE" or "FAILED" response is seen similar to the following:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
1: Initialize PM&C COMPLETE - PM&C initialized
Step 2: of 2 Started: 2012-07-13 08:23:55 running: 29 sinceUpdate: 47
taskRecordNum: 2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
```

Note: Some expected networking alarms may be present.

12. Perform a system healthcheck on PM&C

```
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
```

This command should return no output on a healthy system.

Note: An NTP alarm will be detected if the system switches are not configured.

```
$ sudo /usr/TKLC/smac/bin/sentry status
```

All Processes should be running, displaying output similar to the following:

```
PM&C Sentry Status
------------------

sentryd started: Mon Jul 23 17:50:49 2012
Current activity mode: ACTIVE
Process              PID     Status             StartTS          NumR
------------------ ------ ----------- ------------------------- ----
smacTalk           9039     running   Tue Jul 24 12:50:29 2012  2
smacMon            9094     running   Tue Jul 24 12:50:29 2012  2
hpiPortAudit       9137     running   Tue Jul 24 12:50:29 2012  2
snmpEventHandler   9176     running   Tue Jul 24 12:50:29 2012  2
eclipseHelp        9196     running   Tue Jul 24 12:50:30 2012  2


Fri Aug  3 13:16:35 2012
Command Complete.
```

13. Verify the PM&C application release

Verify that the PM&C application Product Release is as expected.

Note: If the PM&C application Product Release is not as expected, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

```
$ sudo /usr/TKLC/plat/bin/appRev
        Install Time: Fri Sep 28 15:54:04 2012
        Product Name: PMAC
     Product Release: 5.0.0_50.10.0
     Part Number ISO: 872-2441-905
     Part Number USB: 872-2441-105
Base Distro Product: TPD
Base Distro Release: 6.0.0_80.22.0
     Base Distro ISO: TPD.install-6.0.0_80.22.0-CentOS6.2-x86_64.iso
                  OS: CentOS 6.2
```

14. Logout of the virsh console

Exit the virsh console session using *H.1 How to Exit a Guest Console Session on an iLO*.

15. Management Server iLO: Exit the TVOE console.

Run:

```
$ logout
```

You may now close the iLO browser window.

4.3 Configure Aggregation Switches

4.3.1 Configure netConfig Repository

This procedure will configure the netConfig repository for all required services and for each switch to be configured.

At any time, you can view the contents of the netConfig repository by using one of the following commands:

- For switches, use the command: **sudo /usr/TKLC/plat/bin/netConfig --repo listDevices**
- For services, use the command: **sudo /usr/TKLC/plat/bin/netConfig --repo listServices**

Users returning to this procedure after initial installation should run the above commands and note any devices and/or services that have already been configured. Duplicate entries cannot be added; if changes to a device repository entry are required, use the editDevice command. If changes to a services repository entry are necessary, you must delete the original entry first and then add the service again.

IPv4 and IPv6

Platform now supports configuration using IPv4 or IPv6 addresses through netConfig. Wherever IP addresses are required for networking procedures in section 3.1, IPv4 or IPv6 may be used. Commands such as ping or ssh may also be used in these procedures, where for IPv6 cases may need to be "ping6" or "ssh -6" as needed.

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. This may be a virtualized or physical environment. 'Management server' may also accurately describe this location but has been historically used to describe the physical environment while 'Virtual PM&C' was used to describe the virtualized netConfig server. Use of the term 'netConfig server' to describe dual scenarios of physical and virtualized environments will allow for future simplification of network configuration procedures.

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within "<>". Fill these worksheets out based on NAPD, then refer back to these tables for the proper value to insert depending on your system type.

Variable	Value
<management_server_iLO_ip>	
<management_server_mgmt_ip_address>	
<netConfig_server_mgmt_ip_address>	
<switch_backup_user>	admusr
<switch_backup_user_password>	See application documentation
<serial console type>	u=USB, c=PCIe

For the first aggregation switch (4948, 4948E, or 4948E-F): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<device_model>	
<console_name>	
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_ip_address>	
<switch_mgmt_netmask>	
<mgmt_vlanID>	
<control_vlanID>	
<IOS_filename>	
<ip_version>	

For the second aggregation switch (4948, 4948E, or 4948E-F): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<device_model>	
<console_name>	
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_ip_address>	
<switch_mgmt_netmask>	
<mgmt_vlanID>	
<control_vlanID>	
<IOS_filename>	
<ip_version>	

For each enclosure switch (6120XG, 6125G, 6125XLG, or 3020): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<io_bay>	
<OA1_enX_ip_address>	X= the enclosure #
<OA_password>	
<FW_image>	

For each enclosure switch (6120XG, 6125G, 6125XLG, or 3020): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<io_bay>	
<OA1_enX_ip_address>	X= the enclosure #
<OA_password>	
<FW_image>	

1. **Management server iLO**: Log in and launch the integrated remote console.
   a) On the management server, log in to iLO in IE using the password provided by the application: `http://<management_server_iLO_ip>`
   b) For HP servers, click in the Remote Console tab and launch the Remote Console on the server.
   c) Click Yes if the Security Alert dialogue box is displayed.
   d) If you have not already done so, log in as admusr.
2. **Management Server**: Procedure pre-check

   If the installation is not designed for a virtual PM&C, go to *Step 3*.

   If there is a virtual PM&C, log in to the console of the virtual PM&C.

- Verify virtual PM&C installation by issuing the following commands as admusr on the management server:

```
$ sudo /usr/bin/virsh list --all
Id Name State
----------------------------------
6 vm-pmac1A running
```

- If this command provides no output, it is likely that a virtual instance of PM&C is not installed.
  - If there is a virtual PM&C, log in to the console of the virtual PM&C.
  - If the installation is not designed for a virtual PM&C, go to *Step 3*.
- From the management server, log in to the console of the virtual PM&C instance found above.

  Example:

```
$ sudo /usr/bin/virsh console vm-pmac1A
Connected to domain vm-pmac1A
Escape character is ^]
<Press ENTER key>
CentOS release 6.2 (Final)
Kernel 2.6.32-220.7.1.el6prerel6.0.0_80.13.0.x86_64 on an x86_64
```

  If the root user is already logged in, logout and log back in as admusr.

```
[root@pmac ~]# logout
```

```
vm-pmac1A login: admusr
Password:
Last login: Fri May 25 16:39:04 on ttyS4
```

  - If this command fails, it is likely that a virtual instance of PM&C is not installed.
  - If this is unexpected, refer to application documentation or contact *1.4 My Oracle Support (MOS)*.

3. **netConfig Server:** Check that the switch templates directory exists:

```
$ /bin/ls -i /usr/TKLC/smac/etc/switch/xml
```

   If the command returns an error:

```
ls: cannot access /usr/TKLC/smac/etc/switch/xml/: No such file or directory
```

   Create the directory:

```
$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/xml
```

   Change directory permissions:

```
$ sudo /bin/chmod go+rx /usr/TKLC/smac/etc/switch/xml
```

4. **netConfig Server**: Set up netConfig repository with necessary ssh information.

   Use netConfig to create a repository entry that will use the ssh service. This command will provide the user with several prompts. The prompts shown with <variables> as the answers are site specific

that the user MUST modify. Other prompts that don't have a <variable> shown as the answer must be entered EXACTLY as they are shown here.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service
Service type? (tftp, ssh, conserver, oa) ssh
Service host? <netConfig_server_mgmt_ip_address>
Enter an option name <q to cancel>: user
Enter the value for user: <switch_backup_user>
Enter an option name <q to cancel>: password
Enter the value for password: <switch_backup_user_password>
Verify Password: <switch_backup_user_password>
Enter an option name <q to cancel>: q
Add service for ssh_service successful
$
```

To ensure that you entered the information correctly, use the following command and inspect the output, which will be similar to the one shown below.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service
Service Name: ssh_service
Type: ssh
Host: 10.250.8.4
Options:
password: C20F7D639AE7E7
user: admusr
$
```

5. **netConfig Server**: Set up netConfig repository with necessary tftp information.

   Note: If there are no new Cisco (3020, 4948, 4948E or 4948E-F) switches to be configured, go to the next step.

   Use netConfig to create a repository entry that will use the tftp service. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

   - For a PM&C system:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service
Service type? (tftp, ssh, conserver, oa) tftp
Service host? <netConfig_server_mgmt_ip_address>
Enter an option name (q to cancel): dir
Enter a value for user dir: /var/TKLC/smac/image/
Enter an option name(q to cancel): q
Add service for tftp_service successful
```

   - For a non-PM&C system:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service
Service type? (tftp, ssh, conserver, oa) tftp
Service host? <netConfig_server_mgmt_ip_address>
Enter an option name (q to cancel): dir
Enter a value for user dir: /var/lib/tftpboot/
Enter an option name(q to cancel): q
Add service for tftp_service successful
```

6. **netConfig Server**: Set up netConfig repository with necessary OA information.

Note: If there are no new HP 6125G/6125XLG/6120XG switches to be configured, go to the next step.

Use netConfig to create a repository entry that will use the OA service. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=oa_service_en<enclosure
 #>
Service type? (tftp, ssh, conserver, oa) oa
Service host? <OA1_enX_ip_address>
Enter an option name <q to cancel>: user
Enter the value for user: root
Enter an option name <q to cancel>: password
Enter the value for password: <OA_password>
Verify password:<OA_password>
Enter an option name <q to cancel>: q
Add service for oa_service successful
```

7. **netConfig Server**: Run conserverSetup command.

```
$ sudo /usr/TKLC/plat/bin/conserverSetup –<serial console type> -s
<management_server_mgmt_ip_address>
```

You will be prompted for the platcfg credentials.

An example:

```
[admusr@vm-pmac1A]$ sudo /usr/TKLC/plat/bin/conserverSetup -u -s
<management_server_mgmt_ip_address>
Enter your platcfg username, followed by [ENTER]:platcfg
Enter your platcfg password, followed by [ENTER]:<platcfg_password>
Checking Platform Revision for local TPD installation...
The local machine is running:
        Product Name: PMAC
 Base Distro Release: 7.0.0.0.0_86.1.0

Checking Platform Revision for remote TPD installation...
The remote machine is running:
        Product Name: TVOE
 Base Distro Release: 7.0.0.0.0_86.2.0
Configuring switch 'switch1A_console' console server...Configured.
Configuring switch 'switchBA_console' console server...Configured.
Configuring iptables for port(s) 782...Configured.
Configuring iptables for port(s) 1024:65535...Configured.
Configuring console repository service...
Repo entry for "console_service" already exists; deleting entry for:
    Service Name:    console_service
            Type:    conserver
            Host:    <management_server_mgmt_ip_address>
...Configured.


Slave interfaces for bond0:

        bond0 interface:  eth01
        bond0 interface:  eth02
```

- If this command fails, contact *1.4 My Oracle Support (MOS)*.
- Verify the output of the script.

- Verify that your Product Release is based on Tekelec Platform 7.0 (versions 7.0.x.x.x_x.x.x).
- Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

8. **netConfig Server**: Mount the HP Misc Firmware ISO

   Note: If this is a Software Centric deployment, skip this step and proceed to step 9.

```
$ sudo /bin/mount -o loop /var/TKLC/upgrade/<misc_ISO> /mnt/upgrade
```

   Example:

```
$ sudo /bin/mount -o loop /var/TKLC/upgrade/872-2161-113-2.1.10_10.26.0.iso
/mnt/upgrade
```

9. **netConfig Server**: Copy Cisco switch FW to the **tftp_directory**

   Note: If this is a Software Centric deployment, the customer must place the FW files for the Cisco switches (C3020, 4948/E/E-F) into the tftp directory listed below. Otherwise, perform the commands to copy the file from the FW ISO.

   For each Cisco switch model (C3020, 4948/E/E-F) present in the solution, copy the FW identified by **<FW_image>** in the aggregation switch variable table (4948) or enclosure switch variable table (C3020) to the **tftp_service** directory and change the permissions of the file:

   - For a PM&C system: **<tftp_directory> = /var/TKLC/smac/image/**
   - For a non-PM&C system: **<tftp_directory> = /var/lib/tftpboot/**

```
$ sudo /bin/cp /mnt/upgrade/files/<FW_image> <tftp_directory>
$ sudo /bin/chmod 644 <tftp_directory/<FW_image>
```

   Example:

```
$ sudo /bin/cp /mnt/upgrade/files/cat4500e-entservicesk9-mz.122-54.XO.bin
/var/TKLC/smac/image/
$ sudo /bin/chmod 644 /var/TKLC/smac/image/cat4500e-entservicesk9-mz.122-54.XO.bin
```

   If there are no Cisco switches, skip to the next step.

10. **netConfig Server**: Copy HP switch FW to the **ssh** directory

    Note: If this is a Software Centric deployment, the customer must place the FW files for the HP switches into the shh directory listed below. Otherwise, perform the commands to copy the file from the FW ISO.

    For each HP switch model (HP6125G/XLG, HP6120XG) present in the solution, copy the FW identified by **<FW_image>** in the enclosure switch variable tables to the **ssh_service** directory and change the permissions of the file:

```
$ sudo /bin/cp /mnt/upgrade/files/<FW_image> ~<switch_backup_user>/
$ sudo /bin/chmod 644 ~<switch_backup_user>/<FW_image>
```

    Example:

```
$ sudo /bin/cp /mnt/upgrade/files/Z_14_37.swi ~admusr/
$ sudo /bin/chmod 644 ~admusr/Z_14_37.swi
```

If there are no HP switches, skip to the next step.

11. **netConfig Server**: Unmount the ISO

```
$ sudo /bin/umount /mnt/upgrade
```

12. **netConfig Server**: Set up netConfig repository with aggregation switch information.

    Note: If there are no new aggregation switches to be configured, go to the next step.

    Use netConfig to create a repository entry for each switch. The initial command will prompt the user multiple times. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

    - The <device_model> can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact *1.4 My Oracle Support (MOS)*.
    - The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentialsDevice Vendor? Cisco
Device Model? <device_model>
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation)  address for
 management?: <switch_mgmt_ip_address>
Is the management interface a port or a vlan? [vlan]: [Enter]
What is the VLAN ID of the management VLAN? [2]: [mgmt_vlanID]
What is the name of the management VLAN? [management]: [Enter]
What switchport connects to the management server? [GE40]: [Enter]
What is the switchport mode (access|trunk) for the management server port?
[trunk]: [Enter]
What are the allowed vlans for the management server port? [1,2]:
<control_vlanID>, <mgmt_vlanID>
Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.XO.bin]:
<IOS_filename>
Firmware file to be used in upgrade: <IOS_filename>
Enter the name of the upgrade file transfer service: tftp_service
File transfer service to be used in upgrade: tftp_service
Should the init oob adapter be added (y/n)? y
Adding consoleInit protocol for <switch_hostname> using oob...
What is the name of the service used for OOB access? console_service
What is the name of the console for OOB access? <console name>
What is the platform access username? <switch_platform_username>
What is the device console password? <switch_console_password>
Verify password: <switch_console_password>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the device privileged mode password? <switch_enable_password>
Verify password: <switch_enable_password>
Should the live network adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using network...
Network device access already set: <switch_mgmt_ip_address>
Should the live oob adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using oob...
OOB device access already set: console_service
Device named <switch_hostname> successfully added.
```

To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

and check the output, which will be similar to the one shown:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
Device: <switch_hostname>
    Vendor:   Cisco
    Model:    <device_model>
    FW Ver:   0
    FW Filename: <IOS_image>
    FW Service:  tftp_service
    Initialization Management Options
        mgmtIP: <switch_mgmt_ip_address>
        mgmtInt: vlan
        mgmtVlan: <mgmt_vlanID>
        mgmtVlanName: management
        interface: GE40
        mode: trunk
        allowedVlans: <control_vlanID>, <mgmt_vlanID>
    Access:   Network: <switch_mgmt_ip_address>
    Access:   OOB:
                  Service: console_service
                  Console: <console_name>
    Init Protocol Configured
    Live Protocol Configured
$
```

Repeat this step for each 4948 / 4948E / 4948 E-F, using appropriate values for those switches.

13. **netConfig Server**: Set up netConfig repository with 3020 switch information.

    Note: If there are no new 3020s to be configured, go to the next step.

    Note: The Cisco 3020 is not compatible with IPv6 management configuration.

    Use netConfig to create a repository entry for each 3020. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

    - If you do not know any of the required answers, stop now and contact *1.4 My Oracle Support (MOS)*.
    - The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? Cisco
Device Model? 3020
What is the management address? <enclosure_switch_ip>
Enter the name of the firmware file [cbs30x0-ipbasek9-tar.122-58.SE1.tar]:
<FW_image>
Firmware file to be used in upgrade: <IOS_image>
Enter the name of the upgrade file transfer service: <tftp_service>
File transfer service to be used in the upgrade: <tftp_service>
Should the init network adapter be added (y/n)? y
Adding netBootInit protocol for <switch_hostname> using network...
Network device access already set: <enclosure_switch_ip>
What is the platform access username? <switch_platform_username>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the device privileged mode password? <switch_enable_password>
Verify password: <switch_enable_password>
Should the init file adapter be added (y/n)? y
Adding netBootInit protocol for <switch_hostname> using file...
```

```
What is the name of the service used for TFTP access? tftp_service
Should the live network adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using network...
Network device access already set: <enclosure_switch_ip>
Device named <switch_hostname> successfully added.
```

To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

and check the output, which will be similar to the one shown below.

```
$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
Device: <switch_hostname>
    Vendor:   Cisco
    Model:    <device_model>
    FW Ver:   0
    FW Filename: <FW_image>
    FW Service:  tftp_service
    Access:   Network: <enclosure_switch_IP>
Init Protocol Configured
Live Protocol Configured
```

Repeat this step for each 3020, using appropriate values for those 3020s.

Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/image:

WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.

14. **netConfig Server**: Set up netConfig repository with HP 6120XG switch information.

    Note: If there are no 6120XGs to be configured, stop and continue with the appropriate switch configuration procedure.

    Use netConfig to create a repository entry for each 6120XG. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

    - If you do not know any of the required answers, stop now and contact *1.4 My Oracle Support (MOS)*.
    - The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? HP
Device Model? 6120
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for
management?: <switch_mgmt_ip_address>
Enter the name of the firmware file [Z_14_37.swi]: <FW_image>
Firmware file to be used in upgrade: <FW_image>
Enter the name of the upgrade file transfer service: ssh_service
File transfer service to be used in upgrade: ssh_service
Should the init oob adapter be added (y/n)? y
Adding consoleInit protocol for <switch_hostname> using oob...
What is the name of the service used for OOB access? oa_service_en<enclosure #>
```

```
What is the name of the console for OOB access? <io_bay>
What is the platform access username? <switch_platform_username>
What is the device console password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the device privileged mode password? <switch_platform_password>
Verify password: <switch_platform_password>
Should the live network adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using network...
Network device access already set: <switch_mgmt_ip_address>
Should the live oob adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using oob...
OOB device access already set: oa_service_en<enclosure #>
Device named <switch_hostname> successfully added
```

The image is being unpacked and validated. This will take approximately 4 minutes. Once the unpacking, validation, and rebooting have completed, you will be returned to the normal prompt. Proceed with the next step.

To verify that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

and check the output, which will be similar to the one shown:

```
$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
Device:  <switch_hostname>
    Vendor:   HP
    Model:    6120
    FW Ver:   0
    FW Filename: <FW_image>
    FW Service:  ssh_service
    Initialization Management Options
        mgmtIP: <enclosure_switch_IP>
    Access:   Network: <enclosure_switch_IP>
    Access:   OOB:
                  Service: oa_service
                  Console: <console_name>
    Init Protocol Configured
    Live Protocol Configured
```

Repeat this step for each 6120, using appropriate values for those 6120s.

Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/image:

WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.

15. **netConfig Server:** Set up netConfig repository with HP 6125G switch information.

    Note: If there are no 6125Gs to be configured, stop and continue with the appropriate switch configuration procedure.

    Use netConfig to create a repository entry for each 6125G. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

- If you do not know any of the required answers, stop now and contact *1.4 My Oracle Support (MOS)*.
- The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? HP
Device Model?  6125
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation)address for
management? <switch_mgmt_ip_address>
Enter the name of the firmware file [6125-CMW520-R2105.bin]: <FW_image>
Firmware file to be used in upgrade: <FW_image>
Enter the name of the upgrade file transfer service: ssh_service
Should the init oob adapter be added (y/n)? y
Adding consoleInit protocol for <switch_hostname> using oob...
What is the name of the service used for OOB access?oa_service_en<enclosure #>
What is the name of the console for OOB access? <io_bay>
What is the platform access username? <switch_platform_username>
What is the device console password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the device privileged mode password? <switch_platform_password>
Verify password: <switch_platform_password>
Should the live network adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using network...
Network device access already set: <switch_mgmt_ip_address>
Should the live oob adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using oob...
OOB device access already set: oa_service_en<enclosure #>
Device named <switch_hostname> successfully added.
```

Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/image:

WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.

To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

and check the output, which will be similar to the one shown:

16. **netConfig Server:** Set up netConfig repository with HP 6125XLG switch information.

    Note: If there are no 6125XLGs to be configured, stop and continue with the appropriate switch configuration procedure.

    Use netConfig to create a repository entry for each 6125XLG. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that doesn't have a <variable> as an answer must be entered EXACTLY as they are shown here.

    - If you do not know any of the required answers, stop now and contact *1.4 My Oracle Support (MOS)*.

- The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? HP
Device Model? 6125XLG
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation)  address for
 management?: <switch_mgmt_ip_address>
Enter the name of the firmware file [6125XLG-CMW710-R2403.ipe]: <FW_image>
Firmware file to be used in upgrade: <FW_image>
Enter the name of the upgrade file transfer service: ssh_service
File transfer service to be used in upgrade: ssh_service
Should the init oob adapter be added (y/n)? y
Adding consoleInit protocol for <switch_hostname> using oob...
What is the name of the service used for OOB access? oa_service_en<enclosure #>
What is the name of the console for OOB access? <io_bay>
What is the platform access username? <switch_platform_username>
What is the device console password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the device privileged mode password? <switch_platform_password>
Verify password: <switch_platform_password>
Should the live network adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using network...
Network device access already set: <switch_mgmt_ip_address>
Should the live oob adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using oob...
OOB device access already set: oa_service_en<enclosure #>
Device named <switch_hostname> successfully added
```

Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/image:

WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.

To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

and check the output, which will be similar to the one shown:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
Device: <switch_hostname>
Vendor: HP
Model: 6125XLG
FW Ver: 0
FW Filename: <FW_image>
FW Service: ssh_service
Access: Network: <enclosure_switch_IP>
Access: OOB:
        Service: oa_service
        Console: <io_bay>
Init Protocol Configured
```

4.3.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)

This procedure will configure 4948/4948E/4948E-F switches with an appropriate IOS and configuration from a single management server and virtual PM&C for use with the c-Class or RMS platform.

Procedure Reference Tables:

Steps within this procedure may refer to variable data indicated by text within "<>". Refer to this table for the proper value to insert depending on your system type.

Fill in the appropriate value from [2].

Variable	Cisco 4948	Cisco 4948E	Cisco 4948E-F
<IOS_image_file>			

Fill in the appropriate value for this site:

Variable	Value
<switch_platform_username>	See referring application documentation
<switch_platform_password>	
<switch_console_password>	
<switch_enable_password>	
<management_server_mgmt_ip_address>	
<pmac_mgmt_ip_address>	
<switch_mgmtVLAN_id>	
<switch1A_mgmtVLAN_ip_address>	
<mgmt_Vlan_subnet_id>	
<netmask>	
<switch1B_mgmtVLAN_ip_address>	
<switch_Internal_VLANS_list>	
<management_server_mgmtInterface>	
<management_server_iLO_ip>	
<customer_supplied_ntp_server_address>	

Variable	Value
<platcfg_password>	Initial password as provided by Oracle
<management_server_mgmtInterface>	Value gathered from NAPD
<switch_backup_user>	admusr
<switch_backup_user_password>	Check application documentation

Note: The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.

Note: Uplinks must be disconnected from the customer network prior to executing this procedure. One of the steps in this procedure will instruct when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.

Needed Material:

- HP MISC firmware ISO image
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]
- Template xml files on the application media.

Note: Filenames and sample command line input/output throughout this section do not specifically reference the 4948E-F. Template settings are identical between the 4948E and 4948E-F. The original 4948 switch -- as opposed to the 4948E or the 4948E-F is referred to simply by the model number 4948. Where all three switches are referred to, this will be made clear by reference to '4948 / 4948E / 4948 E-F' switches.

Note: If a procedural STEP fails to execute successfully, STOP and contact *1.4 My Oracle Support (MOS)*.

1. **Virtual PM&C:** Verify the IOS image is on the system. If the appropriate image does not exist, copy the image to the PM&C.

   Determine if the IOS image for the 4948/4948E/4948E-F is on the PM&C.

   ```
   $ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file>
   ```

   If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]

2. **Virtual PM&C**: Modify PM&C Feature to allow TFTP.

   Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:

   ```
   $ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
    --enable=1
   $ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
   ```

   Note: Ignore the sentry restart instructions.

   Note: This may take up to 60 seconds to complete.

3. **Virtual PM&C -> Management Server:** Manipulate host server physical interfaces.

   Exit from the virtual PM&C console, by entering **< ctrl-] >** and you will be returned to the server prompt.

   Ensure that the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands:

   ```
   $ sudo /sbin/ifup <ethernet_interface_1>
   $ sudo /sbin/ifdown <ethernet_interface_2>
   $ sudo /sbin/ip addr show <management_server_mgmtInterface> | grep inet
   ```

The command output should contain the IP address of the variable

<management_server_mgmt_ip_address>

Note: On a TVOE host, If you launch the virsh console, i.e., "#**virsh console X**" or from the virsh utility "virsh #**console X"** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**ps -ef |grep virsh**", then kill the existing process "**kill -9 <PID>**". Then execute the "virsh console X" command. Your console session should now run as expected.

4. **Virtual PM&C:** Determine if switch1A PROM upgrade is required.

   Note: ROM & PROM are intended to have the same meaning for this procedure

   Connect to switch1A, check the PROM version.

   Connect serially to switch1A by issuing the following command.

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1A_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]
Press Enter
Switch> show version | include ROM
ROM: 12.2(31r)SGA1
System returned to ROM by reload
```

   Note: If the console command fails, contact *1.4 My Oracle Support (MOS)*.

   Note the IOS image & ROM version for comparison in a following step. Exit from the console by entering**<ctrl-e><c><.>** and you will be returned to the server prompt.

   Check the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in *J.1 Upgrade Cisco 4948 PROM* to upgrade the PROM for switch1A.

5. **Virtual PM&C:**

   Extract the configuration files from the ZIP file copied in *Step 9* of *4.2.2 Setup PM&C*.

```
$ cd /usr/TKLC/smac/etc
$ sudo unzip DSR_NetConfig_templates.zip
```

   This will create a directory called**DSR_NetConfig_Templates** which contains the configuration files for all the supported deployments. Copy the necessary init file from**init/Aggregation** and the necessary config files from**config/TopoX** (where X refers to the appropriate topology) using the following commands. Make sure to replace "X" with the appropriate Topology number.

```
# sudo cp DSR_NetConfig_Templates/init/Aggregation/* .
# sudo cp DSR_NetConfig_Templates/config/TopoX/* .
```

6. **Virtual PM&C:** Modify switch1A_4948_4948E_init.xml and switch1B_4948_4948E_init.xml files for information needed to initialize the switch.

   Update the init.xml files for all values preceded by a dollar sign. For example, if a value has $some_variable_name, that value will be modified and the dollar sign must be removed during the modification.

When done editing the file, save and exit to return to the command prompt.

7. **Virtual PM&C:** Modify 4948E-F_configure.xml for information needed to configure the switches.

   Update the configure.xml file for all values preceded by a dollar sign. For example, if a value has $some_variable_name, that value will be modified and the dollar sign must be removed during the modification.

   When done editing the file, save and exit to return to the command prompt.

   Note: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the Cisco 4948E-F aggregation switches. This function must be configured for IPv4.

8. **Virtual PM&C:** Initialize switch1A

   Initialize switch1A by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml
$
```

   Note: This step takes about 5-10 minutes to complete.

   Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact *1.4 My Oracle Support (MOS)*.

   A successful completion of netConfig will return the user to the prompt.

   Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname
Hostname: switch1A
$
```

   Note: If this command fails, stop this procedure and contact *1.4 My Oracle Support (MOS)*.

9. **Virtual PM&C:** Verify the switch is using the proper IOS image per Platform version.

   Issue the following commands to verify the IOS release on each switch:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware

Version: 122-54.XO

License: entservicesk9

Flash: cat4500e-entservicesk9-mz.122-54.XO.bin
```

10. **Virtual PM&C -> Management Server:** Manipulate host server physical interfaces for switch1B.

    Exit from the virtual PM&C console, by entering **< ctrl-] >** and you will be returned to the server prompt.

Ensure that the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands:

```
$ sudo /sbin/ifup <ethernet_interface_2>
$ sudo /sbin/ifdown <ethernet_interface_1>
$ sudo /sbin/ip addr show <management_server_mgmtInterface> | grep inet
```

The command output should contain the IP address of the variable

<management_server_mgmt_ip_address>

Connect to the Virtual PM&C by logging into the console of the virtual PM&C instance found in step 2 of *4.3.1 Configure netConfig Repository*.

```
$ sudo /usr/bin/virsh console vm-pmac1A
```

Note: On a TVOE host, If you launch the virsh console, i.e "# virsh console X" or from the virsh utility "virsh # console X" command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "ps -ef |grep virsh", then kill the existing process "kill -9 <PID>". Then execute the "virsh console X" command. Your console session should now run as expected.

11. **Virtual PM&C:** Determine if switch1B PROM upgrade is required.

    Note: ROM & PROM are intended to have the same meaning for this procedure

    Connect to switch1A, check the PROM version.

    Connect serially to switch1A by issuing the following command.

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1A_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]
Press Enter
Switch> show version | include ROM
ROM: 12.2(31r)SGA1
System returned to ROM by reload
```

    Check the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in *J.1 Upgrade Cisco 4948 PROM* to upgrade the PROM for switch1B.

    Note: If the console command fails, contact *1.4 My Oracle Support (MOS)*.

    Note the IOS image & ROM version for comparison in a following step. Exit from the console by entering**<ctrl-e><c><.>** and you will be returned to the server prompt.

12. **Virtual PM&C:** Initialize switch1B

    Initialize switch1B by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml
$
```

Note: This step takes about 5-10 minutes to complete.

Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact *1.4 My Oracle Support (MOS)*.

A successful completion of netConfig will return the user to the prompt.

Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname
Hostname: switch1B
$
```

Note: If this command fails, stop this procedure and contact *1.4 My Oracle Support (MOS)*.

13. **Virtual PM&C:** Verify the switch is using the proper IOS image per Platform version.

    Issue the following commands to verify the IOS release on each switch:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware

Version: 122-54.XO

License: entservicesk9

Flash: cat4500e-entservicesk9-mz.122-54.XO.bin
```

14. **Virtual PM&C:** Modify PM&C Feature to disable TFTP.

    Disable the DEVICE.NETWORK.NETBOOT feature.

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=0
$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
```

Note: This may take up to 60 seconds to complete.

15. **Virtual PM&C:** Configure both switches

    Configure both switches by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml
$
```

Note: This may take about 2-3 minutes to complete.

Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact *1.4 My Oracle Support (MOS)*.

A successful completion of netConfig will return the user to the prompt.

16. **Management Server**: Ensure both interfaces are enabled on the TVOE host.

    Exit from the virtual PM&C console by following the instructions in Appendix *H.1 How to Exit a Guest Console Session on an iLO*. This will return the terminal to the server prompt.

Ensure that the interfaces of the server connected to switch1A and switch1B are up by performing the following commands:

```
$ sudo /sbin/ifup <ethernet_interface_1>
$ sudo /sbin/ifup <ethernet_interface_2>
```

17. **Cabinet:** Connect network cables from customer network

    Attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.

    Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active

18. **Virtual PM&C:** Verify access to customer network

    Verify connectivity to the customer network by issuing the following command:

```
$ /bin/ping <customer_supplied_ntp_server_address>
PING ntpserver1 (10.250.32.51) 56(84) bytes of data.
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms
```

19. **Cabinet:** Connect network cables from customer network

    Attach switch1B customer uplink cables and detach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.

    Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

20. **Virtual PM&C:** Verify access to customer network

    Verify connectivity to the customer network by issuing the following command:

```
$ /bin/ping <customer_supplied_ntp_server_address>
PING ntpserver1 (10.250.32.51) 56(84) bytes of data.
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms
```

21. **Cabinet:** Connect network cables from customer network

    Re-attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.

    Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active

22. **Management Server:** Restore the TVOE host back to its original state.

    Exit from the virtual PM&C console by following the instructions in Appendix *H.1 How to Exit a Guest Console Session on an iLO*. This will return the terminal to the server prompt.

    Restore the server networking back to original state:

```
$ sudo /sbin/service network restart
```

23. Perform *E.2 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* for each switch configured in this procedure.

4.4 Configure PM&C

4.4.1 Configure NetBackup Feature

If the PM&C application will be configured with the optional NetBackup feature and the NetBackup client will be installed on this server execute the following procedure with the appropriate NetBackup feature data, otherwise continue with next procedure.

4.4.1.1 Configure PM&C Application

Configuration of the PM&C application is typically performed using the PM&C GUI. This procedure defines application and network resources. At a minimum, you should define network routes and DHCP pools. Unlike initialization, configuration is incremental, so you may execute this procedure to modify the PM&C configuration.

Note: The installer must be knowledgeable of the network and application requirements. The final step will configure and restart the network and the PM&C application; network access will be briefly interrupted.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. **PM&C GUI:** Load GUI and navigate to the Configuration view

   Open web browser and enter:

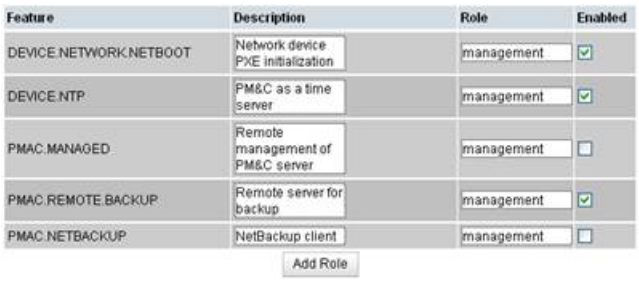
   ```
   https://<pmac_management_network_ip>
   ```

   Login as pmacadmin user.

Navigate to **Main Menu** > **Administration** > **PM&C Configuration**.

2. **PM&C GUI:** Configure optional features

   If NetBackup is to be used, enable the NetBackup feature. Otherwise use the selected features as is. The following image is for reference only:



   The "**Enabled**" checkbox selects the desired features. The "**Role**" field provides a drop-down list of known network roles that the feature may be associated with. The "**Description**" may be edited if desired.

   If the feature should be applied to a new network role (e.g. "**NetBackup**"), click on the "**Add Role**" button. Enter the name of the new role and click on "**Add**". (Note: role names are not significant, they are only used to associate features with networks). The new role name will appear in the "**Role**" drop-down field for features.

   When done, click on the "**Apply**" button. This foreground task will take a few moments, and then refresh the view with an Info or Error notice to verify the action. To discard changes, just navigate away from the view.

3. **PM&C GUI:** Reconfigure PM&C networks

Note: The Network reconfiguration enters a tracked state. After you click on "**Reconfigure**", you should use a "**Cancel**" button to abort.

Click on "**Network Configuration**" in the navigation pane, and follow the wizard through the configuration task.

1. Click on "**Reconfigure**" to display the "**Network**" view. The default "**management**" and "**control**" networks should be configured correctly. Networks may be added, deleted or modified from this view. They are defined with IPv4 dotted-quad addresses and netmasks, or with IPv6 colon hex addresses and a prefix. When complete, click on "**Next**".
2. On the "**Network Roles**" view, you may change the role of a network. Network associations can be added (e.g. "**NetBackup**") or deleted. You cannot add a new role since roles are driven from features. When complete, click on "**Next**".
3. On the "**Network Interfaces**" view, you may add or delete interfaces, and change the IP address within the defined network space. If you add a network (again, for example, "**NetBackup**"), the "**Add Interface**" view is displayed when clicking on "**Add**". This view provides an editable drop-down field of known interfaces. You may add a new device here if necessary. The Address must be an IPv4 or IPv6 host address in the network. When complete, click on "**Next**".
4. On the "**Routes**" view, you may add or delete route destinations. The initial PM&C deployment does not define routes. Most likely you will want to add a default route - the route already exists, but this action defines it to PM&C so it may be displayed by PM&C. Click on "**Add**". The Add Route view provides an editable drop-down field of known devices. Select the egress device for the route. Enter an IPv4 dotted-quad address and netmask or an IPv6 colon hex address and prefix for the route destination and next-hop gateway. Then click on "**Add Route**". When complete, click on "**Next**".
5. On the "**DHCP Ranges**" view, you will need to define DHCP pools used by servers that PM&C manages. Click on the "**Add**" button. Enter the starting and ending IPv4 address for the range on the network used to control servers (by default, the "**control**" network). Click on "**Add DHCP Range**". Only one range per network may be defined. When all pools are defined, click on "**Next**".
6. The "**Configuration Summary**" provides a view of your reconfigured PM&C. Click "**Finish**" to launch the background task that will reconfigure the PM&C application. A Task and Info or Error notice is displayed to verify your action.
7. Verify your reconfiguration task completes. Navigate to: **Main Menu** > **Task Monitoring**. As the network is reconfigured, you will have a brief network interruption. From the Background Task Monitoring view, verify the "**Reconfigure PM&C**" task succeeds.

4. **PM&C GUI:** Set the PM&C Application GUI Site Settings

   Navigate to **Main Menu** > **Administration** > **GUI Site Settings**

   Set the "**Site name**" to a descriptive name, and set the "**Welcome Message**" that is displayed upon login.

5. **PM&C**: Perform PM&C application backup.

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

Note: The backup runs as a background task. To check the status of the background task use the PM&C GUI Task Monitor page, or issue the command " **pmaccli getBgTasks** ". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

6. **PM&C:** Verify the Backup was successful

   Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contactMy Oracle Supportby referring to the*1.4 My Oracle Support (MOS)*section of this document.

   The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C Backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

7. **PM&C:** Save the PM&C backup

   The PM&C backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server. The PM&C backup files are saved in the following directory: "/var/TKLC/smac/backup".

4.4.2 Install and Configure NetBackup Client on PM&C

If the PM&C application will be configured with the optional NetBackup feature and the NetBackup client will be installed on this server execute the following procedure with the appropriate NetBackup feature data, otherwise continue with next procedure.

4.4.2.1 PM&C NetBackup Client Installation and Configuration

This procedure provides instructions for installing and configuring the Netbackup client software on a PM&C application.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. **PM&C GUI:** Verify the PM&C application guest has been configured with "NetBackup" virtual disk.

   Execute *A.4 Configure PM&C Application Guest NetBackup Virtual Disk*.

2. **TVOE Management Server iLO:** Login with PM&C admusr credentials

   Login to iLo using application provided passwords via *L.1 How to Access a Server Console Remotely*

Login to iLO in IE using password provided by application:

```
http://<management_server_iLO_ip>
```

Click in the **Remote Console** tab and launch the Integrated Remote Console on the server.

Click **Yes** if the `Security Alert` pops up.

3. **TVOE Management Server iLO:** Login with PM&C admusr credentials

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **`sudo /usr/bin/virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**`ps -ef |grep virsh`**", then kill the existing process "**`kill -9 <PID>`**". Then execute the "virsh console X" command. Your console session should now run as expected.

   Login to PM&C console using virsh, and wait until you see the login prompt:

```
$ sudo /usr/bin/virsh
virsh # list
 Id    Name                           State
----------------------------------------------------
 4     pmacU17-1                      running

virsh # console pmacU17-1

[Output Removed]

pmacU17-1 login:
```

4. **PM&C:** Perform *A.5 Application NetBackup Client Install/Upgrade Procedures*.

   Note: The following data is required to perform the *A.5 Application NetBackup Client Install/Upgrade Procedures*:

   -
   - The PM&C application NetBackup user is "NetBackup". See appropriate documentation for the password.
   - The paths to the PM&C application software NetBackup notify scripts are:
     - `/usr/TKLC/smac/sbin/bpstart_notify`
     - `/usr/TKLC/smac/sbin/bpend_notify`
   - For the PM&C application the following is the NetBackup server policy files list:
     - `/var/TKLC/smac/image/repository/*.iso`
     - `/var/TKLC/smac/backup/backupPmac*.pef`

   After executing the *A.5 Application NetBackup Client Install/Upgrade Procedures*, the NetBackup installation and configuration on the PM&C application server is complete.

   Note: At the NetBackup Server the NetBackup policy(ies) can now be created to perform the NetBackup backups of the PM&C application.

4.5 HP C-7000 Enclosure Configuration

Note: This section will apply if the installation includes one or more HP C-7000 Enclosures. It will use the HP Onboard Administrator user interfaces (insight display, and OA GUI) to configure the enclosure settings.

4.5.1 Configure Initial OA IP

This procedure will set initial IP address for Onboard Administrator in location OA Bay 1 (left as viewed from rear) and Bay 2, using the front panel display.

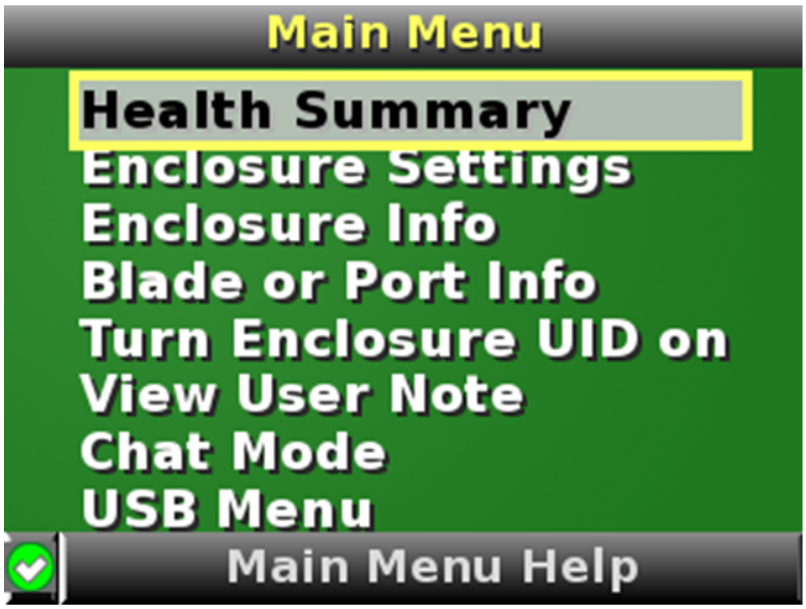
Note: The enclosure should be provisioned with two Onboard Administrators. This procedure needs to be executed only for OABay 1, regardless of the number of OA's installed in the enclosure.

Note: If a procedural *step* fails to execute successfully, *stop* and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. Configure OA's IP.

   Configure OA Bay1 IP address using insight display on the front side of the enclosure.

   You will see the following:



2. Navigate to **Enclosure Settings** and press **OK**.

Note: The OA1 IP and OA2 IP menu settings in this procedure may indicate "OA1 IPv4" or "OA1 IPv6". In either case, select this menu setting to set the OA IP address

3. Navigate to the **OA1 IP menu setting** and press **OK**.
4. If setting the IPv4 address:
   a) Navigate to the **OA1 IPv4** and press **OK**.
   b) On the **OA1 Network Mode** screen, choose **static** and press **OK**.
   c) Select **Accept** and press **OK**.
   d) On the **Change:OA1 IP address** screen, fill in data below and press **OK**.
      1. **IP**
      2. **MASK**
      3. **gateway**
   e) Select **Accept** and press **OK**.
   f) Navigate to **OA2 IP menu setting**on the Insight display and repeat the above steps to assign the IP parameters of OA2.
5. If setting the IPv6 address:
   a) Navigate to the **OA1 IPv6**and press **OK**.
   b) On the **Change: OA1 IPv6 Status** menu, select the **Enabled** option and press **OK**.
   c) Select **Accept** and press **OK**.
   d) On the **Change:OA1 IPv6 Settings** screen, fill in appropriate data below and press **OK**.
      1. Set the **Static IPv6** address to the globally scoped address and prefix, and press **OK**.
      2. Leave the DHCPv6 option as **Disabled**.
      3. Leave the SLAAC option as **Disabled**.
      4. If a static Gateway address is to be configured, navigate to **Static Gateway** and press **OK**.
         a. Select the Static Gateway IPv6 Address and press **OK**.
         b. Select **Set** and press **OK**.
      5. Navigate to **OA2 IP menu setting** on the Insight display and repeat the above steps to assign the IP parameters of OA2.
      6. Select **Accept All** and press **OK**.

      The **Main Menu** is displayed.

4.5.2 Configure Initial OA Settings Using the Configuration Wizard

This procedure will configure initial OA settings using a configuration wizard. This procedure should be used for initial configuration only and should be executed when the Onboard Administrator in OA Bay 1 (left as viewed from rear) is installed and active.

Note: The enclosure should be provisioned with two Onboard Administrators. Note that the OA in Bay 2 will automatically acquire its configuration from the OA in Bay 1 after the configuration is complete.

Note: This procedure should be used for initial configuration only. Follow *N.1 Determining Which Onboard Administrator Is Active* to learn how to correctly replace one of the Onboard Administrators.

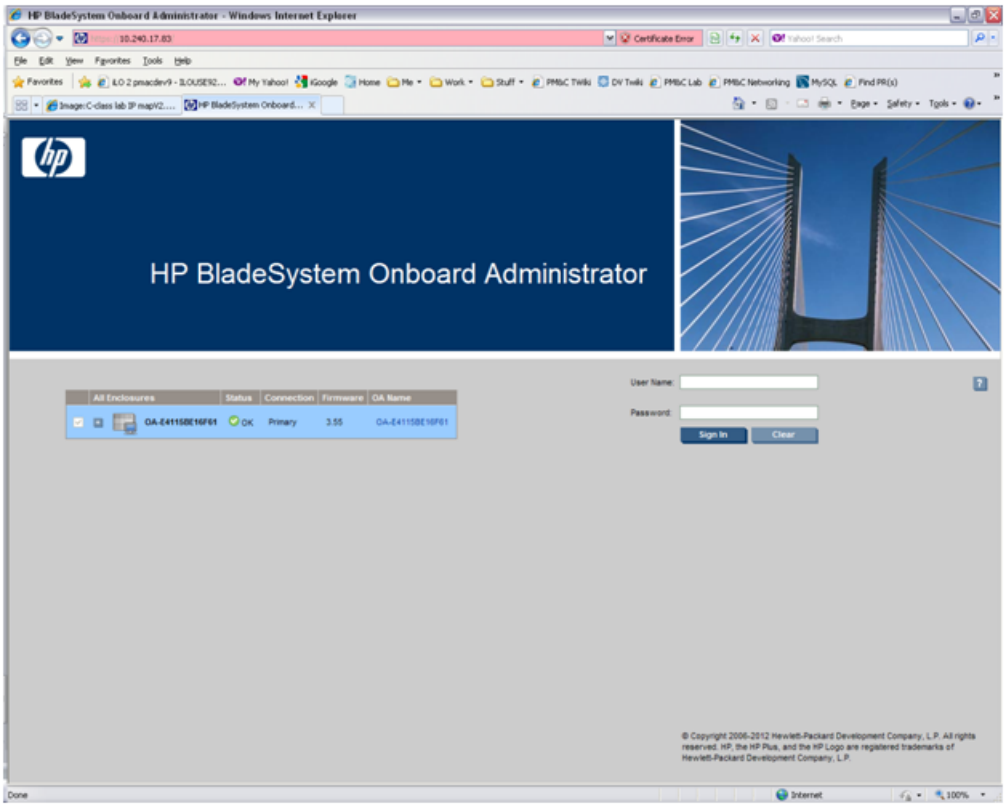
Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **OAGUI:** Login

   Open your web browser and navigate to the OA Bay1 IP address assigned in *4.5.1 Configure Initial OA IP*.

   ```
   http://<OA1_ip>
   ```

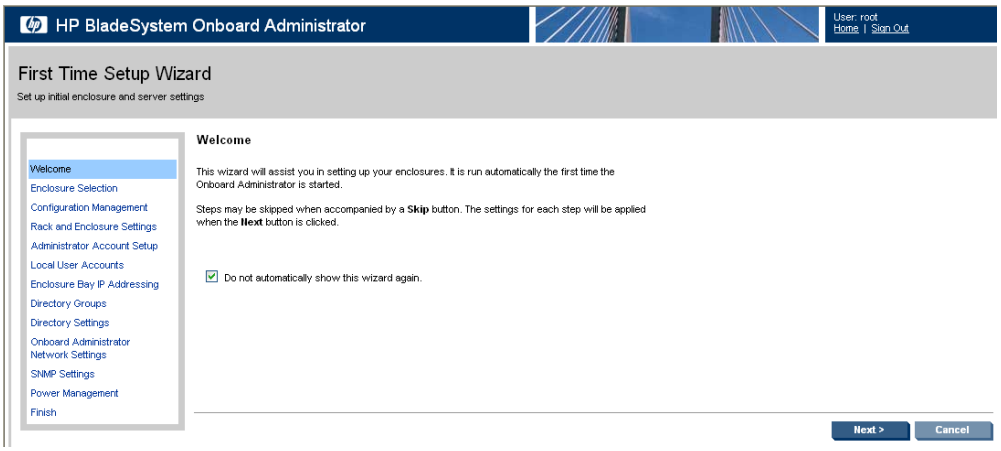
   You will see following:

   Login as an administrative user. Original password is on paper card attached to each OA.

2. **OAGUI:** Run First Time Setup wizard

You will see the main wizard window:



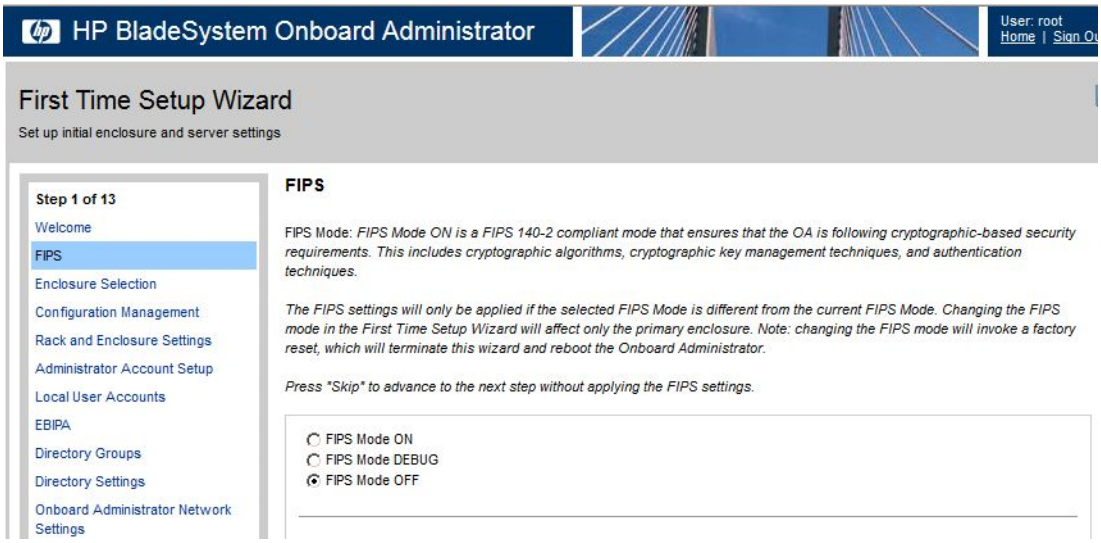
Note: If needed, navigate to **Wizards > First Time Setup** to get to the screen above.

Click on **`Next`** to choose the enclosure you want to configure.

You will see **Rack and Enclosure Settings**:

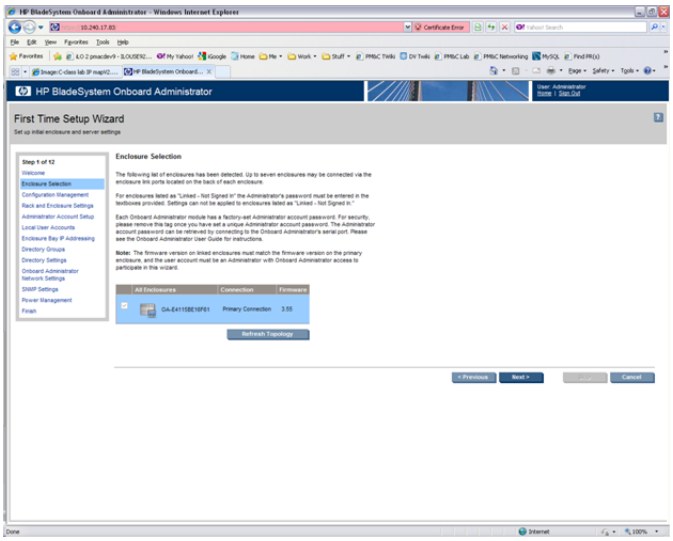
3. **OAGUI:** FIPS

   Click on **Next**. FIPS mode is not currently supported.



4. **OAGUI:** Select enclosure

   Choose enclosure:



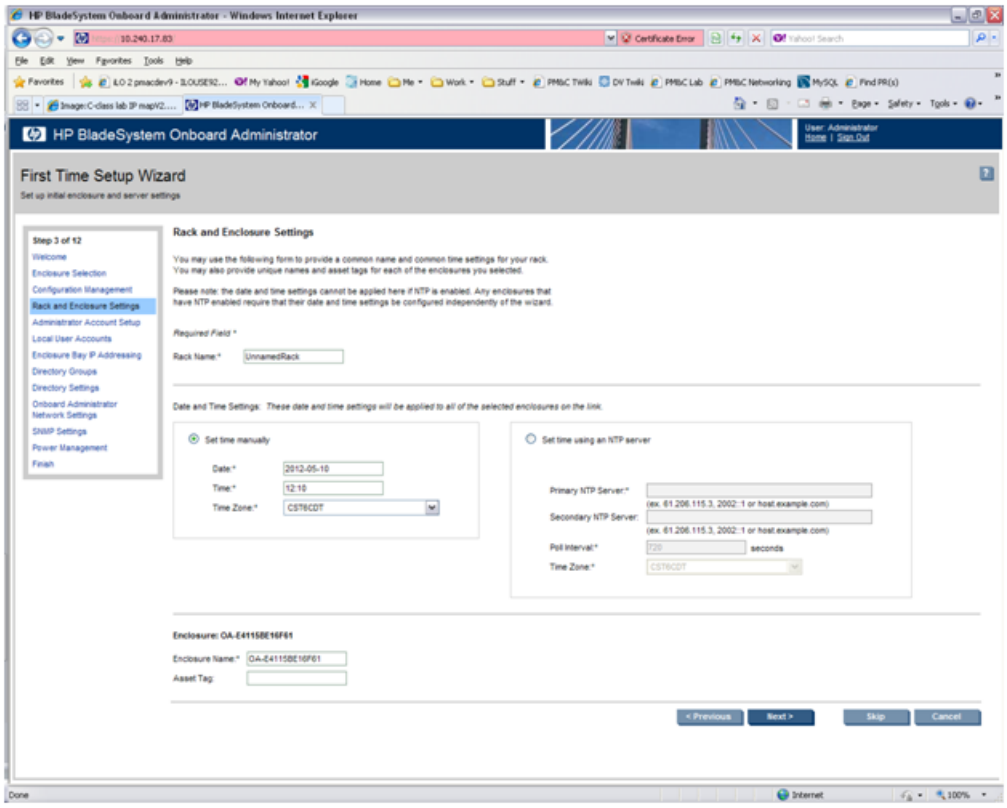
   Click on **Next**.

5. **OAGUI:** Skip Configuration Management

   You will see **`Configuration Management.`** Skip this step. Click **Next**.

6. **OAGUI:** Rack and Enclosure Settings

   You should see this screen:



Fill in **Rack Name** in format **`xxx_xx.`**

Fill in **Enclosure name** in format **`<rack name>_<position>`**

Example:

```
Rack Name: 500_03
Enclosure Name: 500_03_03
```

Note: Enclosure positions are numbered from 1 at the bottom of the rack to 4 at the top.

Check **Set time using an NTP server** item and fill in **Primary NTP server** (which is recommended to be set to the **<customer_supplied_ntp_server_address>**).

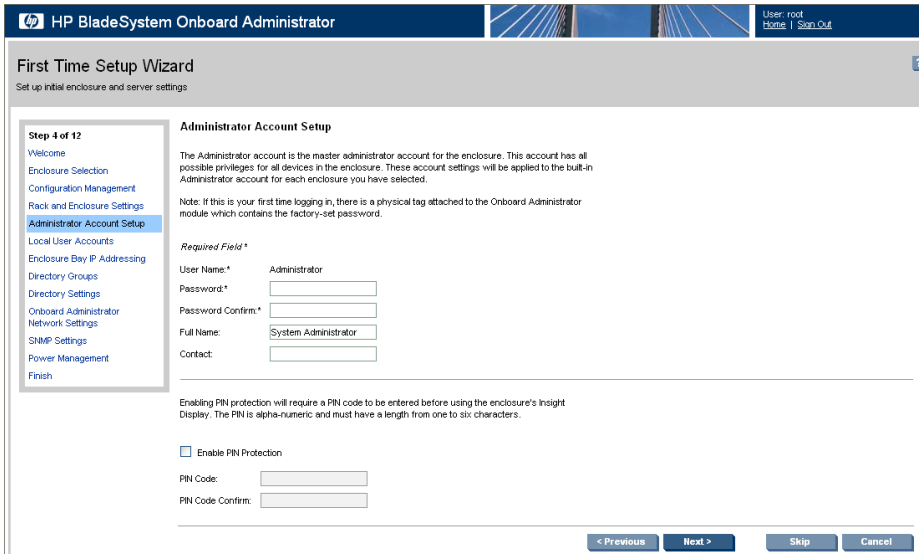
Set **Poll interval** to **720**.

Set **Time Zone** to UTC if customer does not have any specific requirements.

Click on **Next**.

7. **OAGUI:** Change administrator password

   You can see `Administrator Account Setup`:



Change Administrator's password (refer to application documentation) and click on **Next**.

8. **OAGUI:** Create pmacadmin and admusr user.

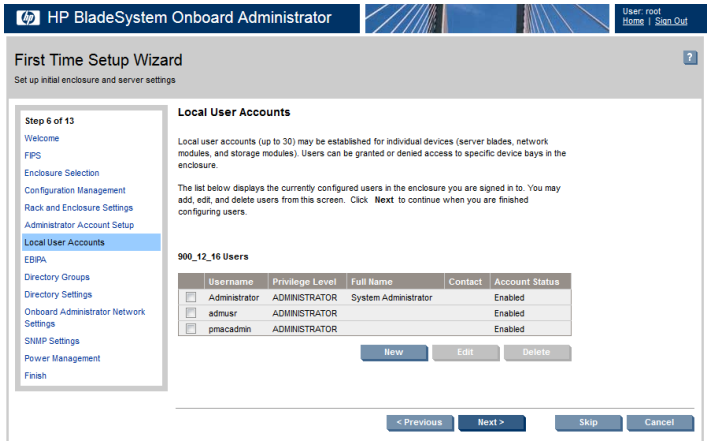
   On the **`Local User Accounts`** screen click on **New** to add **`pmacadmin`** user.

   You will see **`User Settings`** screen. Fill in **User Name** and **Password**. **Privilege Level** set to **Administrator**. Refer to the application documentation for the password.

   Verify that all of the blades have been checked before proceeding to check the checkbox for **Onboard Administrator Bays** under the `User Permissions` section.

   Then click on **Add User**.

   In the same way, create the **admusr** user.

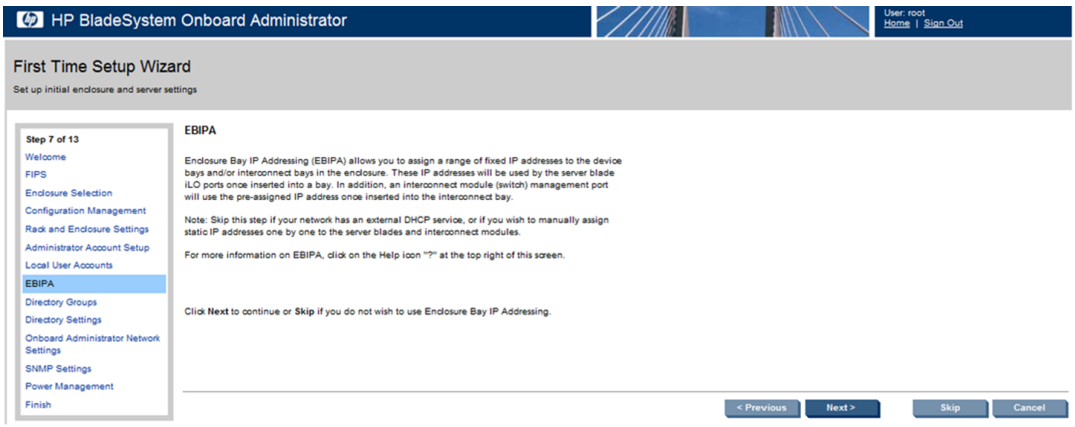


   Then click on **Next**.

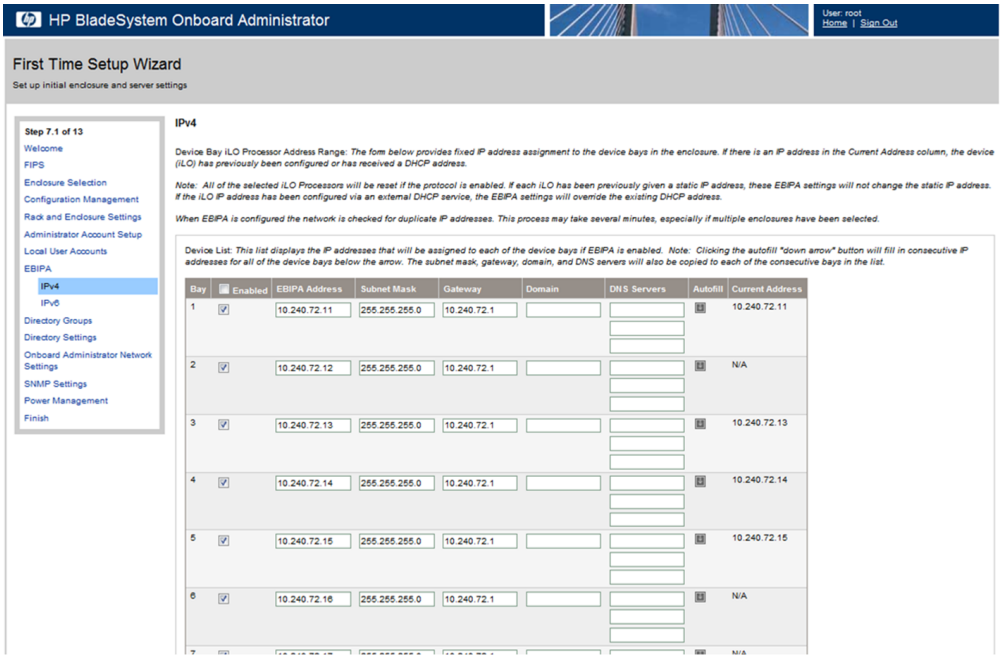
9. **OAGUI:** EBIPA

   a) On the **`EBIPA Settings`** (Enclosure Bay IP Addressing) screen, click on **Next** to continue or **Skip** if the EBIPA has been configured.

Note: Setting up the EBIPA addresses is required.



b) If configuring the OA with IPv4 addresses, select the First Time Setup Wizard **EBIPA: IPv4** and enter the appropriate data. Otherwise, if configuring the OA with IPv6 addresses, skip to the next step.



1. Go to the Device List section of the EBIPA Settings Screen (at the top).
2. Fill in the iLO IP, Subnet Mask, and Gateway fields for Device Bays 1-16.
3. Do not fill in the iLO IP, subnet Mask, or Gateway fields for Device Bays 1A-16A and 1B-16B.

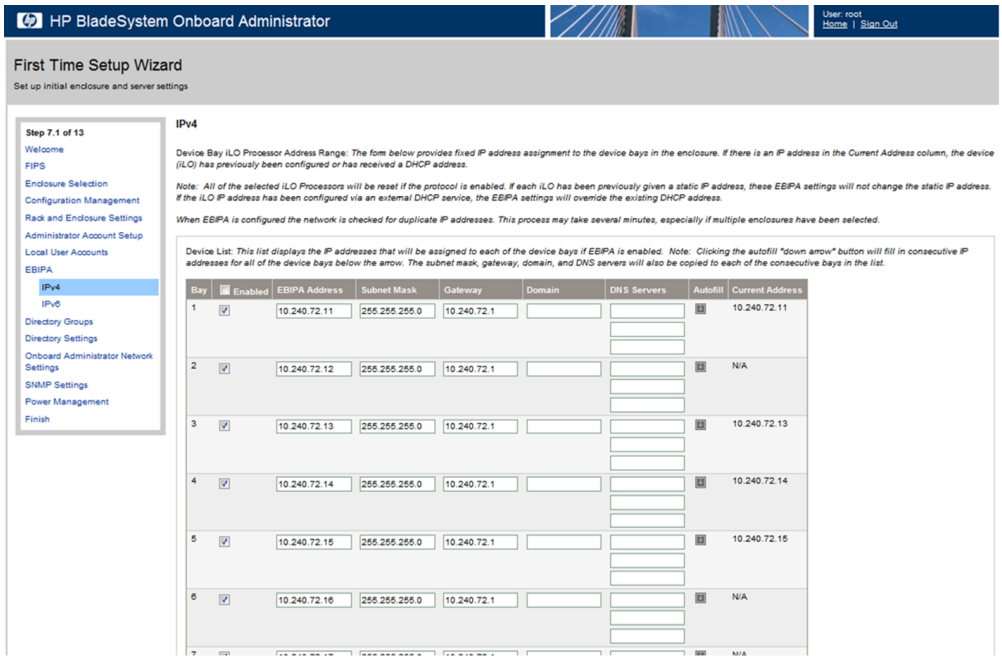
   Note: Bays 1A-16A and 1B-16B are used for double-density blades (i.e., BL2x220c) which are not supported in this release.

4. Click Enabled on each Device Bay 1 through 16 that is in use.

   Note: Any unused slots should have an ip address assigned, but should be disabled.

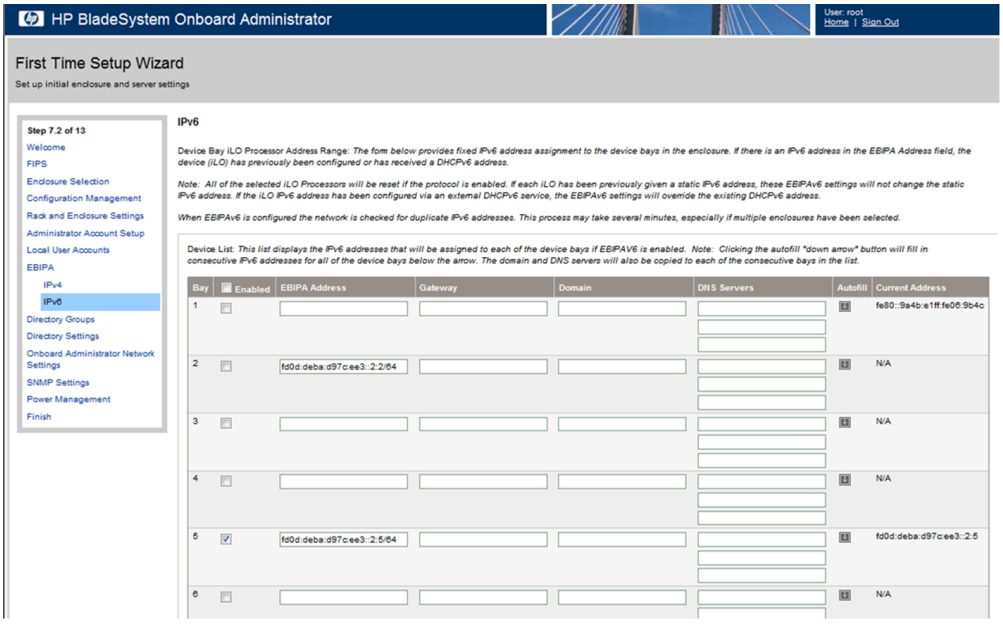
   Note: Do not use autofill as this will fill the entries for the Device Bays 1A through 16B.

5. Scroll down to the InterconnectList (below Device Bay 16B).



6. Fill in the EBIPA Address, Subnet Mask, and Gateway fields for each Interconnect Bay in use. Click Enable on each Interconnect Bay in use.
7. By clicking **Next**, you will apply those settings. System may restart devices such as interconnect devices or iLOs to apply new addresses. After finishing, check the IP addresses to ensure that apply was successful.

c) If configuring the OA with IPv6 addresses, select the First Time Setup Wizard **EBIPA: IPv6** and enter the appropriate data.



1. Go to the Device List section of the EBIPA Settings Screen (at the top).
2. Fill in the iLO IP/prefix and Gateway fields for Device Bays 1-16.
3. Do not fill in the iLO IP/prefix or Gateway fields for Device Bays 1A-16A and 1B-16B.

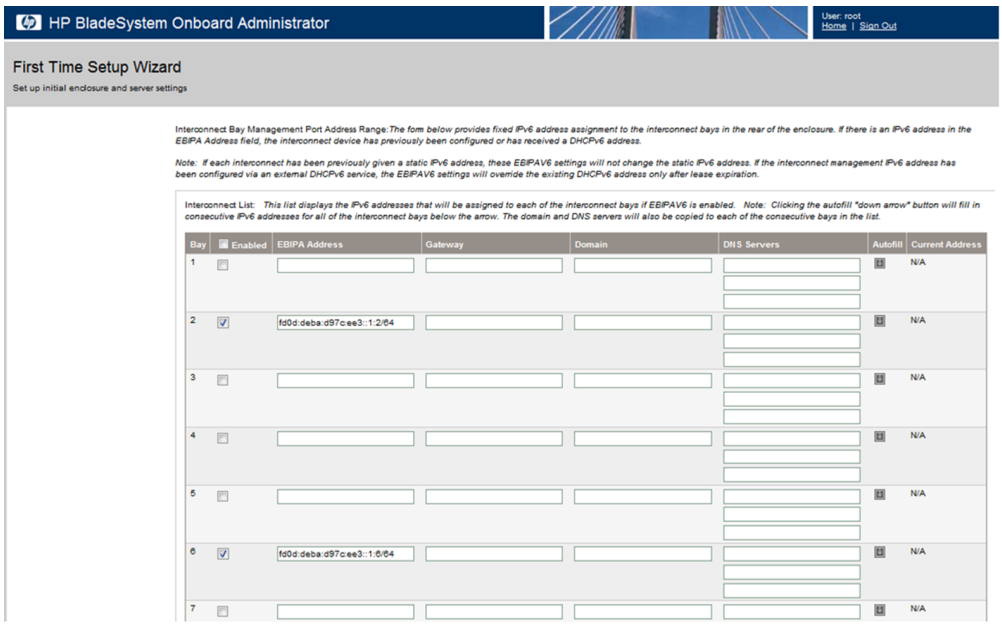
   Note: Bays 1A-16A and 1B-16B are used for double-density blades (i.e. BL2x220c) which are not supported in this release.

4. Click Enabled on each Device Bay 1 through 16 that is in use.

   Note: Any unused slots should have an IP address assigned, but should be disabled.

   Note: Do not use autofill as this will fill the entries for the Device Bays 1A through 16B.

5. Scroll down to the Interconnect List (below Device Bay 16B).



6. Fill in the EBIPA Address/prefix and Gateway fields for each Interconnect Bay in use. Click Enable on each Interconnect Bay in use.
7. By clicking Next, you will apply those settings. The system may restart devices such as interconnect devices or iLOs to apply new addresses. After finishing, check the IP addresses to ensure that apply was successful.

10. **OAGUI:** Skip Directory Groups step

    To skip Directory Groups step, click **Next**.

11. **OAGUI:** Skip Directory Settings step

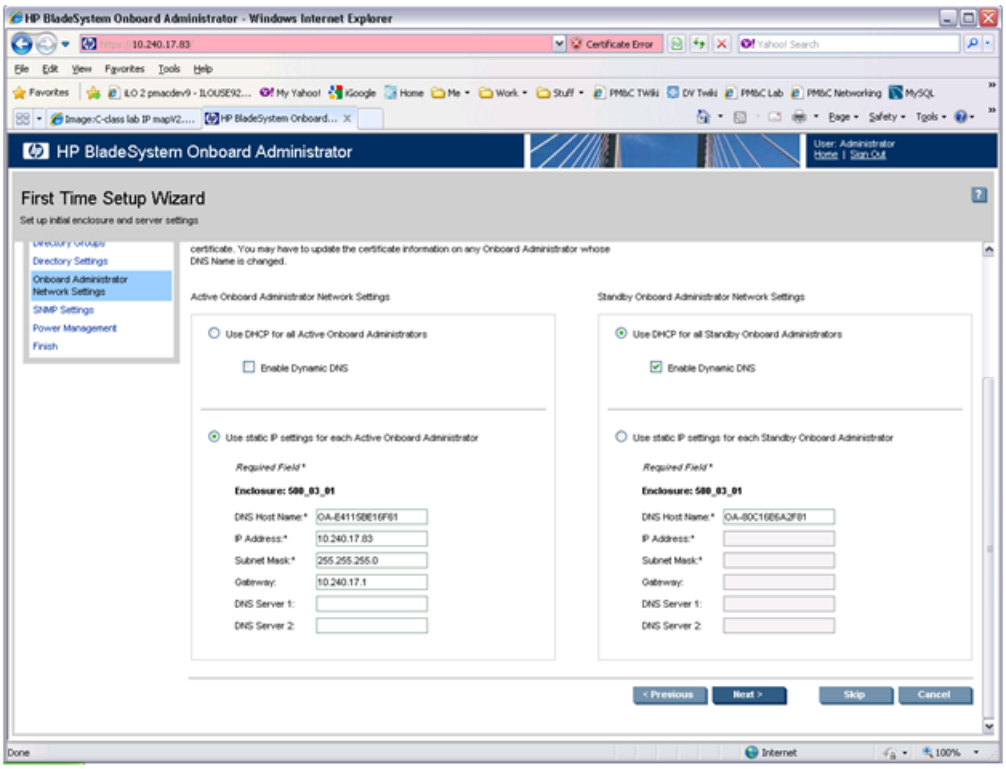
    To skip `Directory Settings` step, click **Next**.

12. **OAGUI:**OA network settings

    On the **`Onboard Administrator Network Settings`** tab you can assign or modify the IP address and the other network settings for the Onboard Administrator(s).

    The **`Active Administrator Network Settings`** pertain to the active OA (OA Bay 1 location during initial configuration). If the second Onboard Administrator is present, the **`Standby`**

`Onboard Administrator Network Settings` will be displayed as well. Click on "Use static IP settings for each Standby Onboard Administrator". Fill in the IP Address, Subnet mask and Gateway for the Standard OA.

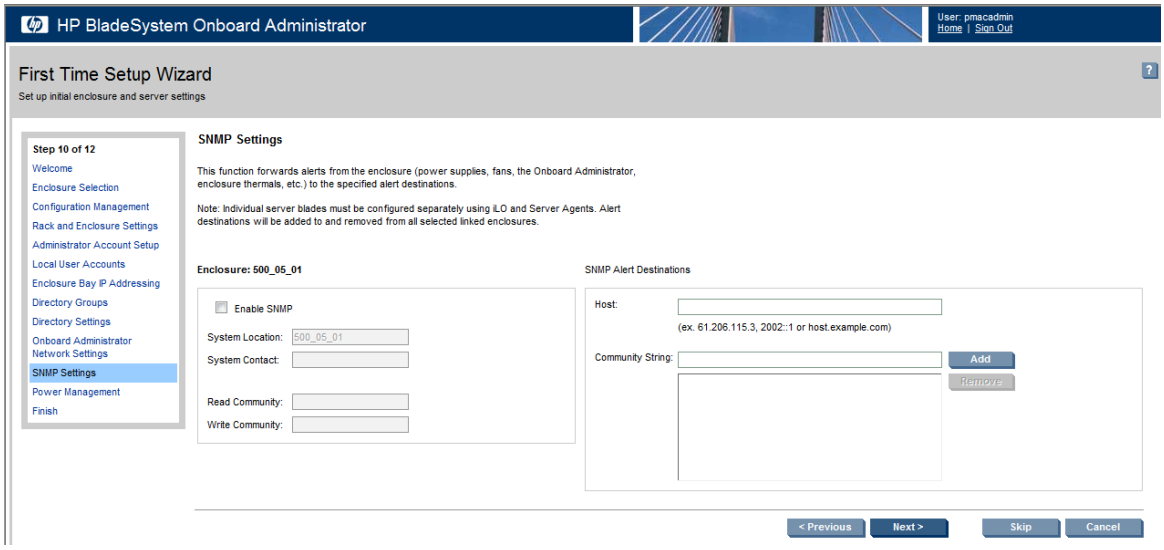


Click on **Next**.

Note: If you change the IP address of the active OA, you will be disconnected. Then, you must close your browser and sign in again using the new IP address.

13. **OAGUI:** SNMP Default Settings

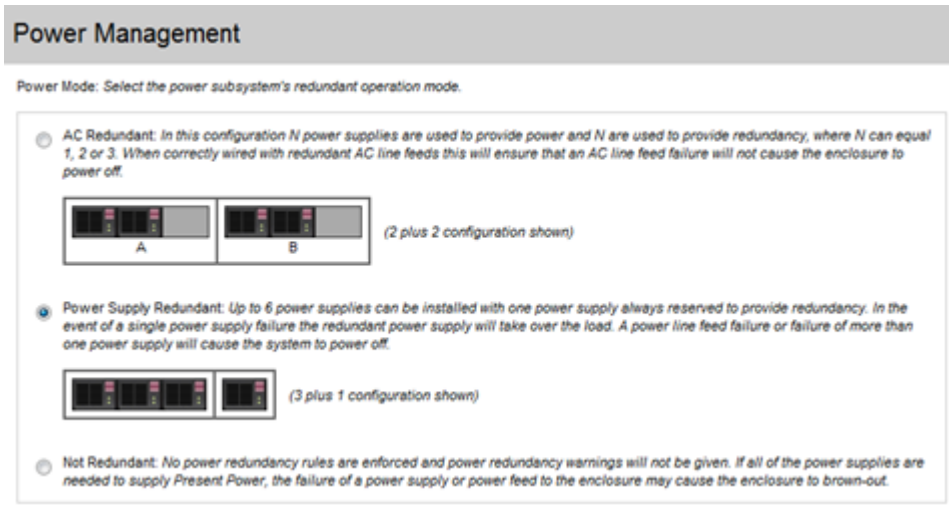
    By default, the **Enable SNMP** check box should be checked. If the customer does not want to have SNMP enabled, see Appendix , *Disabling SNMP on the OA*.



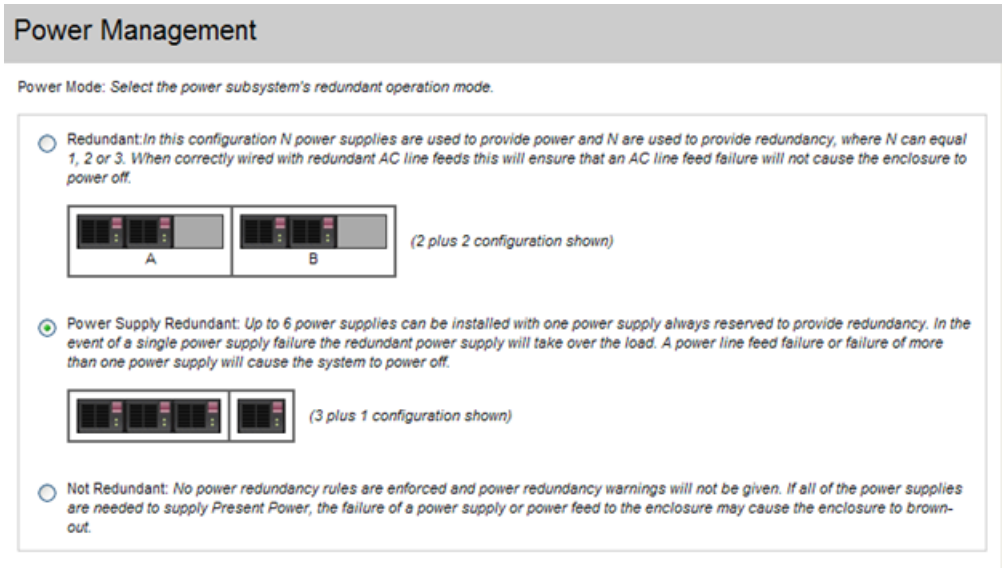
14. **OA GUI:** Power Management

    The Power Mode setting on the Power Management screen must be configured for power supply redundancy. The first available setting on the Power Management screen will be either "AC Redundant" or "Redundant", depending on whether the Enclosure is powered by AC or DC. In either case, select the **second** radio button, "Power Supply Redundant".

    AC-powered Enclosures:



    DC-powered Enclosures:



For all other settings on the Power Management screen, leave the default settings unchanged.

Click on **Next**.

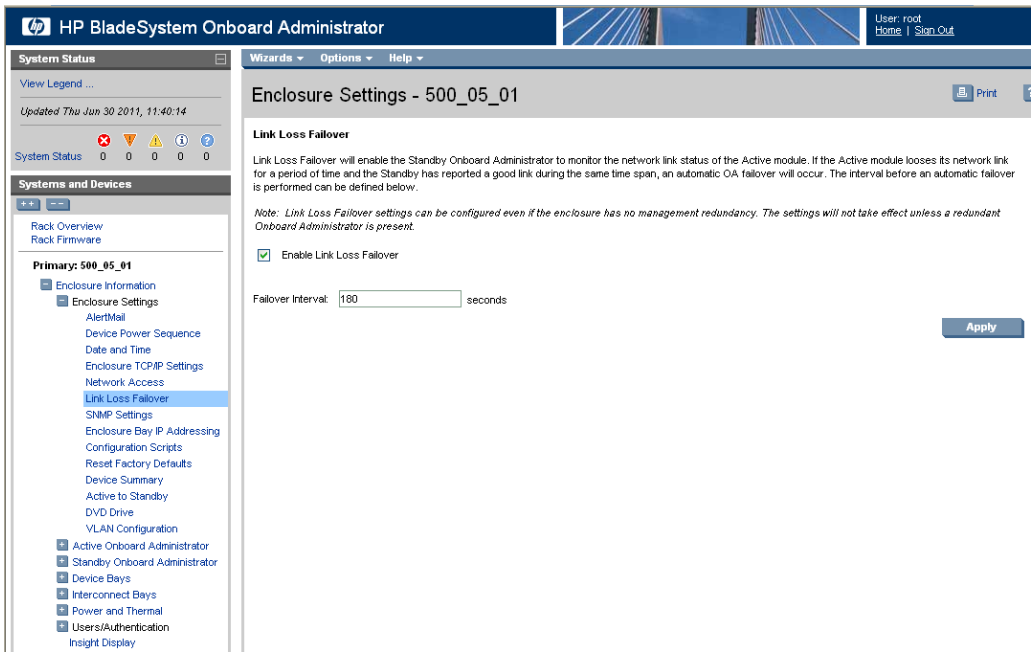
15. **OAGUI:** Finish First Time Setup Wizard

    Click on **Finish**.

    Note: If only one OA has been configured, skip the following step.

16. **OAGUI:** Set Link Loss Failover

    Navigate to **Enclosure Information > Enclosure Settings > Link Loss Failover**



Check the **`Enable Link Loss Failover`** and specify **`Failover Interval`** to be **`180`** seconds.

Click **Apply**.

4.5.3 Configure OA Security

This procedure will disable telnet access to OA.

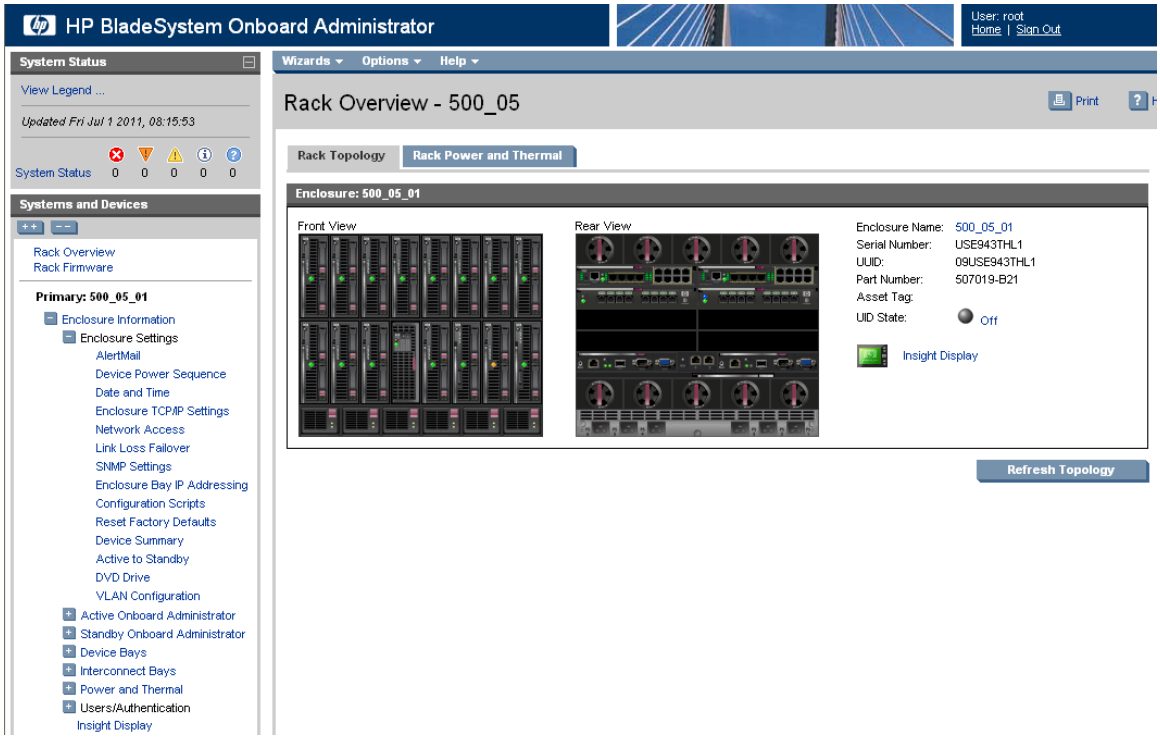
Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **Active OAGUI:** Login

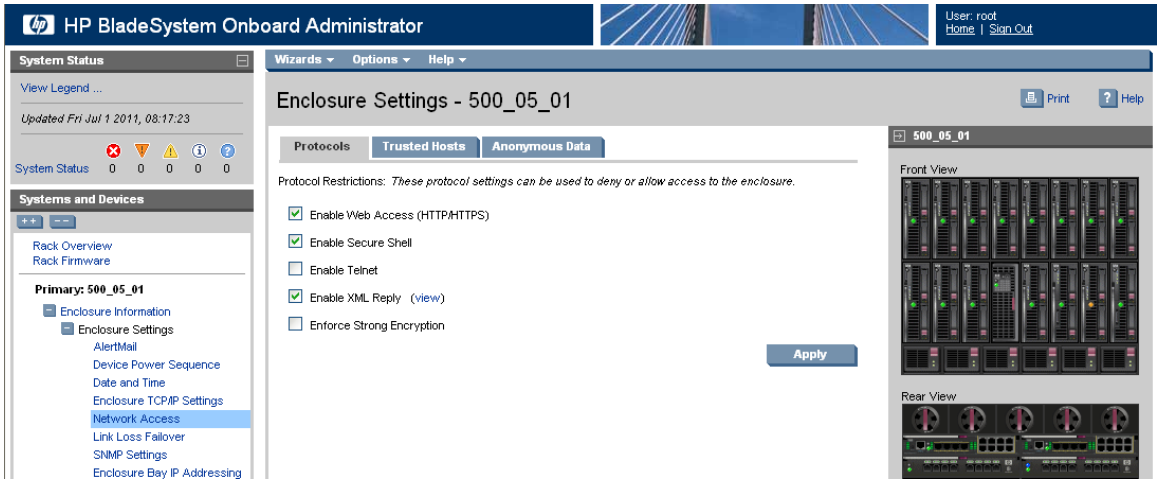
   Navigate to the IP address of the active OA, using *N.1 Determining Which Onboard Administrator Is Active*. Login as an administrative user.

2. **OAGUI:** Disable telnet

   Navigate to **Enclosure Information** > **Enclosure Settings** > **Network Access**.



Then uncheck the **`Enable Telnet`**.



Click on **Apply**.

4.5.4 Upgrade or Downgrade OA Firmware

Software Centric Customers: If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP."

This procedure will update the firmware on the OA's.

Needed material:

- HP MISC firmware ISO image
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]

Note: The enclosure should be provisioned with two Onboard Administrators. This procedure will install the same firmware version on both Onboard Administrators.

Note: This procedure should be used to upgrade or downgrade firmware or to ensure both OA's have the same firmware version. When the firmware update is initiated, the standby OA is automatically updated first.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. Execute section *4.9.2.1 Adding ISO Images to the PM&C Image Repository* to add the HP MISC firmware ISO image.
2. **OAGUI:** Login

   Navigate to the IP address of the active OA, using *N.1 Determining Which Onboard Administrator Is Active*. Log in as an administrative user.

3. **OA GUI:** Check OA firmware versions.

   In the left navigation area, navigate to **Enclosure Information** > **Active Onboard Administrator** > **Firmware Update**.

Examine the **`Firmware Version`** shown in the **`Firmware Information table`**. Verify the version meets the minimum requirement specified by the Release Notes of the *HP Solutions Firmware Upgrade Pack* [2] and that the firmware versions match for both OA's. If it is so the firmware does not need to be changed. Skip the rest of this procedure.

4. Save All OA Configuration

   If one of the two OAs has a later version of firmware than the version provided by the *HP Solutions Firmware Upgrade Pack* [2], this procedure will downgrade it to that version. A firmware downgrade can result in the loss of OA configuration. Before proceeding, ensure that you have a record of the initial OA configuration necessary to execute the following OA configuration procedures, as required by the customer and application:

   a) *4.5.1 Configure Initial OA IP*
   b) *4.5.2 Configure Initial OA Settings Using the Configuration Wizard*
   c) *4.5.3 Configure OA Security*
   d) *4.5.6 Store OA Configuration on Management Server*

5. **OA GUI:** Initiate OA firmware upgrade

   Note: Firmware obtained from a Software Centric Customer should be located at:

   ```
   https://<PM&C_Management_Network_IP>/TPD/<OA_firmware_version>
   ```

   If the firmware needs to be upgraded, click on **Firmware Update** in the left navigation area.

   Enter the appropriate URL in the bottom text box labeled "Image URL". The syntax is:

   ```
   https://<PM&C_Management_Network_IP>/TPD/<HPFW_mount_point>/files/<OA_firmware_version>.bin
   ```

   For example:

   ```
   https://10.240.4.198/TPD/HPFW--872-2488-XXX--HPFW/files/hpoa300.bin
   ```

   Check the **Force Downgrade** box if present.

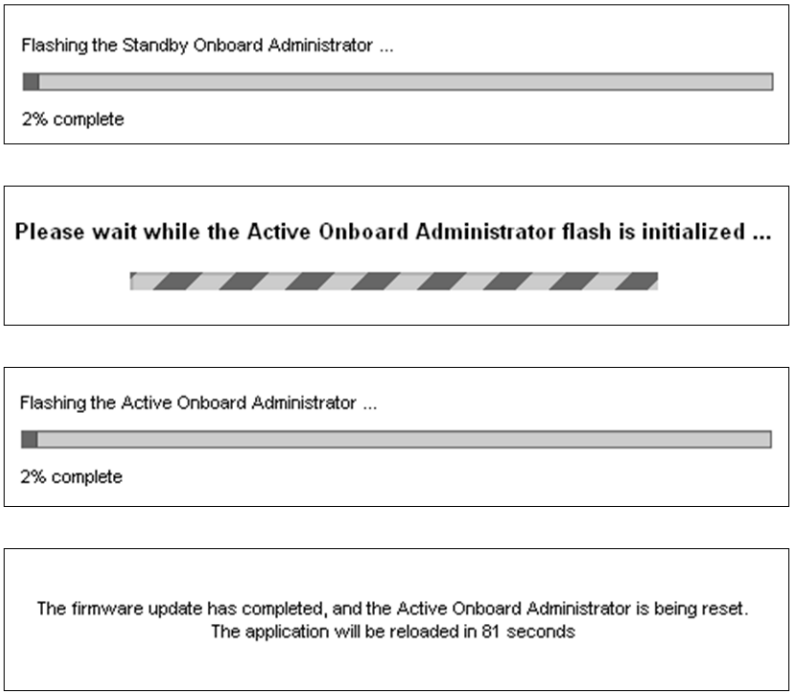
   Click **Apply**

   If a confirmation dialog is displayed, click "**OK**".

   Note: The upgrade may take up to 25 minutes.

6. **OA GUI:** Observe OAfirmware upgrade progress

   You should observe the following updates during the upgrade.



7. **OAGUI:** Reload the HP OA application

   The upgrade is complete when the following is displayed:

   Clear your browser's cache and click to reload the application . The login page should appear momentarily.

8. **OA GUI:** Verify the firmware upgrade

   Log into the OA again. It may take few minutes before the OA is fully functional and accepts the credentials.

   In the left navigation area, navigate to **Enclosure Information** > **Active Onboard Administrator** > **Firmware Update**

   Examine the **`Firmware Version`** shown in the **`Firmware Information table`**. Verify the firmware version information is correct.

9. **OA GUI:** Check/re-establish OA configuration

   Ensure that all OA configuration established by the following procedures is still intact after the firmware update. Re-establish any settings by performing the procedure(s):

   a) *4.5.1 Configure Initial OA IP*
   b) *4.5.2 Configure Initial OA Settings Using the Configuration Wizard*
   c) *4.5.3 Configure OA Security*

d) *4.5.6 Store OA Configuration on Management Server*

4.5.5 Add SNMP Trap Destination on OA

An SNMP trap destination must be added and configured using the Onboard Administrator (OA), or the SNMP must be disabled. One of these actions must be completed as described in this procedure.

1. Either add an SNMP trap destination as follows, or proceed to Step 2 to disable the SNMP.
   a) **Active OA GUI:** Login

      Navigate to the IP address of the active OA. Use *N.1 Determining Which Onboard Administrator Is Active* to determine the active OA. Log in as an administrative user.

   b) **OA GUI:** Navigate to SNMP Settings page

      Navigate to **Enclosure Information** > **Enclosure Settings** > **SNMP Settings**.

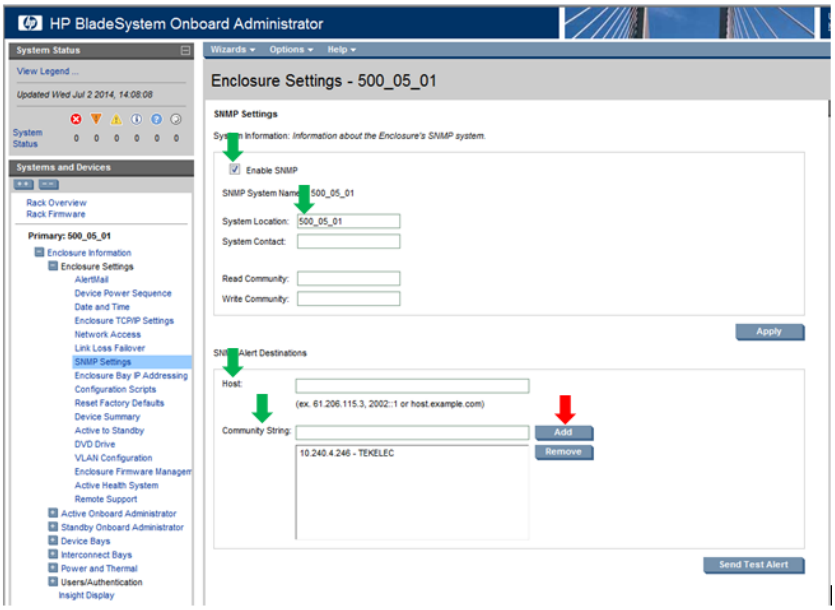
   c) **OA GUI:** Add SNMP trap destination

      If SNMP is not already enabled, check the **Enable SNMP** checkbox and type the **Enclosure name** (shown in the title bar) into the **System Location** box.

      Do not set **Read Community** and **Write Community**.

      For each trap destination, type the host destination information into the **Host** box. Additionally, type the community string into the **Community String** box. Finally, click the **Add** button to the trap destination to the configuration.

      Note: Refer to *3.3 SNMP Configuration*.



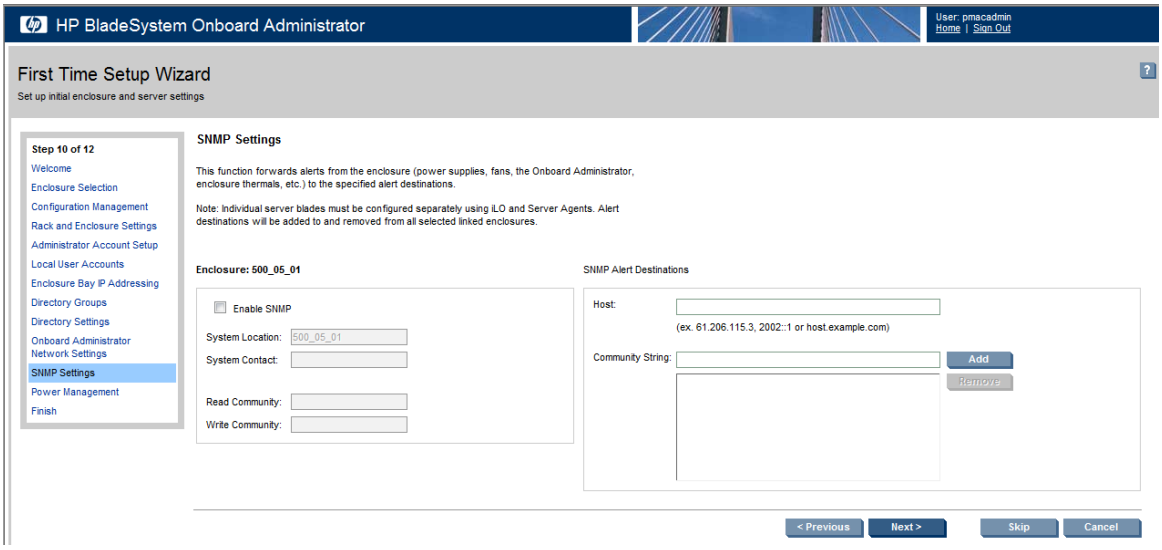
The SNMP trap destination has now been added to the configuration and should show up in the list of configured destinations. Once you are done adding your trap destinations, click **Apply** to activate the configuration. The following progress meter may appear.

When the progress meter disappears, the configuration has been applied.

2. To disable the SNMP, follow these steps:
   a) **If necessary, log in to the Active OA.**
   b) **Navigate to the SNMP Settings.**

      Use either the **First Time Setup Wizard SNMP Settings** menu item or the **Enclosure Information** > **Enclosure Settings** > **SNMP Settings** menu item.

   c) **Uncheck the Enable SNMP checkbox.**



4.5.6 Store OA Configuration on Management Server

This procedure will backup OA settings on the management server.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

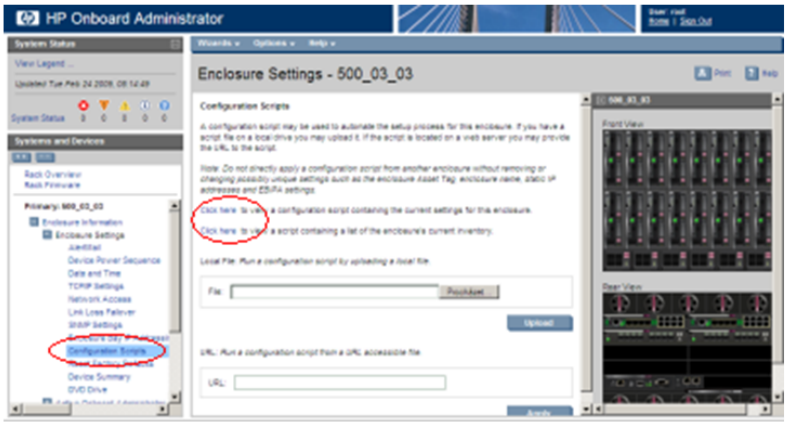
1. **OAGUI:** Login

   Navigate to the IP address of the active OA, using *N.1 Determining Which Onboard Administrator Is Active*. Login as root.

2. **OAGUI:** Store configuration file

   Navigate to the **Enclosure Information** > **Enclosure Settings** > **Configuration scripts**

   On the **`Configuration script`**, open the first configuration file (current settings for enclosure):



   Store this file on local disk.

   For example:

Click **Show Config**.

Copy all the text on the page and save in a text file. Or select **File** > **Save As**, choose a file name and path, and choose **Text file** for the type.

For example, you may choose the following syntax for the configuration file name:

<enclosure ID>_<timetag>.conf

3. **PM&C:** Backup configuration file

   Do the following to backup the file on the PM&C:

   Under directory **/usr/TKLC/smac/etc** you can create your own subdirectory structure. Login to management server via ssh as admusr and create the target directory:

```
$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/OA_backups/OABackup
```

   Change the directory permissions:

```
$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/OA_backups/OABackup
```

   Next, copy the configuration file to the created directory.

   For UNIX users:

```
# scp ./<cabinet_enclosure_backup file>.conf \
admusr@<pmac_management_network_ip>:/home/admusr
```

   Windows users: Refer to *D.1 Using WinSCP* to copy the file to the management server.

   Now, on the PM&C, move the configuration file to the OA Backup folder that you created under /usr/TKLC/smac/etc:

