Oracle® Communications PMAC 6.4

Tekelec Platform Configuration Reference Guide

E81293 Revision 01

February 2017

ORACLE®

Oracle Communications PMAC 6.4 Tekelec Platform Configuration Reference Guide

Copyright © 2016, 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1 Introduction....9

1.1 References....10
1.2 Acronyms....10
1.3 Terminology....11
1.4 My Oracle Support (MOS)....13
1.5 Emergency Response....13
1.6 Customer Training....14
1.7 Locate Product Documentation on the Oracle Help Center Site....14

Chapter 2 Acquiring Firmware....15

2.1 Acquiring Firmware....16
2.1.1 HP....16
2.1.2 Oracle Rack Mount Server....17

Chapter 3 Procedures....18

3.1 Networking....19
3.1.1 Configure netConfig Repository....19
3.1.2 Aggregation Switch - netConfig Procedures....32
3.1.3 C-Class Enclosure Switch - netConfig Procedures....86
3.1.4 Utility Procedures....110
3.2 Brocade Switch - SwitchConfig Procedures....134
3.2.1 Configure Brocade Switches....134
3.2.2 Upgrade Brocade Switch Firmware....137
3.2.3 Configure Zones in Brocade Switches....138
3.2.4 Configure Brocade Switch SNMP Trap Target....142
3.3 SAN Storage Arrays Procedures....146
3.3.1 Set IP on Fibre Channel Disk Controllers....146
3.3.2 Configuring Fibre Channel Disk Controllers....147
3.3.3 Configuring Advanced Settings on MSA2012fc Fibre Channel Disk Controllers....149
3.3.4 Configuring Advanced Settings on P2000 Fibre Channel Disk Controllers....150
3.3.5 Upgrade Firmware on MSA 2012fc Disk Controllers....151
3.3.6 Upgrade Firmware on MSA P2000 Disk Controllers....151

3.3.7 Replacing a Failed Disk in MSA 2012Fc Array....152
3.3.8 Replacing a Failed Disk in MSA P2000 Disk Array....153
3.4 Blade Server Procedures....156
3.4.1 Upgrade Blade Server Firmware....156
3.4.2 Confirm/Upgrade Blade Server BIOS Settings....157
3.4.3 Configure Blade Server iLO Password for Administrator Account....164
3.4.4 Accessing the Server Virtual Serial Port....165
3.4.5 Configure Syscheck Default Route Ping Test....166
3.4.6 Preparing a System for Extended Power Outage....167
3.4.7 Bringing Up a System After Extended Power Outage....167
3.5 C7000 Enclosure Procedures....168
3.5.1 Configure Initial OA IP....168
3.5.2 Configure Initial OA Settings Using the Configuration Wizard....170
3.5.3 Configure OA Security....183
3.5.4 Upgrade or Downgrade OA Firmware....184
3.5.5 Store OA Configuration on Management Server....184
3.5.6 Restore OA Configuration from Management Server....187
3.5.7 Adding a redundant Onboard Administrator to enclosure....189
3.5.8 Replacing Onboard Administrator....189
3.5.9 Updating IPv4 Addressing....193
3.5.10 Updating IPv6 Addressing....197
3.5.11 Add SNMP Trap Destination on OA....201
3.5.12 Delete SNMP Trap Destination on OA....204
3.6 Management Server Procedures....206
3.6.1 IPM Management Server....206
3.6.2 Upgrade Management Server Firmware....206
3.7 PM&C Procedures....208
3.7.1 Deploying Virtualized PM&C Overview....208
3.7.2 Installing TVOE on the Management Server....211
3.7.3 TVOE Network Configuration....212
3.7.4 Deploy PM&C Guest....227
3.7.5 Setup PM&C....229
3.7.6 Configure PM&C Application....236
3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory....240
3.7.8 Edit an Enclosure in the PM&C System Inventory....245
3.7.9 Adding ISO Images to the PM&C Image Repository....247
3.7.10 IPM Servers Using PM&C Application....251
3.7.11 Install/Upgrade Applications Using PM&C....254
3.7.12 Patch Applications Using PM&C....257
3.7.13 Install PM&C on Redundant DL360 or DL380....260
3.7.14 Configure Management Server SNMP Trap Target....263

3.7.15 PM&C NetBackup Client Installation and Configuration....264
3.7.16 Add Rack Mount Server to the PM&C System Inventory....265
3.7.17 Edit Rack Mount Server in the PM&C System Inventory....269
3.7.18 Finding and Adding a Rack Mount Server to the PM&C System Inventory....272
3.7.19 Accepting Upgrades Using PM&C....275
3.7.20 Rejecting Upgrades Using PM&C....277
3.7.21 Accepting Patches Using PM&C....279
3.7.22 Rejecting Patches Using PM&C....281
3.7.23 Initialize PM&C Application....283
3.7.24 Configure PM&C Application Guest NetBackup Virtual Disk....284
3.7.25 PM&C Guest Migrate NetBackup Client to New File System....285
3.7.26 Initialize PM&C Application using CLI....285
3.7.27 Initialize PM&C Application using the GUI....287
3.7.28 Updating the TVOE Host SNMP Community String from the GUI....296
3.7.29 Configure PM&C Application Guest Isoimages Virtual Disk....303
3.7.30 Certificate Management....305
3.7.31 Using the PM&C File Management System....314
3.7.32 Deleting ISO Images From the PM&C Image Repository....318
3.7.33 Configuring PM&C Domain Name System....320
3.7.34 Setting User Authentication on the PM&C....326
3.7.35 Configuring the PM&C into an existing Single-Sign-On (SSO) Domain....328
3.7.36 Configuring an LDAP Server on the PM&C....331
3.7.37 Transfer Image from PM&C Repository to Other Servers....334
3.8 Configuring SAN....337
3.8.1 Configure SAN Storage Using PM&C Application....337
3.8.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation....339
3.9 Virtualization Procedures....341
3.9.1 Create guest server using PM&C application....341
3.9.2 Delete guest server using PM&C application....350
3.9.3 Create guest server from guest archive using PM&C application....353
3.10 General TPD Based Application Procedures....361
3.10.1 Backup Procedure for TVOE....361
3.10.2 Configure NTP on TPD based Application....364
3.10.3 Add SNMP trap destination on TPD based Application....368
3.10.4 Delete SNMP trap destination on TPD based Application....371
3.10.5 Application NetBackup Client Install Procedures....374
3.10.6 Changing SNMP Configuration settings for iLO2....377
3.10.7 Changing SNMP Configuration Settings for iLO 3 and iLO4....381
3.10.8 Change SNMP Configuration Settings for ILOM....385

3.10.9 Netbackup Client Install with nbAutoInstall....386
3.10.10 NetBackup Client Install/Upgrade with platcfg....387
3.10.11 Create LV and Filesystem for NetBackup Client Software....393
3.10.12 Migrate NetBackup Client to New Filesystem....393
3.10.13 Create NetBackup Client Config File....394
3.11 TVOE Host Procedures....395
3.11.1 Enable Virtual Guest Watchdogs as appropriate for the application....395
3.11.2 TVOE NetBackup Client Configuration....396

Appendix A: Using WinSCP....398
A.1 Using WinSCP....399

Appendix B: P2000 MSA USB Driver Installation....401
B.1 P2000 MSA USB Driver Installation....402

Appendix C: Determining which Onboard Administrator is Active....405
C.1 Determining Which Onboard Administrator Is Active....406

Appendix D: Worksheet: netConfig Repository....407
D.1 Worksheet: netConfig Repository....408

Appendix E: PM&C Features Configuration....409
E.1 PM&C Feature Configuration....410

Appendix F: How to Access a Server Console Remotely....412
F.1 How to Access a Server Console Remotely....413

Appendix G: How to Attach an ISO Image to a Server Using the iLO or ILOM....415
G.1 How to Attach an ISO Image to an HP Server Using the iLO....416
G.2 How to Attach an ISO Image to an Oracle Rack Mount Server Using the ILOM....422

Appendix H: How to Exit a Guest Console Session on an iLO....427

H.1 How to Exit a Guest Console Session on an iLO....428

Appendix I: Upgrade Cisco 4948 PROM....429

I.1 Upgrade Cisco 4948 PROM....430

Appendix J: Operational Dependencies on Platform Account Passwords....433

J.1 PM&C Credentials for Communication with Other System Components....434
J.2 PM&C GUI Accounts Credentials....435
J.3 PM&C Linux User Accounts Credentials....436
J.4 NetConfig Manager Password....436

Appendix K: Disabling SNMP on the OA....437

K.1 Disabling SNMP on the OA....438

Appendix L: How to Downgrade Firmware on a 6125G Switch....439

L.1 Downgrade 6125G Switch Firmware....440

Appendix M: How to Downgrade Firmware on a 6125XLG Switch....446

M.1 Downgrade 6125XLG Switch Firmware....447

Appendix N: How to Change Switch Passwords (netConfig)....454

N.1 How to Change Switch Passwords (netConfig)....455

Appendix O: How to Uninstall Symantec NetBackup Client....457

O.1 Uninstall Symantec NetBackup Client....458

Appendix P: How to Increase the PM&C Netbackup Filesystem Size....465

P.1 Increase the PM&C Netbackup Filesystem Size....466

List of Tables

Table 1: Acronyms.....10

Table 2: Terminology.....12

Chapter 1

Introduction

Topics:

- *References.....10*
- *Acronyms.....10*
- *Terminology.....11*
- *My Oracle Support (MOS).....13*
- *Emergency Response.....13*
- *Customer Training.....14*
- *Locate Product Documentation on the Oracle Help Center Site.....14*

This document describes the procedures to configure third-party hardware and platform components. Configurable hardware components include HP ProLiant rack mount and Oracle rack mount servers (RMS) and Cisco switches, HP c7000 enclosures with HP blade servers, HP and Cisco switches, and HP external storage systems. Platform components include the firmware for various hardware components as well as the Platform Management & Configuration (PM&C) application to provision and manage those components when hosting feature applications.

Prior to executing any procedure in this document, power must be available to each component and all network cabling must be in place.

The procedures in this document are not presented in any specific order. Each procedure describes a discrete action. Application engineers will reference individual procedures in their specific installation and configuration procedures. It is the application documentation that will provide the proper sequencing of procedures, application specific supplemental steps, and the passwords to be used during the configuration.

Procedures from this document can be referenced by their section numbers, for example:

Execute Section *3.6.2.1 DL360/DL380 Server Firmware Upgrade*.

For all other Platform Releases, refer to the appropriate document.

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. *TPD Initial Product Manufacture Software Installation Procedure,* E53017
2. *HP Solutions Firmware Upgrade Pack*, version 2.x.x (the latest version is recommended if an upgrade is to be performed, otherwise version 2.2.10 is the minimum). This pack includes both documentation and firmware media.
3. *HP Solutions Firmware Upgrade Pack, Software Centric Release Notes* (the latest version is recommended if an upgrade is performed, otherwise version 2.2.10 is the minimum).
4. *Oracle Firmware Upgrade Pack Release Notes*, version 3.x.x (the latest version is recommended if an upgrade is performed, otherwise version 3.1.7 is the minimum).
5. *Oracle Firmware Upgrade Pack Upgrade Guide*, version 3.x.x
6. *PM&C Incremental Upgrade Procedure, Release 6.2*, E53487
7. *PM&C Disaster Recovery , Release 6.2*, E67647

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
FLOM	Flexible LAN on Motherboard
FMA	File Management Area
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering

Acronym	Definition
HP FUP	HP Firmware Upgrade Pack
iLO	Integrated Lights Out remote management port
iLOM	Integrated Lights Out Manager
IE	Internet Explorer
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MP	Message Processing Server
MSA	Modular Smart Array
NAPD	Network Architecture Planning Diagram
NMS	Network Management System
NO	Network OAM&P Server
OA	HP Onboard Administrator
OAM&P	Operations, Administration, Maintenance, and Provisioning
OS	Operating System (e.g. TPD)
OSDC	Oracle Software Deliverly Cloud
PM&C	Platform Management & Configuration
QOS	Quality of Service
RMS	Rack Mount Server
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SO	System OAM&P server
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:

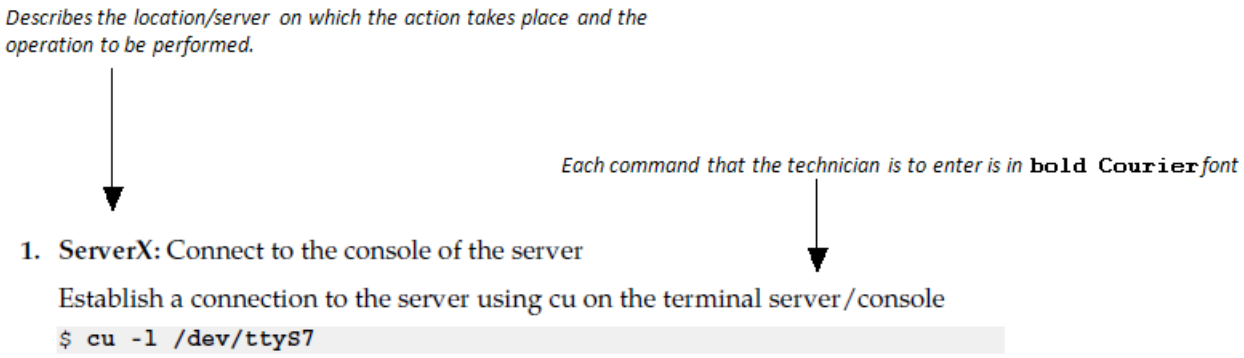


Figure 1: Example Of An Instruction That Indicates The Server To Which It Applies

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 or Oracle RMS 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 Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) 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 *http://www.adobe.com*.

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.
3. Under the Oracle Communications subheading, click the **`Oracle Communications documentation`** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **`PDF`** link, select **`Save target as`** (or similar command based on your browser), and save to a local folder.

Chapter 2

Acquiring Firmware

Topics:

- *Acquiring Firmware.....16*

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 configuration.

Platform 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)
- Oracle Rack Mount Servers
- 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* at Industries -> Communications -> Tekelec.

For customers that purchased their hardware through Oracle, or previously Tekelec, 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 PMAC 6.3 is *HP Solutions Firmware Upgrade Pack 2.2.10*. 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* contains multiple items including media and documentation which are used to upgrade HP firmware.

The two pieces of required documentation provided in the *HP Solutions Firmware Upgrade Pack 2.x.x* releases are:

- HP Solutions Firmware Upgrade Pack Upgrade Guide
- HP Solutions Firmware Upgrade Pack Release Notes

The two 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 MISC Firmware ISO image

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

2.1.2 Oracle Rack Mount Server

The Oracle Firmware Upgrade Pack (FUP) consists of documentation used to assist in the upgrading of Oracle rack mount servers. The pack consists of an *Upgrade Guide* and *Release Notes*. The current minimum supported firmware release for PMAC 6.3 is 3.1.7. However, if a firmware update is required, it is recommended to use the latest available release. Firmware components can be downloaded from My Oracle Support at *https://support.oracle.com*. Refer to the appropriate FUP Release Notes for directions on how to acquire the firmware.

Chapter 3

Procedures

Topics:

- *Networking.....19*
- *Brocade Switch - SwitchConfig Procedures.....134*
- *SAN Storage Arrays Procedures.....146*
- *Blade Server Procedures.....156*
- *C7000 Enclosure Procedures.....168*
- *Management Server Procedures.....206*
- *PM&C Procedures.....208*
- *Configuring SAN.....337*
- *Virtualization Procedures.....341*
- *General TPD Based Application Procedures....361*
- *TVOE Host Procedures.....395*

3.1 Networking

3.1.1 Configure netConfig Repository

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

Prerequisites:

- *3.6.1 IPM Management Server*
- If a PM&C is included in the installation:
  - *3.7.2 Installing TVOE on the Management Server*
  - *3.7.3 TVOE Network Configuration*
  - *3.7.4 Deploy PM&C Guest*
  - *3.7.5 Setup PM&C*

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.

Note: Unless otherwise specified, IPv6 addresses are to use the '<addr>/<prefix>' notation.

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>	

Variable	Value
<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>	

Variable	Value
<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>	

Note: If you have additional enclosure switches, use the worksheets provided in *Worksheet: netConfig Repository*.

1. Management server iLO: Log in and launch the integrated remote console. See *F.1 How to Access a Server Console Remotely*.

2. Management Server: Procedure pre-check

   If the installation is not designed for a virtual PM&C, go to *3.1.1 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 the command produces no instance of a running VM, and 'sudo' was appropriately included in the command, then a PM&C instance is either not installed or not running. If the installation is not designed for a virtual PM&C, go to *3.1.1 Step 3*. Otherwise, continue with this step.
   - 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, log out 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 -l /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
```

Change directory ownership:

```
$ sudo /bin/chown –R pmacd:pmacbackup /usr/TKLC/smac/etc/switch
```

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 [ssh, conserver, oa, tftp]? ssh
SSH host IP? <netConfig_server_mgmt_ip_address>
SSH username: <switch_backup_user>
SSH password: <switch_backup_user_password>
Verify Password: <switch_backup_user_password>
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 the tftp repository information has already been entered for another Cisco model switch (3020, 4948, 4948E, or 4948E-F) then skip this step. The tftp service is common to these switch types. Otherwise, continue with this 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 [ssh, conserver, oa, tftp]? tftp
Service host? <netConfig_server_mgmt_ip_address>
Directory on host? /var/TKLC/smac/image/
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 [ssh, conserver, oa, tftp]? tftp
Service host? <netConfig_server_mgmt_ip_address>
Directory on host? /var/lib/tftpboot/
Add service for tftp_service successful
```

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

   Note: The OA service is common to all HP6125G, HP6125XLG, and HP6120XGs within an enclosure. An OA service must exist for each enclosure when these switch models are in the deployment. If an OA service already exists for each enclosure, then skip this 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 [ssh, conserver, oa, tftp]? oa
Primary OA IP? <OA1_enX_ip_address>
Secondary OA IP? <OA2_enX_ip_address>
OA username? root
OA password? <OA_password>
Verify password:<OA_password>
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: 7.2.0.0.0_88.6.0

Checking Platform Revision for remote TPD installation...
The remote machine is running:
        Product Name: TVOE
 Base Distro Release: 7.2.0.0.0_88.6.0
Configuring switch 'switch1A_console' console server...Configured.
Configuring switch 'switch1B_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 PMAC 6.3.
- 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>
--reuseCredentials
Device Vendor [Cisco, HP]? Cisco
Device Model [3020, 4948, 4948E,4948E-F]? <device_model>
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation)  address for
 management?: <switch_mgmt_ip_address>/<prefix>
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:   <IOS_image>
    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, HP]? Cisco
Device Model [3020, 4948, 4948E,4948E-F]? 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:   <IOS_image>
    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 [Cisco, HP]? HP
Device Model [6120, 6125, 6125XLG]? 6120
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for
management?: <switch_mgmt_ip_address>/<prefix>
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.

Note: The HP6125 has an issue with certain firmware upgrade paths. Entering '0' when prompted for the name of the firmware file bypasses the firmware on initialization path. Firmware operation will be handled in another 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 [Cisco, HP]? HP
Device Model [6120, 6125, 6125XLG]? 6125
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation)address for
management? <switch_mgmt_ip_address>/<prefix>
Enter the name of the firmware file [6125-CMW520-R2105.bin]: 0
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: 6125
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
  Live Protocol Configured
$
```

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 [Cisco, HP]? HP
Device Model [6120, 6125, 6125XLG]? 6125XLG
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation)  address for
 management?: <switch_mgmt_ip_address>/<prefix>
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
```

3.1.2 Aggregation Switch - netConfig Procedures

3.1.2.1 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.

Prerequisites:

- *3.7.2 Installing TVOE on the Management Server*
- *3.7.3 TVOE Network Configuration*
- *3.7.4 Deploy PM&C Guest*
- *3.7.5 Setup PM&C*

- Application management network interfaces must be configured on the management servers prior to executing this procedure.
- Application username and password for creating switch backups must be configured on the management server prior to executing this procedure.

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 *HP Solutions Firmware Upgrade Pack* [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>	
<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 -l /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 any sentry restart instructions that may appear.

   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>

   Connect to the Virtual PM&C by logging into the console of the virtual PM&C instance found in Step 2 of procedure *3.1.1 Configure netConfig Repository*.

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

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **`sudo virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not correct, 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 "$ **`sudo kill -9 <PID>`**". Then execute the "$ **`sudo virsh console X`**" command again. 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 *I.1 Upgrade Cisco 4948 PROM* to upgrade the PROM for switch1A.

5. Virtual PM&C:

   Verify the initialization xml template file and configuration xml template file is present on the system and is the correct version for the system.

```
$ sudo /bin/more /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml
$ sudo /bin/more /usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml
$ sudo /bin/more /usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml
```

   If either file does not exist, copy the files onto the virtual PM&C from the application media using application provided procedures.

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.