```
$ sudo /bin/mv /var/TKLC/home/admusr/<cabinet_enclosure_backup file>.conf
/usr/TKLC/smac/etc/OA_backups/OABackup
```

4. **PM&C:** Perform PM&C application backup to capture the OA backup

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

   Note: The backup runs as a background task. To check that status of the background task use the PM&C GUI Task Monitor page, or issue the command "$ **sudo /usr/TKLC/smac/bin/pmaccli getBgTasks**". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

   Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

5. **PM&C:** Verify the Backup was successful

   Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C Backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
 2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

6. **PM&C**: Save the PM&C backup

   If the NetBackup feature has not been configured for this PM&C, or the Redundant PM&C is not configured in this system, the PM&C backup must be moved to a remote server. Transfer, (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server. The PM&C backup files are saved in the following directory: "/var/TKLC/smac/backup".

7. **OAGUI:** Log out

   Log out from the OA by pressing **Sign Out** at the top-right corner.

4.6 Enclosure and Blades Setup

4.6.1 Add Cabinet and Enclosure to the PM&C System Inventory

This procedure provides the instructions for adding a cabinet and an enclosure to the PM&C system inventory.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. **PM&C GUI:** Login

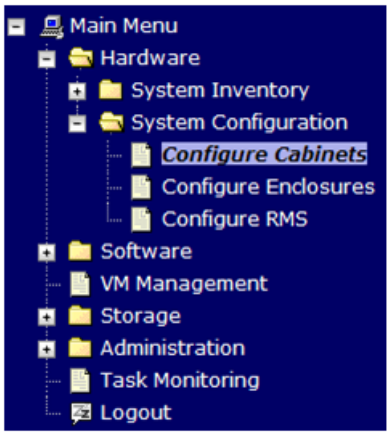
   Open your web browser and enter:

   ```
   https://<pmac_management_network_ip>
   ```

   Login as the pmacadmin user.

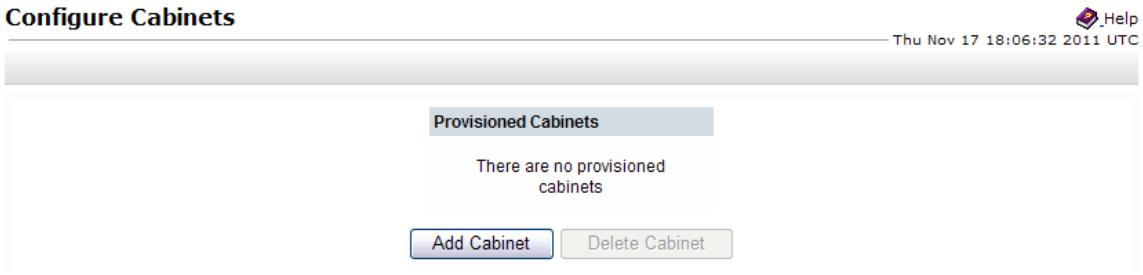
2. **PM&C GUI:** Navigate to Configure Cabinets

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Cabinets**.



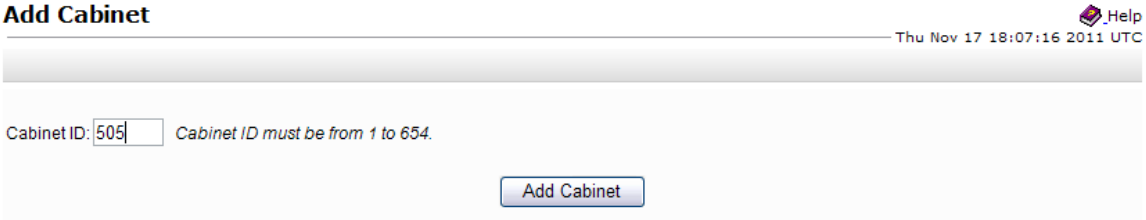
3. **PM&C GUI:** Add Cabinet

   On the **`Configure Cabinets`** panel, press the **Add Cabinet** button



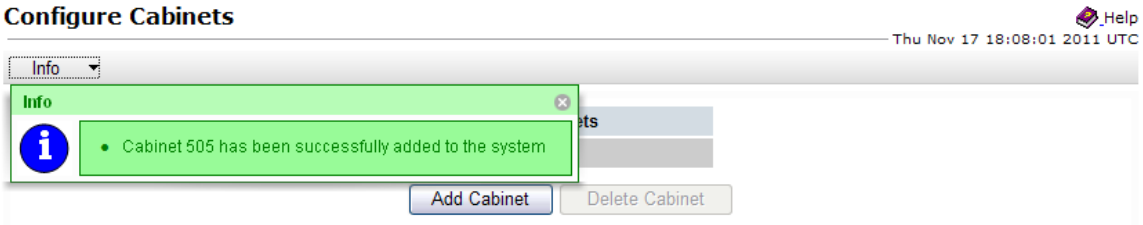
4. **PM&C GUI:** Enter Cabinet ID

   Enter the **`CabinetID`** and press the **Add Cabinet** button.

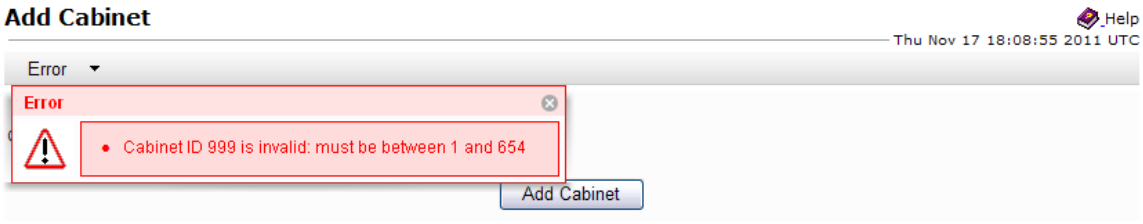


5. **PM&C GUI:** Check errors

   If no error is reported to the user you will see the following:

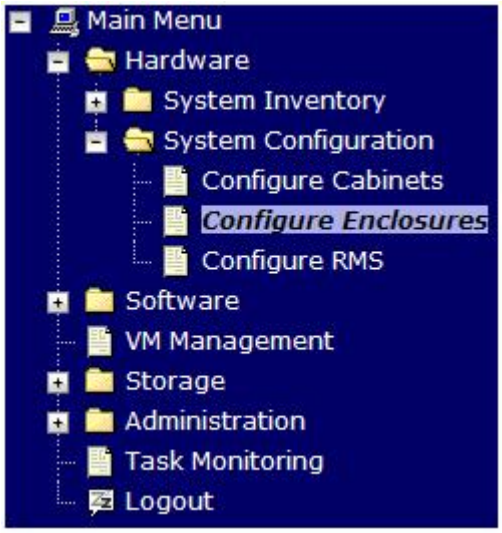


   Or you will see an error message:



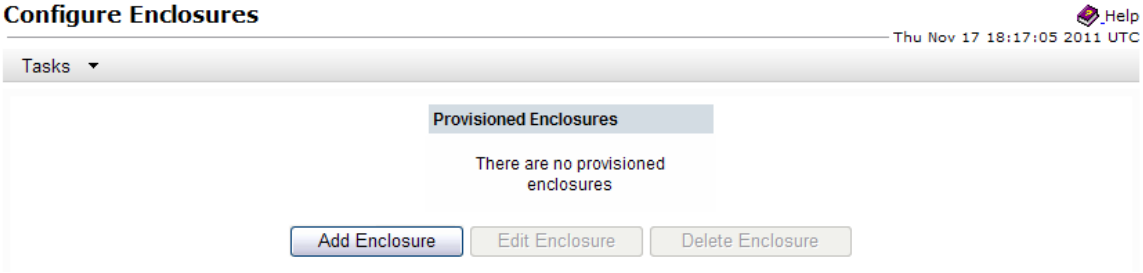
6. **PM&C GUI:** Navigate to Configure Enclosures

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Enclosures**.



7. **PM&C GUI:** Add Enclosure

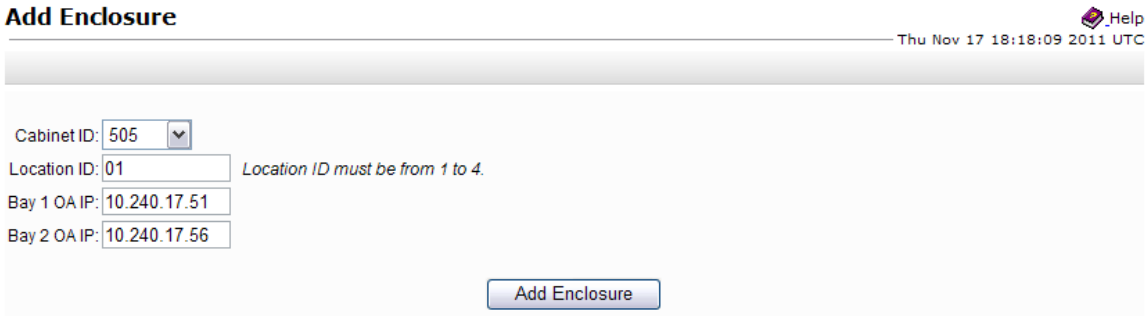
   On the **`Configure Enclosures`** panel, press the **Add Enclosure** button



8. **PM&C GUI:** Provide Enclosure Details

   On the **`Add Enclosure`** panel, enter the **`Cabinet ID`**, **`Location ID`**, and two **`OA IP`** addresses (the enclosure's active and standby OA).

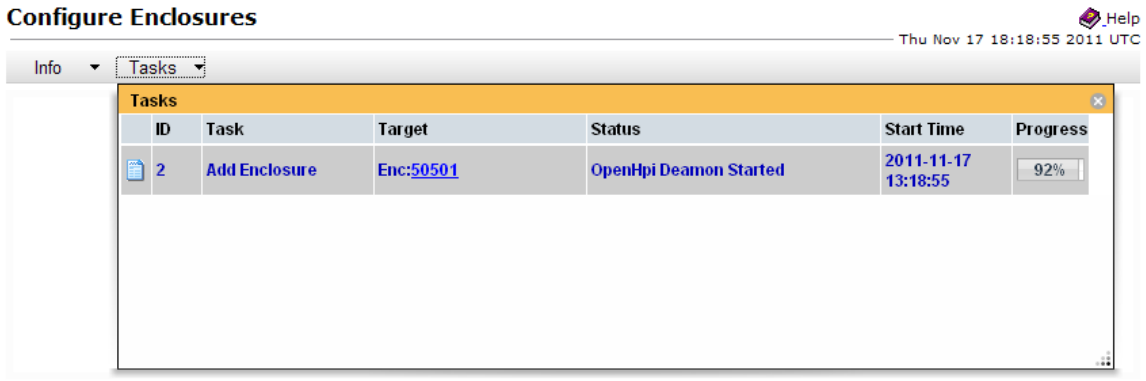
   Then click on **Add Enclosure**.



Note: Location ID is used to uniquely identify an enclosure within a cabinet. It can have a value of 1, 2, 3, or 4. The cabinet ID and location ID will be combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 502 at location 1, will have an enclosure ID of 50201).

9. **PM&C GUI:** Monitor Add Enclosure

   The Configure Enclosures page is then redisplayed with a new background task entry in the Tasks table. This table can be accessed by pressing the**Tasks** button located on the toolbar under the Configure Enclosures heading.



   When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

10. **PM&C:** Perform PM&C application backup.

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

    Note: The backup runs as a background task. To check the status of the background task use the PM&C GUI Task Monitor page, or issue the command "pmaccli getBgTasks". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

    Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

11. **PM&C:** Verify the Backup was successful

Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contactMy Oracle Supportby referring to the*1.4 My Oracle Support (MOS)*of this document.

The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

12. **PM&C:** Save the PM&C backup

    The PM&C backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server. The PM&C backup files are saved in the following directory: "/var/TKLC/smac/backup".

4.6.2 Configure Blade Server iLO Password for Administrator Account

This procedure will change the blade server iLO password for Administrator account for blade Servers in an enclosure.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **PM&C:** Log into the PM&C as admusr using ssh.
2. **PM&C:** Create xml file

   In **`/usr/TKLC/smac/html/public-configs`** create an xml file with information similar to the following example. Change the Administrator password field to a user-defined value.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admusr" PASSWORD="password">
<USER_INFO MODE="write">
<MOD_USER USER_LOGIN="Administrator">
<PASSWORD value="<new Administrator password>"/>
</MOD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

   Save this file as **`change_ilo_admin_passwd.xml`**

   Change the permission of the file

```
$ sudo chmod 644 change_ilo_admin_passwd.xml
```

3. **OA shell:** Login to the active OA

   Log into OA via ssh as root user.

```
login as: root

----------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
----------------------------------------------------------

Firmware Version: 3.00
Built: 03/19/2010 @ 14:13 OA
  Bay
 Number:  1 OA
 Role:       Active
admusr@10.240.17.51's password:
```

   If the **`OA Role`** is not **`Active,`** login into the other OA the enclosure system

4. **OA shell:** Run hponcfg

   Run the following command:

```
> hponcfg all https://<pmac_ip>/public-configs/change_ilo_admin_passwd.xml
```

5. **OA shell:** Check the output

   Observe the output for error messages and refer to the **`HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide`** for troubleshooting

6. **OA shell:** Logout

   Logout from the OA

7. **PM&C:** Remove temporary file

   On the PM&C remove the configuration file you created. This is done for security reasons, so that no one can reuse the file:

```
$ sudo /bin/rm –rf /usr/TKLC/smac/html/public-configs/change_ilo_admin_passwd.xml
```

4.7 Configure Enclosure Switches

If the enclosure switches used are Cisco 3020, execute procedure *4.7.1.1 Configure Cisco 3020 Switch (netConfig)*.

If the switches used are HP 6120XG, execute procedure *4.7.2.1 Configure HP 6120XG Switch (netConfig)*.

If the enclosure switches used are HP6125G, execute procedure *4.7.3.1 Configure HP 6125G Switch (netConfig)*.

If the enclosure switches used are HP6125XLG, execute procedure *4.7.4.1 Configure HP 6125XLG Switch (netConfig)*.

4.7.1 Configure Cisco 3020 Switches

4.7.1.1 Configure Cisco 3020 Switch (netConfig)

This procedure will configure 3020 switches from the PM&C server using templates included with an application.

If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using *4.3.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)*. If the aggregation switches are provided by the customer, the user must ensure that the customer aggregation switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact My Oracle Support and ask for assistance.

This procedure requires that no IPM activity is occurring or will occur during the execution of this procedure.

Note: The Cisco 3020 is not compatible with the IPv6 management configuration.

Needed materials:

- HP MISC firmware ISO image
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]
- Application specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application media.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **Virtual PM&C:** Prepare for switch configuration

   Login as admusr to the PM&C, then run:

   ```
   $ /bin/ping -w3 <mgmtVLAN_gateway_address>
   ```

2. **Virtual PM&C:** Verify network connectivity to 3020 switches

   For each 3020 switch, verify network reachability.

   ```
   $ /bin/ping -w3 <enclosure_switch_IP>
   ```

3. **Virtual PM&C**: Modify PM&C Feature to allow TFTP.

   Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:

   ```
   $ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
    --enable=1
   $ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
   ```

   Note: This may take up to 60 seconds to complete.

4. **Virtual PM&C:** Verify the template xml files are in existence.

   Verify that the initialization xml template file and configuration xml template file are present on the system and are the correct version for the system.

Note: The XML files prepared in advance with the NAPD can be used as an alternative.

```
$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_init.xml
$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_configure.xml
```

If either file does not exist, copy the files from the application media into the directory shown above.

If 3020_init.xml file exists, page through the contents to verify it is devoid of any site specific configuration information other than the device name. If the template file is appropriate, then skip the remainder of this step and continue with the next step.

If 3020_configure.xml file exists, page through the contents to verify it is the appropriate file for the this site and edited for this site. All network information is necessary for this activity. If the template file is appropriate, then skip the remainder of this step and continue with the next step.

5. **Virtual PM&C:** Modify 3020 xml files for information needed to configure the switch.

   Update the 3020_init.xml file for the values noted in the next sentence. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$some_variable_name** will need to be modified, removing the dollar sign and the less than, greater than sign. When done editing the file, save and quit.

   Update the 3020_configure.xml file for the values noted in the next sentence. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$some_variable_name** will need to be modified, removing the dollar sign and the less than, greater than sign. When done editing the file, save and quit.

   ```
   $ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_init.xml
   ```

   ```
   $ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_config.xml
   ```

6. **Virtual PM&C/OA GUI:** Reset switch to factory defaults

   Note: Do not wait for the switch to finish reloading before proceeding to the next step. After completing Step 6 by initiating the reload, proceed to *Step 7*.

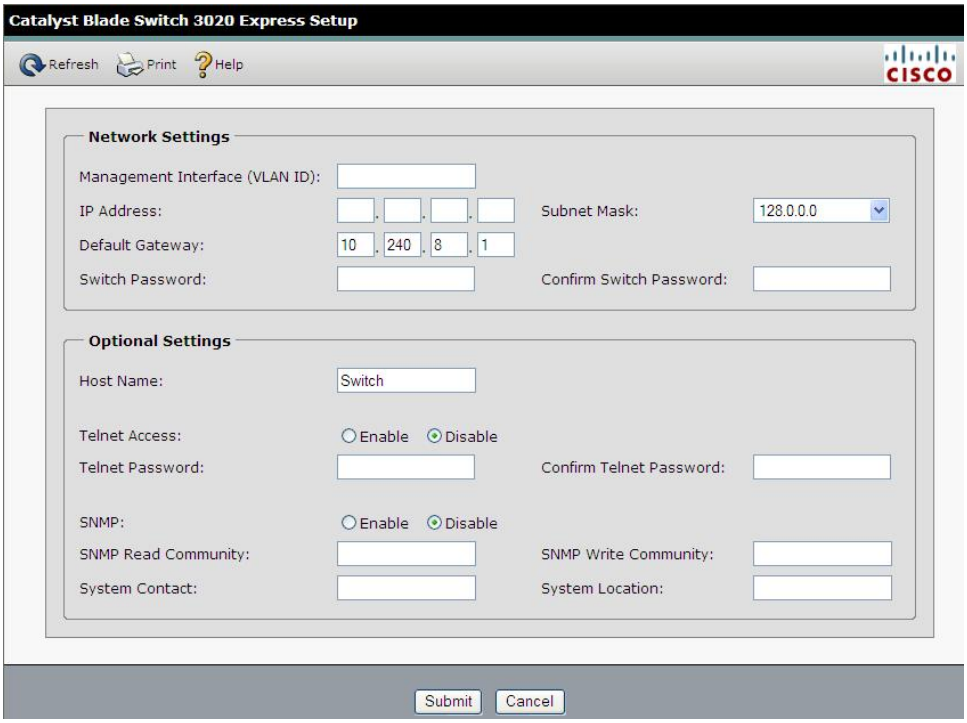
   If the switch has been previously configured using netConfig or previous attempts at initialization have failed, use netConfig to reset the switch to factory defaults by executing the following command:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> setFactoryDefault
   ```

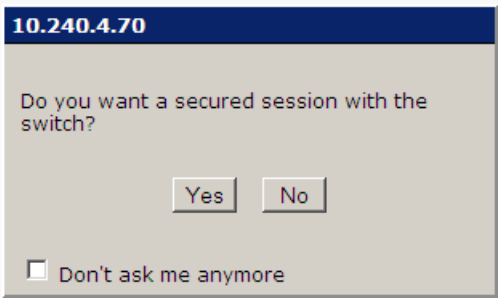
   If the above command failed, use Internet Explorer to navigate to <enclosure_switch_ip_address>.

   A new page will be opened. If you are asked for a username and password, leave the username blank and use the appropriate password provided by the application documentation. Then click **OK**.

   If you are prompted with the "Express Setup" screen, click **Refresh**.

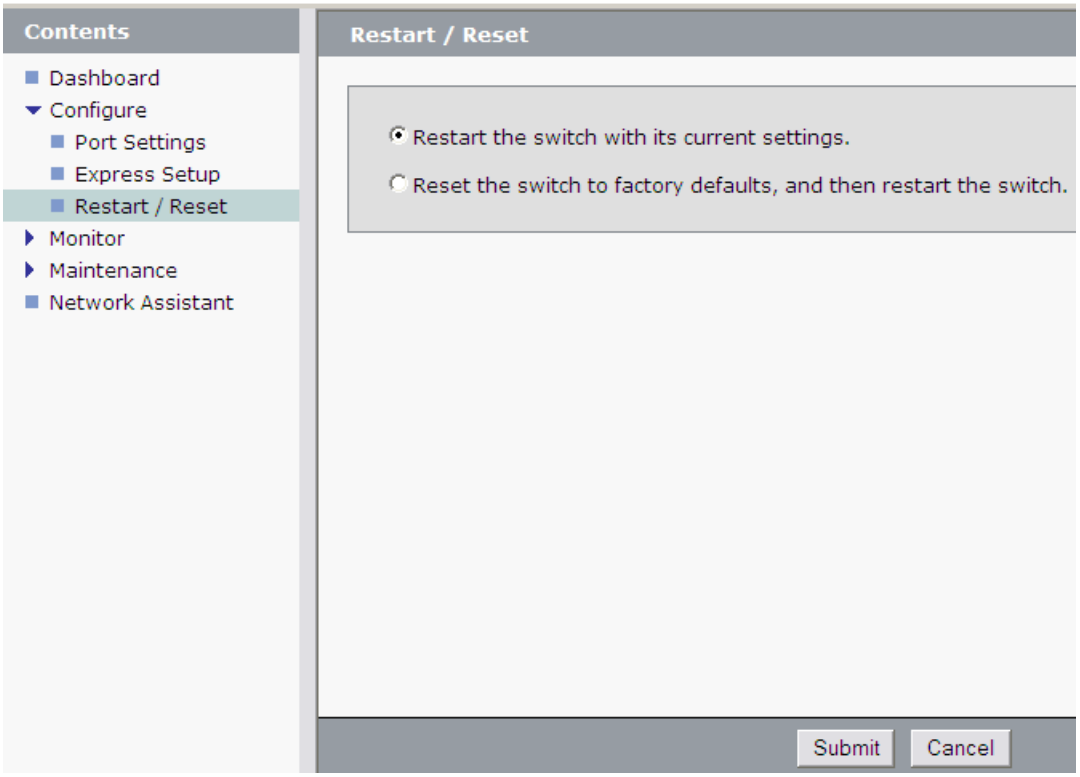


If you are prompted with "Do you want a secured session with the switch?", click on **No**.



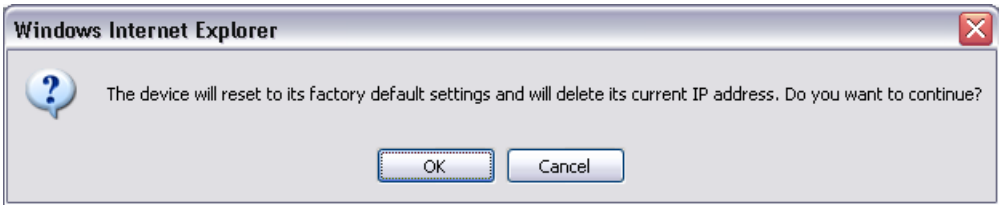
Then a new Catalyst Blade Switch 3020 Device Manager will be opened.

Navigate to **Configure** > **Restart/Reset**.



Click the circle that says "Reset the switch to factory defaults, and then restart the switch". Then click the "**Submit**" button.

A pop-up window will appear that looks like this:



Click OK and the switch will be reset to factory defaults and reloaded.

7. **Virtual PM&C:** Remove the old ssh key and Initialize the switch

   Remove the old ssh key:

```
$ sudo /usr/bin/ssh-keygen -R <enclosure_switch_ip>
```

   The following command must be entered at least 60 seconds and at most 5 minutes after the previous step is completed.

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/3020_init.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/3020_init.xml
Waiting to load the configuration file...
loaded.
```

```
Attempting to login to device...
Configuring....
```

Note: This step takes about 10-15 minutes to complete, it is imperative that you wait until returned to the command prompt. **DO NOT PROCEED UNTIL RETURNED TO THE COMMAND PROMPT**.

Check the output of this command for any errors. A successful completion of netConfig will return the user to the prompt. Due to strict host checking and the narrow window of time in which to perform the command, this command is prone to user error. Most issues are corrected by returning to the previous step and continuing. If this step has failed for a second time, stop the procedure and contact My Oracle Support.

8. **Virtual PM&C:** Reboot the switch using netConfig

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> reboot save=no
```

Wait 2-3 minutes for the switch to reboot. Verify it has completed rebooting and is reachable by pinging it.

```
$ /bin/ping <enclosure_switch_IP>
From 10.240.8.48 icmp_seq=106 Destination Host Unreachable
From 10.240.8.48 icmp_seq=107 Destination Host Unreachable
From 10.240.8.48 icmp_seq=108 Destination Host Unreachable
64 bytes from 10.240.8.13: icmp_seq=115 ttl=255 time=1.13 ms
64 bytes from 10.240.8.13: icmp_seq=116 ttl=255 time=1.20 ms
64 bytes from 10.240.8.13: icmp_seq=117 ttl=255 time=1.17 ms
```

9. **Virtual PM&C:** Configure the switches

Configure both switches by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/3020_configure.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/3020_configure.xml
$
```

Note: This step takes about 2-3 minutes to complete

Check the output of this command for any errors. If the file fails to configure the switch, please review/troubleshoot the file first. If troubleshooting is unsuccessful, stop this procedure and contact My Oracle Support.

A successful completion of netConfig will return the user to the prompt.

10. **Virtual PM&C:** Verify switch configuration

To verify the configuration was completed successfully, execute the following command and review the configuration:

```
# sudo /usr/TKLC/plat/bin/netConfig showConfiguration --device=<switch_name>
Configuration:  = (
   Building configuration...

   Current configuration : 3171 bytes
   !
   ! Last configuration change at 23:54:24 UTC Fri Apr 2 1993 by plat
   !
```

```
   version 12.2

<output removed to save space >

   monitor session 1 source interface Gi0/2 rx
   monitor session 1 destination interface Gi0/1 encapsulation replicate
   end

   )
```

Return to Step 4 and repeat for each 3020 switch.

11. Virtual PM&C: Modify PM&C Feature to disable TFTP.

    Disable the DEVICE.NETWORK.NETBOOT feature:

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=0
$  sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
```

    Note: This may take up to 60 seconds to complete.

12. Perform*E.2 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* for each switch configured in this procedure.
13. **Virtual PM&C:** Clean up FW file

    Remove the FW file from the tftp directory.

```
$ sudo /bin/rm -f /var/TKLC/smac/image/<FW_image>
```

4.7.2 Configure HP 6120XG Switches

4.7.2.1 Configure HP 6120XG Switch (netConfig)

Note: The HP 6120XG enclosure switch supports configuration of IPv6 addresses but it does not support configuration of a default route for those IPv6 interfaces. Instead, the device relies on router advertisements to obtain default route(s) for those interfaces. For environments where IPv6 routes are needed (NTP, etc.), router advertisements will need to be enabled either on the aggregation switch or customer network.

This procedure will configure the HP 6120XG switches from the PM&C server and the command line interface using templates included with an application.

Needed materials:

- HP MISC firmware ISO image
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]
- Application-specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application media

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **Virtual PM&C:** Prepare for switch configuration

If the aggregation switches are supported by Oracle, log in to the management server, then run:

```
$ /bin/ping -w3 <switch1A_mgmtVLAN_address>
$ /bin/ping -w3 <switch1B_mgmtVLAN_address>
$ /bin/ping -w3 <switch_mgmtVLAN_VIP>
```

If the aggregation switches are provided by the customer, log in to the management server, then run:

```
$ /bin/ping -w3 <mgmtVLAN_gateway_address>
```

2. **Virtual PM&C:** Verify network connectivity to 6120XG switches

   For each 6120XG switch, verify network reachability.

```
$ /bin/ping -w3 <enclosure_switch_IP>
```

3. **Virtual PM&C:** Restore switch to factory defaults

   If the 6120XG switch has been configured prior to this procedure, clear out the configuration using the following command:

```
$ /usr/bin/ssh <username>@<enclosure_switch_IP>
Switch# config
Switch(config)# no password all
Password protection for all will be deleted, continue [y/n]? y
Switch(config)# end
Switch# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]? y
(switch will automatically reboot, reboot takes about 120-180 seconds)
```

   Note: You may need to press [ENTER] twice. You may also need to use previously configured credentials.

   If the above procedures fails, log in via telnet and reset the switch to manufacturing defaults. If the above ssh procedures fails, log in via telnet and reset the switch to manufacturing defaults

```
$ /usr/bin/telnet <enclosure_switch_IP>
Switch# config
Switch(config)# no password all (answer yes to question)
Password protection for all will be deleted, continue [y/n]? y
Switch(config)# end
Switch# erase startup-config
(switch will automatically reboot, reboot takes about 120-180 seconds)
```

   Note: The console connection to the switch must be closed, or the initialization will fail.

4. **Virtual PM&C:** Copy switch configuration template from media to the tftp directory.

   Copy switch initialization template and configuration template from the media to the tftp directory.

```
$ sudo /bin/cp -i /<path to media>/6120XG_init.xml /usr/TKLC/smac/etc/switch/xml
$ sudo /bin/cp -i /<path to media>/6120XG_[single,LAG]Uplink_configure.xml
/usr/TKLC/smac/etc/switch/xml
$ sudo /bin/cp -i
/usr/TKLC/plat/etc/TKLCnetwork-config-templates/templates/utility/addQOS_trafficTemplate_6120XG.xml
 /usr/TKLC/smac/etc/switch/xml
```

   - Where **[single,LAG]** are variables for either one of 2 files-see the following:

- `6120XG_SingleUplink_configure.xml` is for one uplink per enclosure switch topology
- `6120XG_LAGUplink_configure.xml` is for LAG uplink topology

5. **Virtual PM&C:** verify the switch configuration file template in the tftp directory

   Verify the switch initialization template file and configuration file template are in the correct directory.

```
$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/
-rw-r--r-- 1 root root 1955 Feb 16 11:36
/usr/TKLC/smac/etc/switch/xml/6120XG_init.xml
-rw-r--r-- 1 root root 1955 Feb 16 11:36
/usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml
-rw-r--r-- 1 root root 702 Sep 10 10:33 addQOS_trafficTemplate_6120XG.xml
```

6. **Virtual PM&C:** Edit the switch configuration file template for site specific information

   Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$<some_variable_name>** will need to be modified, removing the dollar sign and the less than, greater than sign.

```
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6120XG_init.xml
$ sudo /bin/vi
/usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml
```

   Note: For IPv6 Configurations, IPv6 configuration for remote syslog is NOT currently supported on the HP6120XG switches. This function must be configured for IPv4.

7. **Virtual PM&C:** Apply include-credentials command to the switch

   Login to the switch using SSH

```
$ /usr/bin/ssh manager@<enclosure_switch_IP>
Switch# config
Switch(config)# include-credentials
```

   If prompted, answer yes to both questions.

   Log out of the switch.

```
Switch(config)# logout
Do you want to log out [y/n]? y
Do you want to save current configuration [y/n/^C]?  y
```

   Continue to the next step.

8. **Virtual PM&C:** Initialize the switch

   Initialize the switch

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/6120XG_init.xml
```

   This could take up to 5-10 minutes.

   Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contactMy Oracle Support

9. **Virtual PM&C:** Configure the switch

   Configure the switch

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig
   --file=/usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml
   ```

   This could take up to 2-3 minutes.

   Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contactMy Oracle Support

10. **Virtual PM&C:** Apply QoS Settings

    Apply the QoS traffic template settings.

    ```
    $ sudo /usr/TKLC/plat/bin/netConfig
    --file=/usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml
    ```

    Note: The switch will reboot after this command. This step will take 2-5 minutes.

11. **Virtual PM&C:** Verify proper configuration of HP 6120XG switches

    Once each HP 6120XG has finished booting from the previous step, verify network reachability and configuration.

    ```
    $ /bin/ping -w3 <enclosure_switch_IP>
    $ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>
    <switch_platform_username>@<enclosure_switch_IP>'s password:
    <switch_platform_password>
    Switch# show run
    ```

    Inspect the output of `show run`, and ensure that it is configured as per site requirements.

12. **Virtual PM&C:** Repeat steps for each HP 6120XG

    For each HP 6120XG, repeat steps 3-12.

13. Perform *E.1 Backup HP (6120XG, 6125G, 6125XLG) Enclosure Switch* for each switch configured in this procedure.

14. **Virtual PM&C:** Clean up FW file

    Remove the FW file from the tftp directory.

    ```
    $ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>
    ```

4.7.3 Configure HP 6125G Switches

4.7.3.1 Configure HP 6125G Switch (netConfig)

This procedure will configure the HP 6125G switches from the PM&C server & the command line interface using templates included with an application.

Needed materials:

- Application specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application media.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **Virtual PM&C:** Prepare for switch configuration

   If the aggregation switches are provided by Oracle, log into the PM&C, then run:

```
$ /bin/ping -w3 <switch1A_mgmtVLAN_address>
$ /bin/ping -w3 <switch1B_mgmtVLAN_address>
$ /bin/ping -w3 <switch_mgmtVLAN_VIP>
```

   If the aggregation switches are provided by the customer, log into the PM&C, then run:

```
$ /bin/ping -w3 <mgmtVLAN_gateway_address>
```

2. **Virtual PM&C:** Verify network connectivity to OAs.

   For each OA, verify network reachability.

```
$ /bin/ping -w3 <OA1_IP>
$ /bin/ping –w3 <OA2_IP>
```

3. **Virtual PM&C**: Determine which OA is currently active.

   Log into OA1 to determine if it is active:

```
$ /usr/bin/ssh root@<OA1_IP>
```

   The OA is active if you see the following:

```
Using username "root".

--------------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
--------------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  2
OA Role:       Active
root@10.240.8.6's password:
```

   If you see the following, it is standby:

```
Using username "root".

--------------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
--------------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  1
OA Role:       Standby
root@10.240.8.5's password:
```

   Press **<ctrl>** + **C** to close the SSH session.

If OA1 has a role of Standby, verify that OA2 is the active by logging in to it:

```
$ /usr/bin/ssh root@<OA2_IP>
Using username "root".

------------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
------------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  2
OA Role:       Active
root@10.240.8.6's password:
```

In the following steps, OA will mean the 'active OA' and <active_OA_IP> will be the IP address of the active OA.

Note: If neither OA reports Active, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of the document.

Exit the SSH session.

4. **Virtual PM&C:** Restore switch to factory defaults

   If the 6125G switch has been configured prior to this procedure, clear out the configuration using the following command:

```
$/usr/bin/ssh root@<active_OA_IP>
Using username "root".

------------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
------------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  2
OA Role:       Active
root@10.240.8.6's password: <OA_password>
> connect interconnect <switch_IOBAY_#>
Press [Enter] to display the switch console:
```

Note: You may need to press [ENTER] twice. You may also need to use previously configured credentials.

```
<switch>reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash is being cleared.
Please wait ...

MainBoard:
 Configuration file is cleared.
<switch>reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
 This command will reboot the device. Current configuration will be lost, save
current configuration? [Y/N]:n
This command will reboot the device. Continue? [Y/N]: y
```

The switch will automatically reboot; this takes about 120-180 seconds. The switch reboot is complete when you see the following text:

```
[…Output omitted…]
User interface aux0 is available.

Press ENTER to get started.
```

When the reboot is complete, disconnect from the console by entering **<ctrl>** + **<shift>** + **<->**, then '**d**'.

Note: If connecting to the Virtual PM&C through the management server iLO then*L.1 How to Access a Server Console Remotely*applies. Disconnect from the console by entering**<ctrl>** +**<v>**

Exit from the OA terminal:

```
>exit
```

Note: The console connection to the switch must be closed, or the initialization will fail.

5. **Virtual PM&C:** Copy switch configuration template from media to the tftp directory.

   Copy switch initialization template and configuration template from the media to the tftp directory.

```
$ sudo /bin/cp -i /<path to media>/6125G_init.xml  /usr/TKLC/smac/etc/switch/xml
$ sudo /bin/cp -i /<path to media>/6125G_configure.xml
/usr/TKLC/smac/etc/switch/xml
```

6. **Virtual PM&C:** verify the switch configuration file template in the tftp directory

   Verify the switch initialization template file and configuration file template are in the correct directory.

```
$ sudo  /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/
-rw-r--r-- 1 root root 1955 Feb 16 11:36
/usr/TKLC/smac/etc/switch/xml/6125G_init.xml
-rw-r--r-- 1 root root 1955 Feb 16 11:36
/usr/TKLC/smac/etc/switch/xml/6125G_configure.xml
```

7. **Virtual PM&C:** Edit the switch configuration file template for site specific information

   Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$<some_variable_name>** must be modified, removing the dollar sign and the less than, greater than sign.

```
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125G_init.xml
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125G_configure.xml
```

   Note: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the HP6125G switches. This function must be configured for IPv4.

8. **Virtual PM&C:** Initialize the switch

   Note: The console connection to the switch must be closed before performing this step.

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/6125G_init.xml
```

This could take up to 5-10 minutes.

9. **Virtual PM&C:** Verify the switch was initialized

   Verify the initialization succeeded with the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_hostname>
Hostname: <switch_hostname>
```

   This could take up to 2-3 minutes.

   Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contactMy Oracle Support

10. **Virtual PM&C**: Configure the switch

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/6125G_configure.xml
```

   This could take up to 2-3 minutes.

   Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contact My Oracle Support.

11. **Virtual PM&C**: Verify proper configuration of HP 6125G switch

   Once the HP 6125G has finished booting from the previous step, verify network reachability and configuration.

```
$ /bin/ping -w3 <enclosure_switch_IP>
PING 10.240.8.10 (10.240.8.10) 56(84) bytes of data.64 bytes from 10.240.8.10:
icmp_seq=1 ttl=255 time=0.637 ms64 bytes from 10.240.8.10: icmp_seq=2 ttl=255
time=0.661 ms64 bytes from 10.240.8.10: icmp_seq=3 ttl=255 time=0.732 m
$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>
<switch_platform_username>@<enclosure_switch_IP>'s password:
<switch_platform_password>
Switch_hostname> display current-configuration
Inspect the output, and ensure that it is configured as per site requirements.
```

12. **Virtual PM&C**: Repeat steps for each HP 6125G

   For each HP 6125G, repeat *Step 4*-*Step 11*.

13. Perform *E.1 Backup HP (6120XG, 6125G, 6125XLG) Enclosure Switch* for each switch configured in this procedure.

14. **Virtual PM&C:** Clean up FW file

   Remove the FW file from the tftp directory.

```
$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>
```

4.7.4 Configure HP 6125XLG Switches

4.7.4.1 Configure HP 6125XLG Switch (netConfig)

This procedure will configure the HP 6125XLG switches from the PM&C server & the command line interface using templates included with an application.

Needed materials:

- Application specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application media.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **Virtual PM&C:** Prepare for switch configuration

   If the aggregation switches are provided by Oracle, log into the PM&C, then run:

   ```
   $ /bin/ping -w3 <switch1A_mgmtVLAN_address>
   $ /bin/ping -w3 <switch1B_mgmtVLAN_address>
   $ /bin/ping -w3 <switch_mgmtVLAN_VIP>
   ```

   If the aggregation switches are provided by the customer, log into the PM&C, then run:

   ```
   $ /bin/ping -w3 <mgmtVLAN_gateway_address>
   ```

2. **Virtual PM&C:** Verify network connectivity to OAs.

   For each OA, verify network reachability.

   ```
   $ /bin/ping -w3 <OA1_IP>
   $ /bin/ping –w3 <OA2_IP>
   ```

3. **Virtual PM&C**: Determine which OA is currently active.

   Login to OA1 to determine if it is active:

   ```
   $ /usr/bin/ssh root@<OA1_IP>
   ```

   The OA is active if you see the following:

   ```
   Using username "root".

   ------------------------------------------------------------------------------
   WARNING: This is a private system.  Do not attempt to login unless you are an
   authorized user.  Any authorized or unauthorized access and use may be moni-
   tored and can result in criminal or civil prosecution under applicable law.
   ------------------------------------------------------------------------------
   Firmware Version: 3.70
   Built: 10/01/2012 @ 17:53
   OA Bay Number:  2
   OA Role:       Active
   root@10.240.8.6's password:
   ```

If you see the following, it is standby:

```
Using username "root".

------------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
------------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  1
OA Role:       Standby
root@10.240.8.5's password:
```

Press **<ctrl>** + **C** to close the SSH session.

If OA1 has a role of Standby, verify that OA2 is the active by logging in to it:

```
$ /usr/bin/ssh root@<OA2_IP>
Using username "root".

------------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
------------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  2
OA Role:       Active
root@10.240.8.6's password:
```

In the following steps, OA will mean the 'active OA' and <active_OA_IP> will be the IP address of the active OA.

Note: If neither OA reports Active, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of the document.

Exit the SSH session.

4. **Virtual PM&C:** Restore switch to factory defaults

   If the 6125XLG switch has been configured prior to this procedure, clear out the configuration using the following command:

```
$/usr/bin/ssh root@<active_OA_IP>
Using username "root".

------------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
------------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  2
OA Role:       Active
root@10.240.8.6's password: <OA_password>
> connect interconnect <switch_IOBAY_#>
Press [Enter] to display the switch console:
```

Note: You may need to press [ENTER] twice. You may also need to use previously configured credentials.

```
<switch>reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash is being cleared.
Please wait ...

MainBoard:
 Configuration file is cleared.
<switch>reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
 This command will reboot the device. Current configuration will be lost, save
current configuration? [Y/N]:n
This command will reboot the device. Continue? [Y/N]: y
```

The switch will automatically reboot; this takes about 120-180 seconds. The switch reboot is complete when the switch begins the auto configuration sequence.

When the reboot is complete, disconnect from the console by entering **<ctrl>** + **<shift>** + **<->**, then '**d**'.

Note: If connecting to the Virtual PM&C through the management server iLO then *L.1 How to Access a Server Console Remotely* applies. Disconnect from the console by entering **<ctrl> + <v>**

Exit from the OA terminal:

```
>exit
```

Note: The console connection to the switch must be closed, or the initialization will fail.

5. **Virtual PM&C:** Copy switch configuration template from media to the switch backup directory.

   Copy switch initialization template and configuration template from the media to the switch backup directory.

```
$ sudo /bin/cp -i /<path to media>/6125XLG_init.xml  /usr/TKLC/smac/etc/switch/xml
$ sudo /bin/cp -i /<path to media>/6125XLG_configure.xml
/usr/TKLC/smac/etc/switch/xml
```

6. **Virtual PM&C:** Verify the switch configuration file template in the switch backup directory

   Verify the switch initialization template file and configuration file template are in the correct directory.

```
$ sudo  /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/
131195 -rw------- 1 root root   248 May  5 11:01 6125XLG_IOBAY3_template_init.xml
131187 -rw------- 1 root root   248 May  5 10:54 6125XLG_IOBAY5_template_init.xml
131190 -rw------- 1 root root  6194 Mar 24 15:04 6125XLG_IOBAY8-config.xml
131189 -rw------- 1 root root   248 Mar 25 09:43 6125XLG_IOBAY8_template_init.xml
```

7. **Virtual PM&C:** Edit the switch configuration file template for site specific information

   Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content. Values to be modified by the user will be notated in this

step by a preceding dollar sign. So a value that has **$<some_variable_name>** will need to be modified, removing the dollar sign and the less than, greater than sign.

```
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125XLG_init.xml
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml
```

8. **Virtual PM&C:** Initialize the switch

   Note: The console connection to the switch must be closed before performing this step.

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/6125XLG_init.xml
```

   This could take up to 5-10 minutes.

9. **Virtual PM&C:** Verify the switch was initialized

   Verify the initialization succeeded with the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_hostname>
Hostname: <switch_hostname>
```

   This could take up to 2-3 minutes.

   Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contactMy Oracle Support

10. **Virtual PM&C**: Configure the switch

    Configure the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml
```

    This could take up to 2-3 minutes. Note:

    Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contact My Oracle Support.

11. **Virtual PM&C**: Verify proper configuration of HP 6125XLG switch

    Once the HP 6125XLG has finished booting from the previous step, verify network reachability and configuration.

```
$ /bin/ping -w3 <enclosure_switch_IP>
PING 10.240.8.10 (10.240.8.10) 56(84) bytes of data.64 bytes from 10.240.8.10:
icmp_seq=1 ttl=255 time=0.637 ms64 bytes from 10.240.8.10: icmp_seq=2 ttl=255
time=0.661 ms64 bytes from 10.240.8.10: icmp_seq=3 ttl=255 time=0.732 m
$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>
<switch_platform_username>@<enclosure_switch_IP>'s password:
<switch_platform_password>
Switch_hostname> display current-configuration
Inspect the output, and ensure that it is configured as per site requirements.
```

12. For HP 6125XLG switches connected by 4x1GE LAG uplink perform Utility procedure *M.1 Configure Speed and Duplex for 6125XLG LAG Ports (netConfig)*. Otherwise, for deployments with 10GE uplink, continue to the next step.
13. **Virtual PM&C**: Repeat steps for each HP 6125XLG

For each HP 6125XLG, repeat Steps *Step 4*-*Step 12*.

14. For HP 6125XLG switches uplinking with 4x1GE uplink to customer switches, field personnel are expected to work with the customer to set their downlinks to the HP 6125XLG 4x1GE LAG to match speed and duplex set in *Step 12*

    For HP 6125XLG switches uplinking with 4x1GE LAG to product Cisco 4948/E/E-F aggregation switches, perform Utility Procedure 3.1.4.9, Configure Speed and Duplex for LAG Ports for Cisco 4948/E/E-F (netConfig), to match speed and duplex settings from *Step 12*.

    Otherwise, for deployments with 10GE uplink, continue to the next step.

15. Perform *E.1 Backup HP (6120XG, 6125G, 6125XLG) Enclosure Switch* for each switch configured in this procedure.
16. **Virtual PM&C:** Clean up FW file

    Remove the FW file from the tftp directory.

```
$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>
```

4.8 Server Blades Installation Preparation

4.8.1 Upgrade Blade Server Firmware

Software Centric Customers: If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP."

Note: This procedure uses a custom SPP version that cannot be obtained from the customer and therefore cannot be used for a Software Centric Customer. Software Centric Customers must ensure their firmware versions match those detailed in the *HP Solutions Firmware Upgrade Pack, Software Centric Release Notes* document.

This procedure will provide the steps to upgrade the firmware on the Blade servers.

The HP Support Pack for ProLiant installer automatically detects the firmware components available on the target server and will only upgrade those components with firmware older than what is on the current ISO.

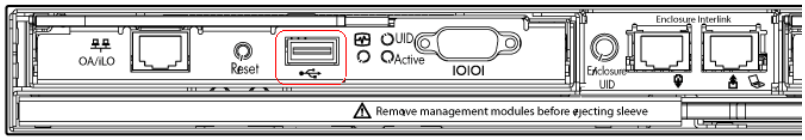
Needed Materials:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]
- USB Flash Drive (4GB or larger and formatted as FAT32)

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. **Local Workstation:** Copy the HP Support Pack for ProLiant (SPP) ISO image to the USB Flash Drive.
2. Insert USB Flash Drive

   Insert the USB Flash Drive with the HP Support Pack for ProLiant ISO into the USB port of the Active OA Module.



3. **Active OA GUI:** Login

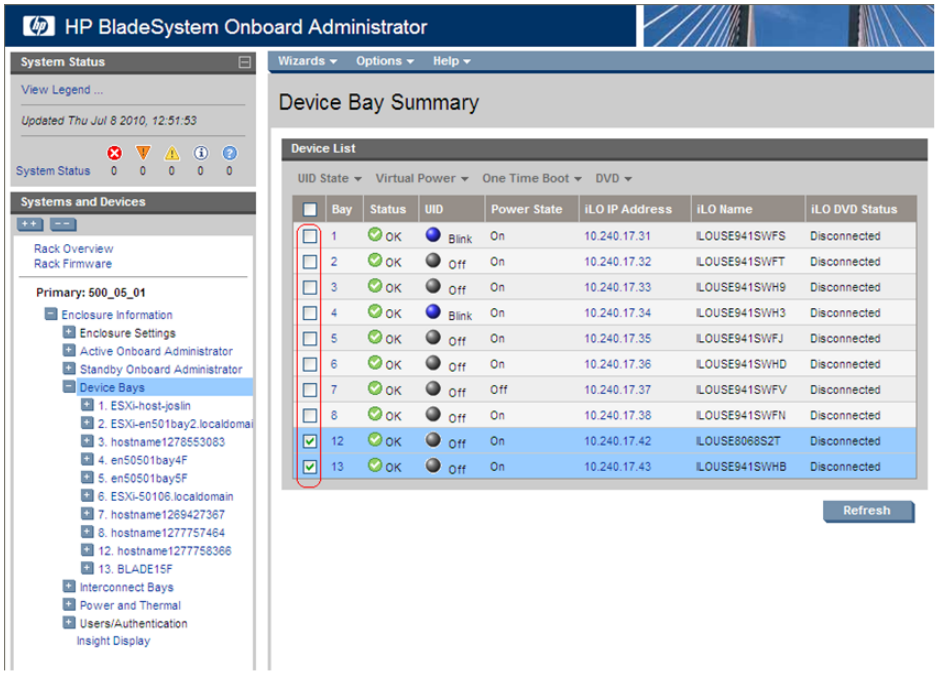
   Navigate to the IP address of the active OA, using *N.1 Determining Which Onboard Administrator Is Active*. Log in as an administrative user.

4. **OA Web GUI:** Access the Device Summary page

   On the left pane, expand the **Device Bays** node to display the **Device Bay Summary** window.

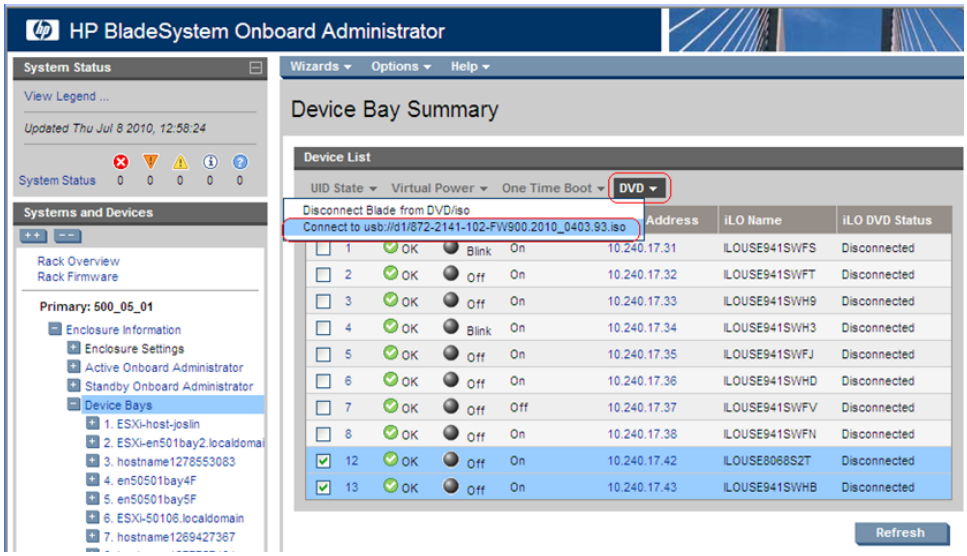
   Select the individual blades to be upgraded by clicking and enabling the corresponding checkbox next to the bay number of the blades.

   Note: A maximum of 8 blades should be upgraded concurrently at one time. If the c7000 enclosure has more than 8 blades they will need to be upgraded in multiple sessions.