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 procedure *3.1.1 Configure netConfig Repository* Step 2.

```
$ 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 switch1B, 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
switch1B_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 *I.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. E xit 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: Ignore any sentry restart instructions that may appear.

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

15. Virtual PM&C: Validate XML file.

    Note: This script validates the XML file to a limited extent:

    - Verifies the file is valid XML
    - Verifies all required options for commands are present
    - Verifies all provided options for commands are valid options
    - Verifies SOME but not all option values

    Validate the XML file before executing it by performing the following command:

    ```
    $ sudo /usr/TKLC/plat/bin/netConfig --file=4948_4948E_configure.xml --testRun >
     /dev/null
    ```

    If nothing is returned then the XML file is valid to the extent defined in the note above. Along with a brief description, errors will return a string indicating the line location of the fault in the XML file.

16. 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.

17. 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>
    ```

18. 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

19. 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
```

20. 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.

21. 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
```

22. 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

23. 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
```

24. Perform *3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* for each switch configured in this procedure.

25. Virtual PM&C: Clean up FW file

    Connect to the PM&C with the virtual console if necessary:

    1. Connect to the Virtual PM&C by logging into the console of the virtual PM&C instance found in Step 2 of procedure *3.1.1 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 receives garbage characters or the output is not correct, then there is likely 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. The console session should now run as expected.

2. Remove the FW file from the tftp directory on the PM&C.

```
$ sudo /bin/rm -f /var/TKLC/smac/image/<FW_image>
```

3.1.2.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (RMS System, No PM&C) (netConfig)

This procedure will configure 4948/4948E/4948E-F switches with an appropriate IOS and configuration from two management servers for use with the rack mount server platform.

This procedure assumes a PMAC 6.3 interconnect. If the system being configured follows a different Platform interconnect, then the appropriate Platform procedures should be followed.

Prerequisites:

- *3.1.1 Configure netConfig Repository*, and
- *3.6.1 IPM Management Server* must be complete before this procedure is attempted.
- Application management network interfaces must be configured on the management servers prior to executing this procedure
- Application username and password for creating switch backups must be configured on the management server prior to executing this procedure.
- netConfig is installed.

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>	
<mgmt_network>	The management network in CIDR format
<management_server_mgmt_ip_address >	

<switch1A_mgmtVLAN_ip_address>	
<netmask>	
<switch1B_mgmtVLAN_ip_address>	
<management_server_iLO_ip>	
<customer_supplied_ntp_server_address>	

Fill in the appropriate value for this site:

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: 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 in an application ISO on an 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 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 My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document

1. Management Server: Verify IOS image is on the system. If the appropriate image does not exist, copy the image to the management server and upload to the switch.

   Determine if the IOS image for the 4948/4948E/4948E-F is on the management server.

   ```
   $ /bin/ls -l /var/lib/tftpboot/<IOS_image_file>
   ```

   If the file exists, continue with the next step. If the file does not exist, copy the file from the firmware media. Ensure the file is specified by the Firmware Upgrade Pack Release Note [3].

2. Management Server: Enable tftp on the system for tftp transfer of IOS upgrade file.

   Execute the commands that enable tftp transfer.

   ```
   $ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd startXinetdService
    service tftp
   Login on Remote: platcfg
   ```

```
Password of platcfg: <platcfg_password>
1
$ sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet
--table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp
--dport 69 -j ACCEPT" --location=1
```

3. Management Server: Verify the firewall is configured properly.

   Execute the following command to check the firewall:

```
$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT
--domain=10platnet --table=filter
Persist    Domain     Table      Chain      Match
-----------------------------------------
yes        10platnet  filter     INPUT      -s <mgmt_network> -p udp --dport 69
 -j ACCEPT
```

4. Management Server: Manipulate host server physical interfaces for switch1A.

   Ensure that the interface of the server connected to switch1A is the only interface up. 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>**

5. Management Server: Get and PROM information for switch1A.

   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.

   To exit from the console, enter**<ctrl-e><c><.>** and you will be returned to the server prompt.

6. Management Server: Determine if switch1A PROM upgrade is required.

   Compare the PROM version from previous step with the version specified in the **List item** for the switch model being used.

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

7. Management Server: Verify the initialization template xml files are in existence on the management server and are the correct versions for the system. If no template file is present, copy over the files from application media.
   a) Verify the initialization xml template files and configuration xml template file are present on the system.

```
$ sudo /bin/more /usr/TKLC/plat/etc/switch/xml/switch1A_4948_4948E_init.xml
$ sudo /bin/more /usr/TKLC/plat/etc/switch/xml/switch1B_4948_4948E_init.xml
$ sudo /bin/more /usr/TKLC/plat/etc/switch/xml/4948_4948E_configure.xml
```

   If the files do not exist, copy the files onto the management server from the application media using application provided procedures.

   b) Verify the xml template files are of the correct version for the system. Ensure the version reported in the following command matches the apiVersion reported in the '<configure apiVersion="x.y">' tag at the beginning of each file.

```
$ sudo /usr/TKLC/plat/bin/netConfig --showVersion
API version: 1.1
```

8. Management Server: Modify **switch1A_4948_4948E_init.xml** and **switch1B_4948_4948E_init.xml** files for information needed to initialize the switch.

   Update the **switch1A_4948_4948E_init.xml** and **switch1B_4948_4948E_init.xml** files for site specific information. Values to be edited in those files are preceded with a dollar sign, an example is $**some_variable_name** . When done editing the file, save and quit.

9. Management Server: Modify **4948_4948E_configure.xml** file for information needed to initialize the switch

   Update the **4948_4948E_configure.xml** file for site specific information. Values to be edited in those files are preceded with a dollar sign, an example is $ **some_variable_name**. When done editing the file, save and quit.

10. Management Server: Initialize switch1A

    Initialize switch1A by issuing the following command:

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

11. Management Server: Verify the switch is using and 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
```

12. Management Server: Manipulate host server physical interfaces for switch1B.

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>

13. Management Server: Determine if switch1B PROM upgrade is required.

Compare the PROM version from previous step with the version specified in the **List item** for the switch model being used.

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

14. Management Server: Initialize switch1B

Initialize switch1B by issuing the following command:

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

15. Management Server: 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
```

16. Virtual PM&C: Validate XML file.

    Note: This script validates the XML file to a limited extent:

    - Verifies the file is valid XML
    - Verifies all required options for commands are present
    - Verifies all provided options for commands are valid options
    - Verifies SOME but not all option values

    Validate the XML file before executing it by performing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --file=4948_4948E_configure.xml --testRun >
 /dev/null
```

    If nothing is returned then the XML file is valid to the extent defined in the note above. Along with a brief description, errors will return a string indicating the line location of the fault in the XML file.

17. Management Server: Configure both switches

    Configure the switch by issuing the following command:

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

    Note: This step takes 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.

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

    Exit from the virtual pmac console, by entering **<ctrl-]>** and you will be returned 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>
```

19. 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

20. Management Server: 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

    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

22. Management Server: 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
```

23. 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

24. Management Server: Restore the management server network back to its original state.

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

25. Management Server: Disable TFTP

    Execute the commands that disable TFTP transfer.

```
$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd stopXinetdService
 service tftp force yes
Login on Remote: platcfg
Password of platcfg: <platcfg_password>
1
$
```

    Ensure that the tftp service is not running by executing the following command. A zero is expected.

```
$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd getXinetdService
 service tftp
Login on Remote: platcfg
Password of platcfg: <platcfg_password>
```

```
0
$
```

If a 1 is returned, repeat this step until getXinetdService returns a zero.

26. Management Server: Remove the iptables rule to allow TFTP

```
$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet
--table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp
--dport 69 -j ACCEPT"
```

27. Management Server: Verify the firewall is configured properly

Execute the following command to check the firewall:

```
$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT
--domain=10platnet --table=filter
Persist    Domain     Table      Chain      Match
-----------------------------------------
```

28. Perform *3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* for each switch configured in this procedure.

3.1.2.3 Configure HP 5900 Aggregation Switches (PM&C Installed) (netConfig)

This procedure will configure 5900 switches to be used in a 10GE-RMS deployment.

Note: In addition to configuring 5900 switches, this procedure includes the steps required to configure the netConfig repository for all required services and switch information.

Prerequisites:

- *3.7.2 Installing TVOE on the Management Server*
- *3.7.3 TVOE Network Configuration*
- *3.7.4 Deploy PM&C Guest*
- *3.7.5 Setup PM&C*

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

- 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, 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.

Note: Unless otherwise specified, IPv6 addresses are to use the '<addr>/<prefix>' notation.

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. '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. In this procedure, 'netConfig server' and 'Virtual PM&C' are synonymous while management server indicates the TVOE host or bare metal server.

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
<switch_backup_user_home_directory>	Fully qualified path to the home directory of <switch_backup_user>
<platcfg_username>	platcfg
<platcfg_password>	See application documentation
<frame IDs>	List (comma and dash separated values) of frames to be added: Valid frame IDs are 1-7
<switch IDs>	List (comma and dash separated values) of switches to be added: Valid switch IDs are A-F
<json file>	JSON file or list of files that define the switch configuration(s)

The following table should be filled out using information for the first HP 5900AF switch. The table should be repeated for each switch to be configured at this site:

Variable	Value
<switch_hostname>	
<switch_username>	
<switch_password>	
<switch_mgmt_ip_address>	CIDR Format
<switch_oobm_ip>	CIDR Format - IPv4 is Required
<mgmt_vlanID>	
<control_vlanID>	

Variable	Value
<oobm_vlanID>	For switch Frame 1 ID A and Frame 1 ID B the oobm_vlanID should be 1
<customer_oam_uplink>	See NAPD or Site Survey information. This should be the switchport or LAG that connects to the customers OAM network
<fw_filename>	

1. Management server iLO: Log in and launch the integrated remote console. See *F.1 How to Access a Server Console Remotely*.

   Note: If executing this procedure in order to add switches/frames after the initial deployment (i.e. a second pass to add hardware to an existing deployment), the virtual PM&C can be accessed directly via SSH instead of iLO and steps 1 and 2 may be skipped.

2. Management Server: Procedure pre-check.

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

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

   Note: If the command produces no instance of a running VM, and 'sudo' was appropriately included in the command, then a PM&C instance is either not installed or not running. Refer to application documentation or contact *1.4 My Oracle Support (MOS)*.

   Log in to the console of the virtual PM&C instance found above.