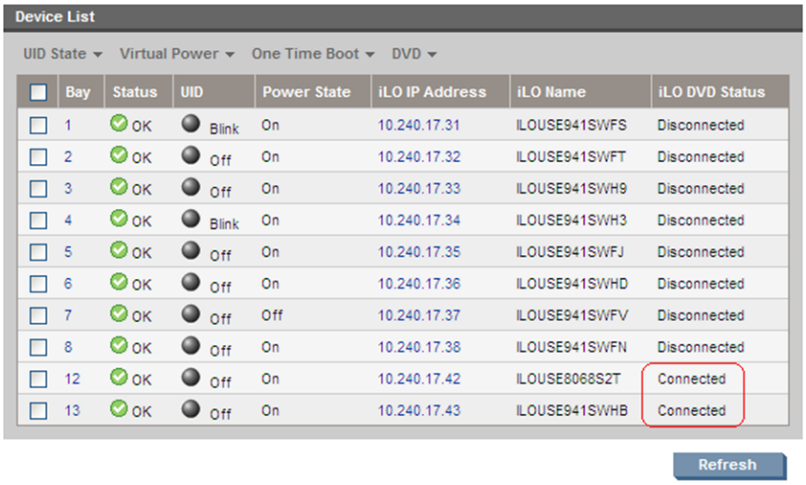
5. **OA Web GUI:** Connect to USB Drive

   Once the blades are selected, connect them to the ISO on the USB Drive, by selecting the **Connect to usb…** item from the **DVD** menu.



6. **OA Web GUI:** Verify Drive Connection

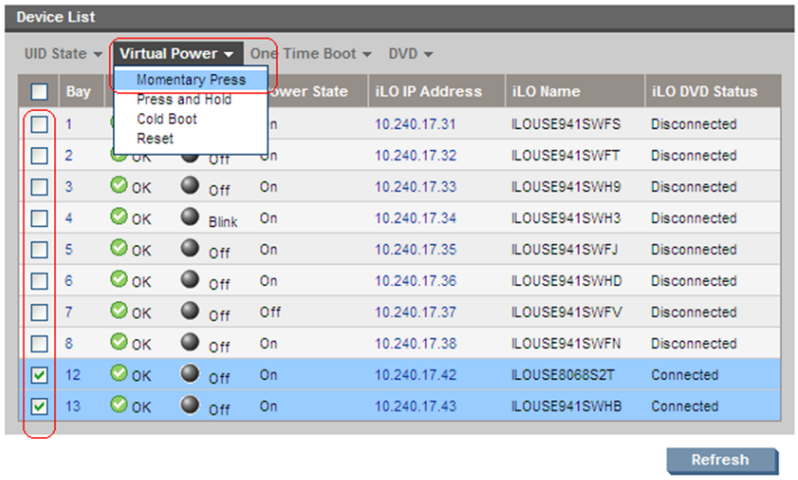
   Once each blade has mounted the ISO media the **`Device List`** table should indicate an **`iLO DVD Status`** as **`Connected`** for each blade that was previously selected.



   Note: The **Refresh** button may need to be clicked in order to see the current status of all blades.

7. **OA Web GUI:** Power Down Blades

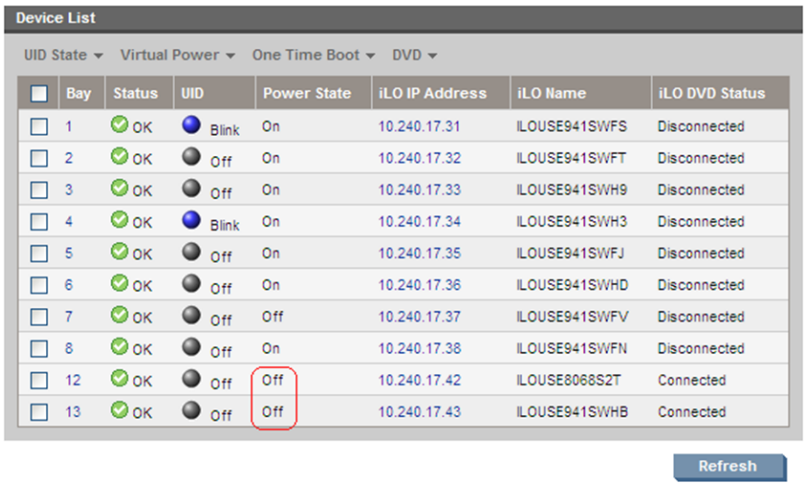
   If needed, reselect the UID checkbox for each blade to be upgraded and then select the **Momentary Press** option under the **`Virtual Power`** menu.



When prompted click the **OK** button to confirm the action.

8. **OA Web GUI:** Verify Power Down

   The power down sequence can take several minutes to complete. When it completes the **`Device List`** table will indicate the **`Power State`** of each select blade to be **`Off`**.



Note: The **Refresh** button may need to be clicked in order to see the current status of all blades.

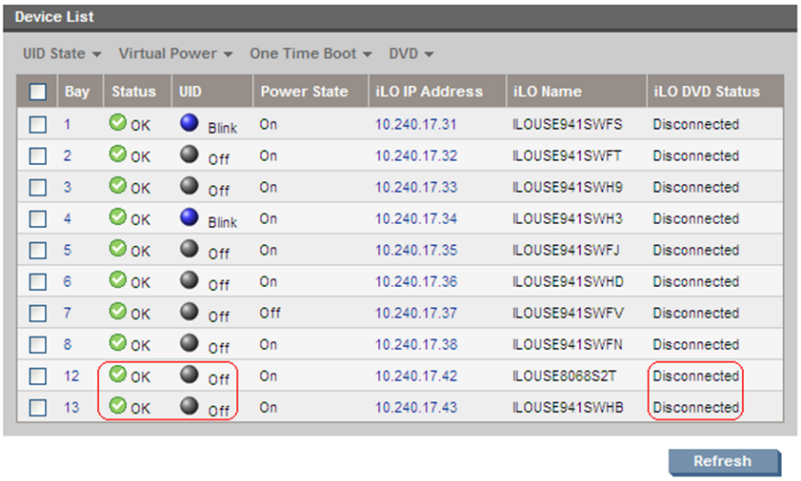
9. **OA Web GUI:** Initiate Firmware Upgrade

   To power the blades back on and begin the automated firmware upgrade process, repeat Steps 7 and 8 this time being sure the **`Power State`** indicates **`On`** for each selected blade.

10. **OA Web GUI:** Monitor Firmware Upgrade

    From this point on each blade will boot into an automated firmware upgrade process that will last approximately 30 minutes. During this time all feedback is provided through the UID lights. The UID light on a server blinks when firmware is actively being applied.

The UID lights will not blink until the server fully boots and the firmware upgrades have started to be applied. If no upgrades are needed the UID lights will not blink, but the server will still reboot and the iLO DVD will disconnected after completion.



Bay	Status	UID	Power State	iLO IP Address	iLO Name	iLO DVD Status
1	OK	Blink	On	10.240.17.31	ILOUSE941SWFS	Disconnected
2	OK	Off	On	10.240.17.32	ILOUSE941SWFT	Disconnected
3	OK	Off	On	10.240.17.33	ILOUSE941SWH9	Disconnected
4	OK	Blink	On	10.240.17.34	ILOUSE941SWH3	Disconnected
5	OK	Off	On	10.240.17.35	ILOUSE941SWFJ	Disconnected
6	OK	Off	On	10.240.17.36	ILOUSE941SWHD	Disconnected
7	OK	Off	Off	10.240.17.37	ILOUSE941SWFV	Disconnected
8	OK	Off	On	10.240.17.38	ILOUSE941SWFN	Disconnected
12	OK	Off	On	10.240.17.42	ILOUSE8068S2T	Disconnected
13	OK	Off	On	10.240.17.43	ILOUSE941SWHB	Disconnected

Upon a successful firmware upgrade, the **`Device List`** table will list each blade with a **Status** of **`OK`**, UID of **`Off`** and the **`iLO DVD Status`** as **`Disconnected`**. At this time the blades will automatically be rebooted.

Note: Make sure all blades have disconnected before continuing. If any blades are still connected after their UIDs have stopped blinking and Status=OK, disconnect them manually by selecting **Disconnect Blade from DVD/ISO from** the DVD menu. If the UID led is solid, a failure has occurred during the firmware upgrade. Use the iLO's integrated remote console or a kvm connection to view the error.

If necessary, repeat Steps 4 through 10 for the remaining blades in the enclosure to be upgraded. Proceed to the next step.

11. Remove USB Flash Drive

The USB flash drive may now safely be removed from the Active OA module.

12. Update Firmware Errata

Check the Release Notes of the *HP Solutions Firmware Upgrade Pack* [2] to see if there are any firmware errata items that apply to the server being upgraded.

If there are firmware errata items that apply to the server being upgraded, there will be a directory matching the errata's ID in the /errata directory of the HP MISC firmware ISO image. The errata directories contain the errata firmware and a README file detailing the installation steps.

4.8.2 Confirm/Upgrade Blade Server BIOS Settings

This procedure will provide the steps to confirm and update the BIOS boot order on the blade servers. All servers should have SNMP disabled. Refer to *Changing SNMP Configuration Settings for iLO*.

For instructions on BIOS configuration for a Gen9 blade or RMS, refer to Appendix *C.2.2 Configuring HP Gen9 Servers*.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

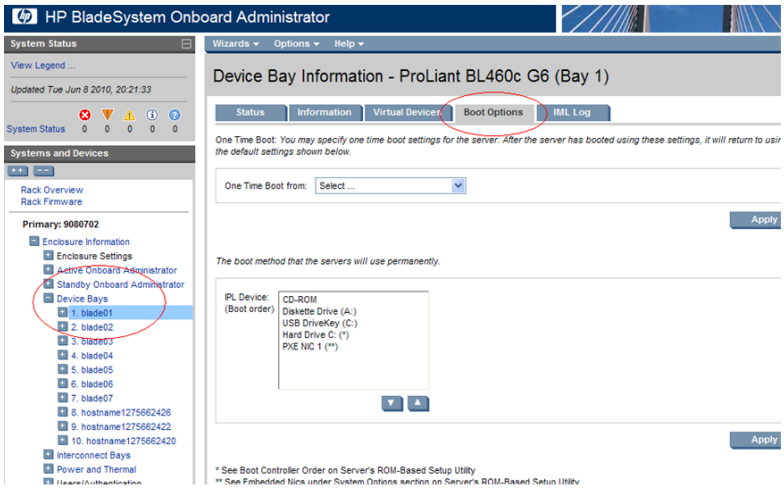
1. **Active OAGUI:** Login

   Navigate to the IP address of the active OA, using *N.1 Determining Which Onboard Administrator Is Active*. Login as an administrative user.

2. **Active OAGUI:** Navigate to device Bay Settings

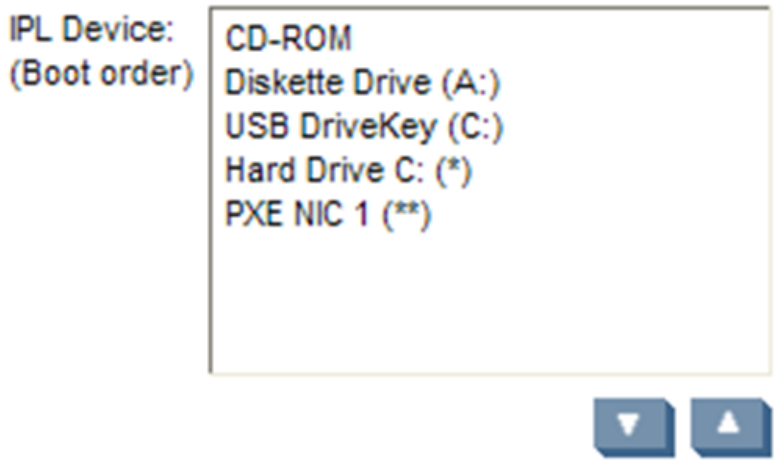
   Navigate to **Enclosure Information** > **Device Bays** > **<Blade 1>**

   Click on **Boot Options** tab.



3. **Active OAGUI:** Verify/update Boot device Order

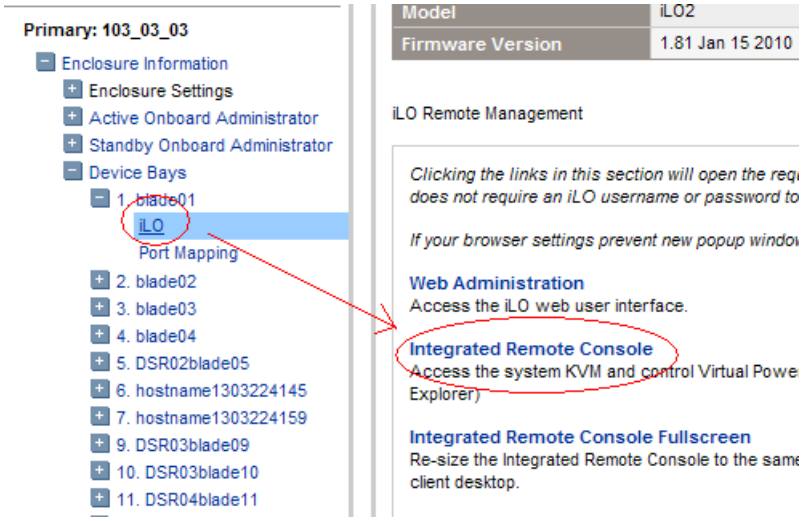
   Verify that the Boot order is as follows. If it is not, use the up and down arrows to adjust the order to match the picture below, then click on **Apply**



4. **OA:** Access the Blade iLO

   Navigate to **Enclosure Information** > **Device Bays** > **<Blade 1>** > **iLO**

   Click on **Integrated Remote Console**



   This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you will be prompted to install an addon to your web browser, follow the on screen instructions to do so.

5. **OA:** Restart the blade and access the BIOS

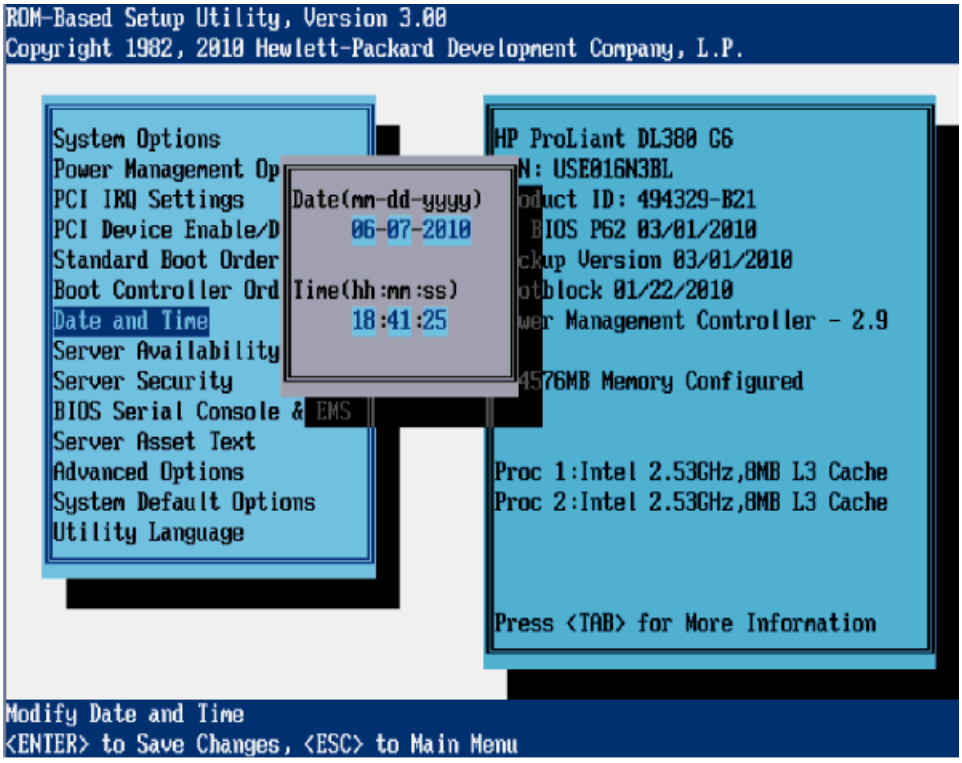
   You might be prompted with a certificate security warning, just press continue.

   Once a prompt is displayed, login onto the blade using the "admusr" username.

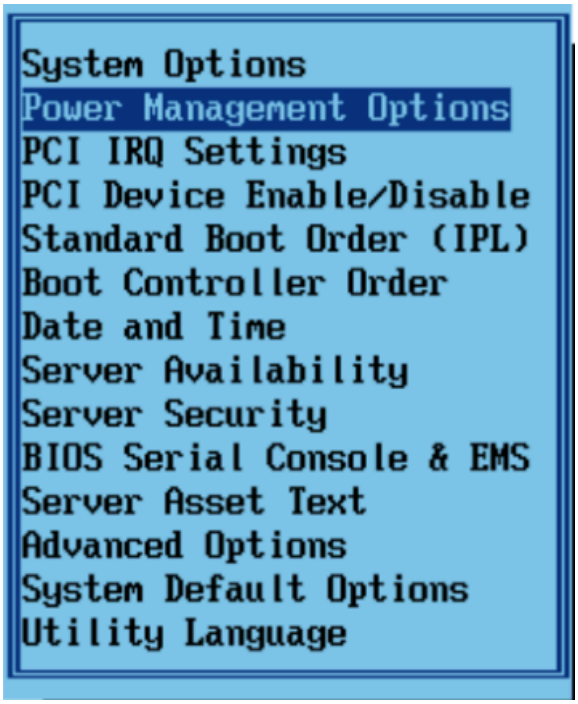
   Once logged in, Reboot the server (using the "reboot" command) and after the server is powered on, as soon as you see <F9=Setup> in the lower left corner of the screen, press **F9** to access the BIOS setup screen.

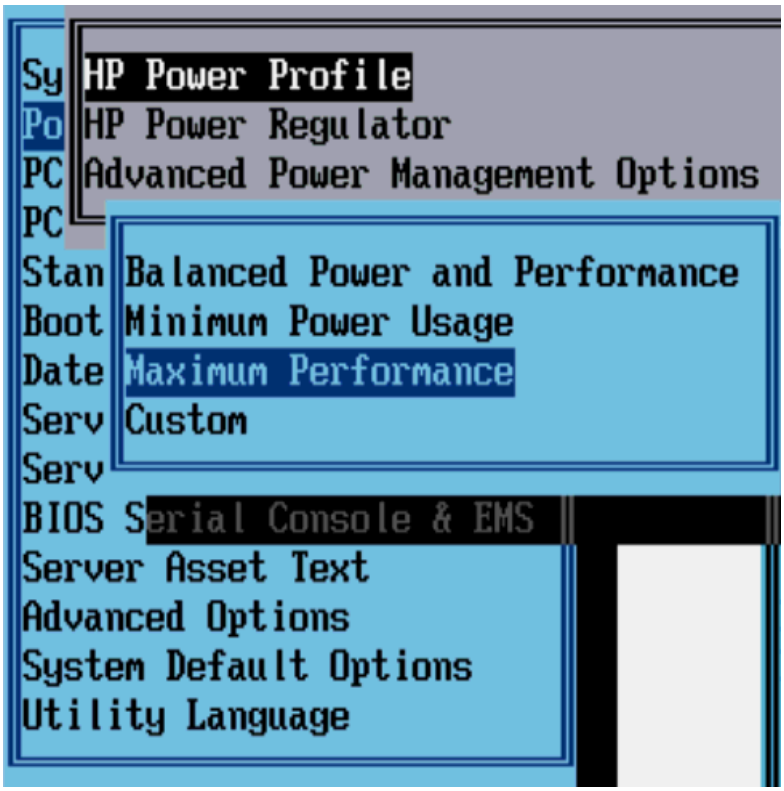
6. **OA:** Updated BIOS settings

1. Scroll to **Date and Time** and press **Enter**
2. Set current date, set current UTC time and press **Enter**



3. Go back to the main menu by pressing **<ESC>** and scroll down to **Power Management Options** and press **Enter**
4. Select **HP Power Profile** and press **Enter**
5. Scroll down to **Maximum Performance** and press **Enter**





6. Press **<ESC>** twice to return to exit the BIOS setup screen and **F10** to confirm, exiting the utility
7. The blade will reboot afterwards

7. **Active OAGUI:** Repeat for the remaining blades

   Repeat Steps 2 through 6 for the remaining blades. Once done, exit out of the OA GUI.

4.9 Installing TVOE on Rack Mount Server(s)

Note: This procedure is specific to RMS servers that will be managed by PM&C, and do not yet have a TVOE environment configured. It requires that the RMS server is on the PM&C control network (i.e., it is able to receive a DHCP IP address from PM&C on the 192.168.1.0 network).

This is an "IPM" activity for a server that will be a Virtual Host.

4.9.1 Add Rack Mount Server to the PM&C System Inventory

This procedure provides instructions for adding a rack mount server to the PM&C system inventory.

Prerequisite:

- The *4.4.1.1 Configure PM&C Application* procedure has been completed.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

Note: You cannot edit the RMS iLO IP address. To change this address, delete, and then add, the RMS with the correct address.

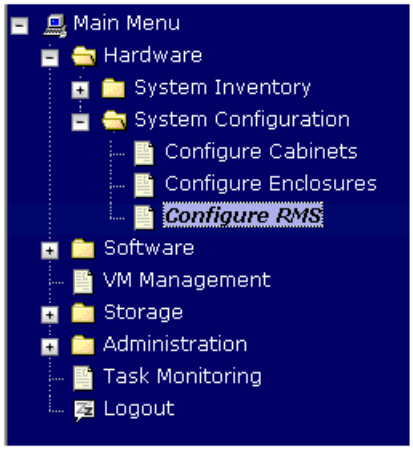
1. **PM&C GUI:** Login

   Open web browser and enter:

   ```
   https://<pmac_management_network_ip>
   ```

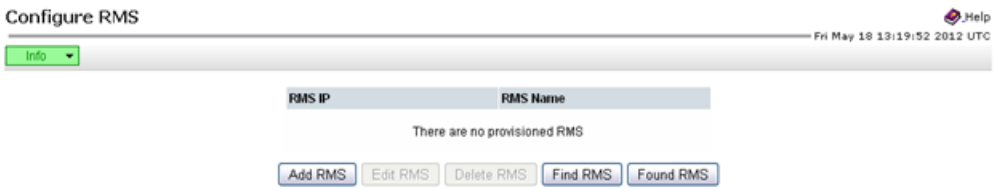
2. **PM&C GUI:** Configure RMS

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure RMS**

3. **PM&C GUI:** Add RMS

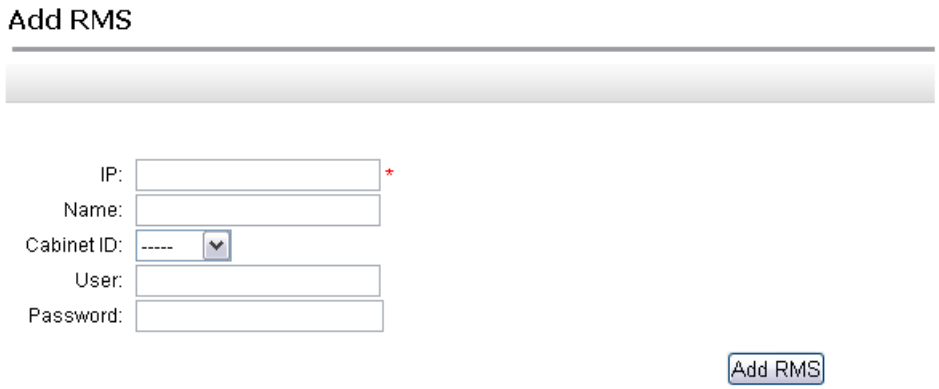
On the Configure RMS panel, click the Add RMS button.



4. **PM&C GUI:** Enter information

   Enter the IP Address of the rack mount server management port (iLO). All the other fields are optional.

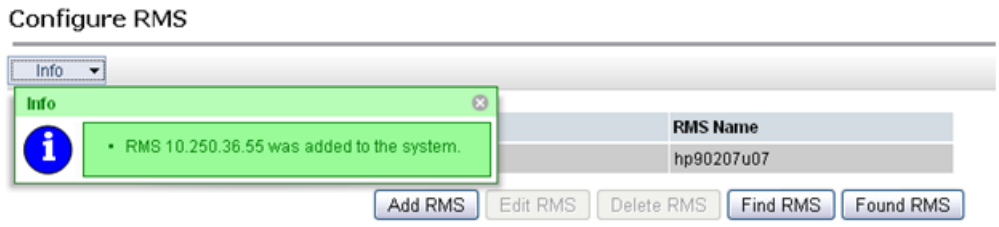
   Then click on the **Add RMS** button.



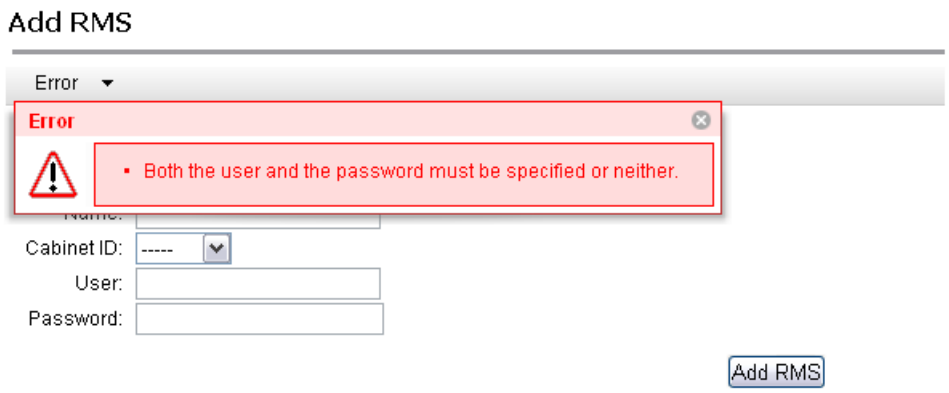
   Note: If the initial credentials provided by Oracle have been changed, enter valid credentials (not to be confused with OS or Application credentials) for the rack mount server management port.

5. **PM&C GUI:** Check errors

   If no error is reported to the user you will see the following:

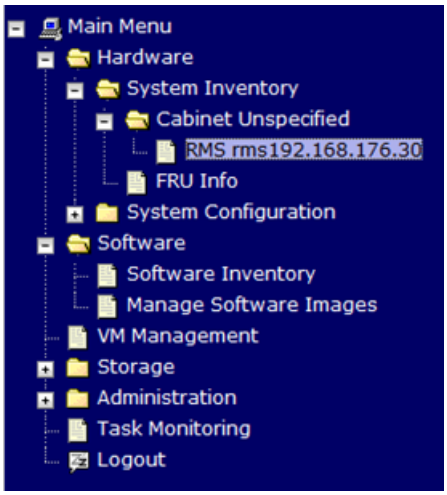


   Or you will see an error message:

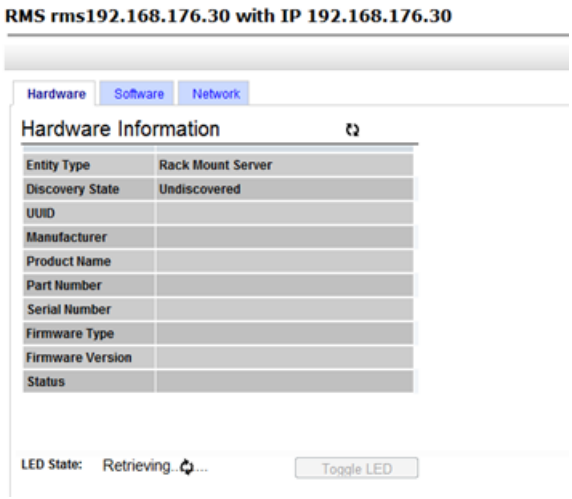


6. **PM&C GUI:**Verify RMS discovered

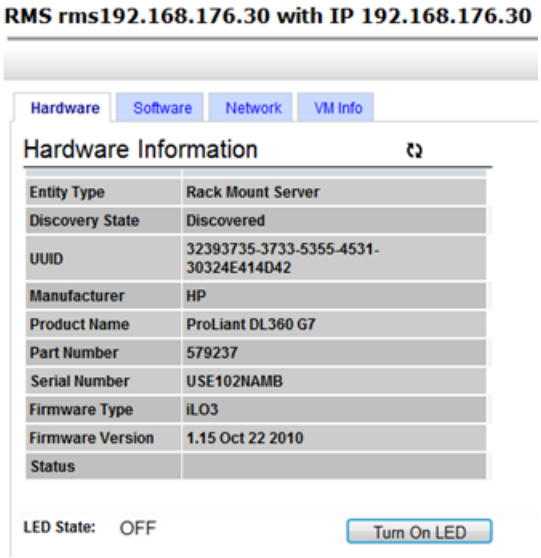
   Navigate to **Main Menu** > **Hardware** > **System Inventory** > **Cabinet xxx** > **RMS yyy** Where **xxx** is the cabinet id selected when adding RMS (or "unspecified") and **yyy** is the name of the RMS.



   The RMS inventory page is displayed.



Periodically refresh the hardware information using the double arrow to the right of the title "Hardware Information" until the "Discovery state" changes from "Undiscovered" to "Discovered". If "Status" displays an error, contact My Oracle Support for assistance.



4.9.2 Add ISO Image to the PM&C Repository

If the Rack Mount Server (RMS) is to be configured as a TVOE hosting application guests execute this procedure using the applicable TVOE ISO as the image to add, otherwise continue to next procedure.

4.9.2.1 Adding ISO Images to the PM&C Image Repository

Note: If the ISO image has already been added to the PM&C Software Inventory in a previous procedure, skip this procedure.

This procedure provides the steps for adding ISO images to the PM&C repository.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. Make the image available to PM&C

   There are two ways to make an image available to PM&C:

   - Attach the USB device containing the ISO image to a USB port of the Management Server.
   - Use sftp to transfer the iso image to the PM&C server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
     - cd into the directory where your ISO image is located (not on the PM&C server)
     - Using sftp, connect to the PM&C management server as the pmacftpusr user . If using IPv6, shell escapes around the IPv6 address may be required.

```
> scp pmacftpusr@[]> sftp pmacftpusr@<pmac_management_network_ip>
> put <image>.iso
```

     - After the image transfer is 100% complete, close the connection

```
> quit
```

   Refer to the documentation provided by application for pmacftpusr password.

2. **PM&C GUI:** Login

   Open web browser and enter:

```
https://<pmac_management_network_ip>
```

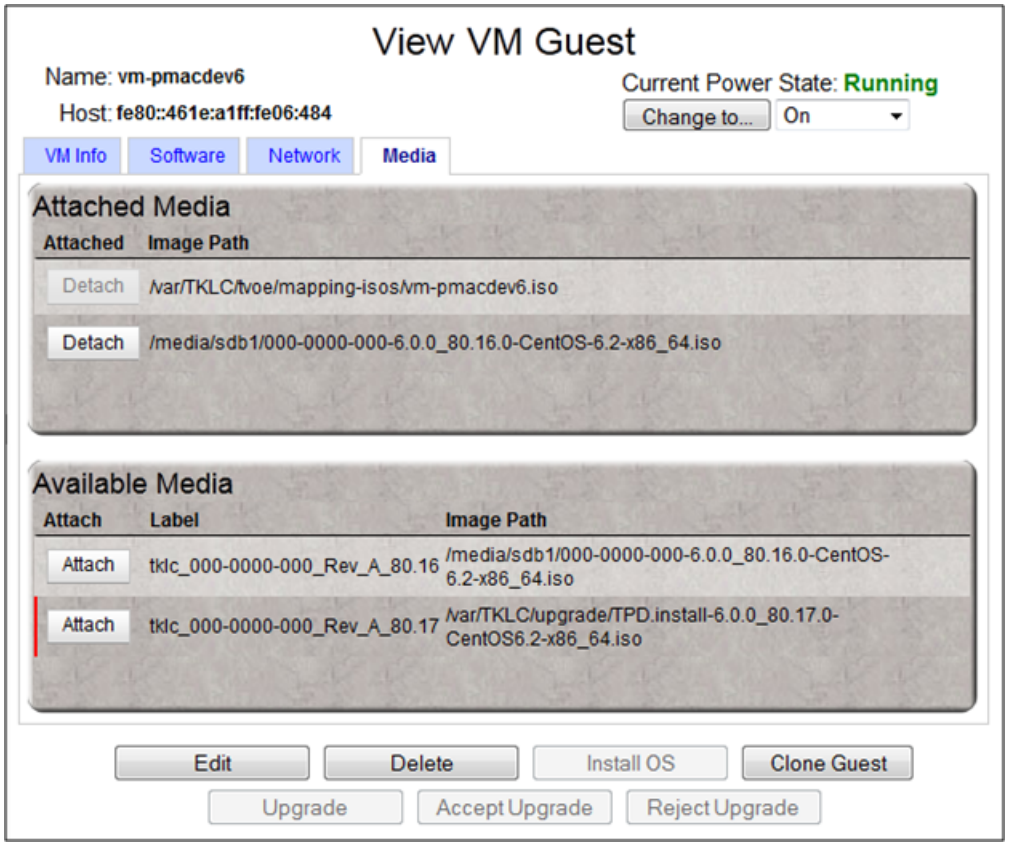
   Login as pmacadmin user.

3. **PM&C GUI:** Attach the software image to the PM&C guest

   If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a USB device, continue with this step.

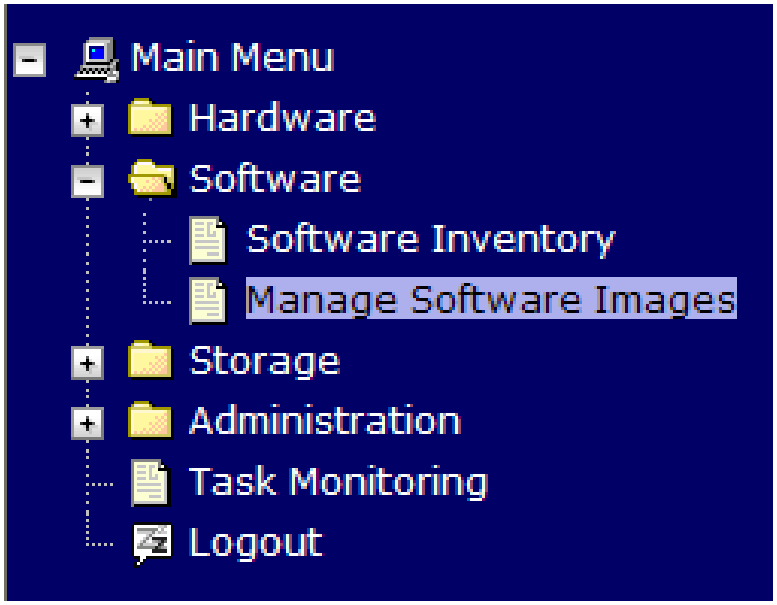
   In the PM&C GUI, navigate to **Main Menu** > **VM Management.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.

   Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button. After a pause, the image will appear in the "**Attached Media**" list.



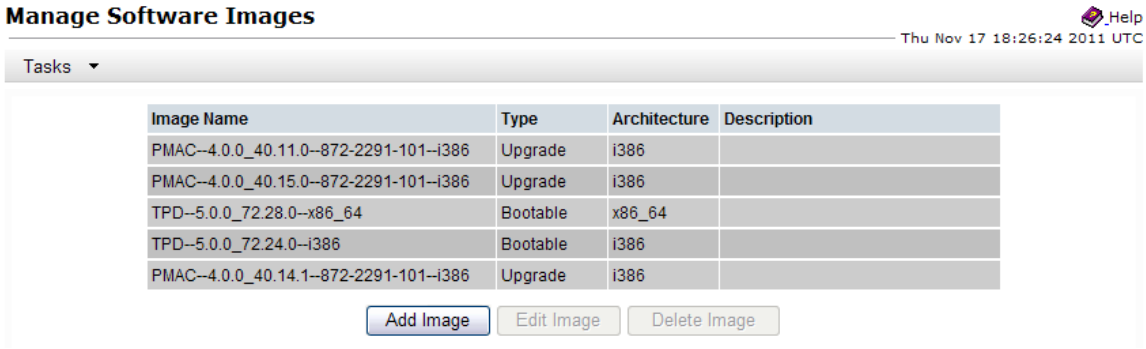
4. **PM&C GUI:** Navigate to Manage Software Images

   Navigate to **Main Menu** > **Software** > **Manage Software Images**



5. **PM&C GUI:**Add image

Press the **Add Image** button .



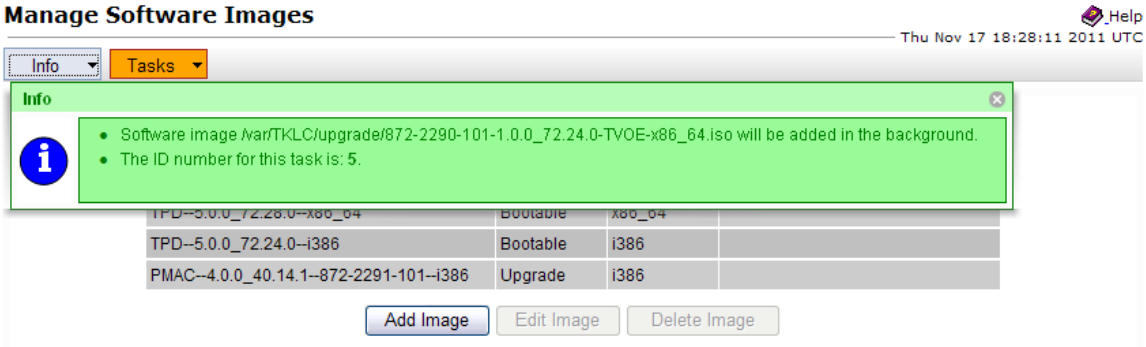
6. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:

   - If in Step 1 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".
   - If the image was supplied on a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.

   Enter an appropriate image description and press the **Add New Image** button.

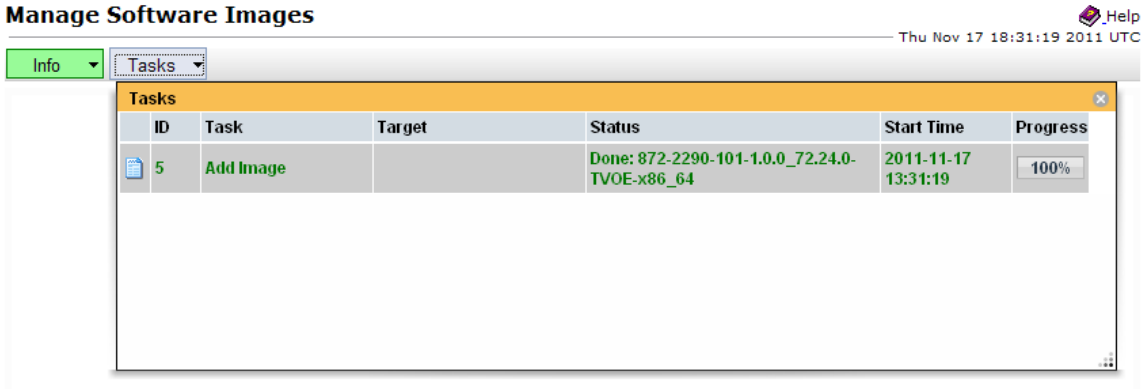
7. **PM&C GUI** Monitor the Add Image status

The `Manage Software Images` page is then redisplayed with a new background task entry in the table at the bottom of the page:



8. **PM&C GUI** Wait until the Add Image task finishes

   When the task is complete, its text changes to green and its Progress column indicates "100%". Check that the correct image name appears in the Status column:



9. **PM&C GUI:** Detach the image from the PM&C guest

   If the image was supplied on USB, return to the PM&C guest's "**Media**" tab used in Step 3, locate the image in the "**Attached Media**" list, and click its "**Detach**" button. After a pause, the image will be removed from the "**Attached Media**" list. This will release the virtual device for future use.

   Remove the USB device from the Management Server.

   Note: If there are additional ISO images to be provisioned on the PM&C, repeat the procedure with the appropriate ISO image data.

10. **PM&C:** Perform PM&C application backup.

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

   Note: The backup runs as a background task. To check the status of the background task use the PM&C GUI Task Monitor page, or issue the command "pmaccli getBgTasks". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

   Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example

provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

11. **PM&C:** Verify the Backup was successful

    Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contactMy Oracle Supportby referring to the*1.4 My Oracle Support (MOS)*of this document.

    The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

12. **PM&C:** Save the PM&C backup

    The PM&C backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server. The PM&C backup files are saved in the following directory: "/var/TKLC/smac/backup".

4.9.3 Initial Product Manufacture of Application Server

The PM&C application is capable of installing bootable software on an application server, RMS or blade server, provisioned on the PM&C through the execution of adding the RMS or the enclosure. The following procedure provides the steps necessary to IPM (either TPD or TVOE) an application server. The appropriate is required to be added to the PM&C repository for this procedure to proceed.

4.9.3.1 IPM Servers Using PM&C Application

This procedure provides the steps for installing TPD using an image from the PM&C image repository.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. **PM&C GUI:** Login

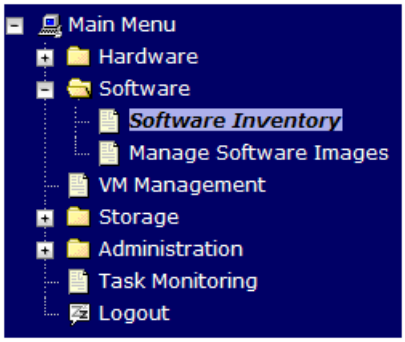
   If needed, open web browser and enter:

```
https://<pmac_management_network_ip>
```

   Login as the pmacadmin user.

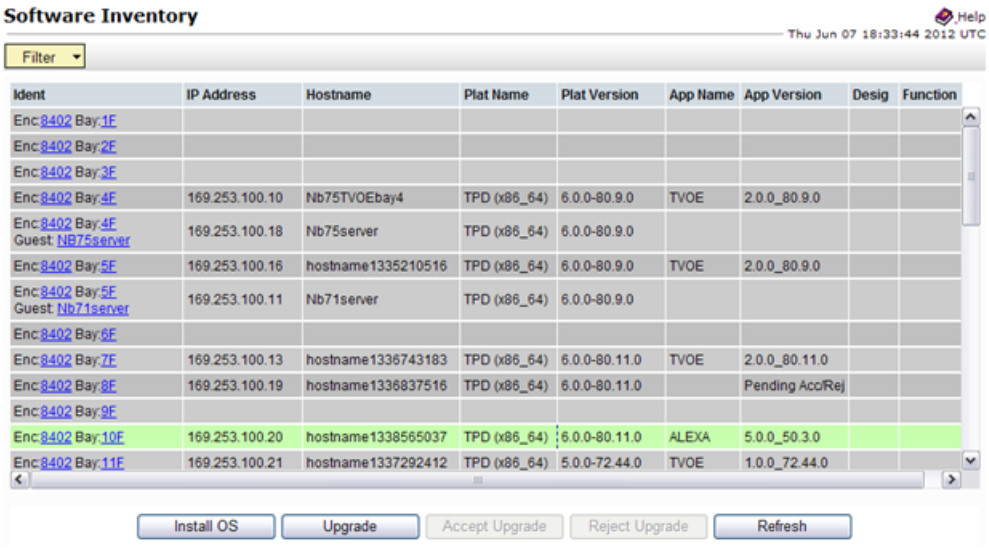
2. **PM&C GUI:** Navigate to the Software Inventory

Navigate to **Main Menu** > **Software** > **Software Inventory**.



3. **PM&C GUI:** Select Servers

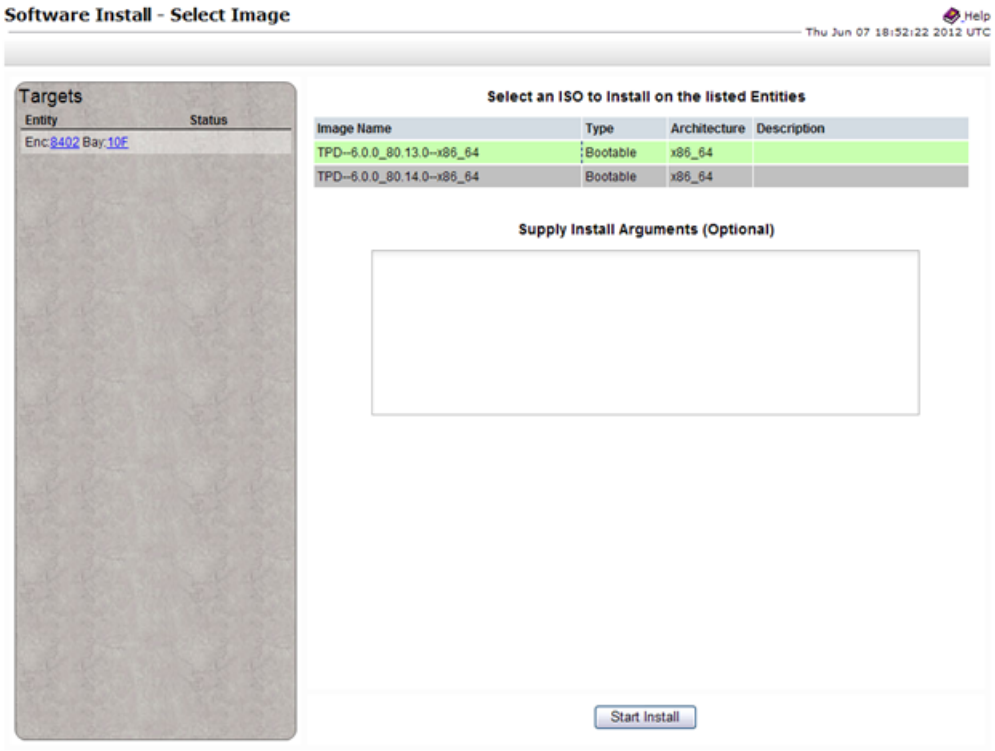
   Select the servers you want to IPM. If you want to install the same OS on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted in green.



   Press the **Install OS** button.

4. **PM&C GUI:** Select Image

   The left side of the screen displays the servers to be affected by the OS installation. From the list of available bootable images on the right side of the screen, select the OS image to install on the selected servers.



5. **PM&C GUI:** Supply Install Arguments (Optional)

   Install arguments can be supplied by entering them into the text box displayed under the list of bootable images. These arguments will be appended to the kernel line during the IPM process. If no install arguments need to be supplied for the OS being installed, leave the install arguments text box empty.

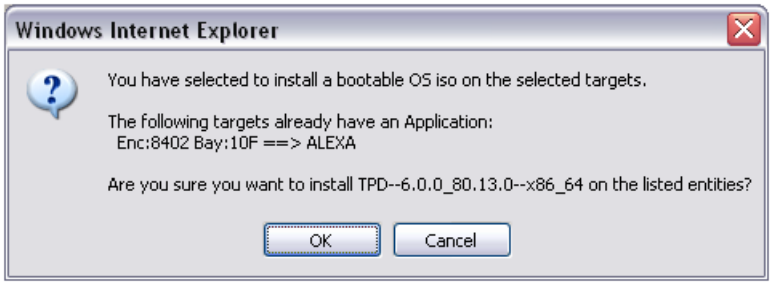
   Note: The valid arguments for a TPD IPM are listed in *TPD Initial Product Manufacture Software Installation Procedure*, E53017 and Appendix*Initial Product Manufacture of Server*.

6. **PM&C GUI:** Start Install

   Press the **Start Install** button.

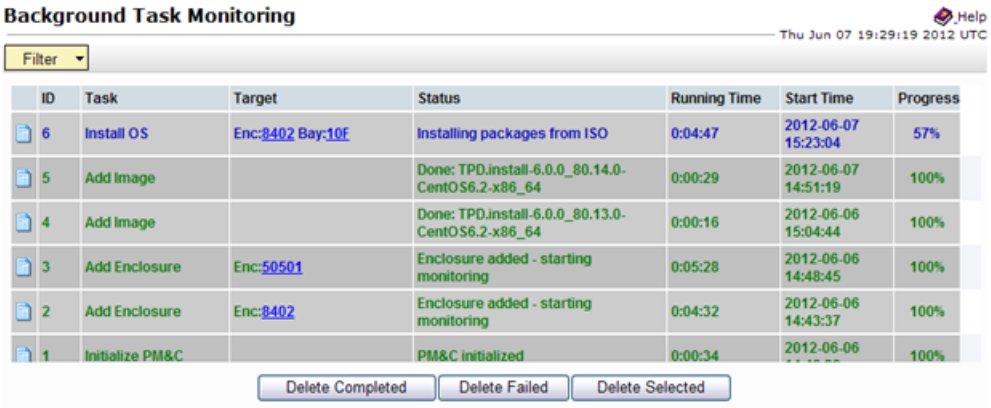
7. **PM&C GUI:** Confirm OS Install

   Press the **OK** button to proceed with the install.



8. **PM&C GUI:** Monitor Install OS

Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Install OS background task. A separate task will appear for each server affected.



When the task is complete and successful, its text will change to green and its Progress column will indicate "100%".

Note: Repeat this procedure for additional RMS servers with appropriate data.

4.9.4 TVOE Configuration on RMS Server

The application is responsible for the configuration of the TVOE. This section is a place holder for the application content. Example section content follows below.

4.9.4.1 Configure NTP on TPD based Application

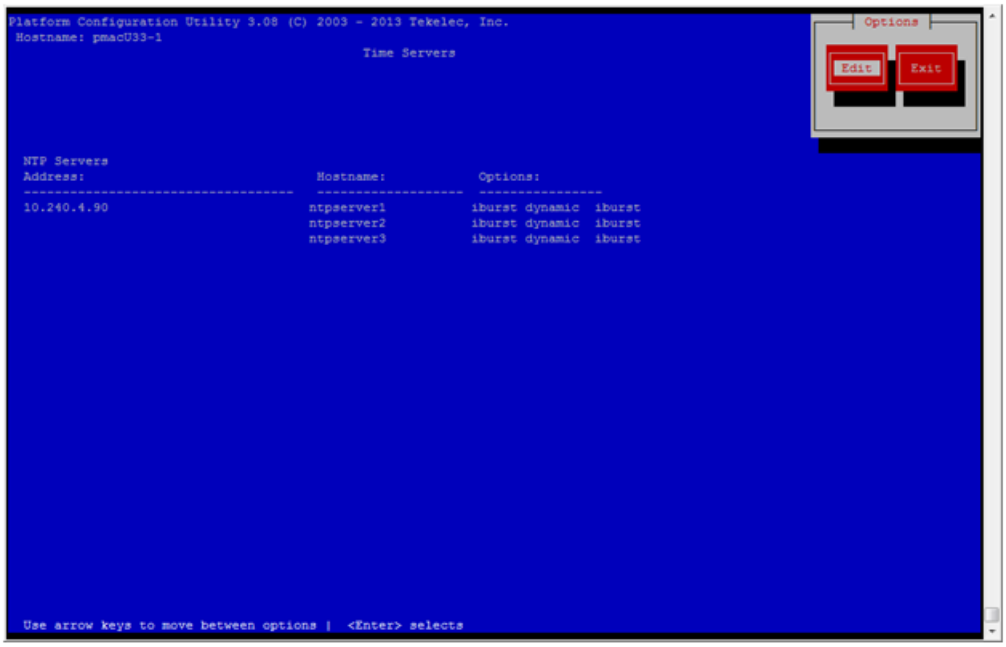
This procedure will configure NTP servers for a server based on TPD.