```
$ 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
```

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **sudo virsh console X**" or from the virsh utility "virsh # **console X"** command and you get garbage characters or output is not correct, 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 "$ **sudo kill -9 <PID>**". Then execute the "$ **sudo virsh console X**" command again. Your console session should now run as expected.

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

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

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

3. netConfig Repo: Execute the configureRepo utility to configure the netConfig repository.

   Answer the prompts using the information collected in tables above. Values in square brackets ([value]) are default values. To use the default value, simply press [ENTER] at the prompt. Values in **BOLD** are entered by the user.

   Note: Multiple switches can be added at the same time by using a dash or comma(s) (e.g. configureRepo --switchID A-B --frameID 1-2 or configureRepo --switchID A,C,F --frameID 1).

```
$ sudo /usr/TKLC/plat/bin/configureRepo --switchID <switch IDs> --frameID <frame
 IDs>
What topology should the repository be configured for (ex. 10GE-RMS,topo1,etc.)?
 [10GE-RMS]:
Would you like to add a(n) ssh service? [Y/N]: y
What is the name of the SSH service? ssh_service
What is the IP address of the SSH service? <netConfig_server_mgmt_ip_address>
What is the username for the SSH service? <switch_backup_user>
What is the password for the SSH service? <switch_backup_user_password>
Would you like to add another ssh service? [Y/N]  n
Would you like to add a(n) tftp service? [Y/N]: n
Would you like to add a(n) conserver service? [Y/N]: n
Would you like to add a(n) oa service? [Y/N]: n
```

   Note: The following prompts will repeat for each FrameID-SwitchID combination to be added. Only one set of prompts is provided as an example of tool execution.

```
Adding Frame 1 Switch A (F1-A)
What type of switch should be added for F1-A? [C9372TX-E]: HP5900
What is the name of switch F1-A? <switch_hostname>
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for
management? <switch_mgmt_ip_address>
What is the switchport mode (access|trunk) for the management server port?
[trunk]:
Is the management interface a port or a vlan? [vlan]:
What is the VLAN ID of the management VLAN? [2]: <mgmt_vlanID>
What is the name of the management VLAN? [management]:
What are the allowed vlans for the management server port? [1-2]:
<control_vlanID>,<mgmt_vlanID>
What switchport connects to the management server? [tenGE1]:
What switchport is used as the customer OAM uplink? [fortyGE3]:
What is the device username? <switch_username>
What is the device password? <switch_password>
What is the OOBM IP address (CIDR notation)? <switch_oobm_IP>
Enter the name of the firmware file [5900_5920-CMW710-F2427.ipe]: <fw_filename>
Enter the directory for file transfers [/home/admusr]:
<switch_backup_user_home_directory>
What is the OOBM VLAN ID? [1]: <oobm_vlanID>
Repo Setup Complete.
```

4. netConfig Server: Verify the FW file is in the appropriate location and has the correct permissions.

```
$ ls –al ~<switch_backup_user>/<fw_filename>
-rw-r--r-- 1 root root 613 Mar 30 12:31 <fw_filename>
```

   If the FW file does not exist, copy the file onto the virtual PM&C.

   To ensure permissions of the file are correct, execute the following command:

```
$ sudo /bin/chmod 644 ~<switch_backup_user>/<fw_filename>
```

5. netConfig Server: Verify the site JSON file exists.

   Verify the configuration JSON file is present on the system and is the correct version for the system.

```
$ sudo /bin/more  /usr/TKLC/smac/etc/switch/<json_file>
```

   If the file does not exist, copy the file onto the virtual PM&C from the application media using application provided procedures.

6. Modify the JSON file(s) with the necessary site information
7. netConfig Server: Initialize and configure the switches with the configureSwitch utility

   Note: The configureSwitch utility allows initialization/configuration of one or many switches with a single execution. If desired, the user can run this utility for each switch one at time rather than all at once. If that is the case, this step should be repeated for each switch. Alternatively, multiple switches can be added at the same time by using a dash or commas (e.g. configureRepo --switchID A-B --frameID 1-3 or configureRepo --switchID A,C,E --frameID 1).

```
$ sudo /usr/TKLC/plat/bin/configureSwitch --frameID <frame IDs> --switchID <switch
 IDs> --file  /usr/TKLC/smac/etc/switch/<json_file> -v
Enter your platcfg username, followed by [ENTER]: <platcfg_username>
Enter your platcfg password, followed by [ENTER]: <platcfg_password>
```

8. Virtual PM&C: Verify proper configuration of the switches

   Once each switch has been configured, verify network reachability and configuration.

```
$ /bin/ping -w3 <switch_IP>
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> showConfiguration
```

   Inspect the output of showConfiguration, and ensure that it is configured as per site requirements. It is important to note that the output of 'showConfiguration' will provide output in vendor specific syntax/language. The user should specifically look for the existence of expected VLANs and IP addresses to verify the configuration is correct.

9. Perform *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch* for each switch configured in this procedure.

3.1.2.4 Configure Cisco 9372TX-E Aggregation Switches (PM&C Installed) (netConfig)

This procedure will configure Cisco 9372TX-E switches to be used in a 10GE-RMS deployment.

Note: In addition to configuring Cisco 9372TX-E switches, this procedure includes the steps required to configure the netConfig repository for all required services and switch information.

Prerequisites:

- *3.7.2 Installing TVOE on the Management Server*
- *3.7.3 TVOE Network Configuration*
- *3.7.4 Deploy PM&C Guest*
- *3.7.5 Setup PM&C*

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

- 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, 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.

Note: Unless otherwise specified, IPv6 addresses are to use the '<addr>/<prefix>' notation.

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. '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. In this procedure, 'netConfig server' and 'Virtual PM&C' are synonymous while management server indicates the TVOE host or bare metal server.

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
<switch_backup_user_home_directory>	Fully qualified path to the home directory of <switch_backup_user>
<platcfg_username>	platcfg
<platcfg_password>	See application documentation
<frame IDs>	List (comma and dash separated values) of frames to be added: Valid frame IDs are 1-7
<switch IDs>	List (comma and dash separated values) of switches to be added: Valid switch IDs are A-F
<json file>	JSON file or list of files that define the switch configuration(s)

The following table should be filled out using information for the first Cisco 9372TX-E switch. The table should be repeated for each switch to be configured at this site:

Variable	Value
<switch_hostname>	
<switch_username>	
<switch_password>	
<switch_mgmt_ip_address>	CIDR Format
<switch_oobm_ip>	CIDR Format - IPv4 is Required
<mgmt_vlanID>	
<control_vlanID>	
<oobm_vlanID>	For switch Frame 1 ID A and Frame 1 ID B the oobm_vlanID should be 1
<customer_oam_uplink>	See NAPD or Site Survey information. This should be the switchport or LAG that connects to the customers OAM network
<fw_filename>	
<ssh_service>	ssh_service to be used for firmware transfer

1. Management server iLO: Log in and launch the integrated remote console. See *F.1 How to Access a Server Console Remotely*.

   Note: If executing this procedure in order to add switches/frames after the initial deployment (i.e. a second pass to add hardware to an existing deployment), the virtual PM&C can be accessed directly via SSH instead of iLO and steps 1 and 2 may be skipped.

2. Management Server: Procedure pre-check.

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

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

   Note: If the command produces no instance of a running VM, and 'sudo' was appropriately included in the command, then a PM&C instance is either not installed or not running. Refer to application documentation or contact *1.4 My Oracle Support (MOS)*.

   Log in to the console of the virtual PM&C instance found above.

```
$ 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
```

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **`sudo virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not

correct, 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 "$ **sudo kill -9 <PID>**". Then execute the "$ **sudo virsh console X**" command again. Your console session should now run as expected.

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

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

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

3. netConfig Repo: Execute the configureRepo utility to configure the netConfig repository.

   Answer the prompts using the information collected in tables above. Values in square brackets ([value]) are default values. To use the default value, simply press [ENTER] at the prompt. Values in **BOLD** are entered by the user.

   Note: Multiple switches can be added at the same time by using a dash or comma(s) (e.g. configureRepo --switchID A-B --frameID 1-2 or configureRepo --switchID A,C,F --frameID 1).

```
$ sudo /usr/TKLC/plat/bin/configureRepo --switchID <switch IDs> --frameID <frame
 IDs>
What topology should the repository be configured for (ex. 10GE-RMS,topo1,etc.)?
 [10GE-RMS]:
Would you like to add a(n) ssh service? [Y/N]: y
What is the name of the SSH service? ssh_service
What is the IP address of the SSH service? <netConfig_server_mgmt_ip_address>
What is the username for the SSH service? <switch_backup_user>
What is the password for the SSH service? <switch_backup_user_password>
Would you like to add another ssh service? [Y/N] n
Would you like to add a(n) tftp service? [Y/N]: n
Would you like to add a(n) console service? [Y/N]: n
Would you like to add a(n) oa service? [Y/N]: n
```

   Note: The following prompts will repeat for each FrameID-SwitchID combination to be added. Only one set of prompts is provided as an example of tool execution.

```
Adding Frame 1 Switch A (F1-A)
What type of switch should be added for F1-A? [C9372TX-E]:
What is the name of switch F1-A? <switch_hostname>
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for
management? <switch_mgmt_ip_address>
What is the switchport mode (access|trunk) for the management server port?
[trunk]:
Is the management interface a port or a vlan? [vlan]:
What is the VLAN ID of the management VLAN? [2]: <mgmt_vlanID>
What is the name of the management VLAN? [management]:
What are the allowed vlans for the management server port? [1-2]:
<control_vlanID>,<mgmt_vlanID>
What switchport connects to the management server? [tenGE1]:
What switchport is used as the customer OAM uplink? [fortyGE3]:
What is the device username? <switch_username>
What is the device password? <switch_password>
What is the OOBM IP address (CIDR notation)? <switch_oobm_IP>
Enter the name of the firmware file [nxos.7.0.3.I4.2.bin]: <fw_filename>
Enter the name of the ssh_service to use for firmware transfers: <ssh_service>
Enter the directory for file transfers [/home/admusr]:
<switch_backup_user_home_directory>
```

```
What is the OOBM VLAN ID? [1]: <oobm_vlanID>
Repo Setup Complete.
```

4. netConfig Server: Verify the FW file is in the appropriate location and has the correct permissions.

   For Cisco 9327TX-E switches, the firmware file is large and should be copied to the /var/TKLC/upgrade directory to prevent inadvertently filling up the / or /home partitions on the PM&C.