1. **Server:** Login as platcfg user

   Login as platcfg user on the server. The platcfg main menu will be shown.

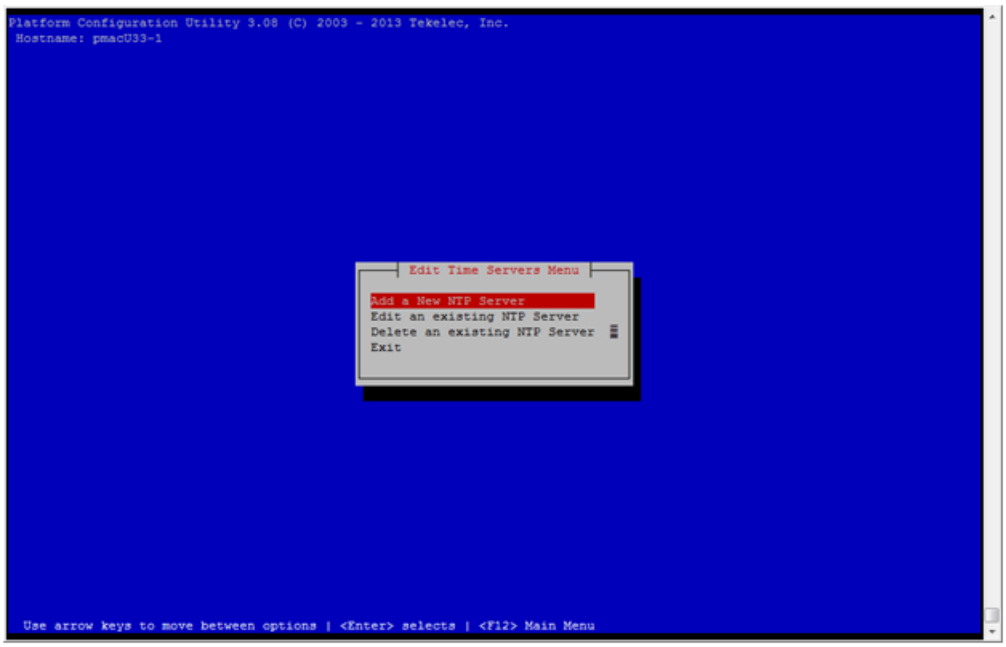
   Note: Refer to *3.4 NTP Strategy*.

2. **Server:** Navigate to Time Servers configuration page. Select the following menu options sequentially: **Network Configuration** > **NTP**. The 'Time Servers' page will now be shown, which shows the configured NTP servers and peers.



3. **Server:** Update NTP Information

   Select **Edit**. The **Edit Time Servers Menu** is displayed.



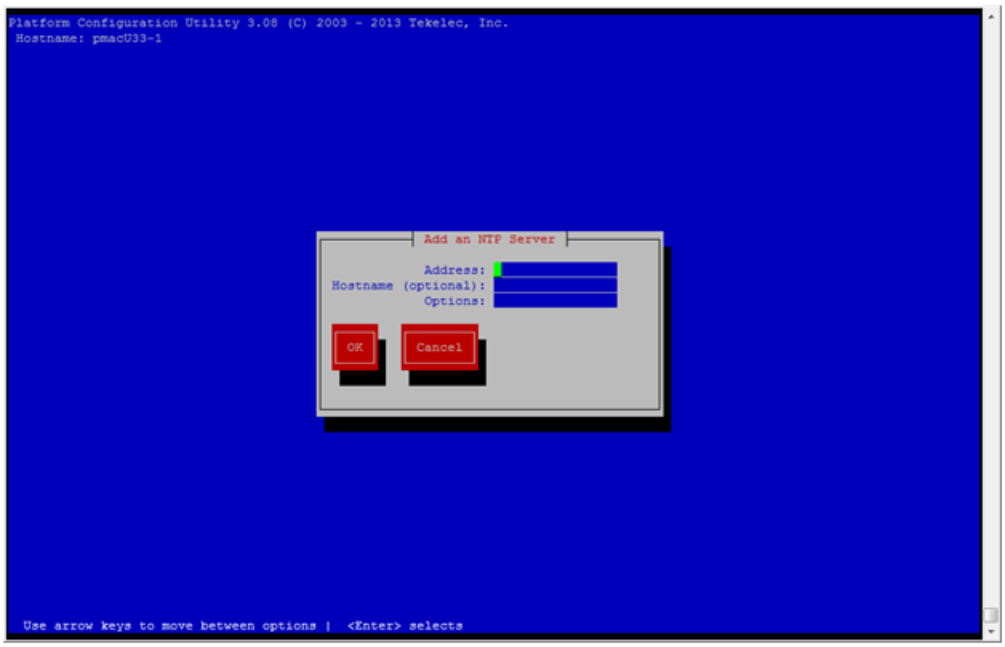
4. **Server:** Edit NTP Information

   Select the appropriate **Edit Time Servers Menu** option. When all Time Server actions are complete exit the **Edit Time Servers Menu**. Remember that (3) NTP sources are required.

   a) **Adding an NTP Server**

1. **Server:** If adding a new NTP server select **Add a New NTP Server**.

   The **Add an NTP Server** window is displayed.



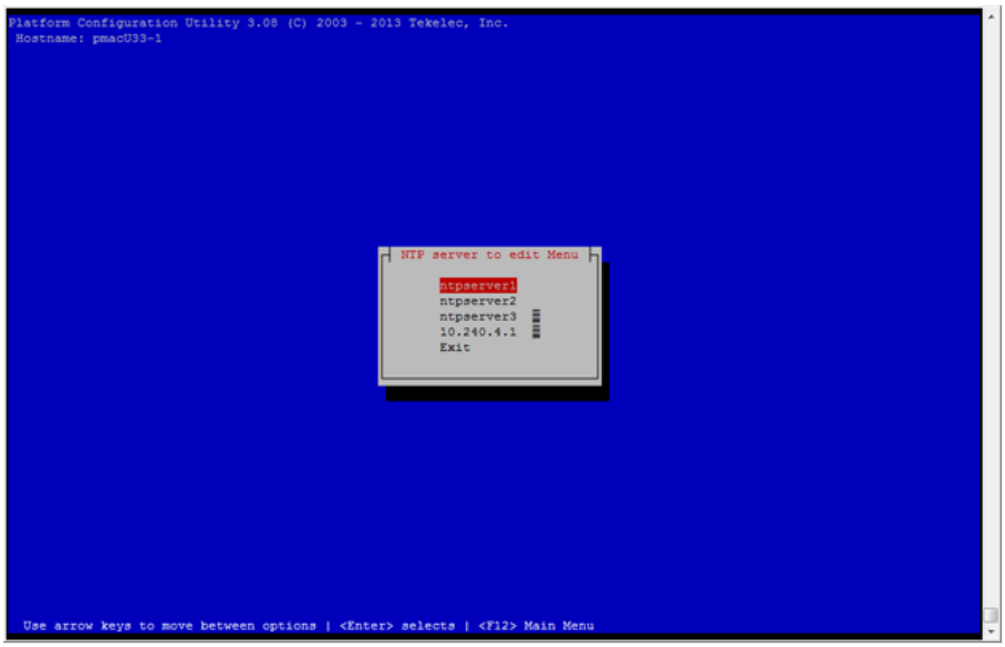
2. **Server:** Enter Appropriate data, and select **OK**

   The NTP server is added. The **Edit Time Servers Menu** is displayed.

b) **Editing an NTP Server**

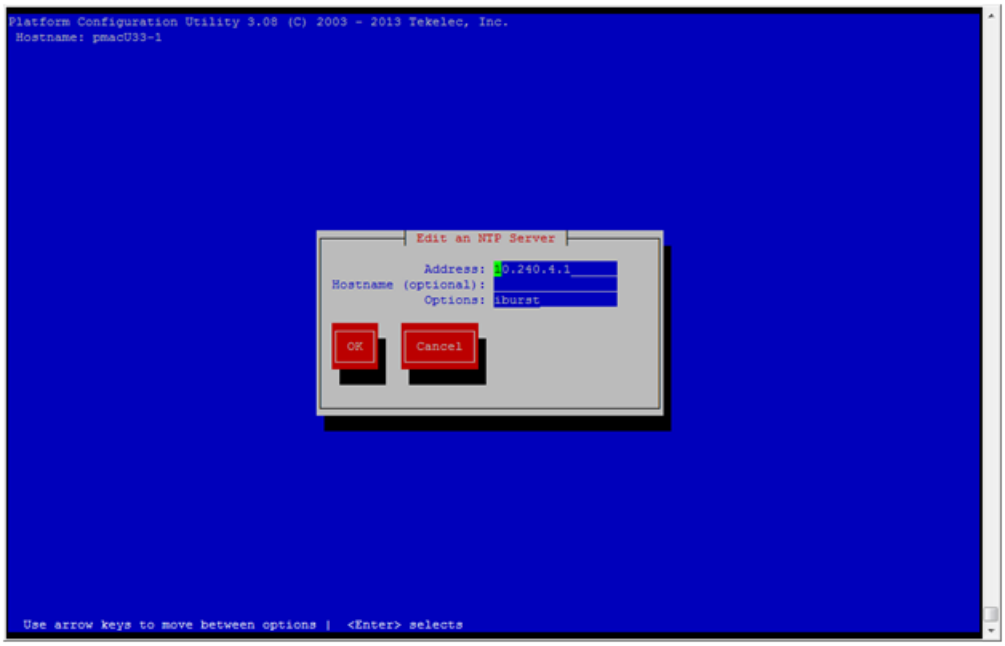
1. **Server:** If editing an existing NTP server select **Edit an existing NTP Server**.

   The **NTP Server to edit Menu** window is displayed.



2. **Server:** Select appropriate NTP server.

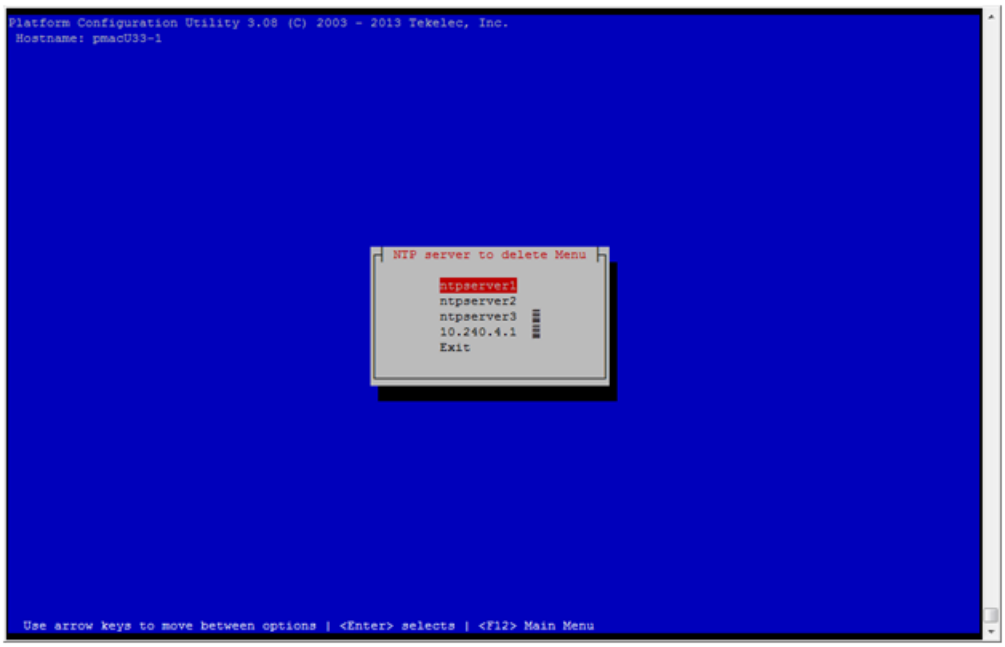
   The **Edit an NTP Server** window is displayed.



c) **Deleting an existing NTP Server**

1. **Server:** If deleting an existing NTP server, select **Delete an existing NTP Server**.

   The **NTP server to delete Menu** is displayed.

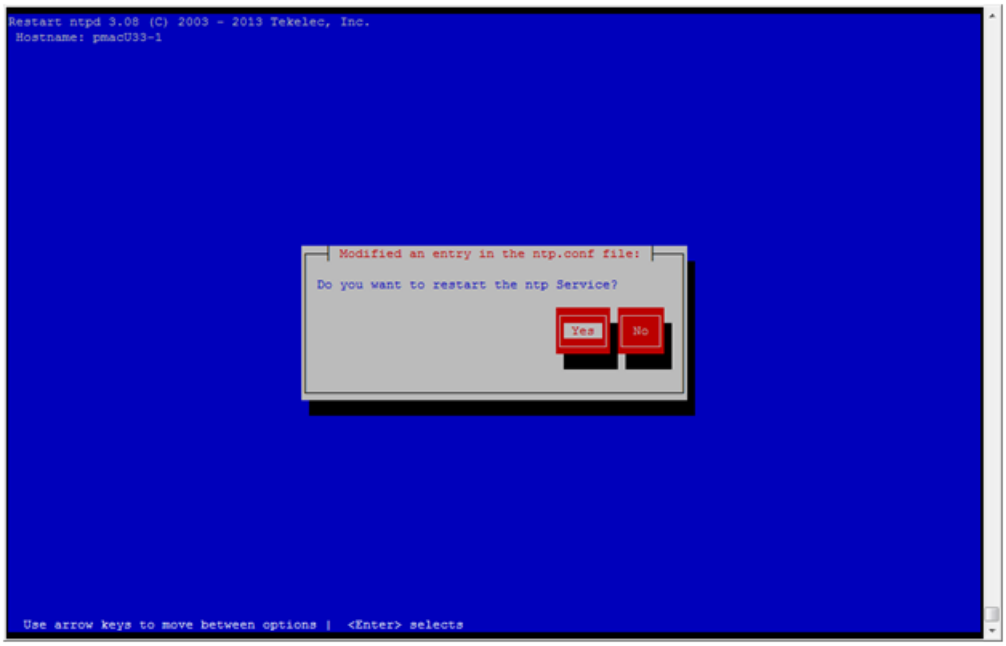


2. **Server:** Select appropriate NTP server.

   The NTP server is deleted. The **Edit Time Servers Menu** is displayed.

5. **Server:** Restart the NTP server

   Upon exit from the **Edit Time Servers Menu** the **Modified an entry in the ntp.conf file** is displayed.



6. **Server:** Exit platcfg.

Select **Exit** on each menu until platcfg has been exited.

4.9.4.2 Add SNMP trap destination on TPD-based Application

This procedure will add an SNMP trap destination to a server based on TPD. All alarm information will then be sent to the NMS located at the destination.

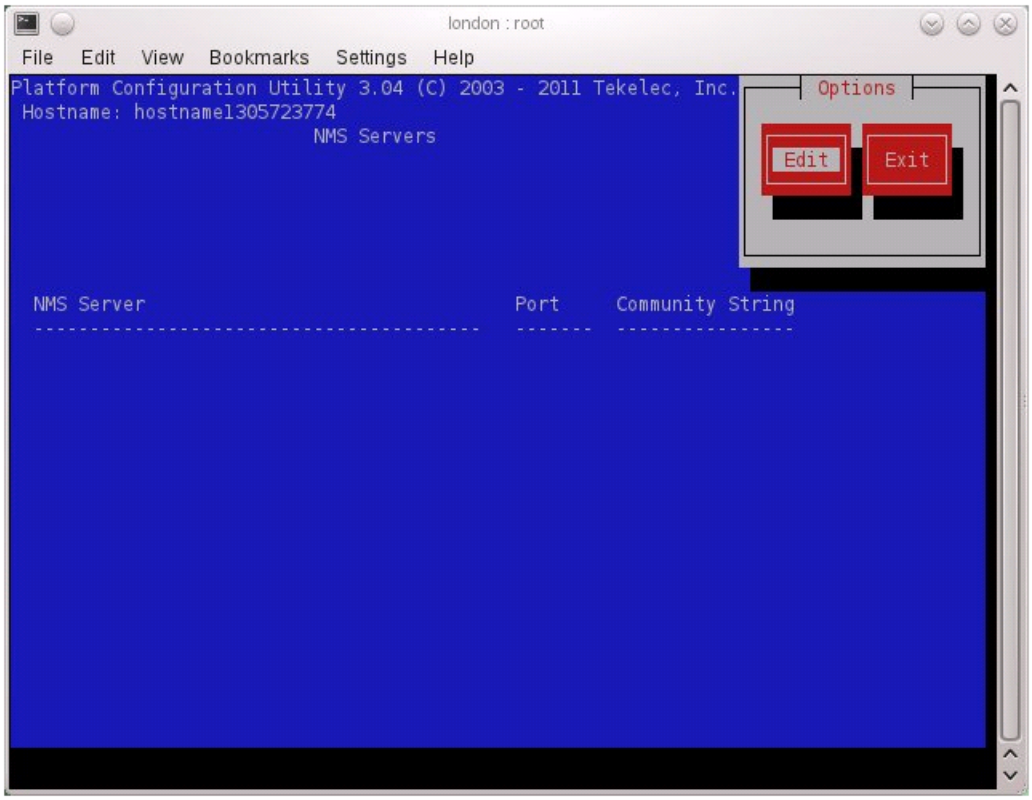
Note: Refer to *3.3 SNMP Configuration*.

1. **Server:** Login as platcfg user

   Login as platcfg user on the server. The platcfg main menu will be shown.

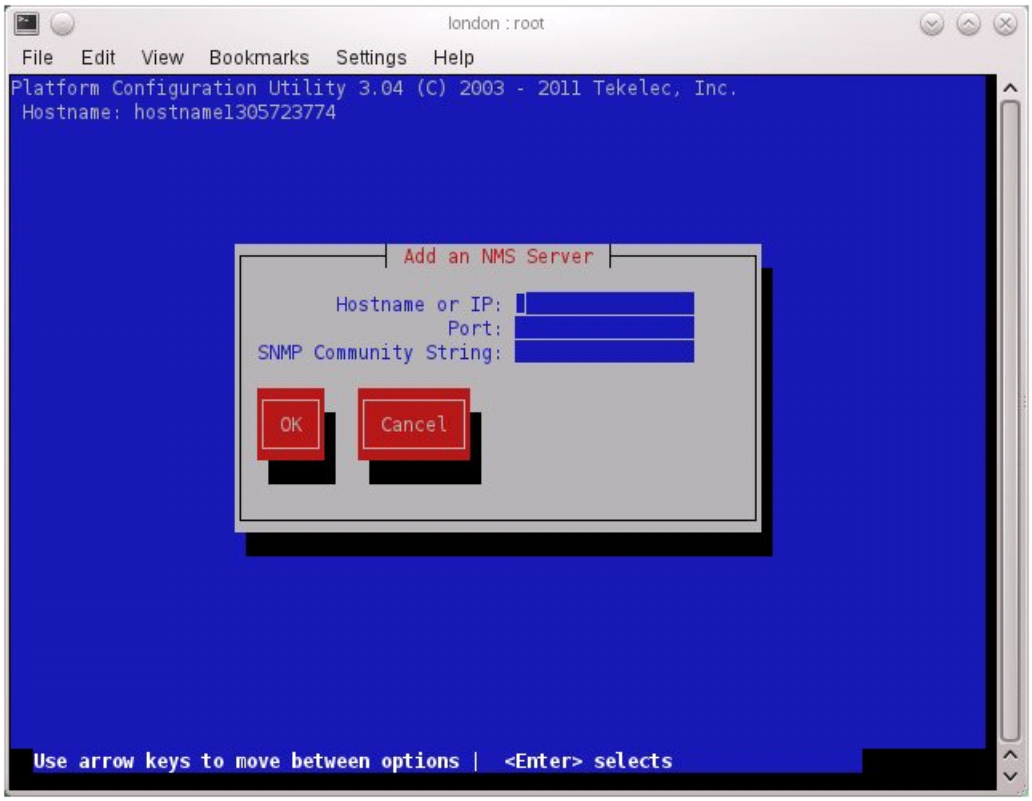
2. **Server:** Navigate to NMS server configuration page

   Select the following menu options sequentially: **Network Configuration** > **SNMP Configuration** > **NMS Configuration**. The 'NMS Servers' page will be shown, which displays all configured NMS servers for the server.



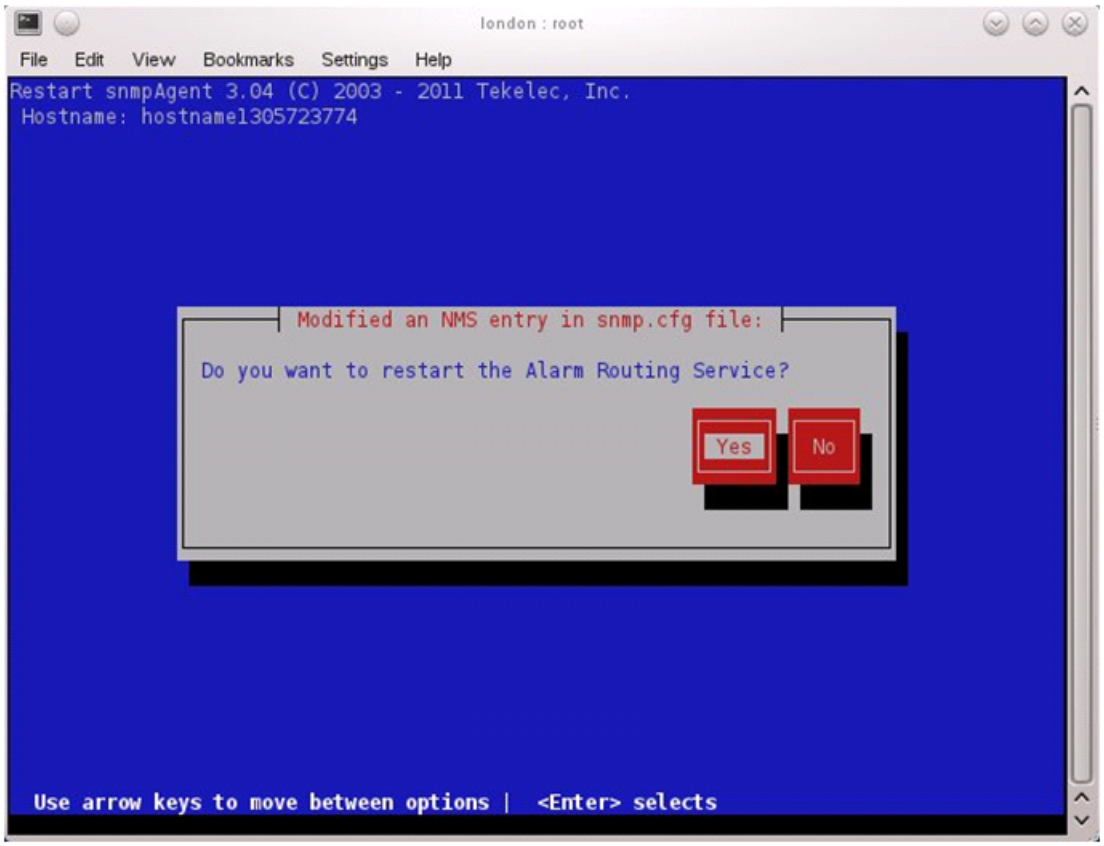
3. **Server:** Add the SNMP trap destination. Refer to section *3.3 SNMP Configuration* for SNMP Trap destination recommendations.

   Select **Edit** and then choose **Add a New NMS Server**. The 'Add an NMS Server' page will be displayed.



Complete the form by entering in all information about the SNMP trap destination. Select **OK** to finalize the configuration.

The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialog will then be presented.



Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented.

4. **Server:** Exit platcfg

   Select **Exit** on each menu until platcfg has been exited.

4.10 Install TVOE on Blade Servers

Install the TVOE Hypervisor platform on blade servers.

4.10.1 Adding ISO Images to the PM&C Image Repository

This procedure provides the steps for adding ISO images to the PM&C repository.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. Make the image available to PM&C

   There are two ways to make an image available to PM&C:

   - Attach the USB device containing the ISO image to a USB port of the Management Server.

- Use sftp to transfer the iso image to the PM&C server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
  - cd into the directory where your ISO image is located (not on the PM&C server)
  - Using sftp, connect to the PM&C management server

```
> sftp pmacftpusr@<pmac_management_network_ip>
> put <image>.iso
```

  - After the image transfer is 100% complete, close the connection

```
> quit
```

Refer to the documentation provided by application for pmacftpusr password.

2. **PM&C GUI:** Login

   Open web browser and enter:

```
https://<pmac_management_network_ip>
```

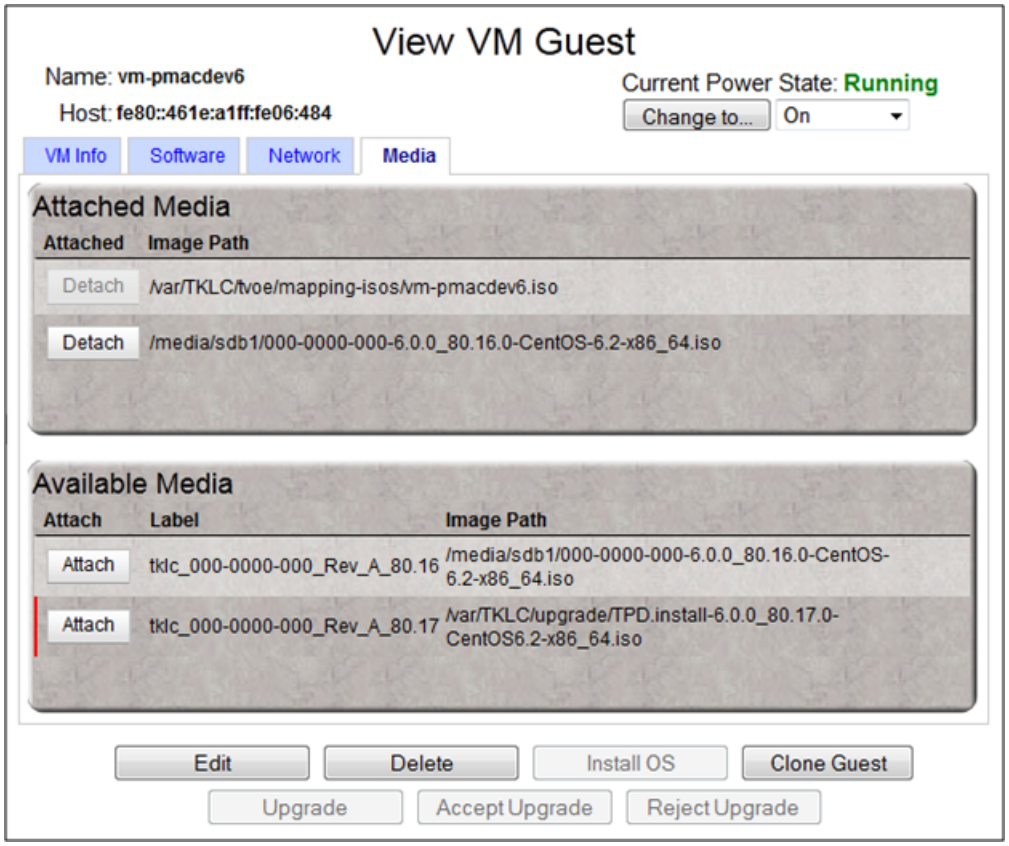
   Login as pmacadmin user.

3. **PM&C GUI:** Attach the software image to the PM&C guest

   If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a USB device, continue with this step.

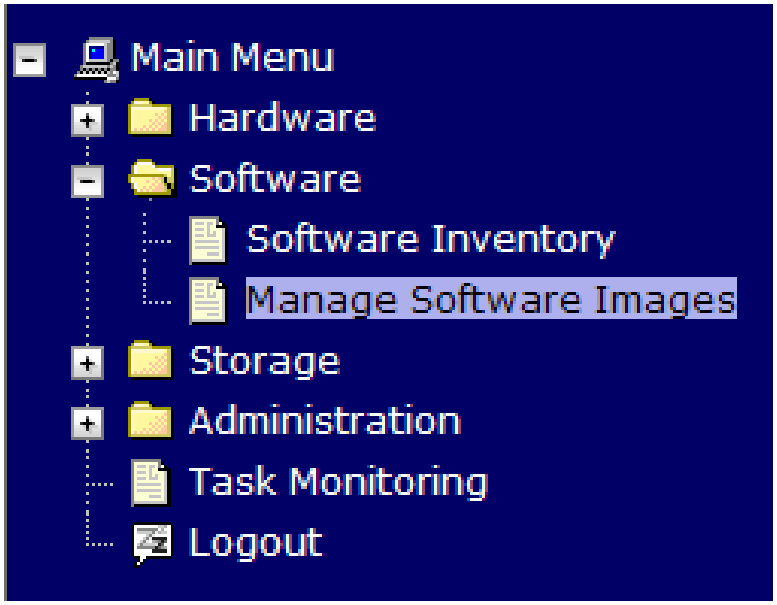
   In the PM&C GUI, nevigate to **Main Menu** > **VM Management**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.

   Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button. After a pause, the image will appear in the "**Attached Media**" list.



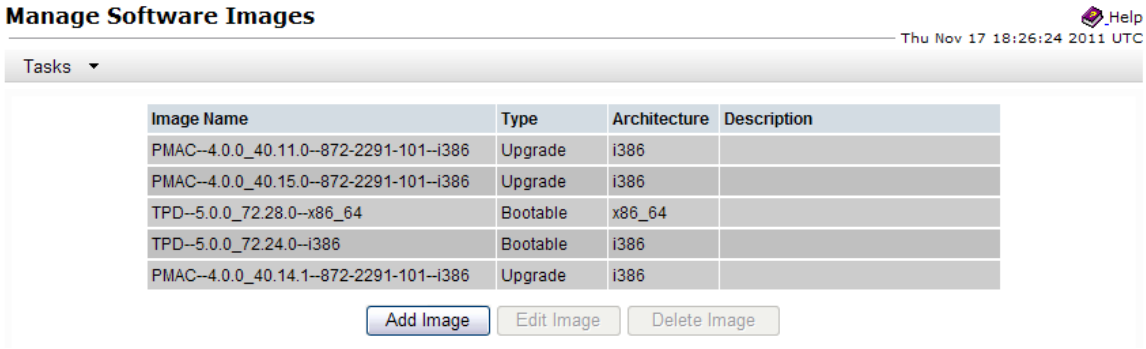
4. **PM&C GUI:** Navigate to Manage Software Images

   Navigate to **Main Menu** > **Software** > **Manage Software Images**



5. **PM&C GUI:**Add image

Press the **Add Image** button .



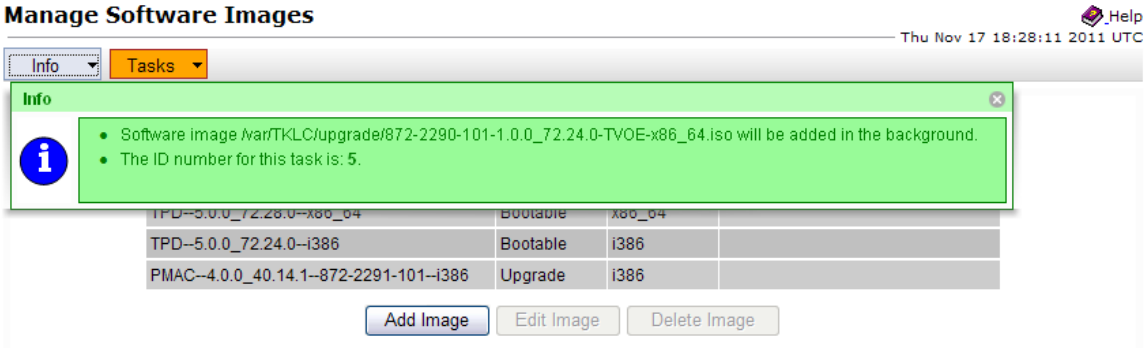
6. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:

   - If in Step 1 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".
   - If the image was supplied on a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.

   Enter an appropriate image description and press the **Add New Image** button.

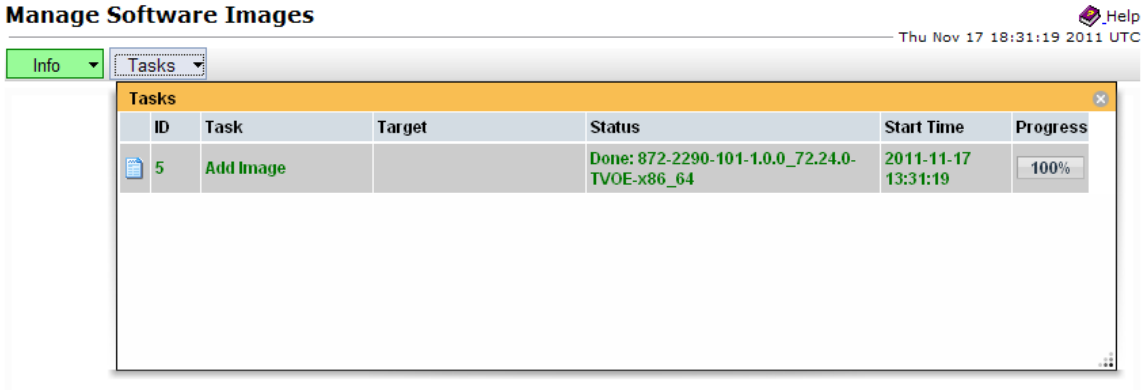
7. **PM&C GUI** Monitor the Add Image status

The `Manage Software Images` page is then redisplayed with a new background task entry in the table at the bottom of the page:



8. **PM&C GUI** Wait until the Add Image task finishes

   When the task is complete, its text changes to green and its Progress column indicates "100%". Check that the correct image name appears in the Status column:



9. **PM&C GUI:** Detach the image from the PM&C guest

   If the image was supplied on USB, return to the PM&C guest's "**Media**" tab used in Step 3, locate the image in the "**Attached Media**" list, and click its "**Detach**" button. After a pause, the image will be removed from the "**Attached Media**" list. This will release the virtual device for future use.

   Remove the USB device from the Management Server.

4.10.2 IPM Servers Using PM&C Application

This procedure provides the steps for installing TPD using an image from the PM&C image repository.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. **PM&C GUI:** Login

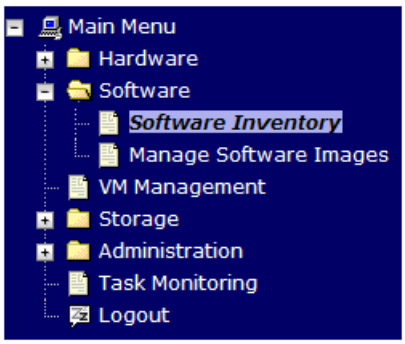
   If needed, open web browser and enter:

```
https://<pmac_management_network_ip>
```

Login as the pmacadmin user.

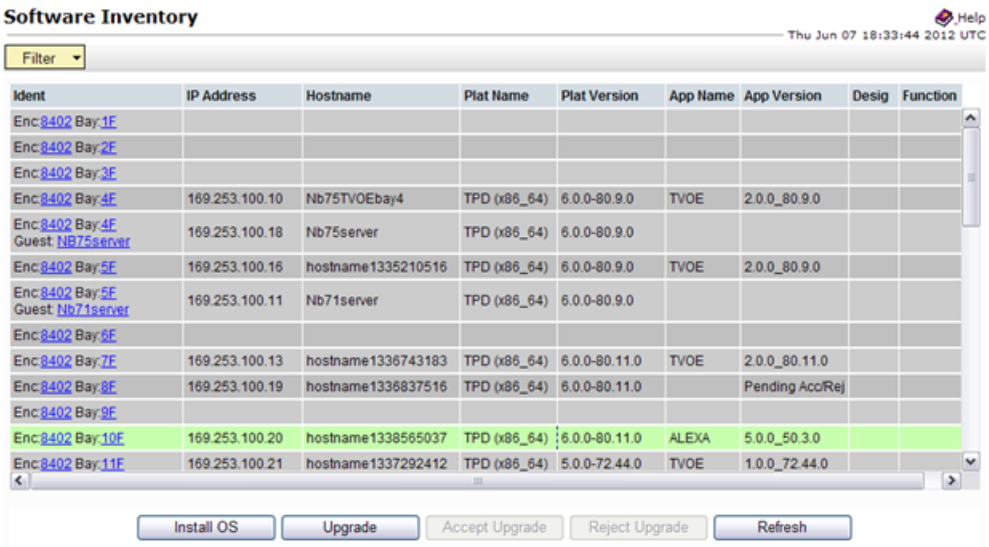
2. **PM&C GUI:** Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory**.



3. **PM&C GUI:** Select Servers

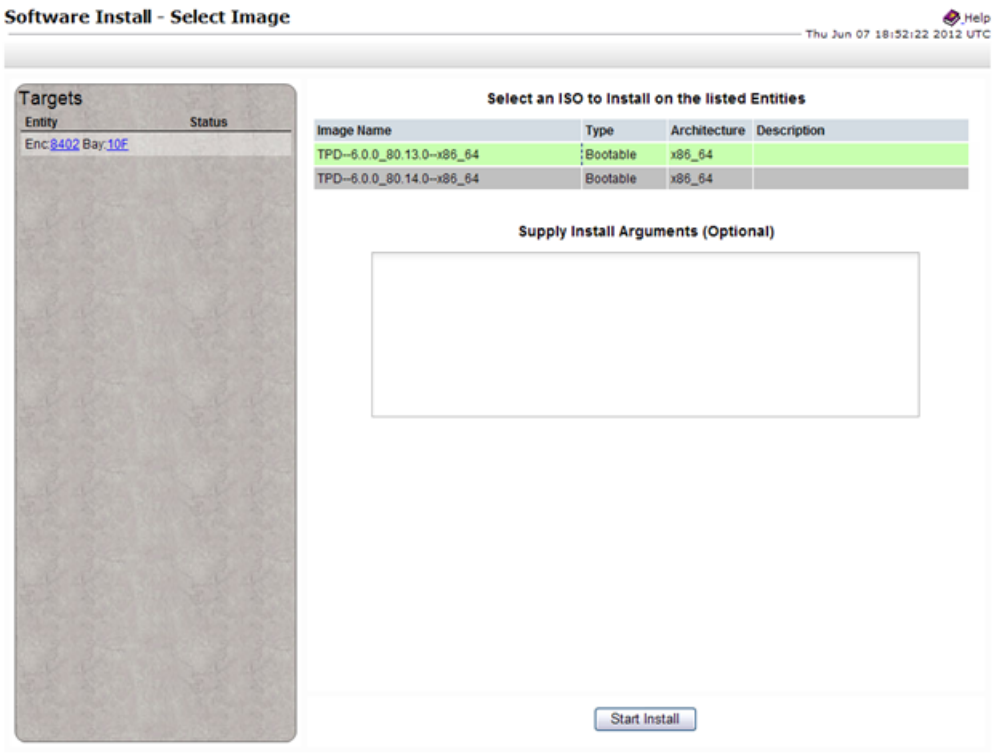
   Select the servers you want to IPM. If you want to install the same OS on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted in green.



   Press the **Install OS** button.

4. **PM&C GUI:** Select Image

   The left side of the screen displays the servers to be affected by the OS installation. From the list of available bootable images on the right side of the screen, select the OS image to install on the selected servers.



5. **PM&C GUI:** Supply Install Arguments (Optional)

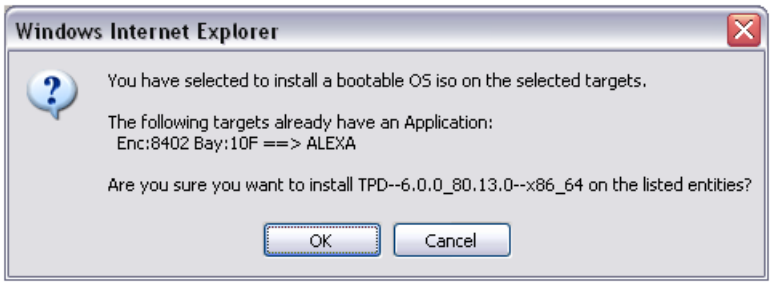
   Install arguments can be supplied by entering them into the text box displayed under the list of bootable images. These arguments will be appended to the kernel line during the IPM process. If no install arguments need to be supplied for the OS being installed, leave the install arguments text box empty.

6. **PM&C GUI:** Start Install

   Press the **Start Install** button.

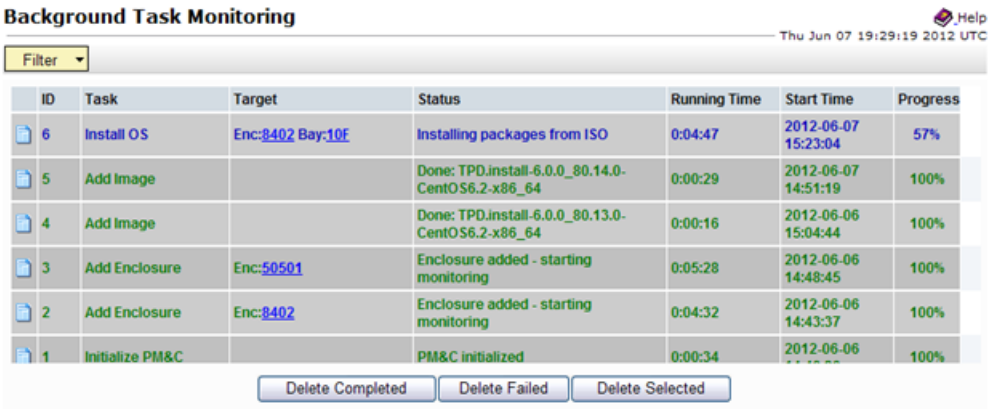
7. **PM&C GUI:** Confirm OS Install

   Press the **OK** button to proceed with the install.



8. **PM&C GUI:** Monitor Install OS

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Install OS background task. A separate task will appear for each server affected.



When the task is complete and successful, its text will change to green and its Progress column will indicate "100%".

Appendix A

NetBackup Procedures (Optional)

Topics:

A.1 Netbackup Client Install/Upgrade with nbAutoInstall

Executing this procedure will enable TPD to automatically detect when a Netbackup Client is installed and then complete TPD related tasks that are needed for effective Netbackup Client operation. With this procedure, the Netbackup Client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Note: If the customer does not have a way to push and install Netbackup Client, then use *A.2 NetBackup Client Install/Upgrade with platcfg*.

Note: It is required that this procedure is executed before the customer does the Netbackup Client install.

1. **If workaround is required**

   As directed by *1.4 My Oracle Support (MOS)*, complete required workarounds to prepare the server.

2. **Enable nbAutoInstall:**

   Execute the following command:

   ```
   $ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable
   ```

   The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly.

   At any time, the customer may now push and install a new version of Netbackup Client.

3. Return to calling procedure if applicable.

A.2 NetBackup Client Install/Upgrade with platcfg

Executing this procedure will push and install NetBackup Client using platcfg menus.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. **Application server iLO:** Login and launch the integrated remote console

   Log in to iLO in IE using password provided by application

   ```
   http://<management_server_iLO_ip>
   ```

   Click in the **Remote Console** tab and launch the **Integrated Remote Console** on the server.

   Click **Yes** if the `Security Alert` pops up.

2. **TVOE Application Server iLO:** If the application is a guest on a TVOE host: Log in with application admusr credentials. If the application is not a guest on a TVOE host continue to step 3.

   Note: On a TVOE host, If you launch the virsh console, i.e., "# **`virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**`ps -ef |grep virsh`**", then kill the existing

process "**kill -9 <PID>**". Then execute the "virsh console X" command. Your console session should now run as expected.

Login to application console using virsh, and wait until you see the login prompt:

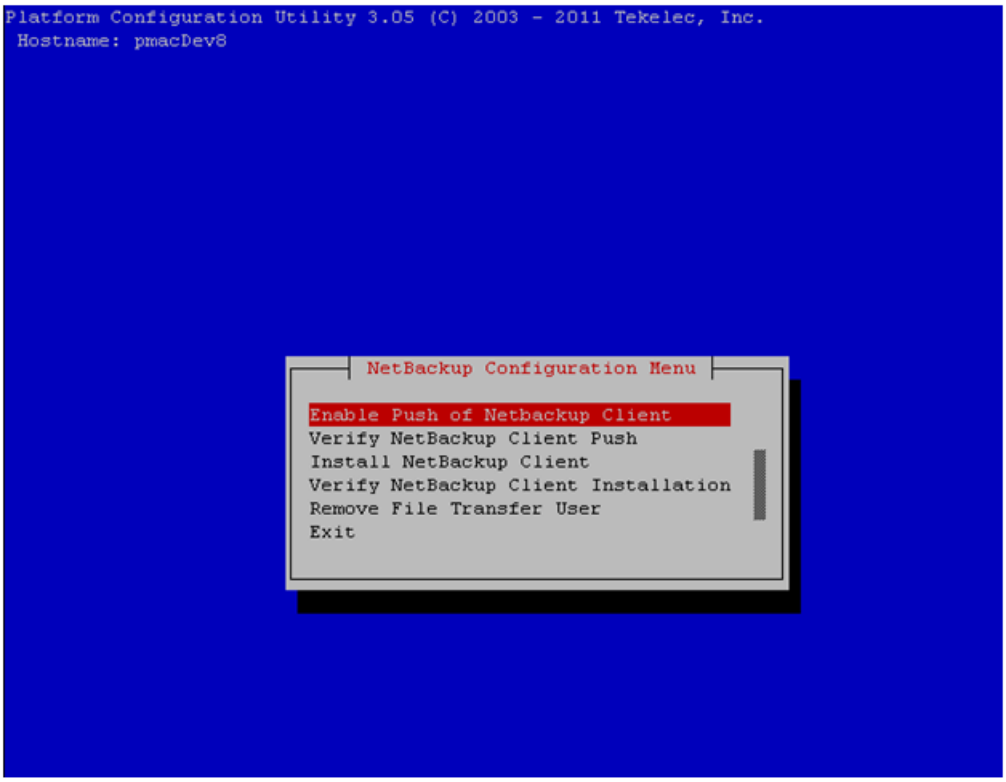
```
$ virsh
$ virsh list --all
Id Name State
----------------------------------
13 myTPD running
20 applicationGuestName running

$ virsh console applicationGuestName
[Output Removed]
Starting ntdMgr: [ OK ]
Starting atd: [ OK ]
'TPD Up' notification(s) already sent: [ OK ]
upstart: Starting tpdProvd...
upstart: tpdProvd started.
CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.14.0.x86_64 on an x86_64
applicationGuestName login:
```

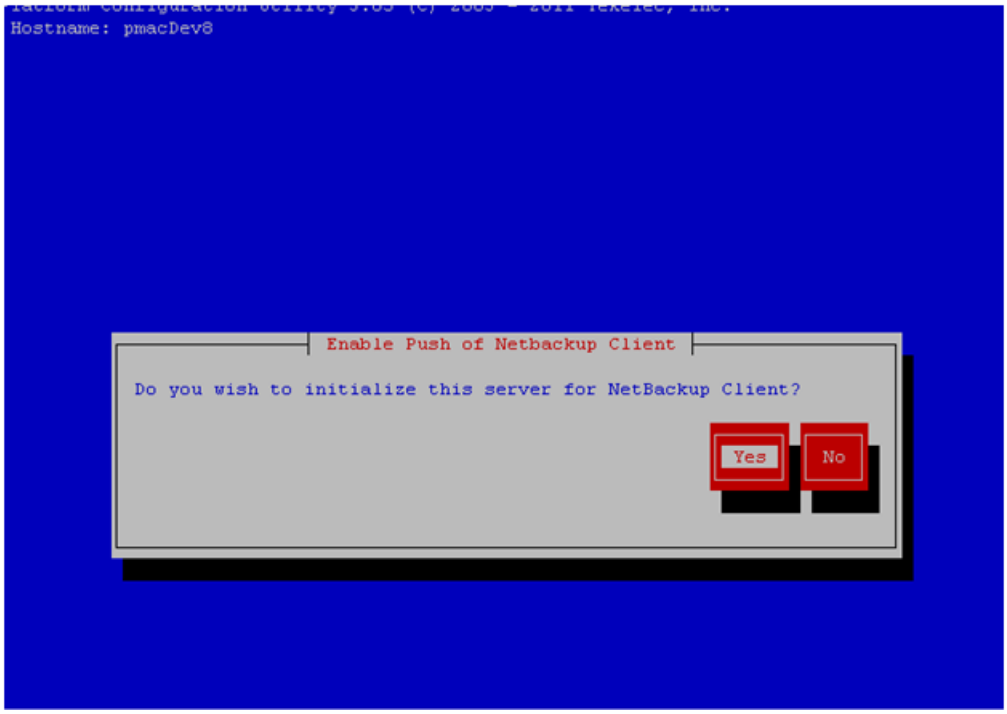
3. **Application Console**: Configure NetBackup Client on application server

```
$ sudo su - platcfg
```

Navigate to **NetBackup Configuration**

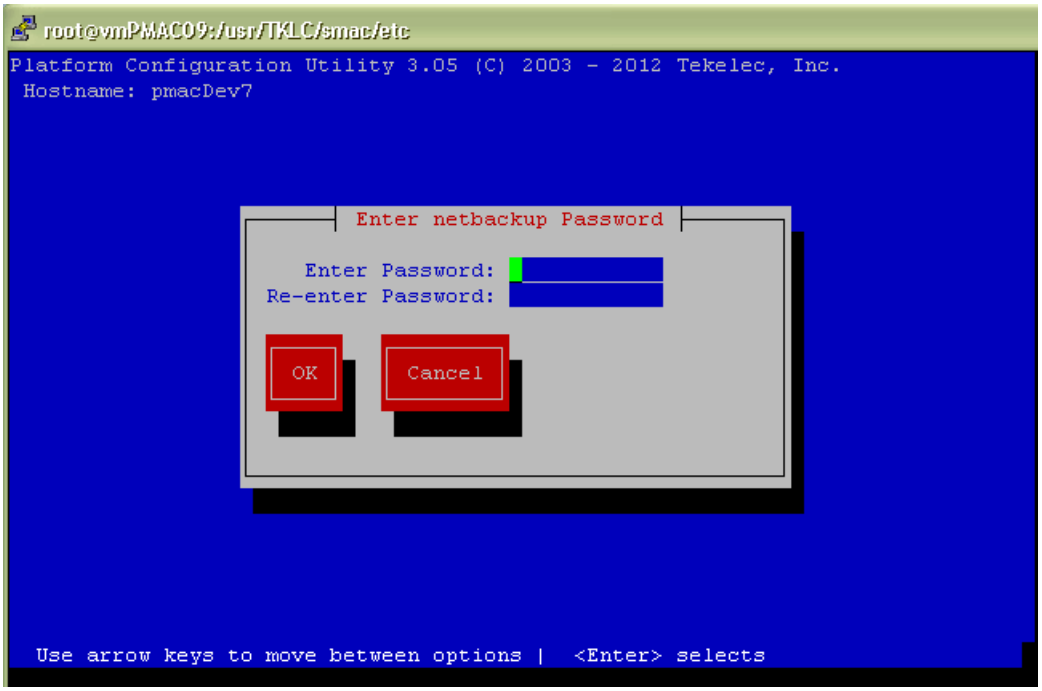


4. **Application Console**: Enable Push of NetBackup Client
   Navigate to **NetBackup Configuration** > **Enable Push of NetBackup Client**



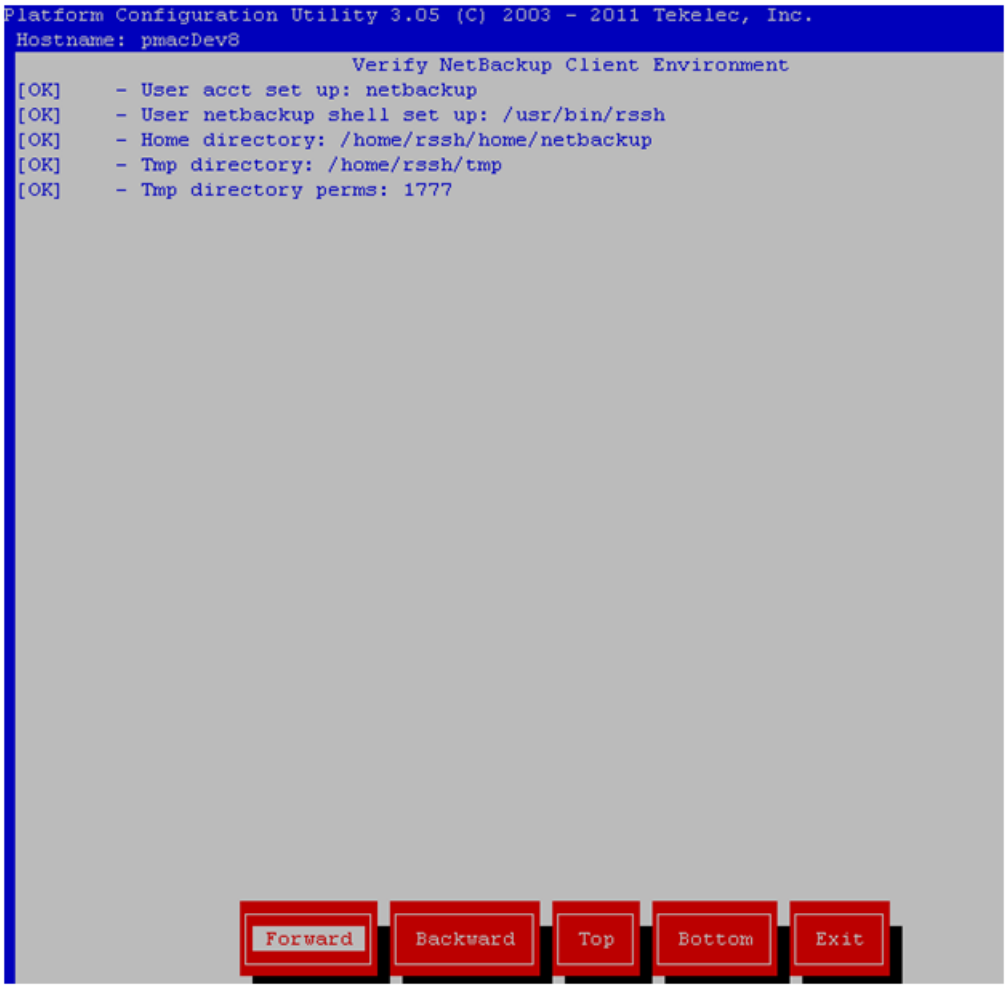
   Select **Yes** to initialize the server and enable the Netbackup client software push.