```
$ ls -al /var/TKLC/upgrade/<fw_filename>
-rw-r--r-- 1 root root 613 Mar 30 12:31 <fw_filename>
```

   If the FW file does not exist, copy the file onto the virtual PM&C.

   To ensure permissions of the file are correct, execute the following command:

```
$ sudo /bin/chmod 644 /var/TKLC/upgrade/<fw_filename>
```

   Execute the following command to confirm the new permissions:

```
$ ls –al /var/TKLC/upgrade/<fw_filename>
-rw-r--r-- 1 root root 696987648 Mar 30 12:31 <fw_filename>
```

   Execute the following command to verify the <switch_backup_user> directory has a symbolic link to the FW file in /var/TKLC/upgrade:

```
$ ls –al ~<switch_backup_user>/<fw_filename>
lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> ->
/var/TKLC/upgrade/<fw_filename>
```

   If the symbolic link does not exist, execute the following series of commands to create the link and verify it was created correctly:

```
$ cd ~<switch_backup_user>
$ ln –s /var/TKLC/upgrade/<fw_filename>
$ ls –al ~<switch_backup_user>/<fw_filename>
lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> ->
/var/TKLC/upgrade/<fw_filename>
```

5. netConfig Server: Verify the site JSON file exists.

   Verify the configuration JSON file is present on the system and is the correct version for the system.

```
$ sudo /bin/more  /usr/TKLC/smac/etc/switch/<json_file>
```

   If the file does not exist, copy the file onto the virtual PM&C from the application media using application provided procedures.

6. Modify the JSON file(s) with the necessary site information
7. netConfig Server: Initialize and configure the switches with the configureSwitch utility.

   Note: The configureSwitch utility allows initialization/configuration of one or many switches with a single execution. If desired, the user can run this utility for each switch one at time rather than all at once. If that is the case, this step should be repeated for each switch. Alternatively,

multiple switches can be added at the same time by using a dash or commas (e.g. configureRepo --switchID A-B --frameID 1-3 or configureRepo --switchID A,C,E --frameID 1).

```
$ sudo /usr/TKLC/plat/bin/configureSwitch --frameID <frame IDs> --switchID <switch
 IDs> --file  /usr/TKLC/smac/etc/switch/<json_file> -v
Enter your platcfg username, followed by [ENTER]: <platcfg_username>
Enter your platcfg password, followed by [ENTER]: <platcfg_password>
```

8. Virtual PM&C: Verify firmware update

   After configureSwitch completes, verify if a final reboot is needed by checking that the Firmware and System versions on the switch match. Execute the following command:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getVersion
   ```

   The following example shows where the System and Firmware versions on the switch do not match and a final reboot is needed:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getVersion
   Firmware Version: 7.0(3)I4(2)
   System Version: 7.0(3)I4(5)
   BIOS Version: 07.51
   ```

   If the System and Firmware versions do not match, reboot the switch, wait until it reboots, and recheck the firmware versions. Execute the following commands to reboot the switch, confirm it's ready to proceed (via ping), and recheck the versions:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> reboot
   $ /bin/ping -w 3 <switch_IP>
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getVersion
   Firmware Version: 7.0(3)I4(2)
   System Version: 7.0(3)I4(2)
   BIOS Version: 07.51
   ```

   Repeat this step for each switch configured with configureSwitch.

9. Virtual PM&C: Verify proper configuration of the switches

   Once each switch has been configured, verify network reachability and configuration.

   ```
   $ /bin/ping -w3 <switch_IP>
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> showConfiguration
   ```

   Inspect the output of showConfiguration, and ensure that it is configured as per site requirements. It is important to note that the output of 'showConfiguration' will provide output in vendor specific syntax/language. The user should specifically look for the existence of expected VLANs and IP addresses to verify the configuration is correct.

10. Perform *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch* for each switch configured in this procedure.

3.1.2.5 Replace a Failed 4948/4948E/4948E-F Switch (PM&C Installed) (netConfig)

The procedure details the steps necessary to replace a failed 4948/4948E/4948E-F switch.

This procedures assumes a PMAC 6.3 interconnect. If the system being configured follows a different Platform interconnect, then the appropriate Platform procedures should be followed.

Prerequisites:

To perform this procedure, complete the following sections:

- *3.7.2 Installing TVOE on the Management Server*
- *3.7.3 TVOE Network Configuration*
- *3.7.4 Deploy PM&C Guest*
- *3.7.5 Setup PM&C*
- A fully configured and operational redundant switch must be in operation. If this is not ensured, connectivity may be lost to the end devices.

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
<PROM_image_file>			
<IOS_image_file>			

Fill in the appropriate value for this site:

Variable	Value
<switch_console_password>	See referring application documentation
<switch_enable_password>	See referring application documentation
<management_server_mgmt_ip_address >	
<switch1A_mgmtVLAN_ip_address>	
<switch1B_mgmtVLAN_ip_address>	
<switch_mgmtVlan_id>	
<management_server_mgmtInterface>	
<management_server_iLO_ip>	
<netmask>	

Ethernet Interface	DL360	DL380	X3-2	X5-2 and X6-2
<ethernet_interface_1>	eth01	eth01	eth01	eth01
<ethernet_interface_2>	eth02	eth02	eth02	eth03

Variable	PMAC 6.3
<management_server_switchport>	gi1/40

Variable	Value

<mgmt_VLAN_ID>	Value gathered from NAPD
<switch_backup_user>	admusr
<switch_backup_user_password>	Check application documentation

Note: The onboard administrators that are connected to the failed switch will be unavailable during this procedure.

Needed Material:

- 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: 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 being 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 My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. Cabinet: Power off failed switch

   If not already done so, power off the failed switch.

   If the failed switch is DC powered, power off using the cabinet breakers, then remove the DC power and ground cables.

   If the failed switch is AC powered, remove the AC power cords from the unit.

2. Cabinet: Find and prepare to replace switch

   If not already done so, determine whether switch1A or switch1B failed, locate the failed switch, and detach all network and console cables from the failed switch.

   Note: If needed label cables prior to removal.

3. Cabinet: Replace switch

   If not already done so, remove failed switch and replace with new switch of same model.

4. Cabinet: Power on replacement switch

   If the switch is DC powered, attach the DC power and ground cables, then power on the replacement switch using the appropriate cabinet breakers.

   Otherwise, connect the AC power cords to the unit (AC).

5. Cabinet: Attach cables to new switch

   Connect all network and console cables to the new switch except the customer uplink cables. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch.

   Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink.

6. 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.

   Note: Check the FW version on the mate switch and select the matching FW image from the backup directory/TFTP directory.

   To check the FW on the mate switch, use the following command:

   If replacing switch1A:

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

   If replacing switch1B:

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

   Version: 122-54.XO

   License: entservicesk9

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

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

   ```
   $ sudo /bin/ls -l /var/TKLC/smac/image/<IOS_image_file>
   $ sudo /bin/ls -l <switch_backup_directory>/<ios_image>
   ```

   If the file exists and is in the TFTP directory, 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.

   If the file is in the backup directory copy it to the TFTP directory:

   ```
   $ sudo /bin/cp -i <switch_backup_directory/<ios_image> /var/TKLC/smac/image/
   ```

7. 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.

8. Management Server: Manipulate host server physical interfaces

   Connect to the management server, and perform the following commands.

   If replacing switch1A:

   ```
   $ 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>

If replacing switch1B:

```
$ 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>

9. Virtual PM&C: Get PROM information for the switch.

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

   Connect to the switch, check the PROM version.

   If replacing switch1A:

   Connect serially to switch1A by issuing the following command.

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1A_console
```

   If replacing switch1B:

   Connect serially to switch1B by issuing the following command.

```
$ 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
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.

```
To exit from the console, enter <ctrl-e><c><.> and you will be returned to the
server prompt.
```

10. Virtual PM&C: Determine if a PROM upgrade is required.

    Compare the PROM version from the previous step with the version specified in the List item for the switch model being used.

    Check the version from the previous step against the version from the release notes referenced. If the versions are different, perform the procedure *I.1 Upgrade Cisco 4948 PROM*, to upgrade the PROM for the switch.

11. Virtual PM&C: Reset switch to factory defaults.

Connect serially to the switch as outlined in *3.1.2.5 Step 11*, and reload the switch 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. Wait for the first switch to finish before repeating this process for the second switch.

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**.

12. Virtual PM&C: Initialize the switch

Note: Older platform init files may not work on PMAC 6.3 systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.

If replacing switch1A, issue 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
$
```

If replacing switch1B, issue 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.

For switch1A:

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

For switch1B:

```
$ 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:

For switch1A:

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

For switch1B:

```
$ 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: Copy the switch backup files to the current directory

```
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<swname>-backup
~<switch_backup_user>/
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<swname>-backup.info
~<switch_backup_user>/
```

Get a list of the file copied over.

Note: 'switch1A' is shown as an example.

```
$ /bin/ls -l
switch1A-backup     switch1A-backup.info
```

15. Virtual PM&C: Issue the restore command

```
$ cd ~<switch_backup_user>
$ sudo /bin/chmod 644 ~<switch_backup_user>/<swname>-backup*
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> restoreConfiguration
 service=ssh_service filename=<swname>-backup
```

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

Connect to the TVOE host and 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. Virtual PM&C: Verify switch configuration

Ping each of the switches' SVI (router interface) addresses to verify switch configuration.

```
$ /bin/ping <switch1A_mgmtVLAN_IP>
$ /bin/ping <switch1B_mgmtVLAN_IP>
```

18. 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 listFirmware
Image: cat4500-ipbasek9-mz.122-53.SG2.bin
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B listFirmware
Image: cat4500-ipbasek9-mz.122-53.SG2.bin
```

19. Cabinet: Connect network cables from customer network

    Attach the customer uplink cables of the switch being replaced and disconnect the uplink cables from the other switch.

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 the uplink cables that were disconnected in *3.1.2.5 Step 19*.

22. Virtual PM&C: Cleanup FW

    Remove the FW images from the users' home directory and TFTP directory with the following command:

```
$ sudo rm ~admusr/<fw_filename>
$ sudo rm /var/TKLC/smac/image/<fw_filename>
```

3.1.2.6 Replace a Failed 4948/4948E/4948E-F Switch (RMS System, No PM&C)(netConfig)

The procedure details the steps necessary to replace a failed 4948/4948E/4948E-F switch.

This procedure assumes a PMAC 6.3 interconnect. If the system being configured follows a different Platform interconnect, then the appropriate Platform procedures should be followed.

Prerequisites:

- *3.6.1 IPM Management Server* is required to be completed before this procedure is attempted.
- A fully configured and operational redundant switch must be in operation (2 and 4 have been completed on the redundant switch). If this is not ensured, connectivity may be lost to the end devices.
- Application username and password for creating switch backups must be configured on the management server prior to executing this procedure.

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
<PROM_image_file>			
<IOS_image_file>			

Fill in the appropriate value for this site:

Variable	Value
<switch_console_password>	See referring application documentation
<switch_enable_password>	See referring application documentation
<management_server_mgmt_ip_address >	
<switch1A_mgmtVLAN_ip_address>	
<switch1B_mgmtVLAN_ip_address>	
<switch_mgmtVlan_id>	
<management_server_iLO_ip>	
<switch_backup_user>	admusr
<switch_backup_user_password>	See referring application documentation

Ethernet Interface	DL360	DL380	X3-2	X5-2 and X6-2
<ethernet_interface_1>	eth01	eth01	eth01	eth01
<ethernet_interface_2>	eth02	eth02	eth02	eth03

Note: The onboard administrators that are connected to the failed switch will be unavailable during this procedure.

Needed material:

- HP MISC 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: 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 being 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 My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. Cabinet: Power off failed switch

   If not already done so, power off the failed switch.

   If the failed switch is DC powered, power off using the cabinet breakers, then remove the DC power and ground cables.

   If the failed switch is AC powered, remove the AC power cords from the unit.

2. Cabinet: Find and prepare to replace switch

   If not already done so, determine whether switch1A or switch1B failed, locate the failed switch, and detach all network and console cables from the failed switch.

   Note: If needed label cables prior to removal.

3. Cabinet: Replace switch

   If not already done so, remove failed switch and replace with new switch of same model.

4. Power on replacement switch

   If the switch is DC powered, attach the DC power and ground cables, then power on the replacement switch using the appropriate cabinet breakers.

   Otherwise, connect the AC power cords to the unit (AC).

5. Cabinet: Attach cables to new switch

   Connect all network and console cables to the new switch except the customer uplink cables. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch.

   Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink.

6. Management Server: Verify the IOS image is on the system. If the appropriate image does not exist, copy the image to the MANAGEMENT SERVER.

   Note: Check the FW version on the mate switch and select the matching FW image from the backup directory. To check the FW on the mate switch, use the following command:

   If replacing switch1A:

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

   If replacing switch1B:

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

```
Version: 122-54.XO

License: entservicesk9

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

   Determine if the IOS image for the 4948/4948E/4948E-F is on the MANAGEMENT SERVER.

```
$ sudo /bin/ls -l /var/lib/tftpboot/<IOS_image_file>
$ sudo /bin/ls -l <switch_backup_directory>/<ios_image>
```

   If the file exists and is in the TFTP directory, 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.

   If the file is in the backup directory copy it to the TFTP directory:

```
$ sudo /bin/cp -i <switch_backup_directory/<ios_image> /var/lib/tftpboot/
```

7. Management Server: Enable tftp on the system for tftp transfer of IOS upgrade file.

   Execute the commands that enable tftp transfer.

```
$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd startXinetdService
 service tftp
Login on Remote: platcfg
Password of platcfg: <platcfg_password>
1
```

```
$ sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet
--table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp
--dport 69 -j ACCEPT" --location=1
```

8. Management Server: Verify the firewall is configured properly.

   Execute the following command to check the firewall:

```
$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT
--domain=10platnet --table=filter
Persist    Domain     Table      Chain      Match
-----------------------------------------
yes        10platnet  filter     INPUT      -s <mgmt_network> -p udp --dport 69
 -j ACCEPT
```

9. Management Server: Manipulating host server physical interfaces

   If replacing switch1A:

```
$ 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>

   If replacing switch1B:

```
$ 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>

10. Management Server: Get PROM information for the switch.

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

    Connect to the switch, check the PROM version.

    If replacing switch1A:

    Connect serially to switch1A by issuing the following command.

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1A_console
```

    If replacing switch1B:

    Connect serially to switch1B by issuing the following command.

```
$ 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
Switch> show version | include ROM
ROM: 12.2(31r)SGA1
System returned to ROM by reload
```

Note: If the console command fails, contact My Oracle Support.

Note the IOS image & ROM version for comparison in a following step.

```
To exit from the console, enter <ctrl-e><c><.> and you will be returned to the
server prompt.
```

11. Management Server: Determine if a PROM upgrade is required.

    Compare the PROM version from the previous step with the version specified in *HP Solutions Firmware Upgrade Pack* [2] in section 1.1 References for the switch model being used.

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

12. Management Server: Reset the switch to factory defaults.

    Connect serially to the switch as outlined in *3.1.2.6 Step 10*, and reload the switch 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. Wait for the first switch to finish before repeating this process for the second switch.

    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**.

13. Management Server: Initialize the switch

    Note: Older platform init files may not work on PMAC 6.3 systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.

    If replacing switch1A, issue the following command:

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

    If replacing switch1B, issue the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/plat/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 My Oracle Support.

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.

For switch1A:

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

For switch1B:

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

Note: If this command fails, stop this procedure and contact My Oracle Support

14. Management Server: Verify the switch is using the proper IOS image per Platform version.

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

    For switch1A:

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

    For switch1B:

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

```
Version: 122-54.XO

License: entservicesk9

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

15. Management Server: Disable tftp

    Execute the commands that disable tftp transfer.

```
$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd stopXinetdService
 service tftp force yes
Login on Remote: platcfg
Password of platcfg: <platcfg_password>
1
$
```

    Ensure that the tftp service is not running by executing the following command. A zero is expected.

```
$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd getXinetdService
 service tftp
Login on Remote: platcfg
Password of platcfg: <platcfg_password>
0
$
```

If a 1 is returned, repeat this step until getXinetdService returns a zero.

16. Management Server: Remove the iptables rule to allow TFTP

```
$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet
--table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp
--dport 69 -j ACCEPT"
```

17. Management Server: Verify the firewall is configured properly

Execute the following command to check the firewall:

```
$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT
--domain=10platnet --table=filter
Persist    Domain     Table      Chain      Match
-----------------------------------------
```

18. Management Server: Copy the switch backup files to the current directory

```
$ sudo /bin/cp -i /usr/TKLC/plat/etc/switch/backup/<switch_hostname>
~<switch_backup_user>/
```

Get a list of the file copied over.

Note: 'switch1A' is shown as an example.

```
$ /bin/ls -l
switch1A-backup     switch1A-backup.info     switch1A-backup.vlan
```

19. Management Server: Issue the restore command

```
cd ~<switch_backup_user>
$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname>
restoreConfiguration service=ssh_service filename=<switch_hostname>-backup
```

20. Management Server: Verify switch configuration

Ping each of the switches SVI (router interface) addresses to verify switch configuration.

```
$ /bin/ping <switch1A_mgmtVLAN_IP>
$ /bin/ping <switch1B_mgmtVLAN_IP>
```

21. Management Server: 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 listFirmware
Image: cat4500-ipbasek9-mz.122-53.SG2.bin
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B listFirmware
Image: cat4500-ipbasek9-mz.122-53.SG2.bin
```

22. Cabinet: Connect network cables from customer network

Attach the customer uplink cables of the switch being replaced and disconnect the uplink cables from the other switch.

23. Management Server: 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
```

24. Cabinet: Connect network cables from customer network.

    Re-attach the uplink cables that were disconnected in *3.1.2.6 Step 22*.

25. Management Server: Cleanup FW

    Remove the FW images from the users' home directory and TFTP directory with the following command:

```
$ sudo rm ~admusr/<fw_filename>
$ sudo rm /var/TKLC/smac/image/<fw_filename>
```

3.1.2.7 Replace a Failed 5900AF Switch (PM&C Installed) (netConfig)

This procedure details the steps necessary to replace a failed 5900AF switch.

This procedure assumes a healthy PM&C with the original netConfig repository intact. If this is not the case and a PMAC disaster recovery needs to be performed, see *PM&C Disaster Recovery* [7]. If a PM&C does not exist and a DR is not possible, disregard this procedure and perform *3.1.2.3 Configure HP 5900 Aggregation Switches (PM&C Installed) (netConfig)*.

Prerequisites:

- A fully configured and operational redundant switch must be in operation. If this is not ensured, connectivity may be lost to the end devices.
- Access to the switch configuration backup file for the failed switch. This generally resides on the PMAC in directory **`/usr/TKLC/smac/etc/switch/backup`** and typically has a name format of **`<switch_hostname>-backup`**. If the file does not exist on the PM&C, work with the local switch administrator to determine if an offloaded copy exists.

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. '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. In this procedure, 'netConfig server' and 'Virtual PM&C' are synonymous while management server indicates the TVOE host or bare metal server.

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 values:

Variable	Value
<switch_backup_user>	admusr
<fw_filename>	

Note: The firmware version must match that of the operational redundant switch. This will be checked in a subsequent step.	
<switch_backup_directory>	/usr/TKLC/smac/etc/switch/backup
<management_server_mgmtInterface>	Value gathered from NAPD
<management_server_mgmt_ip_address>	

Ethernet Interface	Oracle Server
<ethernet_interface_1>	eth01
<ethernet_interface_2>	eth03

Note: The onboard administrators that are connected to the failed switch will be unavailable during this procedure.

Needed Material:

- HP FW file acquired through customer channels
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]

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. Cabinet: Power off failed switch and prepare to replace

   If not already done so, determine whether switch1A or switch1B failed. Locate the switch and power it off. Remove the AC power cords.

2. Cabinet: Find and prepare to replace switch

   Detach all network and console cables from the failed switch.

   Note: If needed, label the cables prior to removal.

3. Cabinet: Replace switch

   Remove failed switch and replace with new switch of same model.

4. Cabinet: Power on replacement switch

   Connect the AC power cords to the unit. Confirm the switch powers on.

5. Cabinet: Attach cables to new switch

   With the exception of the customer uplink cables, connect all network and console cables to the new switch. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch.

   Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink.

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

   Note: Check the FW version on the mate switch and select the matching FW image from the backup directory/TFTP directory. The firmware version must be identical between mating switches.

To check the FW on the mate switch, use the following command (output is for example only):

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<mate_switch_name> getFirmware

Version: 7.1.045

Flash:  = (
5900_5920-cmw710-boot-f2427.bin
5900_5920-cmw710-system-f2427.bin
)

Release: 2427
```

Determine if the matching FW image for the 5900AF is on the Virtual PM&C.

```
$ sudo /bin/ls -l <switch_backup_directory>/<fw_filename>
```

If the appropriate FW file exists, move the image from the switch backup directory to the backup user directory by performing the following command:

```
$ sudo /bin/cp –i <switch_backup_directory/<fw_filename> ~<switch_backup_user>/
```

If the FW image does not exist on the server, copy it to the backup user directory. Change the FW image file permissions by performing the following command:

```
$ sudo /bin/chmod 644 <fw_filename>
```

7. Management Server: Manipulate host server physical interfaces

   Note: This step only pertains to failed switches in the first frame with a switchID of A or B. In other words, the switches which host the management server interfaces. If the failed switch has a switchID of C-F or resides in frame 2 or beyond, this step can be ignored and the user may proceed with *3.1.2.7 Step 8*.