5. **Application Console** Enter NetBackup password and select OK.



6. If the version of NetBackup is 7.6.0.0 or greater, follow the instructions provided by the OSDC download for the version of NetBackup that is being pushed.
7. **Application Console**: Verify Netbackup client software push is enabled.

   Navigate to **NetBackup Configuration** > **Verify NetBackup Client Push**



   Verify list entries indicate "**OK**" for Netbackup client software environment.

   Select "**Exit**" to return to NetBackup Configuration menu.

8. **NetBackup server:** Push appropriate Netbackup client software to application server

   Note: The NetBackup server is not an application asset. Access to the NetBackup server, and location path of the NetBackup client software is under the control of the customer. Below are the steps that are required on the NetBackup server to push the NetBackup client software to the application server. These example steps assume the NetBackup server is executing in a Linux environment.

   Note: The backup server is supported by the customer, and the backup utility software provider. If this procedural STEP, executed at the backup utility server, fails to execute successfully, STOP and contact Customer Support for the backup and restore utility software provider that is being used at this site.

Log in to the NetBackup server using password provided by customer:

Navigate to the appropriate Netbackup client software path:

Note: The input below is only used as an example.

```
$ sudo cd /usr/openv/netbackup/client/Linux/6.5
```

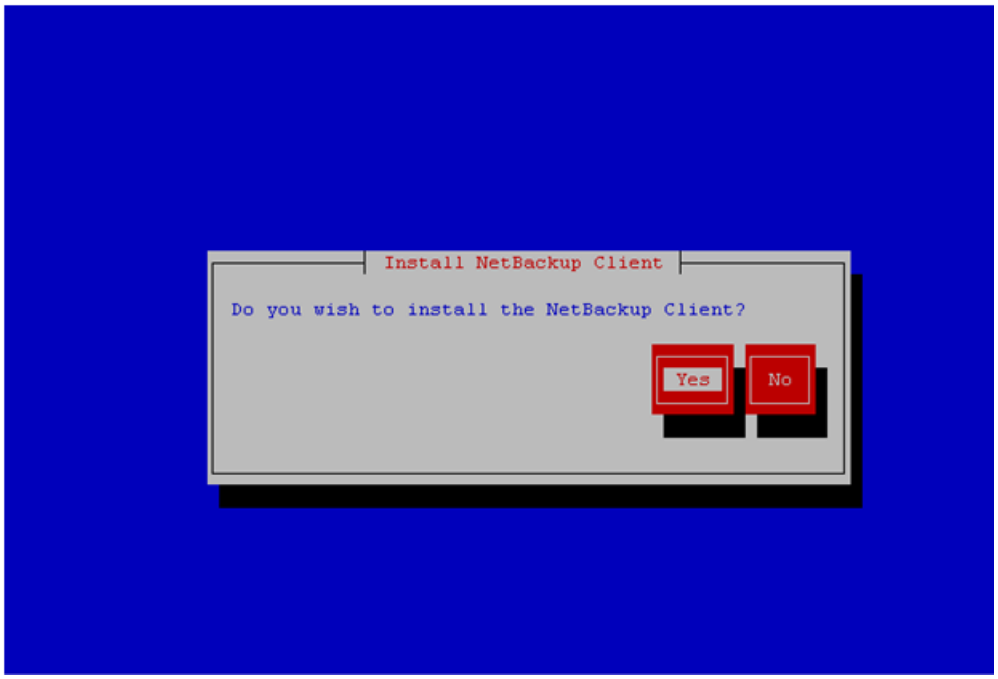
Execute the sftp_to_client NetBackup utility using the application IP address and application NetBackup user:

```
# ./sftp_to_client 10.240.17.106 netbackup
Connecting to 10.240.17.106...
Password:
You are required to change your password immediately (root enforced)
Changing password for netbackup.
(current) UNIX password:
New password:
Retype new password:

sftp completed successfully.

The root user on 10.240.17.106 must now execute the command
"sh /tmp/bp.26783/client_config [-L]". The optional argument,
"-L",is used to avoid modification of the client's current bp.conf file.
```

9. **Application Console:** Install Netbackup client software on application server.
   Navigate to **NetBackup Configuration** > **Install NetBackup Client**

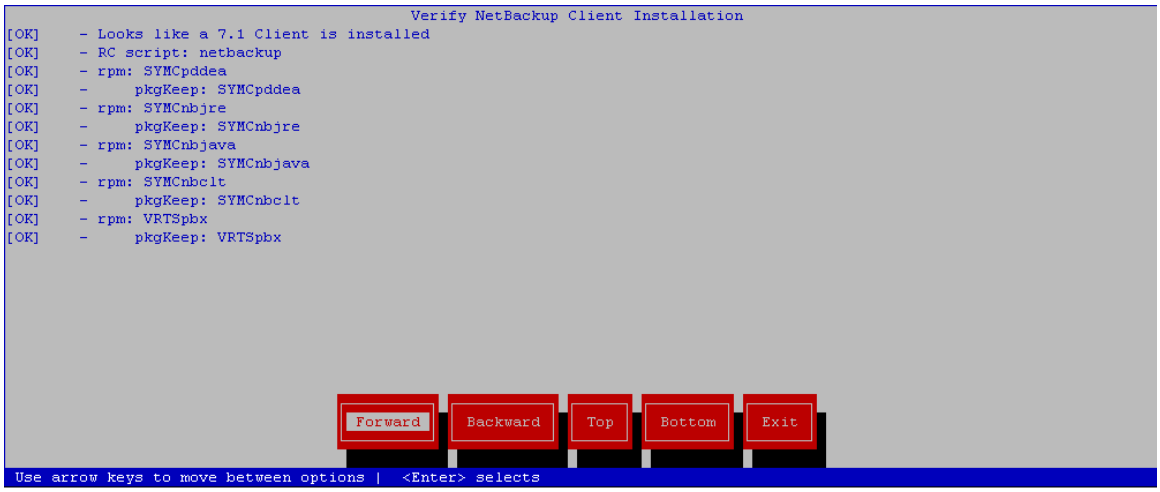


   Select **Yes** to install the Netbackup client software.

   Select "**Exit**" to return to NetBackup Configuration menu.

10. **Application Console:** Verify Netbackup client software installation on the application server.

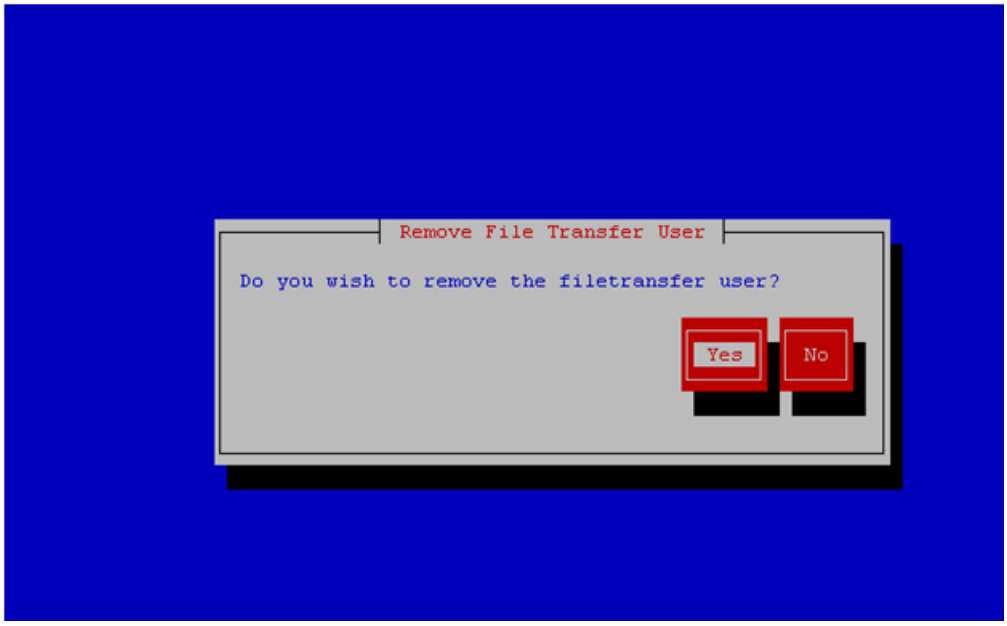
Navigate to **NetBackup Configuration** > **Verify NetBackup Client Installation**.



Verify list entries indicate "OK" for Netbackup client software installation.

Select "Exit" to return to NetBackup Configuration menu.

11. **Application Console:** Disable Netbackup client software transfer to the application server.
    Navigate to **NetBackup Configuration** > **Remove File Transfer User**



Select "Yes" to remove the NetBackup file transfer user from the application server.

12. **Application Console:** Verify that the server has been added to the `/usr/openv/netbackup/bp.conf` file

```
$ sudo cat /usr/openv/netbackup/bp.conf
CLIENT_NAME = 10.240.34.10
SERVER = NB71server
```

13. **Application server iLO:** Exit platform configuration utility (platcfg)
14. Return to calling procedure if applicable.

A.3 Create NetBackup Client Config File

This procedure will copy a NetBackup Client config file into the appropriate location on the TPD based application server. This config file will allow a customer to install previously unsupported versions of NetBackup Client by providing necessary information to TPD.

The contents of the config file should be provided by My Oracle Support. Contact *1.4 My Oracle Support (MOS)* if you are attempting to install an unsupported version of NetBackup Client.

1. **Server:** Create NetBackup Client Config File

   Create the NetBackup Client config file on the server using the contents that were previously determined. The config file should be placed in the /usr/TKLC/plat/etc/netbackup/profiles directory and should follow the following naming conventions:

   NB$ver.conf

   Where $ver is the client version number with the periods removed. For the 7.5 client the value of $ver would be 75 and the full path to the file would be:

   `/usr/TKLC/plat/etc/netbackup/profiles/NB75.conf`

   Note: The config files must start with "NB" and must have a suffix of ".conf". The server is now capable of installing the corresponding NetBackup Client.

   The server is now capable of installing the corresponding NetBackup Client.

2. **Server:** Create NetBackup Client config file script.

   Create the NetBackup Client config script file on the server using the contents that were previously determined. The config script file should be placed in the /usr/TKLC/plat/etc/netbackup/scripts directory. The name of the NetBackup Client config script file should be determined from the contents of the NetBackup Client config file. As an example for the NetBackup 7.5 client the following is applicable:

   NetBackup Client config:

```
/usr/TKLC/plat/etc/netbackup/profiles/NB75.conf
```

   NetBackup Client config script:

```
/usr/TKLC/plat/etc/netbackup/scripts/NB75
```

A.4 Configure PM&C Application Guest NetBackup Virtual Disk

1. **PM&C GUI:** Determine if the PM&C application guest is configured with a "NetBackup" virtual disk.

   Navigate to "**Virtual Machine Management**" view and select the PM&C application guest from the "**VM Entities**" list.

2. **PM&C GUI:** Determine if the "Virtual Disks" list contains the "NetBackup" device.

   If the "NetBackup" device exists for the PM&C application guest then return to the procedure that invoked this procedure. Otherwise continue with this procedure.

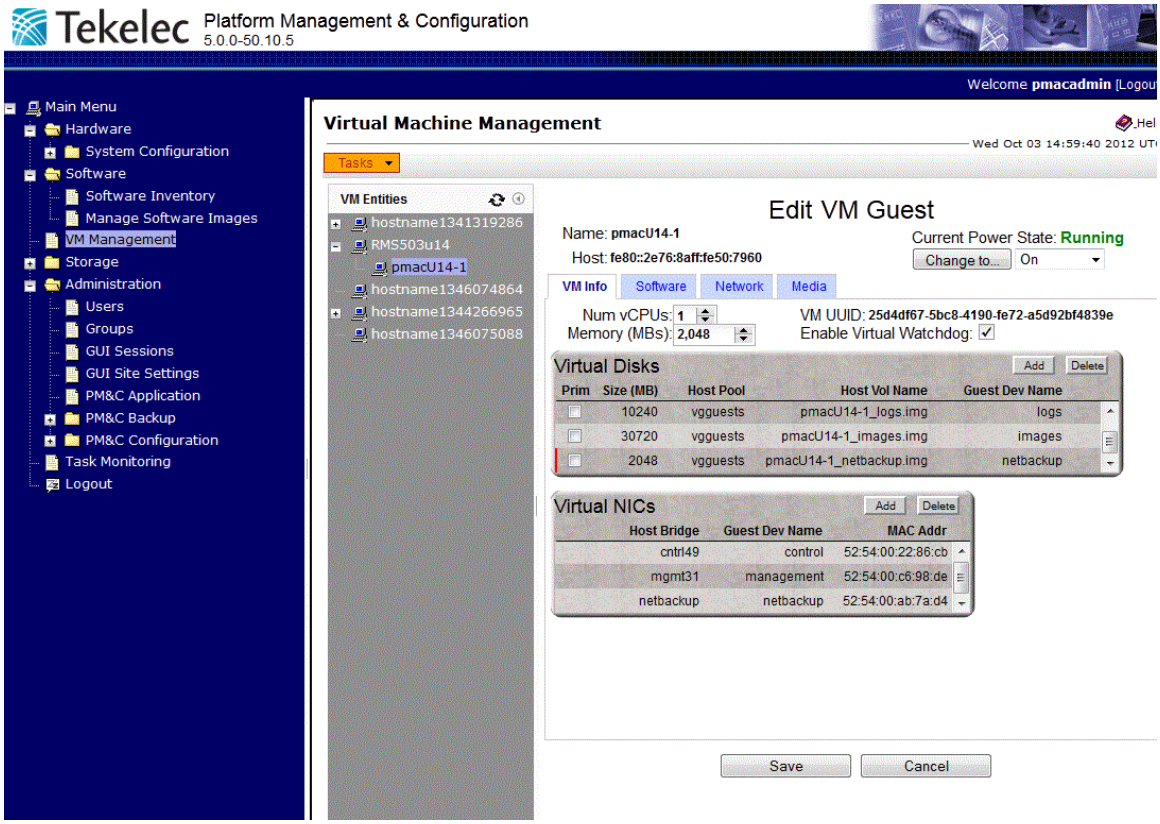
3. **PM&C GUI:** Edit the PM&C application guest to add the "NetBackup" virtual disk.

   Click "Edit" and enter the following data for the new NetBackup virtual disk.

   - Size (MB): "2048"
   - Host Pool: "vgguests"
   - Host Vol Name: "<pmacGuestName>_netbackup.img"
   - Guest Dev Name: "netbackup"

   Note: The "Guest Dev Name" must be set to "netbackup" for the PM&C application to mount the appropriate host device. The <pmacGuestName> variable should be set to this PM&C guest's name to create a unique volume name on the TVOE host of the PM&C.

4. **PM&C GUI:**Verify the new NetBackup virtual disk data and save.



5. **PM&C GUI:** Confirm the PM&C application guest edit.

   A confirmation dialog will be presented with the message, "Changes to the PMAC guest: <pmacGuestName> will not take effect until after the next power cycle. Do you wish to continue?". Click "OK" to continue.

6. **PM&C GUI:** Confirm the Edit VM Guest task has completed successfully.

   Navigate to the Background Task Monitoring view. Confirm that the guest edit task has completed successfully.

7. **TVOE Management server iLO:** Shutdown the PM&C application guest.

   Note: In order to configure the PM&C application with the new NetBackup virtual disk the PM&C application guest needs to be shut down and restarted. Refer to *PM&C Incremental Upgrade, Release 5.7 and 6.0*, E54387, Appendix O, "Shutdown PM&C 5.5 or Later Guest."

8. **TVOE Management Server iLO:** Start the PM&C application guest.

   Note: To configure the PM&C application with the new netbackup virtual disk, the PM&C application guest needs to be shut down and restarted.

   Using virsh utility on TVOE host of PM&C guest, start the PM&C guest. Query the list of guests until the PM&C guest is "running".

```
$ sudo /usr/bin/virsh
virsh # list --all
Id Name State
----------------------------------
20 pmacU14-1 shut off

virsh # start pmacU14-1
Domain pmacU14-1 started

virsh # list --all
Id Name State
----------------------------------
20 pmacU14-1 running
```

9. Return to the procedure that invoked this procedure.

A.5 Application NetBackup Client Install/Upgrade Procedures

NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite is for the purpose of supporting Disaster Recovery at the customer site. This procedure provides instructions for installing or upgrading the Netbackup client software on an application server.

Note: Platform 7.0.0 only supports NetBackup 7.1 and NetBackup 7.5 clients, while Platform 7.0.1 only supports NetBackup 7.1, NetBackup 7.5, and NetBackup 7.6 clients. If the NetBackup Client that is being installed is not supported, contact customer support for guidance on creating a config file that will allow for install of unknown NetBackup Clients. *A.3 Create NetBackup Client Config File* can be used once the contents of the config are known.

Note: Failure to install the NetBackup Client properly (i.e., by neglecting to execute this procedure) may result in the NetBackup Client being deleted during a Oracle software upgrade.

1. **Choose NetBackup Client Install Path**

   There are two different ways to install NetBackup Client. The following is a guide to which method to use:

   - If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools then use *A.1 Netbackup Client Install/Upgrade with nbAutoInstall*. This is not common and if the answer to the previous question is not known then do not use *A.1 Netbackup Client Install/Upgrade with nbAutoInstall*.
   - If you don't use *A.1 Netbackup Client Install/Upgrade with nbAutoInstall*, use *A.2 NetBackup Client Install/Upgrade with platcfg*.

   Chosen Procedure: _____

2. **Execute the procedure chosen in Step 1**
3. **Application Console:** Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias.

   Note: If NetBackup Client has successfully been installed then you can find the NetBackup server's hostname in the "/usr/openv/netbackup/bp.conf" file. It will be identified by the "SERVER" configuration parameter as is shown in the following output:

   List NetBackup servers hostname:

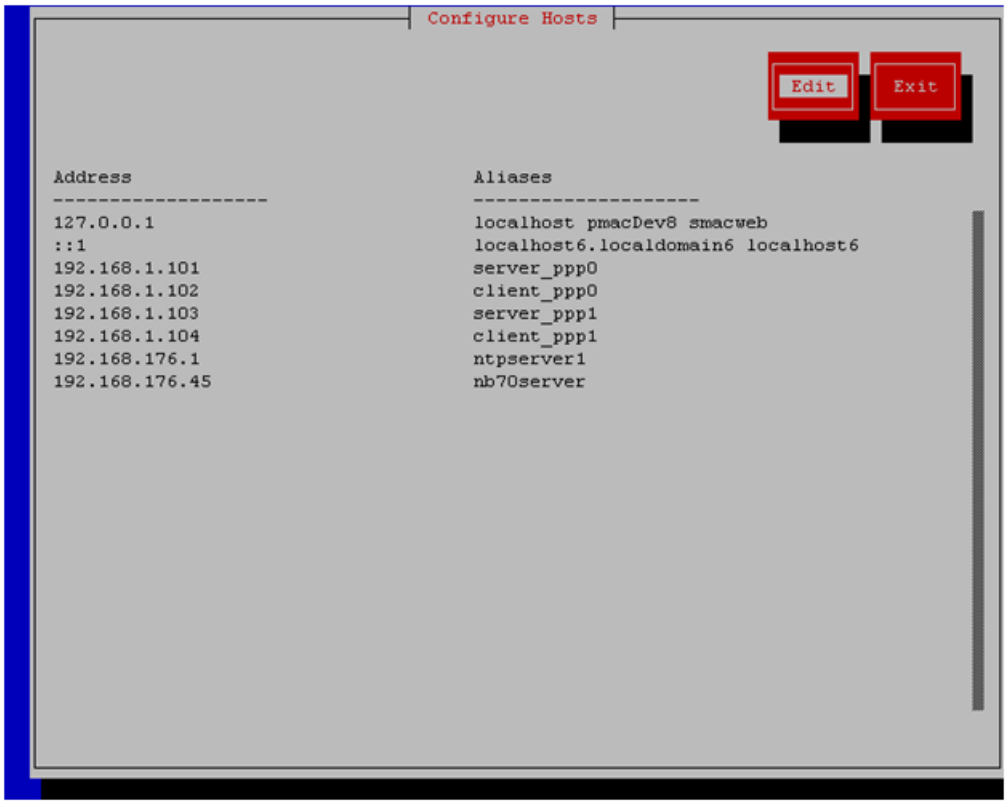
```
$ sudo cat /usr/openv/netbackup/bp.conf
SERVER = nb70server
CLIENT_NAME = pmacDev8
```

   Note: : In the case of nbAutoInstall NetBackup Client may not yet be installed. For this situation the "/usr/openv/netbackup/bp.conf" cannot be used to find the NetBackup server alias.

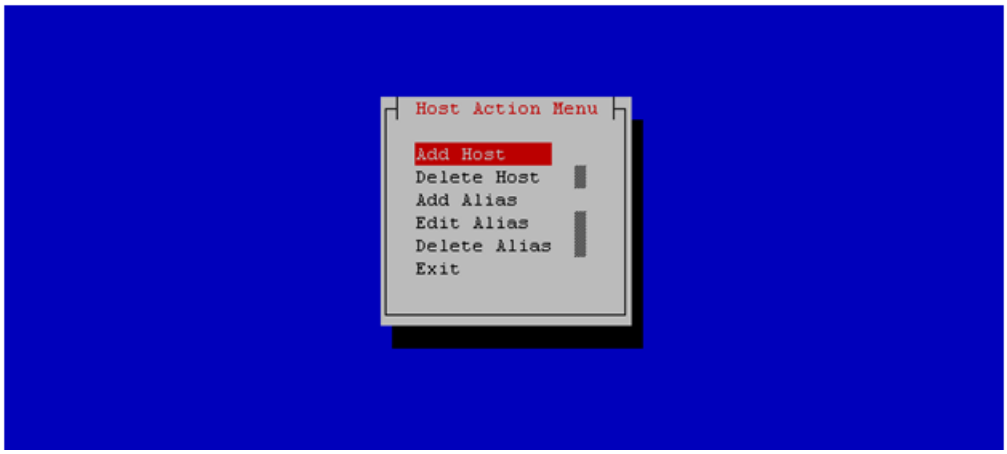
   Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
$ sudo su - platcfg
```

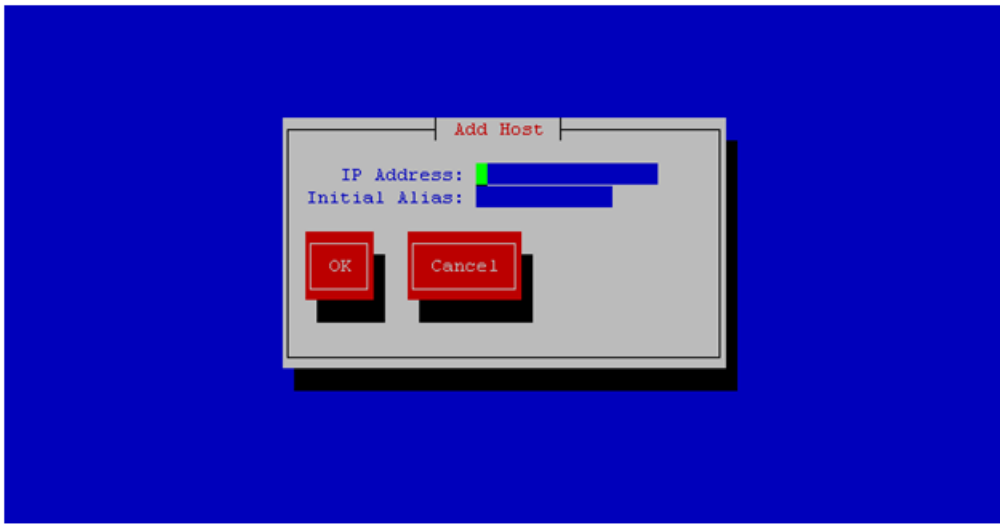
   Navigate to **Network Configuration** > **Modify Hosts File**



Select **Edit**, the Host Action Menu will be displayed.



Select "**Add Host**", and enter the appropriate data



Select "**OK**", confirm the host alias add, and exit Platform Configuration Utility

4. **Application Console:** Create a link for the application provided NetBackup client notify scripts to path on application server where NetBackup expects to find them.

   Note: Link notify scripts from appropriate path on application server for given application.

```
$ sudo mkdir -p /usr/openv/netbackup/bin/
$ sudo ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify
$ sudo ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify
```

5. **Application Console**: Netbackup client software installation complete; if applicable return to calling procedure.

Appendix B

Worksheet: netConfig Repository

Topics:

B.1 Worksheet: netConfig Repository

Copy the following table as needed for each additional enclosure switch (6120XG, 6125G, 6125XG, or 3020):

Variable	Value
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<io_bay>	
<OA1_enX_ip_address>	X= the enclosure #
<OA_password>	
<FW_image>	

Appendix C

Initial Product Manufacture of Server

Topics:

C.1 Setting Server's CMOS Clock

The date and time in the server's CMOS clock must be set accurately before running the IPM procedure. There are a number of different ways to set the server's CMOS clock.

Note: The IPM installation process managed by PM&C for blade servers automatically sets the server's CMOS clock, so there is no need to set the server CMOS clock when using PM&C.

C.2 Configure the RMS Server BIOS Settings

C.2.1 Configuring HP DL360/380 Servers

Follow these steps to configure HP DL360/380 server BIOS settings for supported models of G6, G7, Gen8, and Gen9 servers.

1. Reboot the server and after the server is powered on, press the <F9> key when prompted to access the ROM-Based Setup Utility.

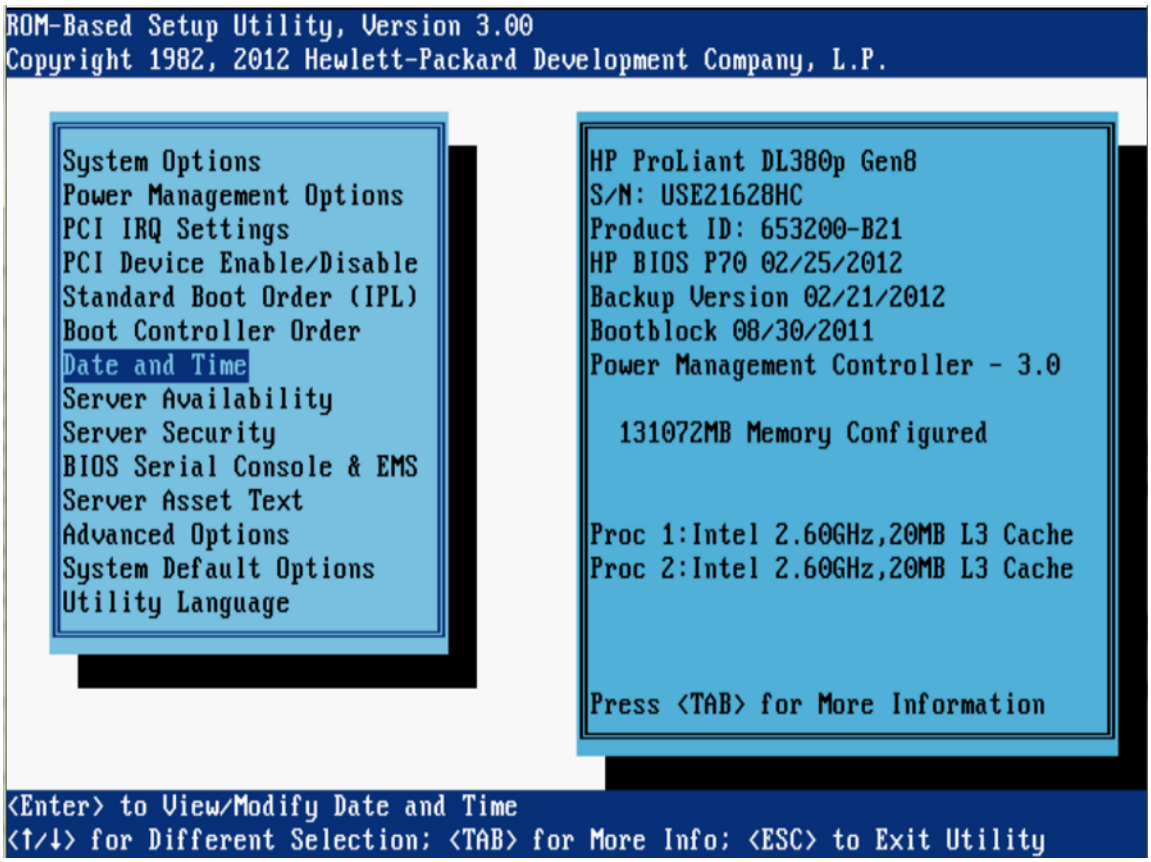


Figure 3: Example HP BIOS Setup

2. Select **Date and Time**.
   a) Set the server date and time to GMT (Greenwich Mean Time).
   b) Press <ESC> to navigate to the main menu.
3. Select **Server Availability**.
   a) Change **Automatic Power-On** to **Enabled**.
   b) Change **Power-On Delay** to **No Delay**.
   c) Press <ESC> to navigate to the main menu.
4. Select **System Options**.
   a) Select Processor Options.
   b) Change **Intel® Virtualization Technology** to Enabled.
   c) Press <ESC> to return to System Options.
   d) Select **Serial Port Options**.
   e) Change **Embedded Serial Port** to **COM2**.
   f) Change **Virtual Serial Port** to **COM1**.
   g) Press <ESC> to navigate to the main menu.
5. Press <ESC> to Save and Exit from the ROM-Based Setup Utility.

C.2.2 Configuring HP Gen9 Servers

The HP Gen9 systems can have UEFI boot enabled. Since TPD is configured to use the Legacy BIOS option, both blade and rackmount Gen9s should have their BIOS settings checked before IPM. Rack mount servers should also have the iLO serial port configured at this time. Directions for both settings are provided below.

1. If this is a rack mount server, connect via a VGA monitor and USB keyboard. If a blade server is being configured, use the iLO Integrated Remote Console.
2. Reboot/reset the server.
3. Press the F9 key to access the **System Utilities** menu when **<F9 System Utilities>** appears in the lower left corner of the screen.
4. Select the **System Configuration** menu.
5. Select the **BIOS/Platform Configuration (RBSU)** menu.
6. Select the **Boot Options** menu.
7. If the Boot Mode is not **Legacy BIOS** mode, press <Enter> to open the **BIOS** mode menu. Otherwise, skip to Step 9.
8. Select **Legacy BIOS Mode**.
9. Press <Esc> once to back out to the **BIOS/Platform Configuration (RBSU)** menu.
   If a blade server is being configured, skip to Step 17, otherwise continue to Step 10.
10. Select the **System Options** menu, then select the **Serial Port Options** menu.
11. Change **Embedded Serial Port** to **COM2**.
12. Change **Virtual Serial Port** to **COM1**.
13. Press <Esc> twice to back out to the **BIOS/Platform Configuration (RBSU)** menu.
14. Select the **Server Availability** menu.
15. Set **Automatic Power-On** to **Restore Last Power State**.

16. Set **Power-On Delay** to **No Delay** then press <Esc> once to back out to the **BIOS/Platform Configuration (RBSU)** menu.
17. Select the **Power Management** menu.
18. Set **HP Power Profile** to **Maximum Performance**. Press <Esc> once to back out to the **BIOS/Platform Configuration (RBSU)** menu.
19. Press <F10> to save the updated settings, then <y> to confirm the settings change.
20. Press <Esc> twice to back out to the **System Utilities** menu.
21. Select **Reboot the System** and press <Enter> to confirm.

C.3 OS IPM Install

The IPM installation media must now be inserted into the system. Installation will then begin by resetting (or power cycling) the system so that the BIOS can find and then boot from the IPM installation media. The reboot steps are different for the different rack mount servers.

Note: On the HP G5 rack mount servers, this procedure can be accomplished by using either a DB9 serial cable plugged into the serial port in the back of the unit, or the VGA monitor and keyboard

Note: On the HP G6 and newer HP servers, this procedure can be accomplished by either configuring an IP address on the iLO/ILOM and accessing the console using the iLO/ILOM, or the VGA monitor and keyboard. The remote media function of the iLO/ILOM can also be used to provide access to the installation media.

C.3.1 HP Rack Mount Servers - Boot from CD/DVD/USB

1. Insert the OS IPM media (CD/DVD or USB) into the CD/DVD tray/USB slot of the Application Server.
2. Power cycle the server:
   a) For HP Rack Mount servers, hold the power button in until the button turns amber, then release. Wait 5 seconds, then press the power button and release it again to power on the system.
3. For some servers, you must select a boot method so that the server does not boot directly to the hard drive:
   a) For HP rack mount servers, press F11 when prompted to bring up the boot menu and select the appropriate boot method.
4. Proceed to steps in *C.4 IPM Command Line Procedures*.

C.4 IPM Command Line Procedures

1. Figure 3 is a sample output screen indicating the initial boot from the install media was successful. The information in this screen output is representative of TPD 7.0.0.0.0.

   Note: Based on the deployment type, either TPD or TVOE can be installed.

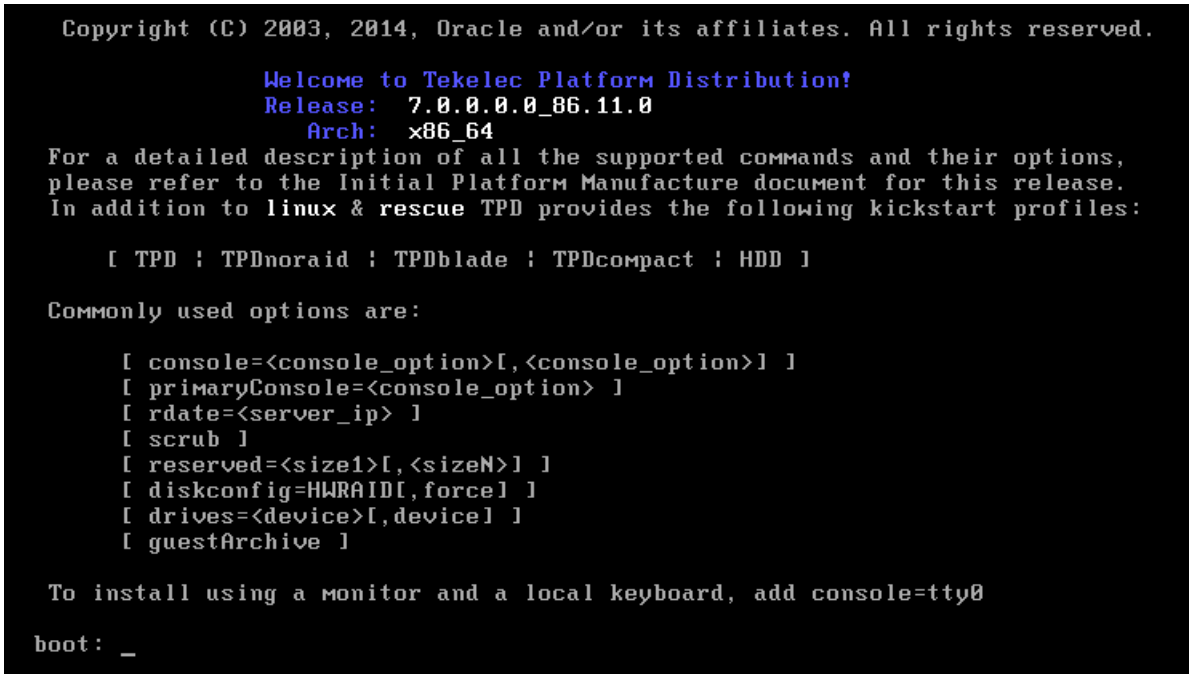


Figure 4: Example Boot from Media Screen, TPD 7.0.0.0.0

2. Optional Step: If media has not been previously verified, perform a media check now; refer to *C.6 Media Check*.
3. The command to start the installation is dependent upon several factors, including the type of system, knowledge of whether an application has previously been installed or a prior IPM install failed, and what application will be installed.

   Note: Text case is important, and the command must be typed exactly.

   Starting with TPD 6.0, when IPMing HP G6 and newer hardware , if no diskconfig or drives option is passed, the correct diskconfig option is appended to the IPM command, without the force option. This option verifies the disk configuration is correct before proceeding with the install. If the configuration is not correct, it will stop the installation without changing the disk configuration so that you can reboot and start over, manually passing the diskconfig option you want with the force option.

   An example command to enter is:

```
TPDnoraid diskconfig=HPHW,force console=tty0
```

   After entering the command to start the installation, the Linux kernel will load, as in the following screenshot:

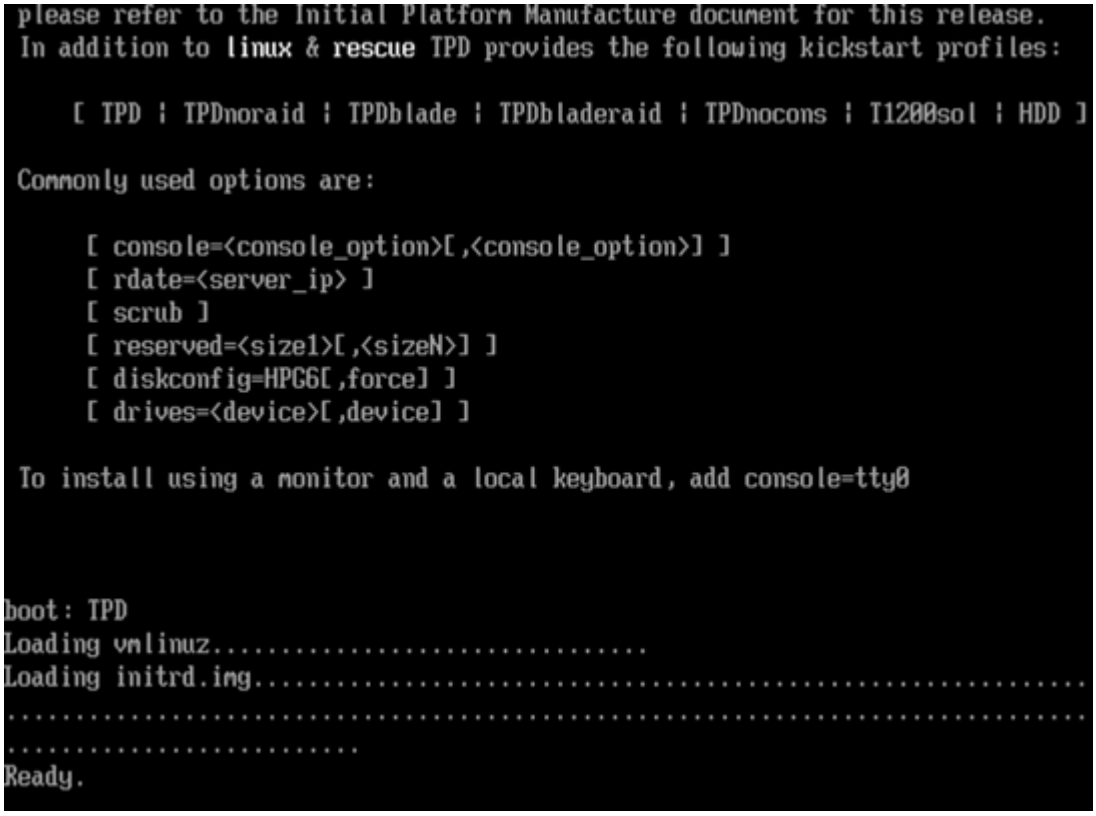


Figure 5: Example Kernel Loading Output

4. After a few seconds, additional messages will begin scrolling by on the screen as the Linux kernel boots, and then the drive formatting and file system creation steps will begin:

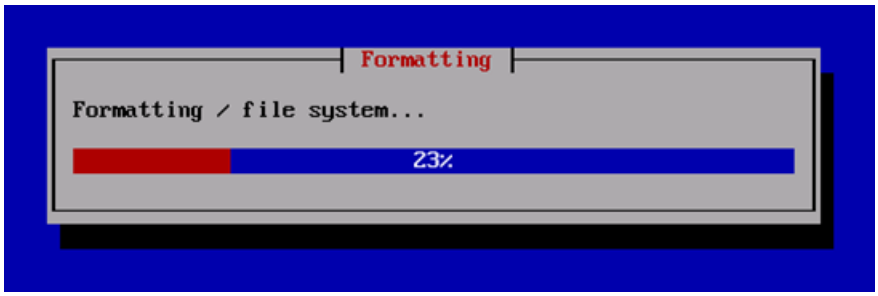


Figure 6: Example File System Creation Screen

5. Once the drive formatting and file system creation steps are complete, the following screen will appear indicating that the package installation step is about to begin.

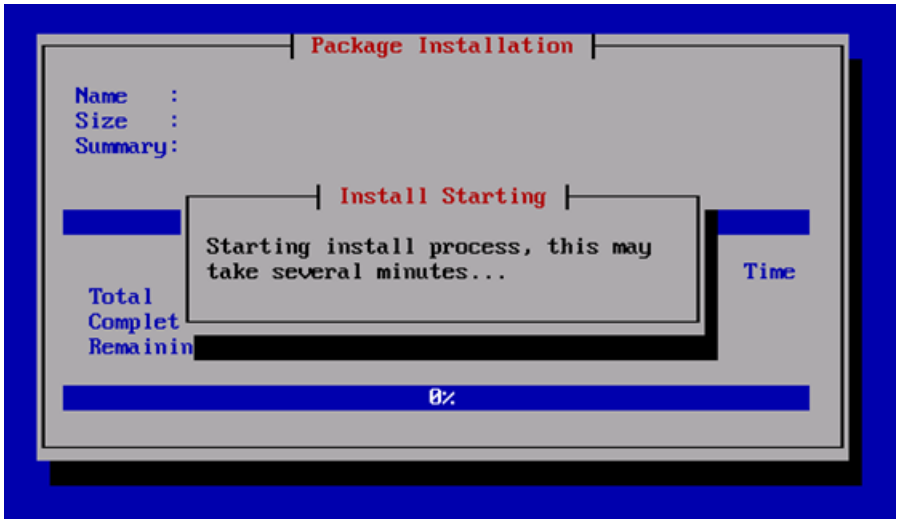


Figure 7: Example Package Installation Screen

6. Once the screen shown in Figure 6, Example Package Installation Screen Appears, it may take several minutes before anything change. However, after a few minutes, you will see a screen similar to that below, showing the status of the package installation step. For each package, there will be a status bar at the top indicating how much of the package has been installed, with a cumulative status bar at the bottom indicating how many packages remain. In the middle, you will see text statistics indicating the total number of packages, the number of packages installed, the number remaining, and current and projected time estimates:

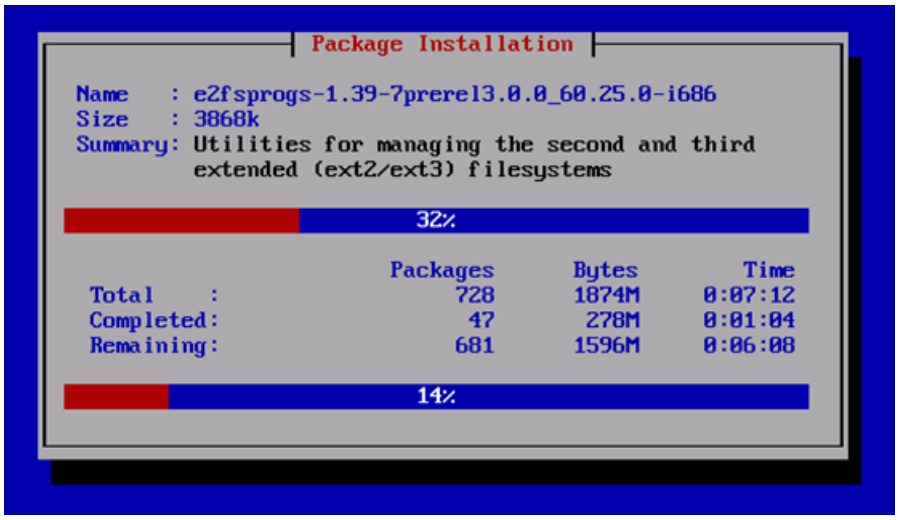


Figure 8: Example Installation Statistics Screen

7. Once all the packages have been successfully installed, the following screen will appear, letting you know the installation process is complete. **Remove the installation media** (DVD or USB key) and then press <ENTER> to reboot the system.

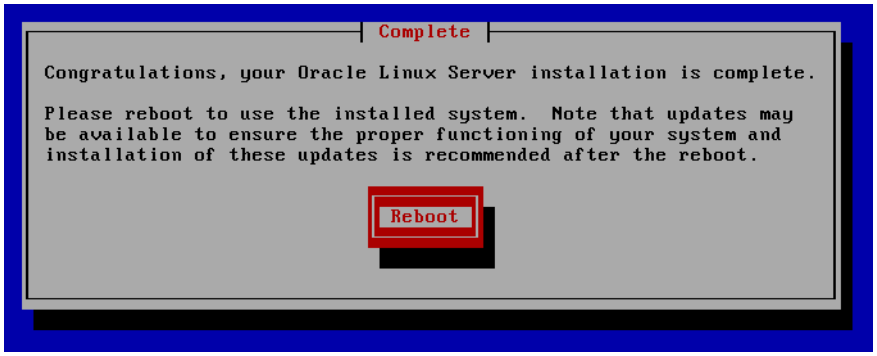


Figure 9: Example Installation Complete Screen

8. After a few minutes, the the server boot sequence will start and eventually display that it is booting the new IPM load.

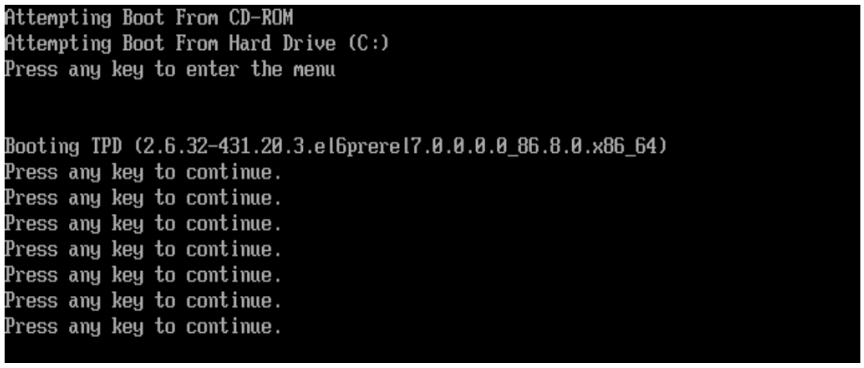


Figure 10: Example Boot Loader Output

9. A successful IPM platform installation process results in a user login prompt.

C.5 Post Install Processing

1. Log in as user syscheck, and the system health check runs automatically. This will check the health of the server, and print out an OK if the tests passed, or a descriptive error of the problem if anything failed. The screenshot below shows a successful run of syscheck, where all tests pass, indicating the server is healthy.

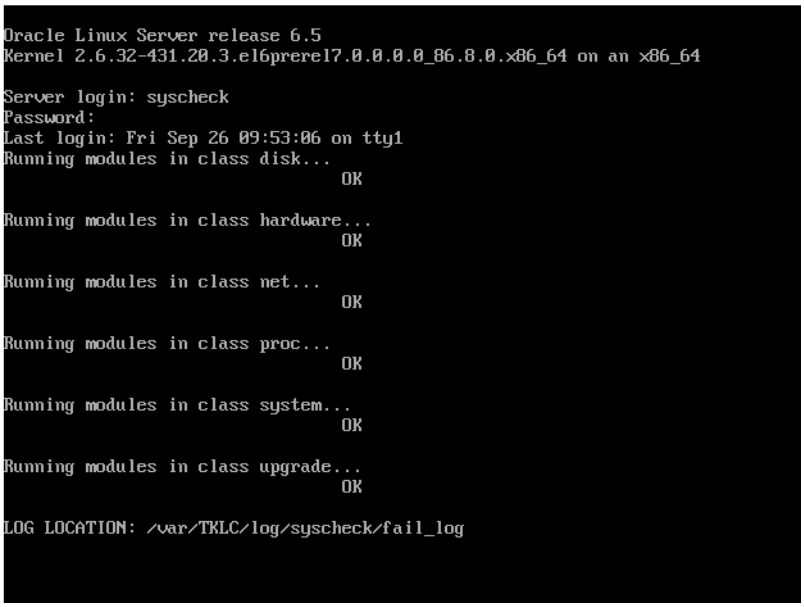


Figure 11: Example Successful Syscheck Output

Since an NTP server will not normally be configured at this point, syscheck may fail due to the NTP test as shown in *Figure 12: Example Syscheck Output with NTP Error*. The error shown in Figure 13 is acceptable and can be ignored.

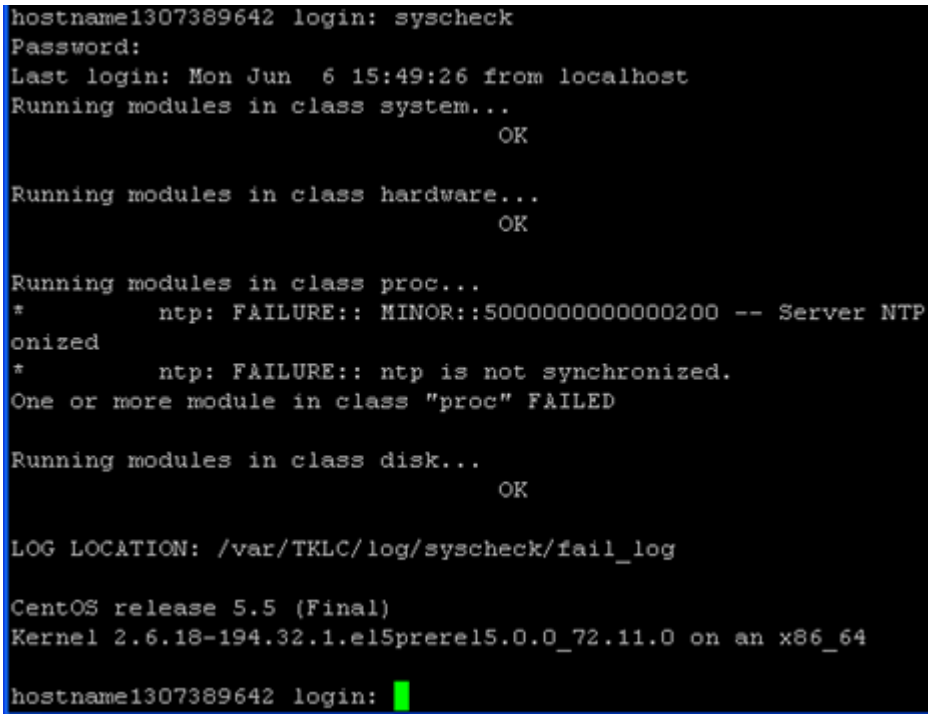


Figure 12: Example Syscheck Output with NTP Error

Figure 13: Example Syscheck Disk Failure Output indicates a disk failure in one of the syscheck tests. If the server is using software disk mirroring (RAID1), the syscheck disk test will fail until the disks

have synchronized. The amount of time required to synchronize the disks varies with disk speed and capacity. Continue executing system check every 5 minutes (by logging in as syscheck to run syscheck again) until the health check executes successfully as shown in *Figure 11: Example Successful Syscheck Output*. If the disk failure persists for more than two (2) hours, or if system check returns any other error message besides a disk failure or the NTP error shown in Figure 11, do not continue. Contact My Oracle Support and report the error condition.

```
Running modules in class hardware...
                                OK

Running modules in class proc...
                                OK

Running modules in class disk...
One or more module in class "disk" FAILED

Running modules in class system...
                                OK

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

Figure 13: Example Syscheck Disk Failure Output

2. Verify that the IPM completed successfully by logging in as admusr and running the `verifyIPM` command. No output is expected. Contact Customer Service if any output is printed by the `verifyIPM` command.

```
$ sudo /usr/TKLC/plat/bin/verifyIPM
```

```
Congratulations!
Application Server IPM Process is complete and Post-install checks have passed...
You have successfully completed this procedure.
Refer to sales order to load appropriate application.
```

C.6 Media Check

Media Check only works on CD/DVDs. USB media should be validated when it is created, because the validation steps are dependent on how it was created.

1. Refer to *C.3.1 HP Rack Mount Servers - Boot from CD/DVD/USB* to automatically boot from the DVD or USB IPM media.
2. The screen output shown below indicates the initial boot from DVD is successful. Enter the command `linux mediacheck` and press <Enter>.

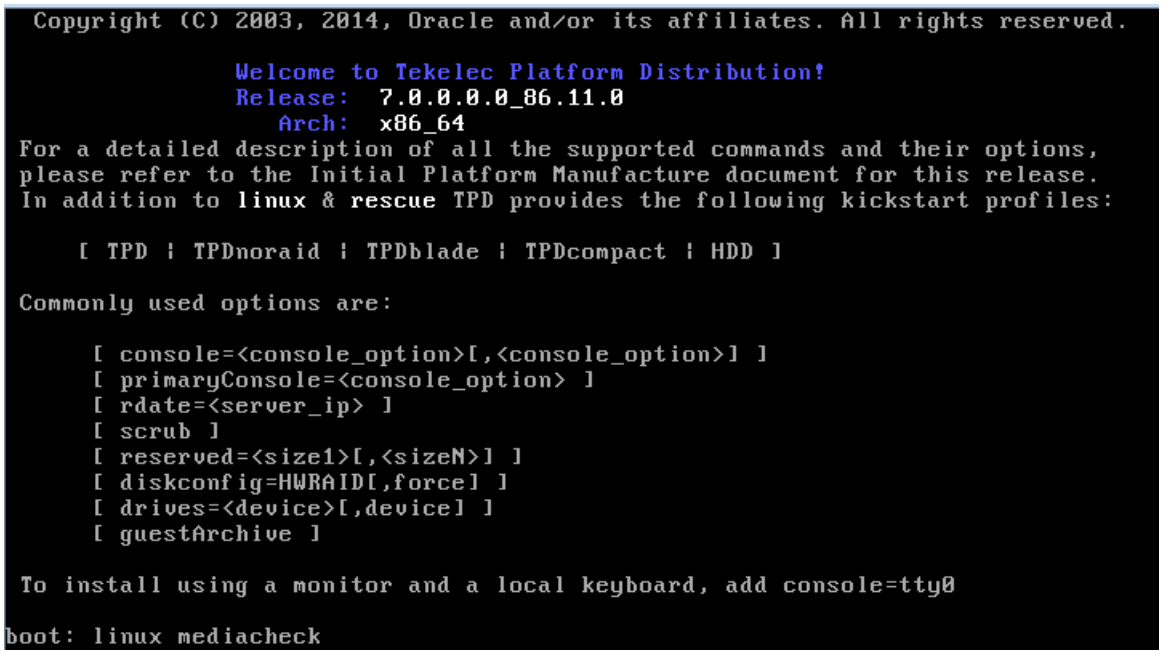


Figure 14: Example Media Check Command

3. When the following screen appears, press <Tab> until **OK** is highlighted and then press <Enter>.

Figure 15: Example Media Test Dialog

4. Next, press <Tab> until **Test** is highlighted, and press <Enter> to begin testing the currently installed media.

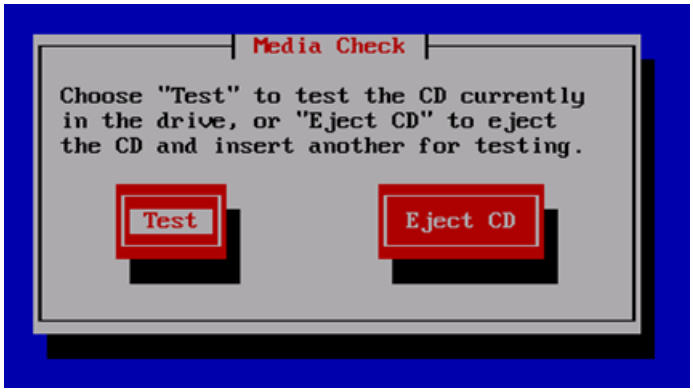


Figure 16: Example Dialog with Test Highlighted

5. The media check begins, with a status bar indicating the progress, as shown in the screen shot below:

Figure 17: Example Media Check Progress Screen

6. If the media check is successful, the following screen will be displayed. Press **Enter** to continue.

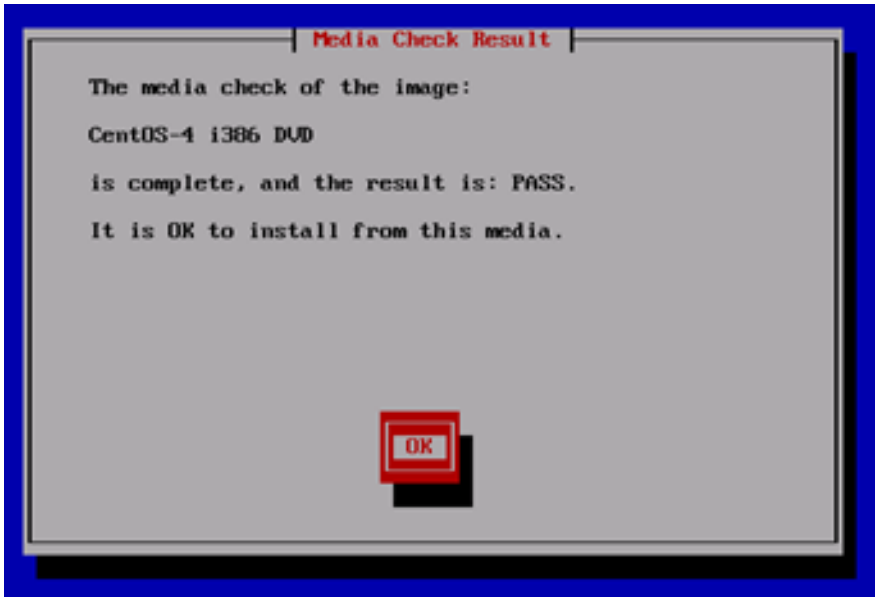


Figure 18: Example Media Check Result

7. To test additional media, remove original media, insert new media, press <Tab> until **Test** is highlighted and press <Enter>. If no additional media is available and the media check passed, remove the current media, insert the original media (first disk or USB pen), press <Tab> until **Continue** is highlighted and press <Enter> to continue the installation again.

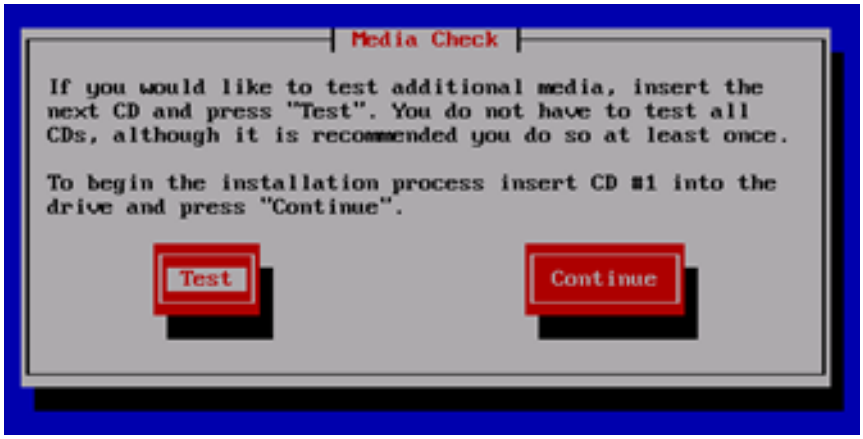


Figure 19: Example Media Check Continuation Dialog

C.7 Initial Product Manufacture Arguments

1. reserved

The reserved option provides the capability to create one or more extra partitions that are not made part of the vgroot LVM volume group. The sizes of the partition(s) are indicated after "reserved=" and are separated by commas without any whitespace if there are more than one. The sizes use a suffix to indicate whether the value is in units of megabytes ('M') or gigabytes ('G'). In this context, a megabyte is 10242 and a gigabyte is 10243.

In the case of a software RAID-1 configuration, such as TPD (but not TPDnoraid), a single value will actually cause the creation of a partition on 2 drives and a metadevice (md) that incorporates the two partitions.

Examples:

1. TPD reserved=2G - On a T1200, this will create reserved partitions on sda and sdb of 2 GB, and a RAID-1 metadevice using those reserved partitions.
2. TPDnoraid reserved=512M – On an HP server, this will create a reserved partition on sda of 0.5 GB.
3. TPDnoraid reserved=4G,128M – On an HP server, this will create two reserved partitions on cciss/c0d0 of 4 GB and of 128 MB.

The partition(s) or metadevice(s) can be used by storageMgr to create a DRBD device or LVM physical volume. However, to do so, one will need to know the partition number or metadevice number.

Numbering of partitions is performed by anaconda and is controlled by anaconda. Therefore, to get the partition number, a developer would need to examine the partition table after an IPM to determine the number. Also, this number may change due to changes in anaconda in future releases of TPD.

2. scrub

This option is typically used as part of the IPM process on machines that have had TPD loaded in the past. The usage of the "scrub" option is used to ensure that the disk and logical volume partitioning that occurs during the early phase of IPM operates correctly. Note that this option should not be used during hardware USB media based IPM since doing so will erase the TPD installation media.

It is extremely important to understand that the "scrub" option will remove all data from ALL attached disk devices to the machine being IPM'ed.

Note: this includes disk drives that are not mentioned in the "drives" parameter as well as USB install media. Therefore, whenever the "scrub" option is used, any and all disk drives attached to the machine being IPM'ed, including those not mentioned in the "drives" parameter, will lose all of their data. Technically, this is accomplished by writing zeroes to the entire disk of each attached disk drive.

3. diskconfig

This option is intended to direct the IPM process to configure the disks in different ways. At this time diskconfig supports the following options:

- HPHW – specify that the server is an HP server that should be configured to use hardware RAID1 (mirroring). This option only applies to HP servers G6 and above. The expected configuration is that the first two physical drives on the array controller in slot 0 of the server will be configured as one logical disk. This is the default if no diskconfig or drives option is passed.
- HPSW – specify that the server is an HP server that should be configured to use software RAID1 (mirroring). This option only applies to HP servers G6 and above. This mode is intended for use during development and testing and is not supported on fielded systems.
- force – specify that if the current disk configuration does not match the desired configuration, that the desired configuration should forcibly installed. Loss of data on any disk on the same RAID disk controller may result.

Appendix D

Using WinSCP

Topics:

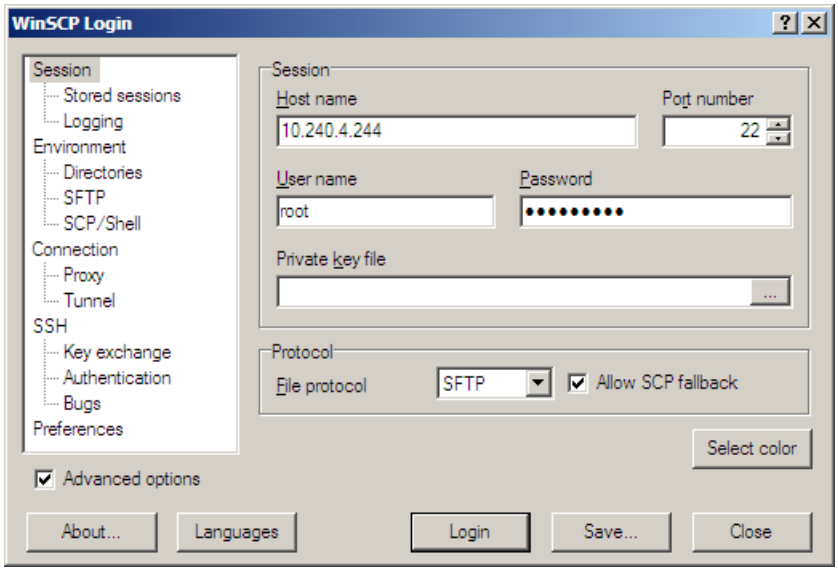
D.1 Using WinSCP

The following is an example of how to copy a file from the management server to your PC desktop

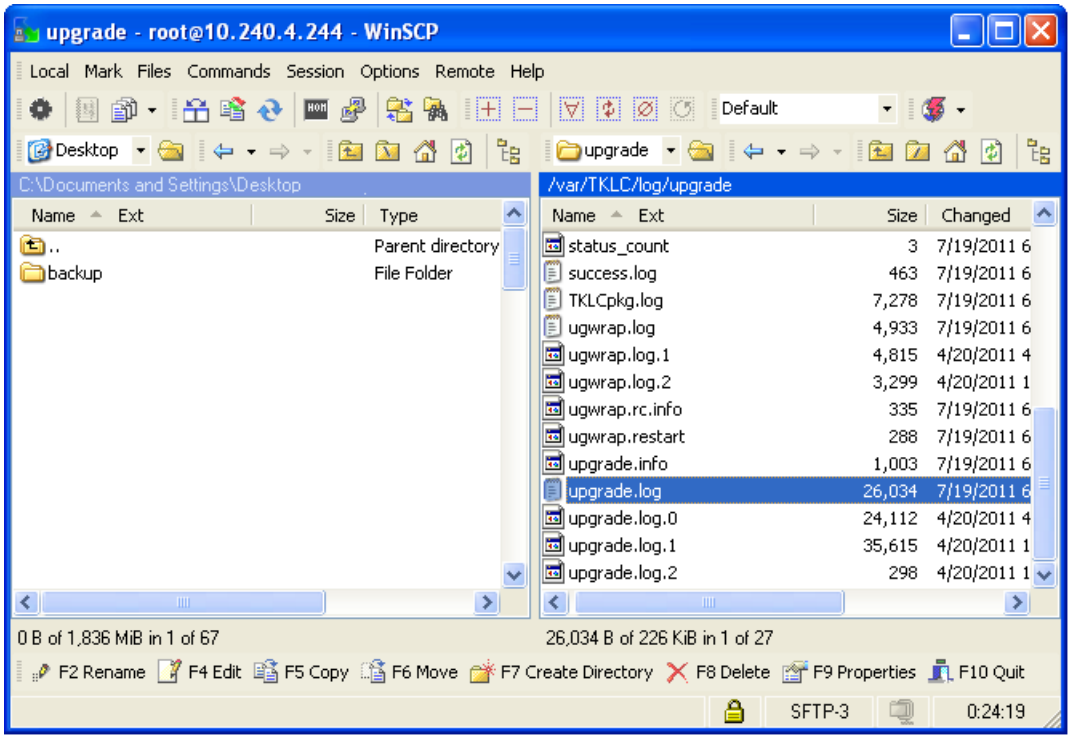
1. **Download the WinSCP Application**
   Download the WinSCP application:

   ```
   http://winscp.net/eng/download.php
   ```

2. **Connect to the management server**
   After starting this application, navigate to Session and enter: **<management_server_IP>** into the `Host name` field, **root** into the `User name` field, and **<root_password>** into the `Password` field. Click **Login**.



3. **Copy the target file from the management server**
   On the left is your own desktop filesystem. Navigate within it to Desktop directory. On the right side is the management server file system. Within it, navigate into the location of the file you would like to copy to your desktop. Highlight the file in the management server file system by pressing the insert key, then press **F5** to copy the file.



4. **Close the WinSCP application**

   Then close application by pressing **F10** and confirm to terminate session by pressing **OK**.

Appendix E

Backup Procedures

Topics:

E.1 Backup HP (6120XG, 6125G, 6125XLG) Enclosure Switch

This procedure should be executed after every change to the switch configuration after completing *4.7.2.1 Configure HP 6120XG Switch (netConfig)* and/or *4.7.3.1 Configure HP 6125G Switch (netConfig)* and/or *4.7.4.1 Configure HP 6125XLG Switch (netConfig)*.

Prerequisites:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed
- *4.1.1 Installing TVOE on the Management Server* must be completed
- *4.2.1 Deploy PM&C Guest* must be completed
- *4.7.2.1 Configure HP 6120XG Switch (netConfig)*
- *4.7.3.1 Configure HP 6125G Switch (netConfig)*
- *4.7.4.1 Configure HP 6125XLG Switch (netConfig)*

Procedure Reference Tables:

Variable	Value
<switch_name>	hostname of the switch

1. Ensure that the directory where the backups will be stored exists.

```
$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/backup
```

   If you receive an error such as the following:

```
-bash: ls: /usr/TKLC/smac/etc/switch/backup: No such file or directory
```

   Then the directory must be created by issuing the following command:

```
$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/backup
```

   Then change the directory permissions:

```
$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/switch/backup
```

2. Execute the backup command

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration
service=ssh_service filename=<switch_name>-backup
```

3. Copy the files to the backup directory.

```
$ sudo /bin/mv -i ~admusr/<switch>-backup* /usr/TKLC/smac/etc/switch/backup
```

4. Verify switch configuration was backed up by cat <switch_name> and inspecting its contents to ensure it reflects the latest known good switch configurations.

```
$ sudo /bin/ls -i /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup*
$
```

```
$ sudo /bin/cat /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup
$
```

5. Save FW files:

   If a firmware upgrade, switch replacement, or an initial install (which performed a FW upgrade during initialization) was performed, back up the FW image used by performing the following command:

```
$ sudo /bin/mv -i ~<switch_backup_user>/<fw image> <switch_backup_directory>/
```

6. **PM&C:** Perform PM&C application backup.

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

   Note: The backup runs as a background task. To check the status of the background task use the PM&C GUI Task Monitor page, or issue the command "pmaccli getBgTasks". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

   Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

7. **PM&C:** Verify the Backup was successful

   Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contactMy Oracle Supportby referring to the*1.4 My Oracle Support (MOS)*of this document.

   The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

8. **PM&C:** Save the PM&C backup

   The PM&C backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server. The PM&C backup files are saved in the following directory: "/var/TKLC/smac/backup".

9. Repeat *Step 2*-*Step 8* for each HP switch to be backed up.

E.2 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)

Prerequisites for RMS system Aggregation Switch:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed.
- *4.1.4 TVOE Network Configuration*
- *4.3.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)*
- Application username and password for creating switch backups must be configured on the management server prior to executing this procedure.

Oracle-Provided Aggregation Switch Prerequisites for c-Class system Aggregation Switch:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed.
- *4.1.1 Installing TVOE on the Management Server* must be completed.
- *4.1.4 TVOE Network Configuration* must be completed.
- *4.2.1 Deploy PM&C Guest* must be completed.
- *4.3.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)*

Prerequisites for Cisco 3020 Enclosure switches:

Procedure Reference Tables:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed.
- *4.1.1 Installing TVOE on the Management Server* must be completed.
- *4.1.4 TVOE Network Configuration* must be completed.
- *4.2.1 Deploy PM&C Guest* must be completed.
- *4.7.1.1 Configure Cisco 3020 Switch (netConfig)*

Variable	Value
<switch_backup_user> (also needed in switch configuration procedure)	admusr
<switch_backup_user_password> (also needed in switch configuration procedure)	Check application documentation
<switch_name>	hostname of the switch
<switch_backup_directory>	**Non-PM&C System:** /usr/TKLC/plat/etc/switch/backup
	PM&C System: /usr/TKLC/smac/etc/switch/backup

1. Verify switch is at least initialized correctly and connectivity to the switch by verifying hostname

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> getHostname
Hostname: switch1A
$
```

Note: The value beside "Hostname:" should be the same as the <switch_name> variable.

2. Run command "netConfig --repo showService name=ssh_service" and look for ssh service.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service
    Service Name:    ssh_service
            Type:    ssh
            Host:    10.250.62.85
            Options:
               password: C20F7D639AE7E7
               user: admusr
$
```

   In the ssh_service parameters, the value for 'user:' will be the value for the variable <switch_backup_user>.

3. Verify existence of the backup directory.

```
$ sudo /bin/ls -i <switch_backup_directory>
```

   If the output contains

```
ls: cannot access <switch_backup_directory>: No such file or directory
```

   create the directory with:

```
$ sudo /bin/mkdir -p <switch_backup_directory>
```

   Change directory permissions:

```
$ sudo /bin/chmod go+x <switch_backup_directory>
```

4. Execute the backup command

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration
service=ssh_service filename=<switch_name>-backup
```

5. Verify switch configuration was backed up by cat <switch_name>-backup and inspect its contents to ensure it reflects the latest known good switch configurations. Then, copy the files over to the backup directory.

```
$ sudo /bin/ls -i ~<switch_backup_user>/<switch_name>-backup*
$
$ sudo /bin/cat ~<switch_backup_user>/<switch_name>-backup*
$
$ sudo /bin/chmod 644 <switch_name>-backup*
$
$ sudo /bin/mv -i  ~admusr/<switch name>-backup* <switch_backup_directory>/
```

   Note: The cat command may leave garbled text on the next terminal prompt. Disregard this text.

   Example:

```
[admusr@pmac ~]$
PuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTY
```

6. **PM&C:** Perform PM&C application backup.

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

Note: The backup runs as a background task. To check the status of the background task use the PM&C GUI Task Monitor page, or issue the command "pmaccli getBgTasks". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

7. **PM&C:** Verify the Backup was successful

Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contactMy Oracle Supportby referring to the*1.4 My Oracle Support (MOS)*section of this document.

The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C Backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

8. **PM&C:** Save the PM&C backup

The PM&C backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server. The PM&C backup files are saved in the following directory: "/var/TKLC/smac/backup".

9. Repeat steps *Step 1*, *Step 4*-*Step 8* for each switch to be backed up.

Appendix F

How to Access a Server Console Using the iLO

Topics:

F.1 How to Access a Server Console Using the iLO

1. **Access the iLO GUI**

   Using a laptop or desktop computer connected to the customer network, navigate with Internet Explorer to the IP address of the iLO of the Management Server. Log in to the iLO as the user "Administrator".

2. **If the iLO is an iLO 2, configure Hot Keys**

   The iLO GUI will indicate the iLO version as iLO 2 ("Integrated Lights-Out 2"), iLO 3, iLO 4, etc. If this is an iLO 2, perform the following Hot Key configuration:

   a) Click the **Remote Console** tab
   b) Click the **Settings** menu item and then the **Hot Keys** sub-tab
   c) In the row starting with **Ctrl-T** change the first dropdown to **L_CTRL** and the second dropdown to **]** (right bracket). The rest of the dropdowns in the row should be **NONE**.
   d) Click **Save Hot Keys**

   As a result, pressing **Ctrl-T** rather than **Ctrl-]** will now exit the console of a TVOE guest and return to the console of the TVOE host.

3. **Launch the Remote Console Window**

   Navigate to **Remote Console** > **Remote Console** to launch the remote console in a new window.

4. **Log in to the Console**

   In the Remote Console window, log in to the console as user "admusr":

```
login as: admusr
Password:
Last login: Wed Jun  5 17:52:28 2013
[admusr@tvoe ~]$
```

5. **Return to the referencing procedure**

   Return to the procedure which referenced this appendix.

Appendix G

Onboard Administrator Procedures

Topics:

This appendix has been deleted from Platform 6.7.

G.1 Replacing Onboard Administrator

This information has been deleted from Platform 6.7.

This procedure describes how to replace OA in an enclosure with Redundant OA.

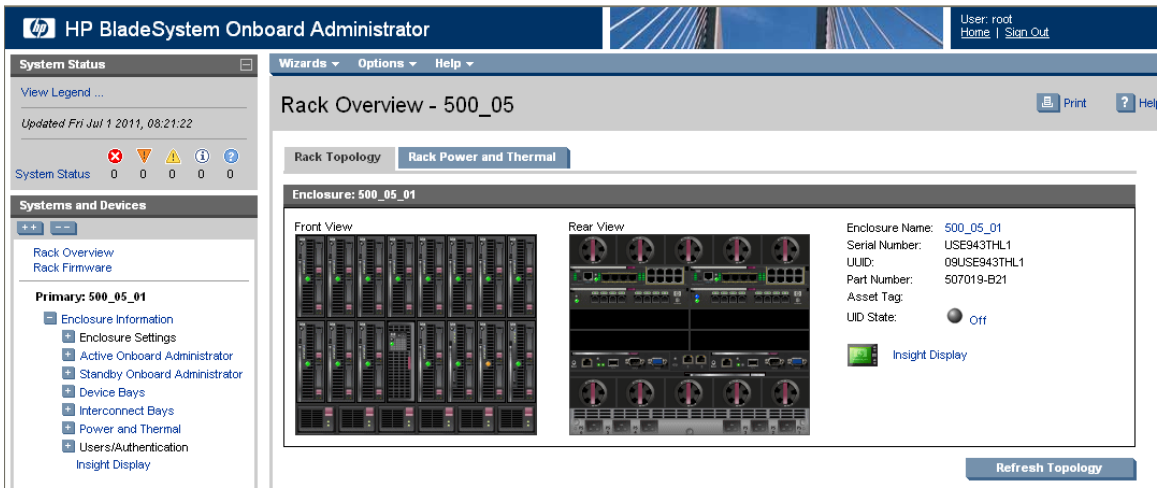
Note: The transfer of configuration occurs only from OA in Bay 1 to OA in Bay 2. Therefore in order to keep the current configuration of the system, the insertion of new OA into the OABay 1 location should be avoided.

Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to *1.4 My Oracle Support (MOS)*.

1. **OAGUI:** Login to the active OA

   Navigate to the IP address of the active OA, using *N.1 Determining Which Onboard Administrator Is Active*. Login as root.

   You will see the following page.



2. **OA GUI:** Record the IP configuration of the Active and Standby OAs.

   Navigate to Enclosure Information > Active Onboard Administrator > TCP/IP Settings. Record the Active OA's IP Address, Subnet Mask, and Gateway here:

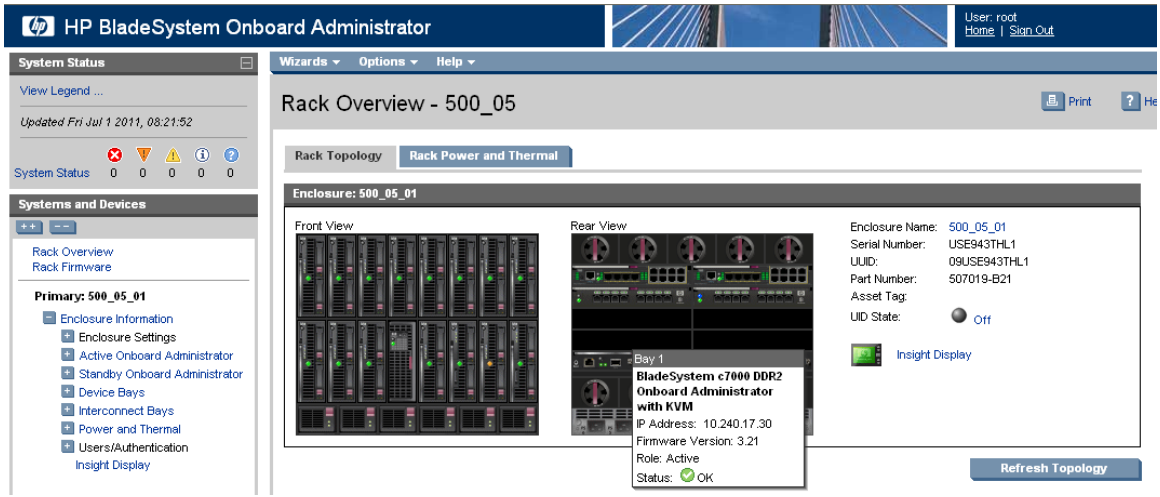
Active OA IP Address:	
Active OA Subnet Mask:	
Active OA Gateway:	

   Navigate to Enclosure Information > Standby Onboard Administrator TCP/IP Settings. Record the Standby OA's IP Address, Subnet Mask, and Gateway here:

Standby OA IP Address:	
Standby OA Subnet Mask:	
Standby OA Gateway:	

3. **OAGUI:** Note the location of the active OA

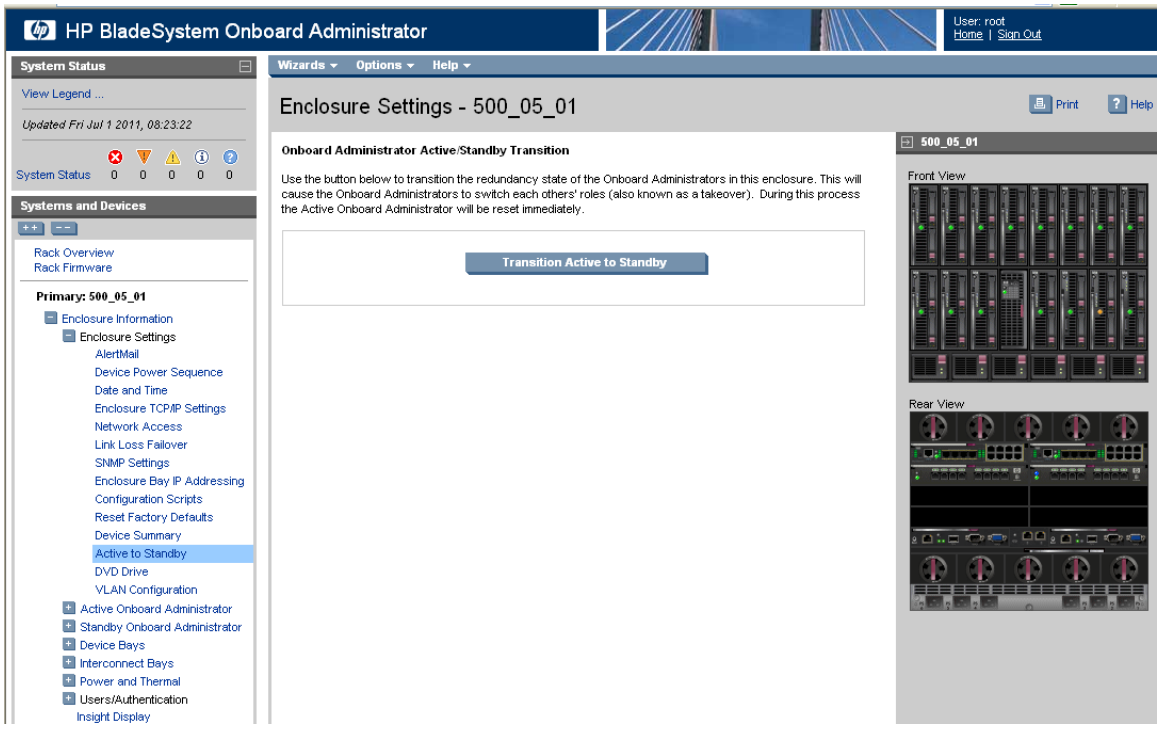
   Note the location of the active onboard administrator within the enclosure. The active OA will have the Active LED on, as in the figure below. You may also mouse over the OA and see its role.



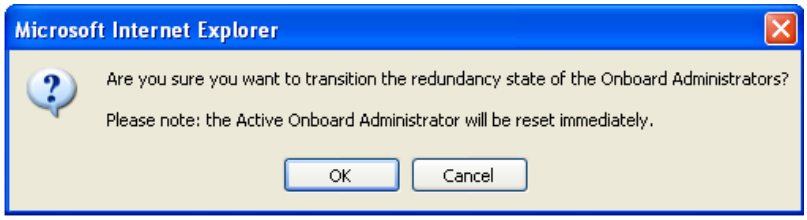
   If the OA you would like to replace is not the active OA for the enclosure, skip to step 5. Otherwise, continue with step 4.

4. **OAGUI:** Force active OA into standby mode

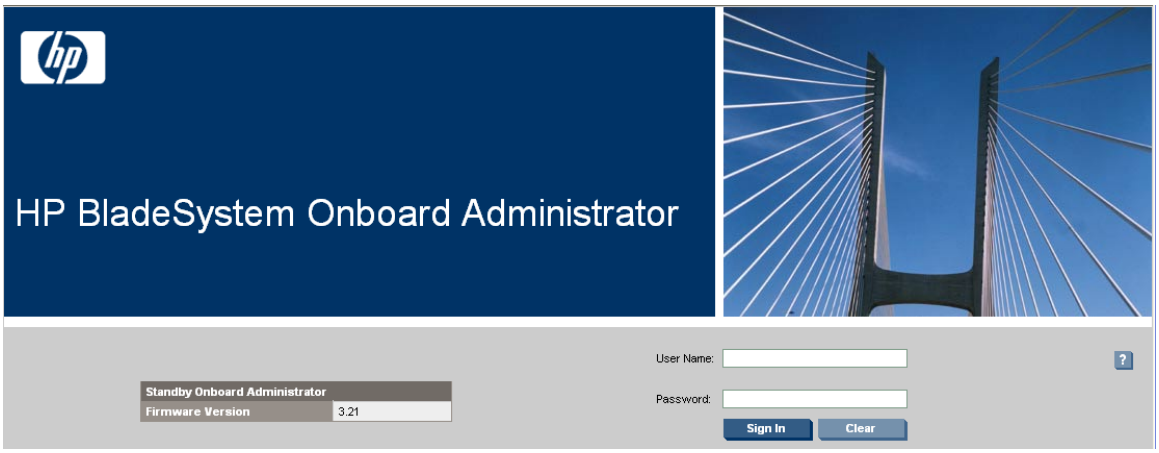
   On the left-hand side navigate to **Enclosure Information** > **Enclosure Settings** > **Active to Standby**, then click on the **Transition Active to Standby** button.



   Answer OK the following question:



Wait about five minutes , until the application reloads itself and the following page appears:



5. Remove the OA to be replaced

   If you need to replace the Onboard Administrator from the OA Bay 2 location (right as viewed from rear) , remove it and skip to step 7.

   If you need to replace the Onboard Administrator from the OA Bay 1 location (left as viewed from rear), remove it and proceed with step 6.

6. Move the OA from OABay 2 location into the OABay 1 location

   Move the OA from OA Bay 2 location into the OA Bay 1 location. Wait five minutes so that the Onboard Administrator can initialize.

7. Install the new OA

   Insert the new Onboard Administrator into OA Bay 2 of the enclosure and wait five minutes so it can get its configuration from the other OA and to initialize itself.

8. **OAGUI:** Login to the active OA

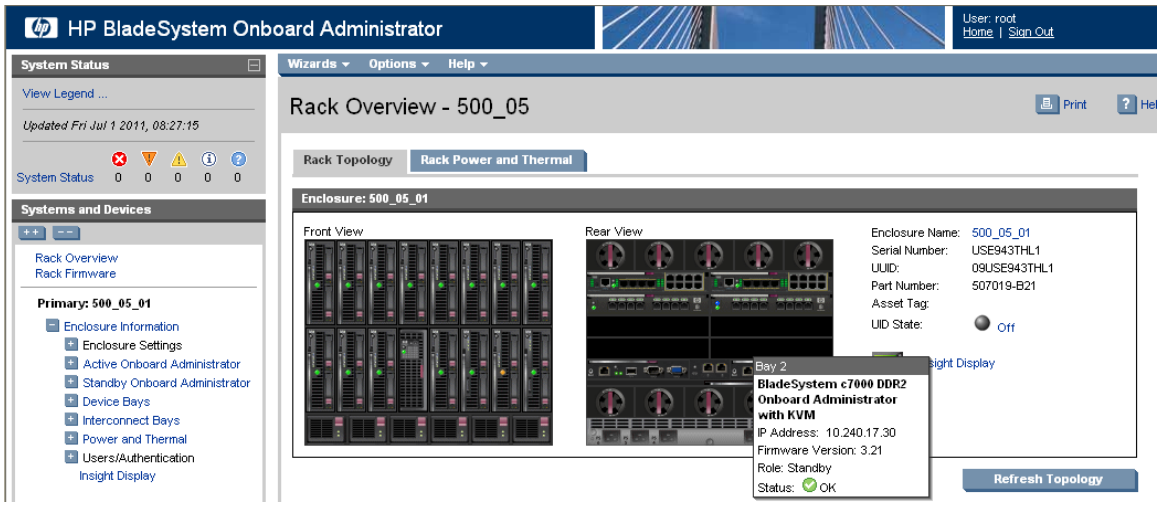
   Navigate to the IP address of the active OA, using *N.1 Determining Which Onboard Administrator Is Active*. Login as root.

9. **OA GUI:** Re-establish the OA's IP configuration

   Refer to the OA IP configuration settings recorded in Step 2 of this procedure. The current settings of each OA should be unique and should match the recorded settings for either the Active or Standby OA. The Active OA may now have the Standby OA's recorded settings and vice versa. If changes are needed, perform *4.5.1 Configure Initial OA IP*.

10. **OAGUI:** Verify the status of Onboard Administrators

On the **`Rear View`** mouse over each OA and verify the that the **`Status`** value is **`OK`**. If the status of one OA or the other is shown as "Degraded" because of a firmware version mismatch, perform *4.5.4 Upgrade or Downgrade OA Firmware*.



11. **PM&C CLI:** Delete OA SSH keys

    Log in to the PM&C CLI as admusr. Execute these three commands:

```
$ sudo /usr/bin/ssh-keygen -R <Active-OA-IP> -f ~pmacd/.ssh/known_hosts
$ sudo /usr/bin/ssh-keygen -R <Standby-OA-IP> -f ~pmacd/.ssh/known_hosts
$ sudo /bin/chown pmacd:pmacd ~pmacd/.ssh/known_hosts
```

    New SSH keys will be established by PM&C the next time it logs in to each OA.

Appendix H

How to Exit a Guest Console Session on an iLO

Topics:

H.1 How to Exit a Guest Console Session on an iLO

1. **Enter the appropriate control sequence for the iLO version**

   If the main iLO GUI window indicates that this is an iLO 2 ("Integrated Lights-Out 2"), press **Ctrl-T**. Otherwise, press **Ctrl-]**.

   This step corresponds to the configuration of iLO 2 Hot Keys performed in *L.1 How to Access a Server Console Remotely*.

2. **Return**
   Return to the procedure which referenced this appendix.

Appendix I

Changing SNMP Configuration Settings for iLO

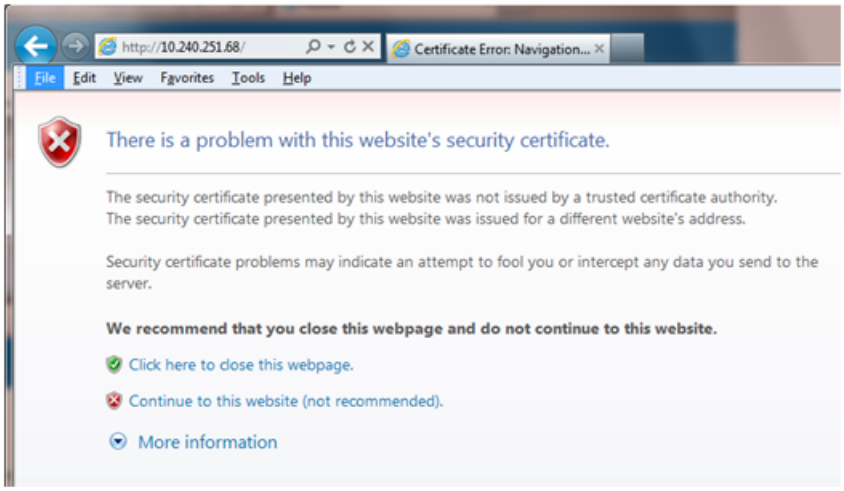
Topics:

I.1 Changing SNMP Configuration settings for iLO2

This procedure provides instructions to change the default SNMP settings for the HP ProLiant iLO 2 devices.

Perform this procedure for every iLO 2 device on the network. For instance, for every HP ProLiant G1/G5/G6 Blade and Rack Mount server.

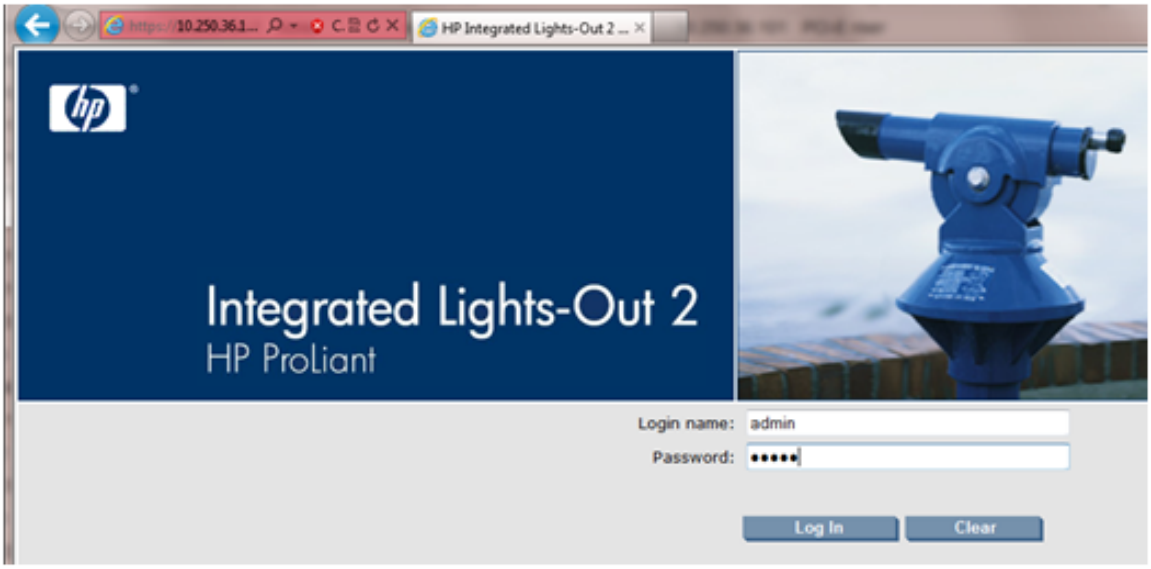
1. **From Workstation:** Launch Internet Explorer 7.x or higher and connect to the iLO2 device using "https://"



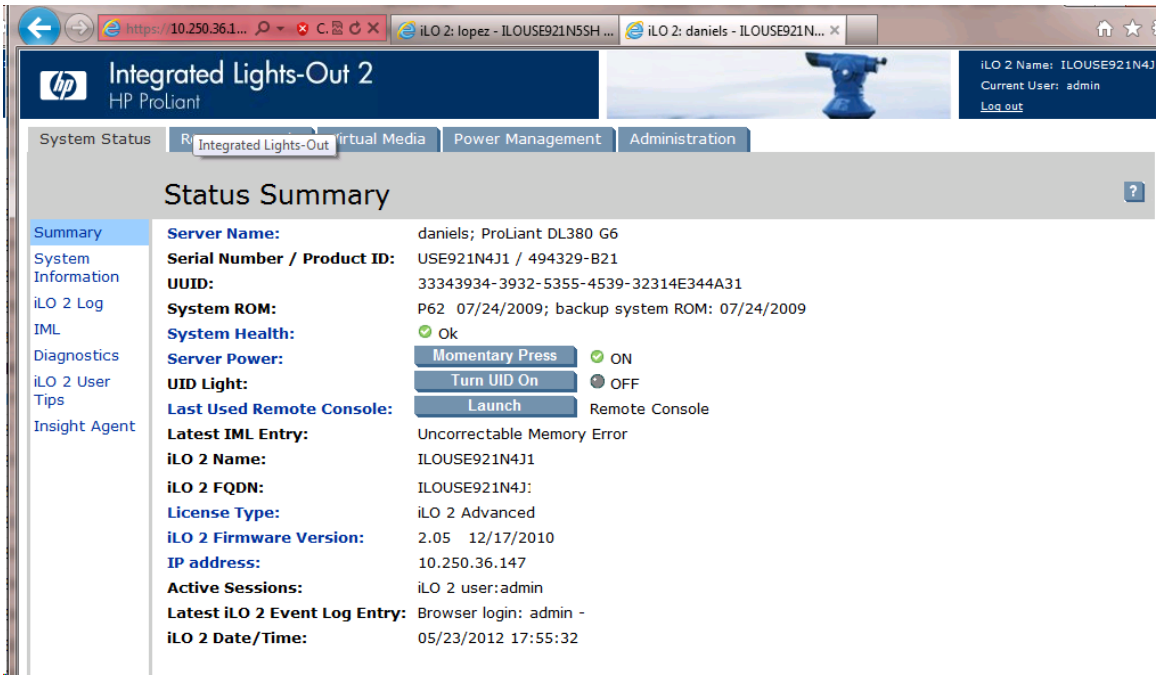
2. **iLO2 Web UI:**

   The user should be presented the login screen shown below.

   Login to the GUI using an Administrator account name and password.



3. **iLO2 Web UI:** The user should be presented the iLO2 System Status page as shown on the right



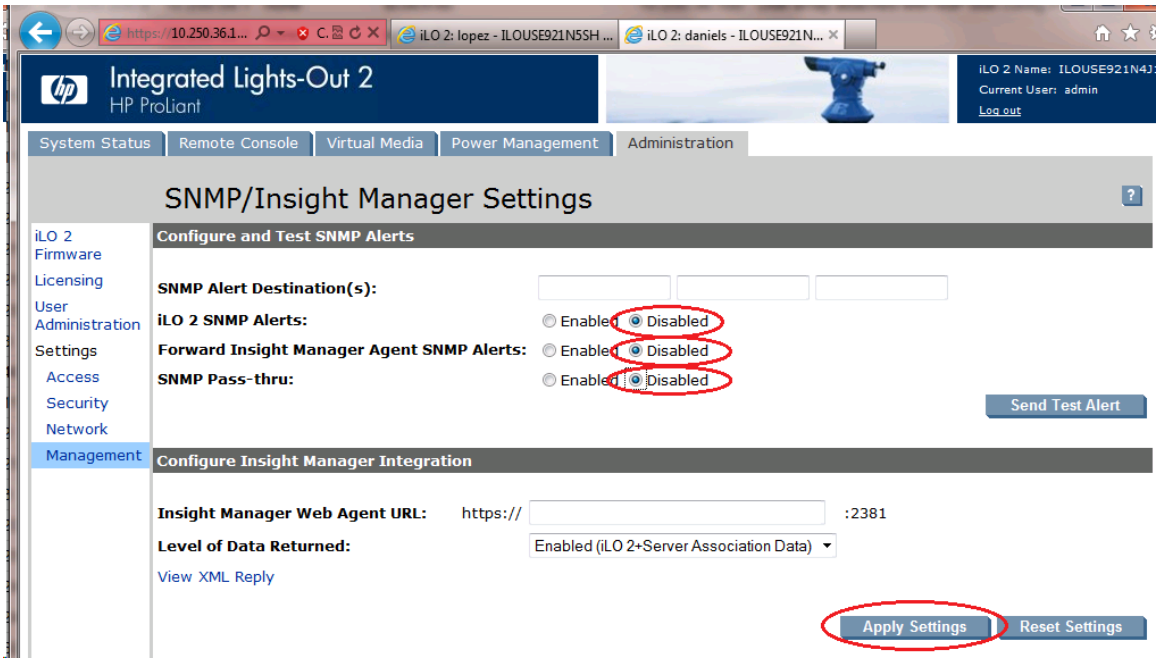
4. **iLO 2 Web UI:**
   1. Select the [Administration] tab on the top navigation bar.
   2. Select the [Management] menu item on the left navigation bar to display the SNMP Settings page.

5. **iLO2 Web UI:**

   The user should be presented the SNMP/Insight Manager Settings page.

   1. Select option [Disabled] for each of the 3 SNMP settings as shown to the right
   2. Click [Apply Settings] to save the change.