   Connect to the management server and perform the following commands.

   If replacing switch with an identity of frameID 1 switchID A:

   ```
   $ 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>**.

   If replacing switch with an identity of frameID 1 switchID B:

   ```
   $ 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>**.

8. Virtual PM&C: Initialize the switch.

Initialize the switch by performing the following command:

```
$ sudo /usr/TKLC/plat/bin/initializeSwitch --switch <switch_hostname>
Enter your platcfg username, followed by [ENTER]: <platcfg_username>
Enter your platcfg password, followed by [ENTER]: <platcfg_password>
```

9. Virtual PM&C: Copy the switch backup files to the home directory of the <switch_backup_user>

   Copy the switch backup files to the home directory by performing the following command:

```
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup
~<switch_backup_user>/
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup.info
 ~<switch_backup_user>/
```

10. Virtual PM&C: Issue the restore command.

    Issue the restore command by performing the following command:

```
$ cd ~<switch_backup_user>
$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname>
restoreConfiguration service=ssh_service filename=<switch_hostname>-backup
```

11. Management Server: Ensure both interfaces are enabled on the host server.

    Connect to the management server and perform the following commands:

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

12. Physical Switch: Install Uplink Cables

    Once the switch has been configured, attach the customer uplink cables of the switch being replaced.

13. Virtual PM&C: Verify connectivity and configuration.

    Verify network reachability and configuration by performing the following commands:

```
$ /bin/ping -w3 <switch_IP>
$ /usr/TKLC/plat/bin/netConfig –-device=<switch_hostname> showConfiguration
```

    Inspect the output of showConfiguration, and ensure that it is configured as per site requirements. It is important to note that the output of 'showConfiguration' will provide output in vendor specific syntax/language. The user should specifically look for the existence of expected VLANs and IP addresses to verify the configuration is correct.

14. Virtual PM&C: Cleanup FW

    Remove the FW images from the users' home directory with the following command:

```
$ sudo rm ~admusr/<fw_filename>
```

3.1.2.8 Replace a Failed 9372TX-E Switch (PM&C Installed) (netConfig)

This procedure details the steps necessary to replace a failed 9372TX-E switch.

This procedure assumes a healthy PM&C with the original netConfig repository intact. If this is not the case and a PMAC disaster recovery needs to be performed, see *PM&C Disaster Recovery* [7]. If a PM&C does not exist and a DR is not possible, disregard this procedure and perform *3.1.2.4 Configure Cisco 9372TX-E Aggregation Switches (PM&C Installed) (netConfig)*.

Prerequisites:

- A fully configured and operational redundant switch must be in operation. If this is not ensured, connectivity may be lost to the end devices.
- Access to the switch configuration backup file for the failed switch. This generally resides on the PMAC in directory **`/usr/TKLC/smac/etc/switch/backup`** and typically has a name format of **`<switch_hostname>-backup`**. If the file does not exist on the PM&C, work with the local switch administrator to determine if an offloaded copy exists.

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. '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. In this procedure, 'netConfig server' and 'Virtual PM&C' are synonymous while management server indicates the TVOE host or bare metal server.

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 values:

Variable	Value
<switch_backup_user>	admusr
<fw_filename> **Note:** The firmware version must match that of the operational redundant switch. This will be checked in a subsequent step.	
<switch_backup_directory>	/usr/TKLC/smac/etc/switch/backup
<management_server_mgmtInterface>	Value gathered from NAPD
<management_server_mgmt_ip_address>	

Ethernet Interface	Oracle Server
<ethernet_interface_1>	eth01
<ethernet_interface_2>	eth03

Note: The onboard administrators that are connected to the failed switch will be unavailable during this procedure.

Needed Material:

- Cisco FW file acquired through *1.4 My Oracle Support (MOS)*

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. Cabinet: Power off failed switch and prepare to replace

   If not already done so, determine whether switch1A or switch1B failed. Locate the switch and power it off. Remove the AC power cords.

2. Cabinet: Find and prepare to replace switch

   Detach all network and console cables from the failed switch.

   Note: If needed, label the cables prior to removal.

3. Cabinet: Replace switch

   Remove failed switch and replace with new switch of same model.

4. Cabinet: Power on replacement switch

   Connect the AC power cords to the unit. Confirm the switch powers on.

5. Cabinet: Attach cables to new switch

   With the exception of the customer uplink cables, connect all network and console cables to the new switch. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch.

   Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink.

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

   Note: Check the FW version on the mate switch and select the matching FW image from the backup/upgrade directory. The firmware version must be identical between mating switches.

   To check the FW on the mate switch, execute the following command (output is for example only):

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<mate_switch_name> getFirmware

Version: 7.0.3.I4.2

Flash: nxos.7.0.3.I4.2.bin
```

   Determine if the matching FW image for the 9372TX-E is on the Virtual PM&C.

```
$ sudo /bin/ls -l <switch_backup_directory>/<fw_filename>
```

   or

```
$ sudo /bin/ls -l /var/TKLC/upgrade/<fw_filename>
```

   If the appropriate FW file exists, verify that a symbolic link exists to the firmware file in the backup user directory by executing the following command (output is for example only):

```
$ sudo /bin/ls -al ~<switch_backup_user>/*.bin
lrwxrwxrwx  1 root   root         37 Dec 16 16:42 nxos.7.0.3.I4.2.bin ->
/var/TKLC/upgrade/nxos.7.0.3.I4.2.bin
```

If the link exists, verify it is correct by verifying that the FW file exists in the location pointed to by the link (note: the FW file location pointed to by the link is everything after the "->" in the output of the previous command). The output below is for example only, and is based on the example output given above:

```
$ sudo /bin/ls -al /var/TKLC/upgrade/nxos.7.0.3.I4.2.bin
-rw-r--r-- 1 admusr admgrp 696987648 Nov 30 13:38
/var/TKLC/upgrade/nxos.7.0.3.I4.2.bin
```

If the link does not exist, or is incorrect, remove the existing link and create the correct link by executing the following commands:

```
$ cd ~<switch_backup_user>
$ sudo /bin/rm -f ~<switch_backup_user>/<name_of_incorrect_link>
$ cd ~<switch_backup_user>
$ ln -s <switch_backup_directory>/<fw_filename>
$ ls -al ~<switch_backup_user>/<fw_filename>
lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> ->
/var/TKLC/upgrade/<fw_filename>
```

If the FW image does not exist on the virtual PM&C, copy it to the switch backup directory. Change the FW image file permissions by executing the following command:

```
$ sudo /bin/chmod 644 /var/TKLC/upgrade/<fw_filename>
```

Execute the following command to confirm the new permissions:

```
$ ls -al /var/TKLC/upgrade/<fw_filename>
-rw-r--r-- 1 root root 696987648 Mar 30 12:31 <fw_filename>
```

Verify the <switch_backup_user> directory has a symbolic link to the FW file in /var/TKLC/upgrade.

```
$ ls -al ~<switch_backup_user>/<fw_filename>
lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> ->
/var/TKLC/upgrade/<fw_filename>
```

If the symbolic link does not exist, execute the following commands to create the link and verify it was created correctly:

```
$ cd ~<switch_backup_user>
$ ln -s /var/TKLC/upgrade/<fw_filename>
$ ls -al ~<switch_backup_user>/<fw_filename>
lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> ->
/var/TKLC/upgrade/<fw_filename>
```

7. Management Server: Manipulate host server physical interfaces

   Note: This step only pertains to failed switches in the first frame with a switchID of A or B. In other words, the switches which host the management server interfaces. If the failed switch has a switchID of C-F or resides in frame 2 or beyond, this step can be ignored and the user may proceed with *3.1.2.8 Step 8*.

   Connect to the management server and perform the following commands.

If replacing switch with an identity of frameID 1 switchID A:

```
$ 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>**.

If replacing switch with an identity of frameID 1 switchID B:

```
$ 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>**.

8. Virtual PM&C: Initialize the switch.

   Initialize the switch by performing the following command:

```
$ sudo /usr/TKLC/plat/bin/initializeSwitch --switch <switch_hostname>
Enter your platcfg username, followed by [ENTER]: <platcfg_username>
Enter your platcfg password, followed by [ENTER]: <platcfg_password>
```

9. Virtual PM&C: Copy the switch backup files to the home directory of the <switch_backup_user>

   Copy the switch backup files to the home directory by performing the following command:

```
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup
~<switch_backup_user>/
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup.info
 ~<switch_backup_user>/
```

10. Virtual PM&C: Issue the restore command.

    Issue the restore command by performing the following command:

```
$ cd ~<switch_backup_user>
$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname>
restoreConfiguration service=ssh_service filename=<switch_hostname>-backup
```

11. Management Server: Ensure both interfaces are enabled on the host server.

    Connect to the management server and perform the following commands:

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

12. Physical Switch: Install Uplink Cables

    Once the switch has been configured, attach the customer uplink cables of the switch being replaced.

13. Virtual PM&C: Verify connectivity and configuration.

    Verify network reachability and configuration by performing the following commands:

```
$ /bin/ping -w3 <switch_IP>
$ /usr/TKLC/plat/bin/netConfig –-device=<switch_hostname> showConfiguration
```

Inspect the output of showConfiguration, and ensure that it is configured as per site requirements. It is important to note that the output of 'showConfiguration' will provide output in vendor specific syntax/language. The user should specifically look for the existence of expected VLANs and IP addresses to verify the configuration is correct.

14. Virtual PM&C: Cleanup FW

Remove the FW images from the users' home directory with the following commands:

```
$ sudo rm ~admusr/<fw_filename>
$ sudo rm <switch_backup_directory>/<fw_filename>
```

3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)

Prerequisites for RMS system Aggregation Switch:

- *3.6.1 IPM Management Server* must be completed.
- *3.1.2.1 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.

Prerequisites for c-Class system Aggregation Switch:

- *3.6.1 IPM Management Server* must be completed
- *3.7.2 Installing TVOE on the Management Server* must be completed
- *3.7.3 TVOE Network Configuration* must be completed
- *3.7.4 Deploy PM&C Guest* must be completed
- *3.1.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)*

Prerequisites for Cisco 3020 Enclosure switches:

- *3.6.1 IPM Management Server* must be completed
- *3.7.2 Installing TVOE on the Management Server* must be completed
- *3.7.3 TVOE Network Configuration* must be completed
- *3.7.4 Deploy PM&C Guest* must be completed
- *3.1.3.1 Configure Cisco 3020 Switch (netConfig)*

Procedure Reference Tables:

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 -l <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>
```