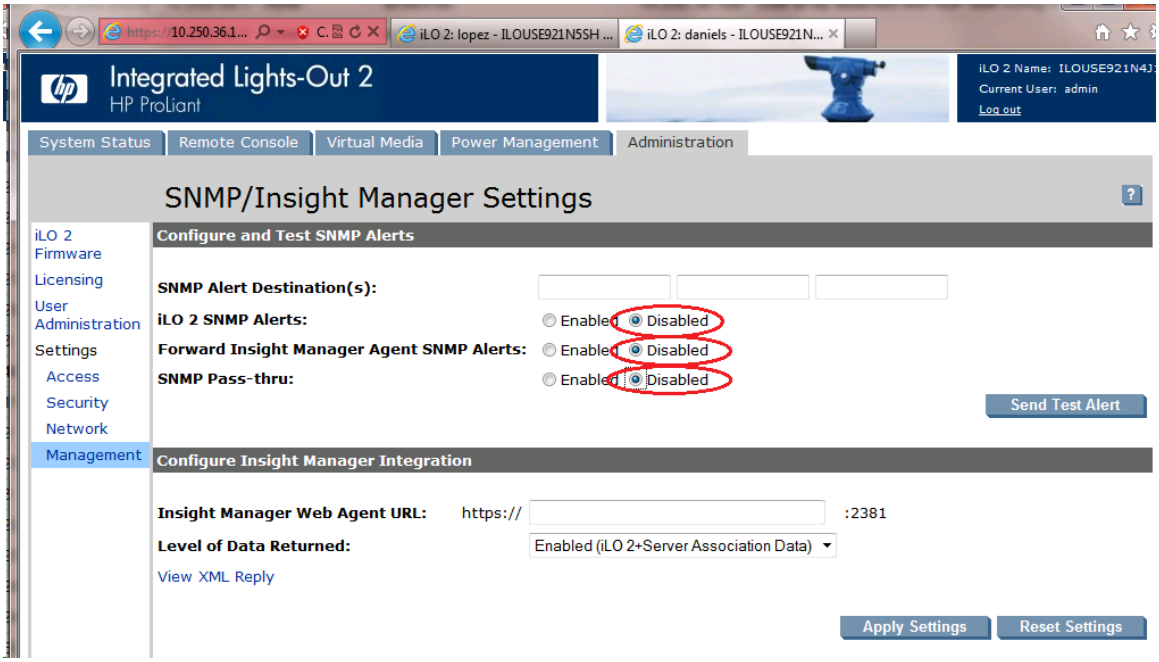
   The web page will refresh but no specific indication will be given that settings have been saved.



6. **iLO 2 Web UI:**

   To verify the setting change navigate away from the SNMP/Insight Manager Settings page and then go back to it to verify the SNMP settings as shown on the right.

   1. Click [Log out] link in upper right corner of page to log out of the iLO Web UI.



7. Complete for remaining iLO2 devices

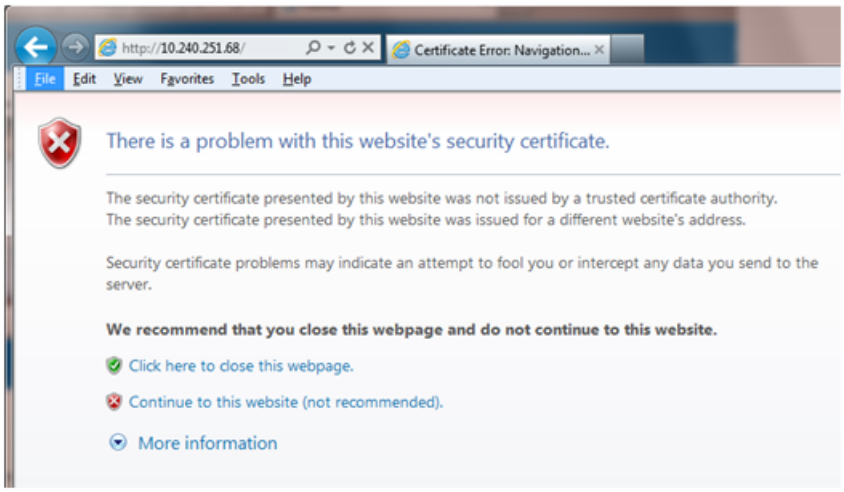
   Repeat this procedure all remaining iLO 2 devices on network.

I.2 Changing SNMP Configuration Settings for iLO 3 and iLO4

This procedure provides instructions to change the default SNMP settings for the HP ProLiant iLO 3 devices.

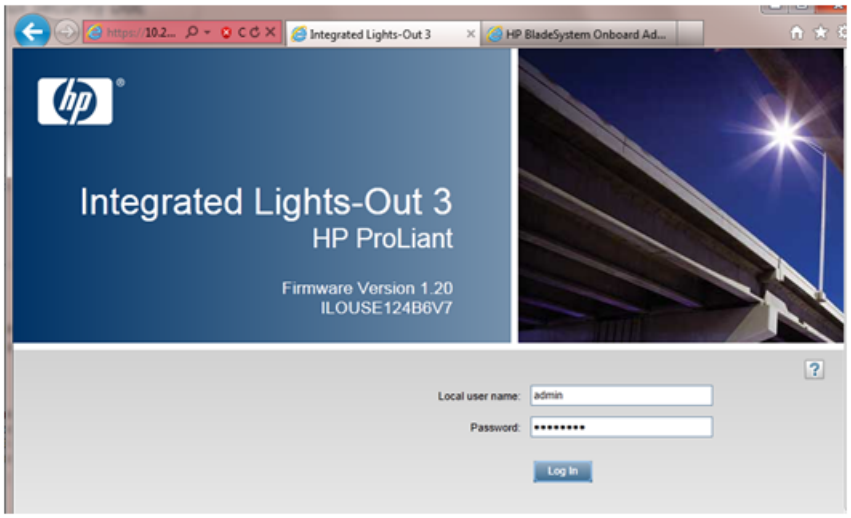
Perform this procedure for every iLO 3 device on the network. For instance, for every HP ProLiant G7 Blade and Rack Mount server.

1. **From Workstation:** Launch Internet Explorer 7.x or higher and connect to the iLO 3/iLO 4 device using "https://"



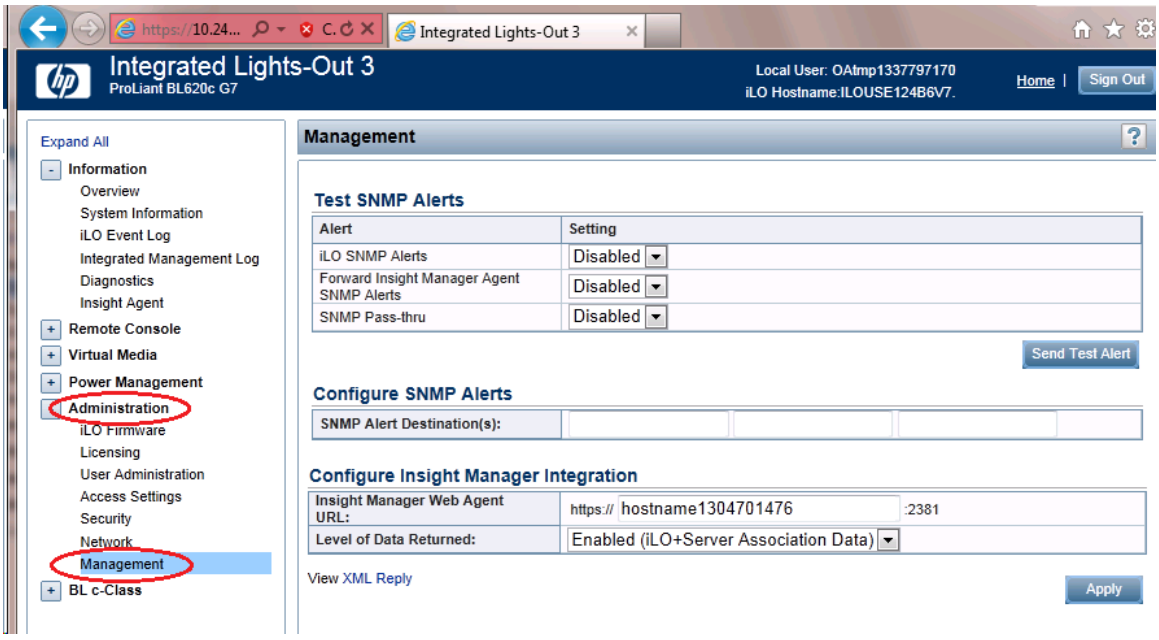
2. **iLO 3/iLO 4 Web UI:**
   The user should be presented the login screen shown below.

   Login to the GUI using an Administrator account name and password.



3. **iLO 3/iLO 4 Web UI:**
   The user should be presented the iLO 3/iLO 4 Overview page as shown below.

4. **iLO 3/iLO 4 Web UI:**
   1. Expand the [Administration] menu item in the left hand navigation pane.
   2. Select the [Management] sub-menu item to display the Management configuration page.

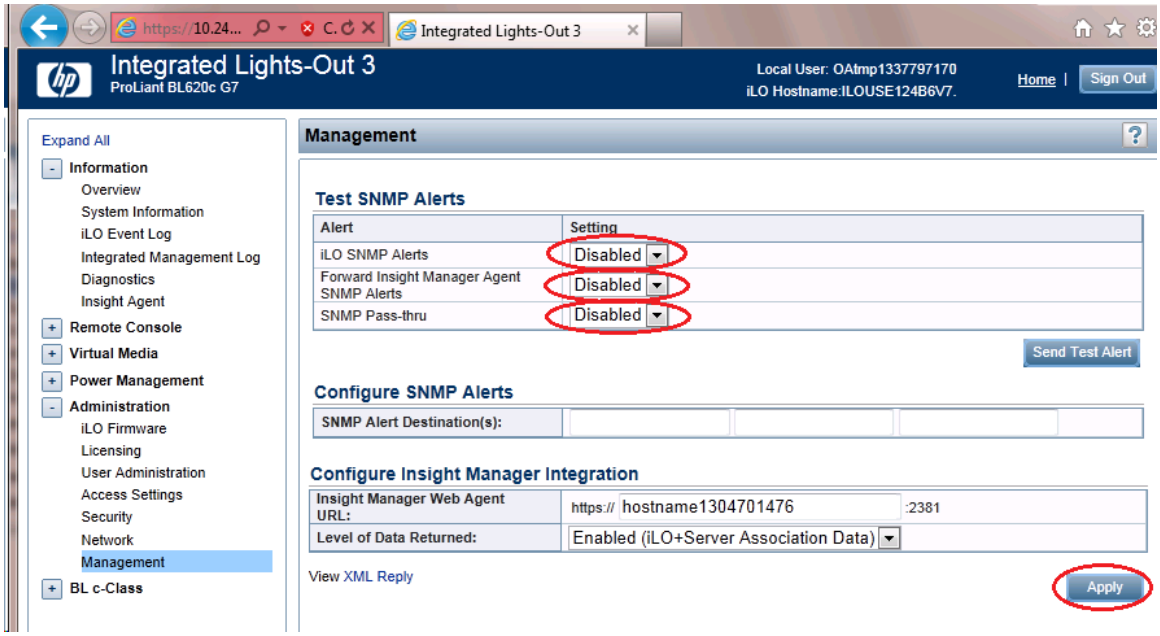


5. **iLO 3/iLO 4 Web UI:**

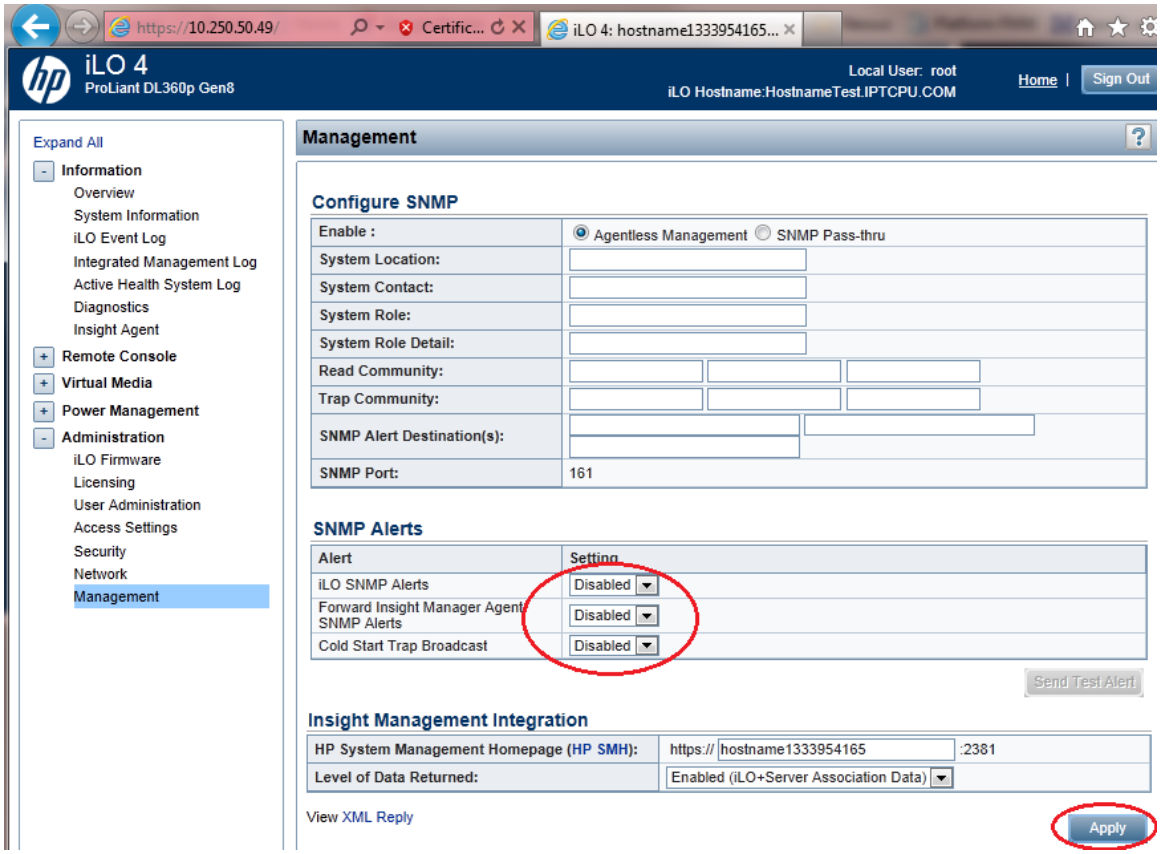
   The user should be presented the Management configuration page as shown on the right.
   1. Select setting [Disabled] for each of the 3 SNMP Alerts options as shown to the right.
   2. Click [Apply] to save the change.

On the iLO 3 the web page will refresh but no specific indication will be given that settings have been saved.

iLO3 Web UI:



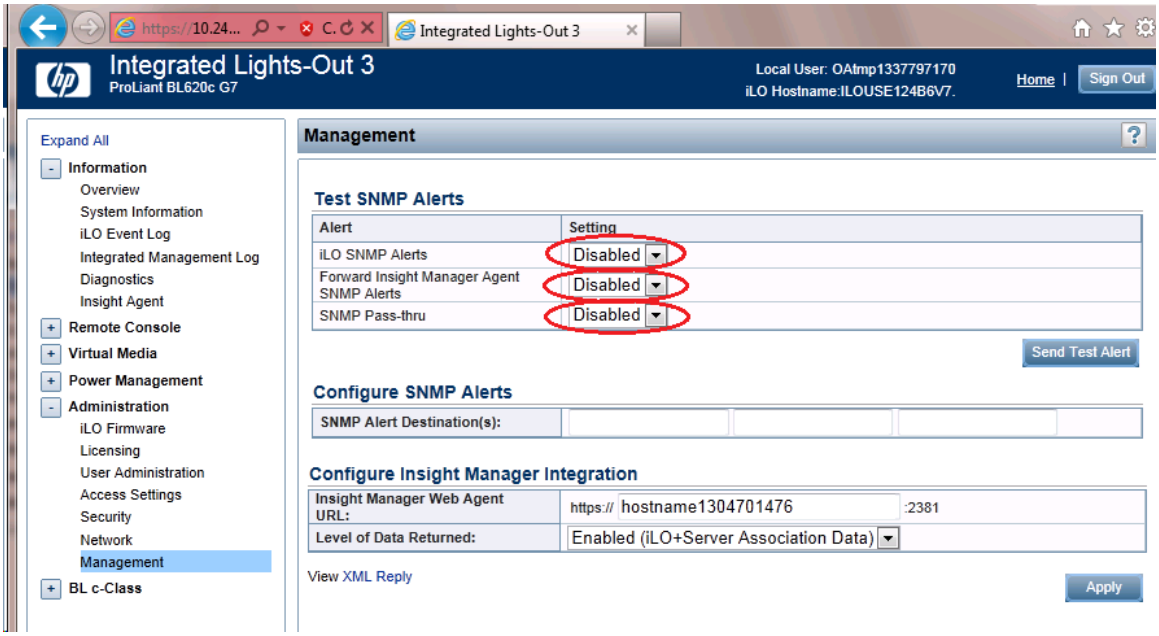
iLO4 Web UI:



6. **iLO 3/iLO 4 Web UI:**

   To verify the setting changes navigate away from the Management configuration page and then go page back to it to verify the SNMP settings as shown on the right.

   1. Click [Sign Out] link in upper right corner of page to log out of the iLO Web UI.



7. Complete for remaining iLO3/iLO 4 devices
   Repeat this procedure all remaining iLO 3/iLO 4 devices on network.

Appendix J

Upgrade Cisco 4948 PROM

Topics:

J.1 Upgrade Cisco 4948 PROM

1. **Virtual PM&C/Management Server:** Verify that the PROM image is on the system.

   If the appropriate image does not exist, copy the image to the server.

   Determine if the PROM image for the 4948/4948E/4948E-F is on the system.

   For a PM&C system:

   ```
   $ ls /var/TKLC/smac/image/<PROM_image_file>
   ```

   For a NON-PM&C system:

   ```
   $ ls /var/lib/tftpboot/<PROM_image_file>
   ```

   If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the Release Notes of the *HP Solutions Firmware Upgrade Pack* [2].

2. **Virtual PM&C/Management Server:** Attach to switch console.

   If upgrading the firmware on switch1B, connect serially to the switch by issuing the following command as admusr on the server:

   ```
   $ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
   switch1A_console
   Enter platcfg@pmac5000101's password: <platcfg_password>
   [Enter `^Ec?' for help]
   Press Enter
   ```

   If the switch is not already in enable mode ("switch#" prompt) then issue the "**enable**" command, otherwise continue with the next step.

   ```
   Switch> enable
   Switch#
   ```

   If upgrading the firmware on switch1B, connect serially to switch1B by issuing the following command as admusr on the PM&C server:

   ```
   $ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
   switch1B_console
   Enter platcfg@pmac5000101's password: <platcfg_password>
   [Enter `^Ec?' for help]
   Press Enter
   ```

   If the switch is not already in enable mode ("switch#" prompt), then issue the "**enable**" command, otherwise continue with the next step.

   ```
   Switch> enable
   Switch#
   ```

3. **Virtual PM&C/Management Server (switch console session):** Configure ports on the 4948/4948E/4948E-F switch.

To ensure connectivity, ping the management server's management vlan ip <pmac_mgmt_ip_address> address from the switch.

```
Switch# conf t
```

If upgrading the firmware on switch1A, use these commands:

```
Switch(config)# vlan <switch_mgmtVLAN_id>
Switch(config-vlan)# int vlan <switch_mgmtVLAN_id>
Switch(config-if)# ip address <switch1A_mgmtVLAN_ip_address> <netmask>
Switch(config-if)# no shut
Switch(config-if)# int gi1/40
```

If upgrading the firmware on switch1B, use these commands:

```
Switch(config)# vlan <switch_mgmtVLAN_id>
Switch(config-vlan)# int vlan <switch_mgmtVLAN_id>
Switch(config-if)# ip address <switch1B_mgmtVLAN_ip_address> <netmask>
Switch(config-if)# no shut
Switch(config-if)# int gi1/40
```

If the model is 4948, execute these commands:

```
Switch(config-if)# switchport trunk encap dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
Switch(config-if)# end
Switch# write memory
```

If the model is 4948E or 4948E-F, execute these commands:

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
Switch(config-if)# end
Switch# write memory
```

Now issue ping command:

Note: The ip address **<pmac_mgmt_ip_address>** should be in the reference table at the beginning of the Cisco 4948 configuration procedure that referenced this procedure.

```
Switch# ping <pmac_mgmtVLAN_ip_address>
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to <pmac_mgmt_ip_address>, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round trip min/avg/max = 1/1/4 ms
```

If ping is not successful , double check that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact My Oracle Support.

4. **Virtual PM&C/Management Server (Switch console session):** Upgrade PROM

```
Switch# copy tftp: bootflash:
Address or name of remote host []? <pmac_mgmt_ip_address>
Source filename []? <PROM_image_file>
Destination filename [<PROM_image_file>]? [Enter]
Accessing tftp://<pmac_mgmt__ip_address>/<PROM_image_file>...
```

```
Loading <PROM_image_file> from <pmac_mgmt__ip_address> (via Vlan2): !!!!!! [OK-
 45606 bytes]
45606 bytes copied in 3.240 secs (140759 bytes/sec)
Switch#
```

5. **Virtual PM&C/Management Server (Switch console session):** Reload the switch

```
Switch# reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm] [Enter]
=== Boot messages removed ===
```

Type **[Control-C]** when ***Type control-C to prevent autobooting*** is displayed on the screen.

6. **Virtual PM&C/Management Server (Switch console session):** Upgrade PROM

```
rommon 1 > boot bootflash:<PROM_image_file>
=== PROM upgrade messages removed ===
System will reset itself and reboot within few seconds....
```

7. **Virtual PM&C/Management Server (Switch console session):** Verify Upgrade

The switch will reboot when the firmware upgrade completes. Allow it to boot up. Wait for the following line to be printed:

```
Press RETURN to get started!
Would you like to terminate autoinstall? [yes]: [Enter]
Switch> show version | include ROM
ROM: 12.2(31r)SGA1
System returned to ROM by reload
```

Review the output and look for the ROM version. Verify that the version is the desired new version. If the switch does not boot properly or has the wrong ROM version, contact My Oracle Support.

8. **Virtual PM&C/Management Server:** Reset switch to factory defaults.

Connect serially to the switch as outlined in *Step 4*, and reload by performing the following commands:

```
Switch# write erase
Switch# reload
```

Wait until the switch reloads, then exit from console, enter **<ctrl-e><c><.>** and you will be returned to the server prompt.

Note: There might be messages from the switch, if asked to confirm, press enter. If asked yes or no, type in '**no**' and press enter.

Appendix K

Operational Dependencies on Platform Account Passwords

Topics:

This appendix describes the operational dependencies on Platform account passwords, in order to provide guidance in cases when the customer insists on modifying a default password. Note that changing passwords should be attempted only on systems that are fully configured and stable. Modifying passwords during system installation is strongly discouraged.

Note that prior to modifying the passwords stored on PM&C, you should perform backup of PM&C databases, in case you might need to return to default passwords. To accomplish this, execute steps *Step 5* through *Step 7* (inclusive) in procedure *4.4.1.1 Configure PM&C Application*. To restore the passwords stored in the backup file, you can refer to steps 4 through 9 (inclusive), in Procedure 1 of the *PM&C Disaster Recovery, Release 5.7 and 6.0*, E54388.

K.1 PM&C Credentials for Communication with Other System Components

This section covers the credentials that can be changed using the PM&C updateCredentials utility and the Platform dependencies users must be aware of to keep PM&C fully functional. Only the credentials that PM&C considers to be user accessible are listed here.

1. **oaUser**

   PM&C uses these credentials to communicate with OAs for all enclosures it monitors. Therefore, all active OAs must be updated to have the new credentials and then the updateCredentials should be used to match the credentials PM&C uses. Lastly, all enclosures already provisioned in the PM&C must be rediscovered.

   a) To update the credentials on the OA's, log into the active OA GUI. On the left hand side of the OA GUI, navigate to **Users/Authentication > Local Users > pmacadmin**. After supplying the new password, click on **Update User**.
   b) To update the credentials on the PM&C, execute the following on the UI:

```
$ sudo/usr/TKLC/smac/bin/updateCredentials --type=oaUser
```

   c) To rediscover an enclosure already provisioned in the PM&C inventory, log into the PM&C GUI and navigate to **Hardware > System Inventory > Cabinet XXX > Enclosure XXXXX** and click the "Rediscover Enclosure..." button.

2. **msa**

   All SAN controllers PM&C is expected to communicate with must be updated to have the new credentials and then the updateCredentials should be used to match credentials PM&C uses.

   a) To update the credentials, log into Fibre Channel Disk Controller via ssh as a manage user. Then execute:

```
# set password manage
```

   b) To update the credentials on the PM&C, execute the following in the UI:

```
$ sudo/usr/TKLC/smac/bin/updateCredentials --type=msa
```

3. **tpdPlatCfg**

   Changing these credentials has no impact on PM&C functionality.

   a) To update the credentials, log into the UI with platcfg credentials and execute:

```
$ passwd
```

4. **tvoeUser**

   TVOE administrator passwords need to be changed for all TVOE hosts PM&C is expected to communicate with and then the updateCredentials should be used to match the credentials PM&C uses. Note each time a new TVOE is installed its default password will have to be updated to match.

   a) To update the credentials, log into the TVOE UI with the admusr credentials and execute:

```
$ passwd
```

b) To update the credentials on the PM&C, execute the following on the UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=tvoeUser
```

5. **backupPassword**

   PM&C backup images are encrypted. The passphrase to encrypt the backup files may be changed. This *only* changes the encryption for future backups; prior backups cannot be restored without changing to the original pass phrase as shown below. A restore task that fails with a "Failed to decrypt backup file" reason is an indication of this condition.

   a) To update the passphrase on a PM&C, exceute the following in the UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=backupPassword
```

6. **remoteBackupUser**

   If pmacop credentials are changed on a redundant PM&C, the updateCredentials should be used to match credentials the primary PM&C uses.

   a) To update the credentials on a redundant PM&C, log into the redundant PM&C UI with the pmacop credentials and execute:

```
$ passwd
```

   b) To update the credentials on the primary PM&C, execute the following in primary PM&C UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=remoteBackupUser
```

7. **oobUser**

   These credentials are used to communicate with the iLO of RMS, when no other credentials have been specified when the RMS was provisioned in PM&C. So the user has the option to modify this default password, or the RMS can be edited/added in the GUI with its specific credentials.

   a) To update the credentials on an RMS iLO, log into the iLO GUI and navigate to **Administration > User Administration**. Check the box next to root password and click the **Edit** button. After the password is changed, click **Update User**.

   b) To modify the default oobUser credentials on the PM&C, execute the following in the UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=oobUser
```

   c) To add a RMS to PM&C system inventory with its unique iLO password, refer to *4.9.1 Add Rack Mount Server to the PM&C System Inventory*.

   d) To edit iLO password of a specific RMS already in PM&C system inventory, refer to *O.1 Edit Rack Mount Server in the PM&C System Inventory*.

K.2 PM&C GUI Accounts Credentials

Modification of any of the PM&C GUI accounts has no system impact. The PM&C GUI users can be updated by logging into the PM&C GUI as pmacadmin, and navigating to **Administration > Users**.

Select the user from the first **Username** pull down menu and click the **Set Password** button. Then enter the new password twice and click the **Continue** button.

K.3 PM&C Linux User Accounts Credentials

PM&C Linux User Accounts Credentials

Modification of any PM&C Linux user account has no system impact with the exception of the "pmacop" user and "admusr" credentials. If pmacop credentials are changed on a redundant PM&C, the updateCredentials should be used to match the credentials that the primary PM&C uses. If admusr credentials are changed after configuration of the netconfig repository, then netconfig services must be deleted and re-added using the new credentials.

1. To update the pmacop credentials on a redundant PM&C, log in to the redundant PM&C UI with the pmacop credentials and execute:

```
$ passwd
```

2. To update the pmacop credentials the primary PM&C uses to communicate with the redundant PM&C, execute the following in primary PM&C UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=pmacop
```

Appendix L

How to Access a Server Console Remotely

Topics:

L.1 How to Access a Server Console Remotely

Procedure Reference Table:

Steps within this procedure may refer to variable data indicated by text within "<>". Refer to this table for the proper value to insert depending on your system type.

Variable	Value
<ilo_admin_user>	Privileged username for HP iLO access

1. **Access the iLO/ILOM GUI**

   Using a laptop or desktop computer connected to the customer network, navigate with Internet Explorer to the IP address of the iLO/ILOM of the Management Server. Click on "Continue to this website (not recommended)." if prompted.

   For HP servers:

   a) Log in to the iLO as the user <ilo_admin_user>
   b) If the iLO is an iLO 2, configure Hot Keys

      The iLO GUI will indicate the iLO version as iLO 2 ("Integrated Lights-Out 2"), iLO 3, iLO 4, etc.

      If this is an iLO 2, perform the following Hot Key configuration:

      1. Click the **Remote Console** tab
      2. Click the **Settings** menu item and then the **Hot Keys** sub-tab
      3. In the row starting with **Ctrl-T** change the first dropdown to **L_CTRL** and the second dropdown to **]** (right bracket). The rest of the dropdowns in the row should be **NONE**.
      4. In the row starting with **Ctrl-v:** change the first drop down to **L_CTRL,** the second dropdown to **R_Shift** and the third dropdown to "-". The rest of the dropdowns in the row should be **NONE**.

         Click **Save Hot Keys**. As a result, pressing **Ctrl-T** rather than **Ctrl-]** exits the console of a TVOE guest and return to the console of the TVOE host. And pressing **Ctrl-v** disconnects the switch console session.

2. **Launch the Remote Console Window**

   For HP servers:

   Click the **Remote Console** tab and select **Remote Console** to launch the remote console in a new window.

   If prompted, click "Continue" on the popup labeled "Security Warning" that asks "Do you want to continue?".

   For Oracle rack mount servers:

   Launch the **Remote Console** window by clicking on the **Launch** button beside **Remote Console** in the **Actions** frame.

If prompted, click "Continue" on the popup labeled "Security Warning" asking "Do you want to continue?".

If prompted, click "Run" on the popup asking "Do you want to run this application?"

3. **Log in to the Console**

   In the Remote Console window, log in to the console as user "admusr":

```
login as: admusr
Password:
Last login: Wed Jun  5 17:52:28 2013
[admusr@tvoe ~]$
```

Appendix M

Configure Speed and Duplex for 6125XLG LAG Ports (netConfig)

Topics:

M.1 Configure Speed and Duplex for 6125XLG LAG Ports (netConfig)

This utility procedure is intended only for use with 1GE LAG uplinks from HP 6125XLG enclosure switches to Cisco 4948/E/-F product aggregation switches or the customer network. Configuring speed and duplex on the LAG ports turns off auto-negotiation for the individual links, and must be performed on both switches for all participating LAG links. This procedure addresses a known weakness with auto-negotiation on 1GE SFPs and the 6125XLG which causes 1GE links to take longer than expected to become active.

1. **Virtual PM&C:** List configured link aggregation groups on the 6125XLG enclosure switch. Capture the LAG id connected to the 4948/E/E-F product aggregation switch or the customer network. In the following example, LAG id 1 is identified as the 4x1GE LAG requiring speed and duplex configuration.

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> listLinkAggregations

LAG: 1
```

2. **Virtual PM&C:** Get the list of interfaces configured for the LAG on the 6125XLG. In the following example, LAG id 1 is inspected, and is shown to include interfaces tenGE17-20.

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> getLinkAggregation
 id=1


Type: Dynamic

Description: ISL_to_agg_switch

Switchport: =(
link-type trunk
vlan all
)

Interfaces: =(
tenGE17
tenGE18
tenGE19
tenGE20
)
```

3. **Virtual PM&C:** Inspect the switch LAG port configurations and verify speed and duplex are set on the LAG interfaces, as shown in this example:

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> setSwitchport
interface=tenGE17-20 speed=1000 duplex=full
```

4. **Virtual PM&C:** Inspect the switch LAG port configurations and verify speed and duplex are set on the LAG interfaces, as shown in this exapmle:

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> getSwitchport
interface=tenGE17-20

Switchport: trunk
```

```
Description: Ten-GigabitEthernet1/1/5 Interface

Speed: 1000Mbps

Duplex: full

VLAN =(
1(default
2-4094
)

Default VLAN: 1
```

Appendix N

Determining which Onboard Administrator is Active

Topics:

N.1 Determining Which Onboard Administrator Is Active

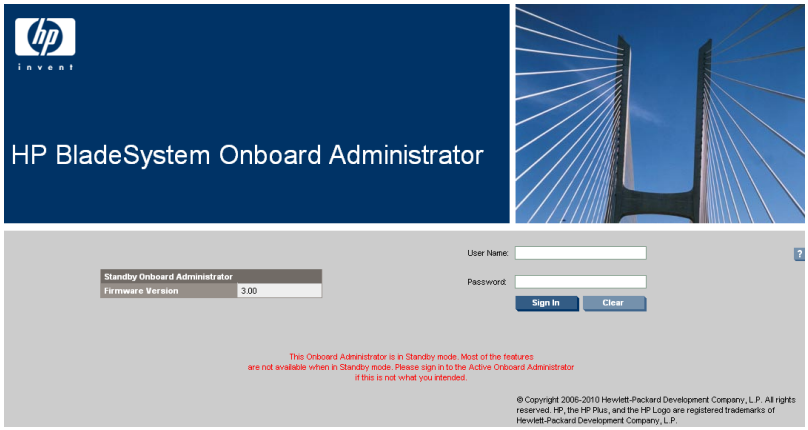
This appendix describes how to determine which Onboard Administrator is active in an enclosure with two OAs.

OA GUI: Determine which OA is Active

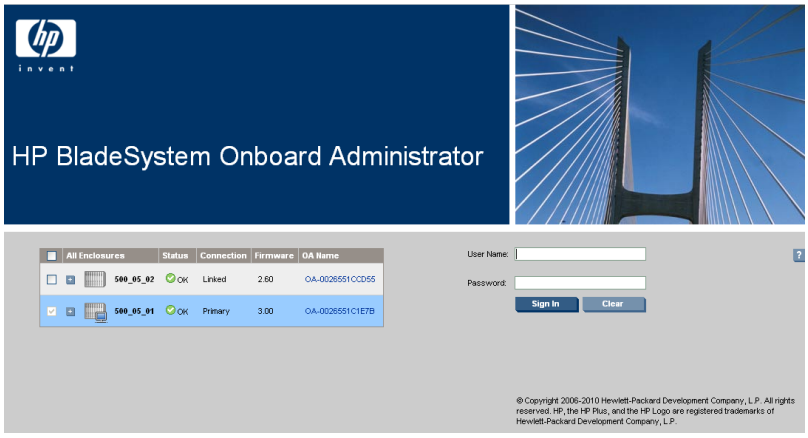
Open your web browser and navigate to the IP address of one of the Administrators:

```
https://<OA_ip>
```

If you see the following page, you have navigated to a GUI of the Standby Onboard Administrator as indicated by the red warning. In such case, navigate to the other Onboard Administrator IP address.



If you navigate the GUI of active Onboard Administrator GUI, the enclosure overview table is available in the left part of the login page as below.



Appendix O

Edit Rack Mount Server in the PM&C System Inventory

Topics:

O.1 Edit Rack Mount Server in the PM&C System Inventory

This procedure provides instructions to edit a rack mount server in the PM&C system inventory. This option is used to modify the name, cabinet, or credentials of an already provisioned rack mount server.

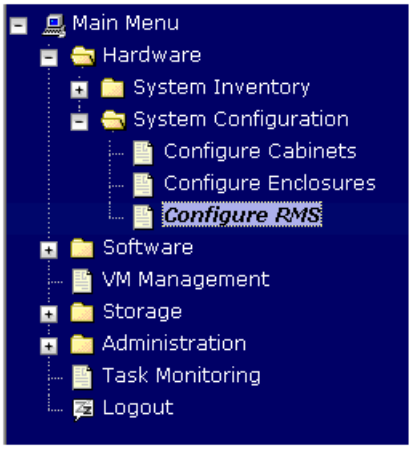
1. **PM&C GUI:** Login

   Open web browser and enter:

   ```
   https://<pmac_management_network_ip>
   ```

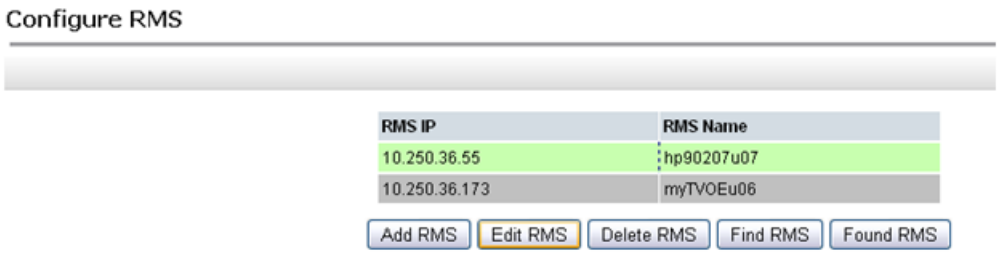
2. **PM&C GUI:** Configure RMS

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure RMS**.

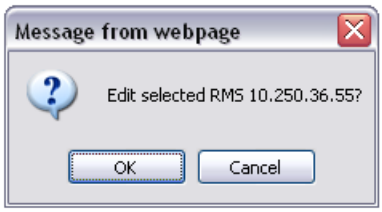
3. **PM&C GUI:** Edit RMS

   On the Configure RMS panel, select one row in the list of rack mount servers and click the **Edit RMS** button.

4. **PM&C GUI:** Confirmation

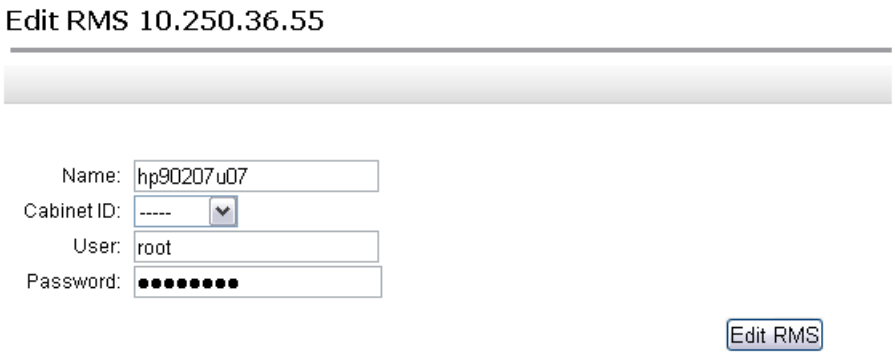
   A popup window appears asking you to confirm your desire to edit the rack mount server, click OK.



5. **PM&C GUI:** Edit RMS

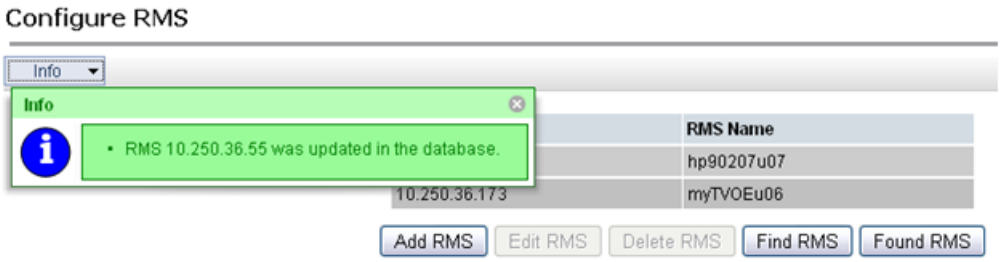
   In the Edit RMS panel, modify the field that needs to be altered.

   Then click on the **Edit RMS** button.

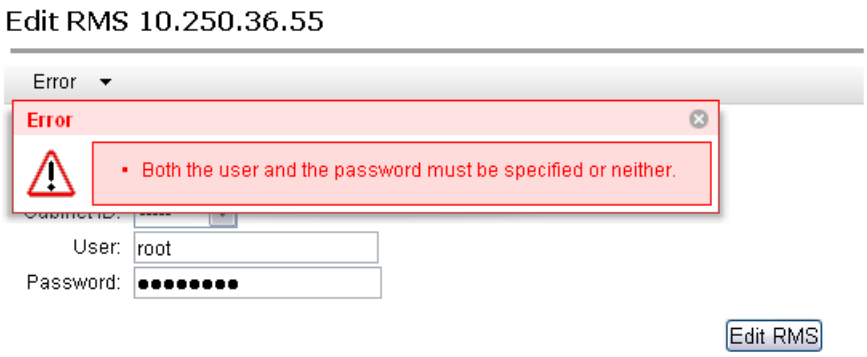


6. **PM&C GUI:** Check errors

   If no error is reported to the user you will see the following:



   Or you will see an error message:


Edit RMS 10.250.36.55
Error
Error
Both the user and the password must be specified or neither.
User:
root
Password:
Edit RMS

Appendix P

Install NetBackup Client on TVOE Server (optional)

Topics:

This procedure includes all information necessary to install the NetBackup software on the TVOE Host. This must be done after the Aggregate Switches are properly configured. The procedure assumes all necessary NetBackup network configuration has been completed from *4.1 Configure and IPM Management Server*.

Note: The steps in this appendix can only be performed after the Aggregation Switches in *4.3 Configure Aggregation Switches* have been properly configured.

R.1 Set Up and Install NetBackup Client

If NetBackup is configured on this system, this step will set up and install the NetBackup Client on a TVOE host.

Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to back up the following files from the TVOE host:

```
/var/TKLC/bkp/*.iso
```

1. **TVOE Server:** Log in as the admusr user.
2. **TVOE Server:** Open firewall ports for NetBackup using the following commands:

```
$ sudo ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt
/usr/TKLC/plat/etc/iptables
$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig
```

3. **TVOE Server:** Enable platcfg to show the NetBackup Menu Items by executing the following commands:

```
$ sudo platcfgadm --show NBConfig
$ sudo platcfgadm --show NBInit
$ sudo platcfgadm --show NBDeInit
$ sudo platcfgadm --show NBInstall
$ sudo platcfgadm --show NBVerifyEnv
$ sudo platcfgadm --show NBVerify
```

4. Use the **vgguests** volume group to create an LV and filesystem for the NetBackup Client software.
   a) **Server:** Log in as the admusr user.
   b) **Server:** Create a storageMgr configuration file that defines the LV to be created.

```
$ sudo echo "lv --mountpoint=/usr/openv --size=2G --name=netbackup_lv --vg=$VG
> /tmp/nb.lvm
```

   This example uses the $VG as the volume group. Replace $VG with the desired volume group as specified by the application group.

   c) **Server:** Create the LV and filesystem by using storageMgr.

```
$ sudo /usr/TKlC/plat/sbin/storageMgr /tmp/nb.lvm
```

   This will create the LV, format it with a filesystem, and mount it under /usr/openv/.

   Example output:

```
Called with options: /tmp/nb.lvm
VG vgguests already exists.
Creating lv netbackup lv.
Volume netbackup_lv will be created.
Success: Volume netbackup_lv was created.
Creating filesystem, this may take a while.
Updating fstab for lv netbackup_lv.
Configuring existing lv netbackup_lv.
```

The LV for NetBackup has been created.

5. NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite is for the purpose of supporting Disaster Recovery at the customer site. This procedure provides instructions for installing or upgrading the Netbackup Client software on an application server.

   See *A.3 Create NetBackup Client Config File* for more information.

   Note: Failure to install the NetBackup Client properly (i.e., by neglecting to execute this procedure) may result in the NetBackup Client being deleted during an Oracle software upgrade.

   a) **Choose NetBackup Client Install Path:**

      There are two different ways to install NetBackup Client. The following is a guide to which method to use:

      - See *A.1 Netbackup Client Install/Upgrade with nbAutoInstall* for more information.
      - See *A.2 NetBackup Client Install/Upgrade with platcfg* for more information.

      Chosen Procedure: _____

   b) Execute the chosen procedure.

   c) **Application Console:**

      Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias.

      Note: If NetBackup Client has successfully been installed then the NetBackup server's hostname in the "/usr/openv/netbackup/bp.conf" file. It will be identified by the "SERVER" configuration parameter as is shown:

      List NetBackup server's hostname:

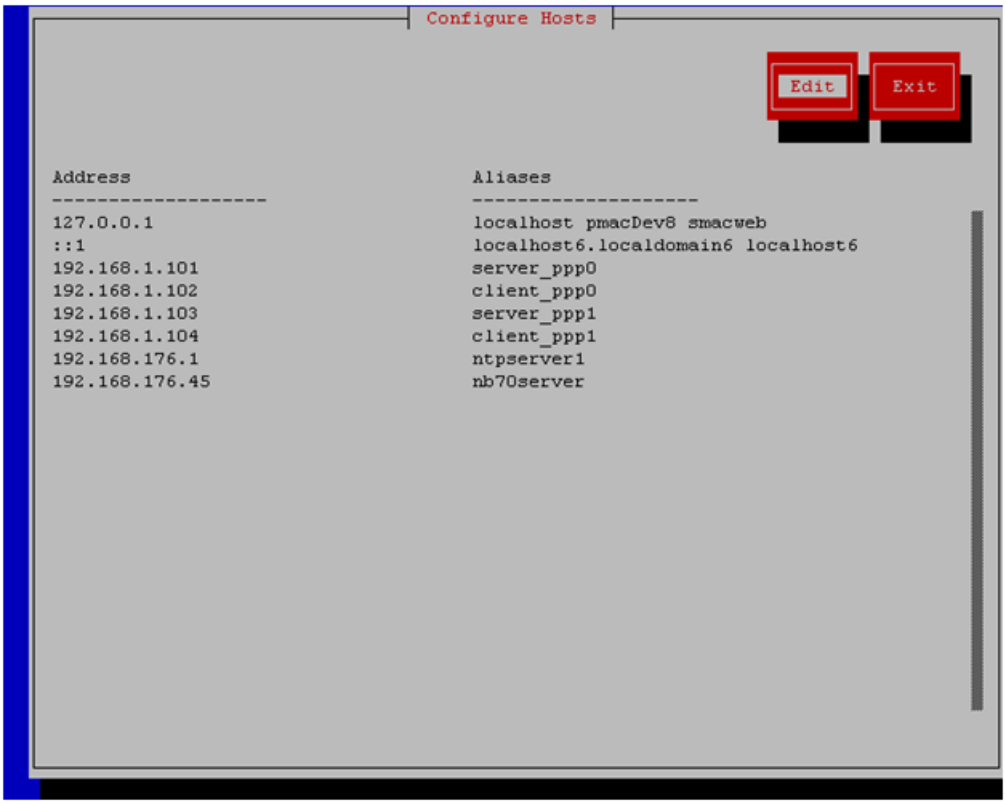
```
$ sudo cat /usr/openv/netbackup/bp.confSERVER = nb70server CLIENT_NAME = pmacDev8
```

      Note: In the case of nbAutoInstall NetBackup Client may not yet be installed. For this situation the "/usr/openv/netbackup/bp.conf" file cannot be used to find the NetBackup server alias.

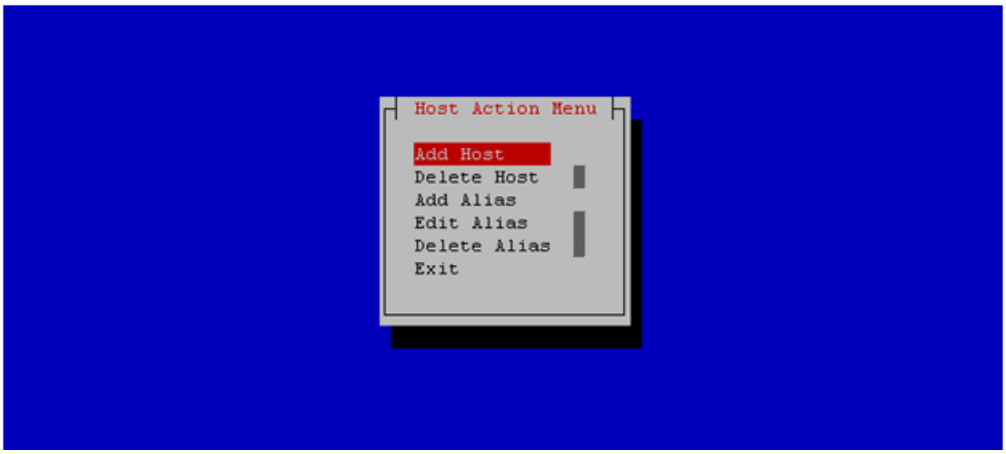
      Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
$ sudo su - platcfg
```

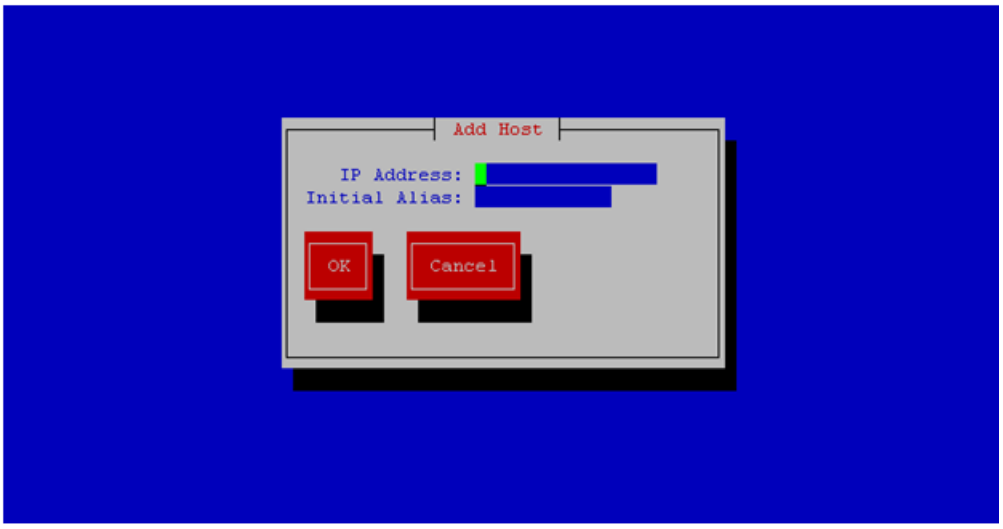
      Navigate to **Network Configuration** > **Modify Hosts File**



Select **Edit**. The Host Action Menu will be displayed.



Select **Add Host** and enter the appropriate data.



Select **OK**, confirm the host alias was added, and exit the Platform Configuration Utility.

6. **TVOE Server:** Create softlinks for TVOE-specific NetBackup notify scripts.

```
$ sudo mkdir -p /usr/openv/netbackup/bin
$ sudo ln -s /usr/TKLC/plat/sbin/bpstart_notify
/usr/openv/netbackup/bin/bpstart_notify
$ sudo ln -s /usr/TKLC/plat/sbin/bpend_notify
/usr/openv/netbackup/bin/bpend_notify
```

Application Console: Netbackup client software installation complete.

Appendix Q

Disabling SNMP on the OA

Topics:

P.1 Disabling SNMP on the OA

1. **If necessary, log in to the Active OA.**
2. **Navigate to the SNMP Settings.**

   Use either the **First Time Setup Wizard SNMP Settings** menu item or the **Enclosure Information** > **Enclosure Settings** > **SNMP Settings** menu item.

3. **Uncheck the Enable SNMP checkbox.**