   If this is a PM&C System, change ownership:

```
$ sudo /bin/chown –R pmacd:pmacbackup <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 -l ~<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. Save FW Files:

   If a firmware upgrade, switch replacement, or an initial install (which performed a FW upgrade during initialization) was performed, backup the FW image used by performing one of the following commands:

   If the FW upgrade was performed with TFTP:

   If on a PM&C system:

   ```
   $ sudo /bin/mv -i /var/TKLC/smac/image/<fw_image> <switch_backup_directory>/
   ```

   If on a non-PM&C system:

   ```
   $  sudo /bin/mv -i /var/lib/tftpboot/<fw_image> <switch_backup_directory>/
   ```

   If the FW upgrade was performed with SCP:

   ```
   $ sudo /bin/mv -i ~<switch_backup_user>/<fw_image> <switch_backup_directory>/
   ```

   Otherwise, proceed to the next step.

7. Repeat steps *3.1.2.9 Step 1*, *3.1.2.9 Step 4* - *3.1.2.9 Step 6* for each switch to be backed up.

3.1.2.10 Replace a Failed Telco T5C-24GT

This procedure will configure a Telco T5C-24GT switch with an appropriate configuration from its corresponding T1200 server.

Note: This procedure assumes a T1200 server running TPD 6.7 or higher and connected serially to the Telco T5C-24GT switch console port via /dev/ttyUSB1.

Procedure Reference Tables: Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within "<>". Fill in the appropriate values for the site.

Variable	Value
<T1200_server_RMM_ip>	
<T1200_server_RMM_user>	
<T1200_server_RMM_user_password>	
<T1200_server_password>	
<Telco_switch_name>	

<Telco_switch_password>	
<Telco_switch_enable_password>	
<T5CL3_24G_firmware_image_file>	
<Remote_customer_target_ip>	

Notes:

- See the T1200 Solutions Firmware Upgrade Pack (Tekelec part# 909-1618-001) for appropriate T5CL3_24G firmware image.
- See *3.1.2.10 Substep g* for determining appropriate value of <Remote_customer_target_ip>

1. Telco T5CL3_24G: Identify and power down the failed Telco switch. Label and disconnect all cables connected to the Telco switch. Remove the defective Telco switch.
2. Telco T5CL3_24G: Installation of replacement switch

   Install new Telco switch and re-cable all cables, except for uplinks to customer network. Connect power and power on switch.

   In the ssh_service parameters, the value for 'user:' will be the value for the variable <switch_backup_user>.
3. Management server Remote Management Module (RMM): Log in to the RMM.
   - Using IE, log into the RMM using the username and password provided by <T1200_server_RMM_user> and <T1200_server_RMM_user_password>:

     http://<T1200_server_RMM_ip>
4. Management server Remote Management Module (RMM): Launch and log in to the Telco T1200 server via the Remote Console.
   - Click on the **Console** icon in the upper left corner to launch the **Remote Console** on the server.
   - Click on **Don't Block** if the **Security Warning** window pops up.

     Note: Different versions of Internet Explorer may present additional security prompts.

     If not already done so, log in as admusr using the <T1200_server_password> password.
5. Management server: Procedure pre-check - Verify Telco switch console connection.
   - Determine whether needed minicom files are already available by issuing the following command:

```
$ /bin/ls -l /etc/minirc.*
```

     If the file "minirc.<Telco_switch_name>" is not listed, proceed with the rest of this step, otherwise skip to *3.1.2.10 Step 6*.
   - Set up the serial connections to the switch by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/remoteConsole  --add --name=<Telco_switch_name>
--bps=9600 --port=ttyUSB1
```

6. Management server: Attach to the switch console.

- Connect serially to the switch by issuing the following command as admusr on the management server:

```
$ sudo /usr/bin/minicom <Telco_switch_name>

Welcome to minicom 2.1

OPTIONS: History Buffer, F-key Macros, Search History Buffer, I18n
Compiled on Jan   7 2007, 01:16:05.

Press CTRL-A Z for help on special keys

Press Enter
Password:  <Telco_switch_password>
T5C-24GT>
Switch> enable
Password: <Telco_switch_enable_password>
T5C-24GT#
```

If the "enable" command above prompts for a password, the switch is not in a factory default configuration. This may be due to a previous configuration attempt. If this is the case, please continue with *3.1.2.10 Step 7*. If not and the switch is in a factory default configuration, skip to *3.1.2.10 Step 8*.

7. Management Server (switch console session): Initialize switch to factory default configuration.

   - Type the following commands in the switch console session to restore the switch to factory default configuration:

```
T5C-24GT# write erase
wait …
T5C-24GT# reload no-save
Proceed with reload? [y/n] : y
Rebooting…
[Additional output omitted]
```

   - The switch will reboot in a factory default configuration. Once the switch has rebooted and you will see the following, indicating the switch is back up:

```
User Access Verification
Password:
```

8. Management Server (switch console session): Exiting the switch console and minicom session.

   To exit the console session and minicom program:

   - If you are at the "T5C-24GT# " or "T5C-24GT>" prompt in the switch console session , log out first by typing exit and pressing **Enter**.
   - After you log out of the switch, exit the minicom session by pressing **CTRL** and **A**, press **X**, then press **Enter**

9. Management Server: Verify that the switch configuration file exists.

   Verify vlan.conf exists.

```
$ /bin/ls -l  /usr/TKLC/plat/etc/vlan.conf
/usr/TKLC/plat/etc/vlan.conf
```

If the file "vlan.conf" file does not exist, stop and contact *1.4 My Oracle Support (MOS)*.

10. Management Server: Verify that the switch firmware binary exists.

    Check to see if the correct firmware binary is present on the system.

```
$ /bin/ls -l /var/TKLC/switchconfig/<T5CL3_24G_firmware_image_file>
```

    If the appropriate image does not exist, please check the T1200 Solutions Firmware Upgrade Pack (Tekelec part# 909-1618-001), or contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document. If the appropriate image does exist, continue with *3.1.2.10 Step 11*.

11. Management Server: Check the tftp status.

    Check to see if the tftp service is enabled.

```
$ /sbin/chkconfig --list tftp
tftp off
```

    If the tftp service is set to "off" continue with this step. If the tftp service is set to "on", skip to *3.1.2.10 Step 12*.

    To turn on tftp, run the following command:

```
$ sudo /sbin/chkconfig  tftp on
```

    Verify that it is now enabled:

```
$ /sbin/chkconfig --list tftp
tftp on
```

12. Management Server: Check xinetd service is running

```
$ sudo /sbin/service xinetd status
```

    If the output from the above command is:

```
xinetd (pid  xxxx) is running...
```

    Run the following command:

```
$ sudo /sbin/service xinetd restart
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                             [  OK  ]
```

    If the output from the above command is:

```
xinetd is stopped
```

    Run the following command:

```
$ sudo /sbin/service xinetd start
Starting xinetd:                                             [  OK  ]
```

13. Management Server: Modify iptables to allow tftp.

Run iptablesAdm to modify iptables to allow the switch to pull configuration data from the server.

```
$ sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet
--table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp
--dport 69 -j ACCEPT" --location=1
```

14. Management Server: Verify the firewall is configured properly.

    Execute the following command to check the firewall:

```
$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT
--domain=10platnet --table=filter
Persist    Domain     Table      Chain      Match
-----------------------------------------
yes        10platnet  filter     INPUT      -s <mgmt_network> -p udp --dport 69
 -j ACCEPT
```

15. Management Server: Run switchconfig to configure the switch.

```
$ sudo /usr/TKLC/plat/sbin/switchconfig --swname=<Telco_switch_name>
Successfully enabled on switch <Telco_switch_name>.
Reloading switch <Telco_switch_name> with defaults, please standby…
Switch <Telco_switch_name> successfully set to default configuration.
Successfully started management VLAN on <Telco_switch_name>.
Startup configuration created OK.
Successfully uploaded startup config for <Telco_switch_name>.
Removing config file <Telco_switch_name>.startup-config from /var/lib/tftpboot.
Reloading switch <Telco_switch_name>, please standby…
Reload of switch <Telco_switch_name> complete.
Switch <Telco_switch_name> successfully configured.
```

    Note: This step will take approximately 20 minutes to complete.

16. Management Server: Stop the xinetd service.

    Stop the xinetd service once the switch has been upgraded and configured:

```
$ sudo /sbin/service xinetd stop
Stopping xinetd:                                           [ OK ]
```

17. Management Server: Disable tftp services.

    Disable the tftp service by running the following command:

```
$ sudo /sbin/chkconfig tftp off
```

18. Telco T5CL3_24G: Connect uplink cables.

    Connect the uplink cables from the new Telco switch to the customer network.

19. Management Server: Test network flow/traffic through both Telco switches.

    To ensure traffic is flowing through both Telco switches properly after a RMA procedure, start up a ping on each T1200 server:

```
$ /bin/ping <Remote_customer_target_ip>
```

    Notes

- If the management server is a SOAM, use the IP address of the NOAM VIP for <Remote_customer_target_ip>.
- If the management server is an NOAM, use the address of the SOAM VIP for <Remote_customer_target_ip>.

With these pings running on each server, perform the following steps:

a) On the Management Server connected to the replacement Telco switch, force it to use eth01 by running the following command:

```
$ sudo /sbin/ifenslave –c bond1 eth01
```

b) On the mated Management server connected to the mated Telco switch, force it to use eth02 by running the following command:

```
$ sudo /sbin/ifenslave –c bond1 eth02
```

If either server is not pinging correctly or has stopped responding at this point, please contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

c) On the new/replacement Telco switch, unplug the customer uplink cables.

d) Verify that the pings from each server are still reaching <Remote_customer_target_ip>.

There may be a brief pause after unplugging the uplink cables as the mated switch takes over the VRRP interfaces (less than 5 seconds).

- If the pings are no longer reaching <Remote_customer_target_ip> on both servers, stop and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.
- If the pings continue, this verifies that the mated switch is performing as expected by sending traffic to the customer network, and traffic is flowing to it over the ISL from the replacement Telco switch.

e) Replace the uplink cables to the customer network on the replacement Telco switch.

f) On the mated Telco switch, unplug the customer uplink cables.

g) Verify that the pings from each server are still reaching <Remote_customer_target_ip>.

Again, there may be a brief pause after unplugging the uplink cables as the replaced Telco switch takes over the VRRP interfaces (less than 5 seconds).

- If the pings are no longer reaching <Remote_customer_target_ip> on both servers, stop and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.
- If the pings continue, this verifies that traffic is flowing over the replacement Telco switch to the customer network and over the ISL and that both switches are functioning as expected.

h) Replace the uplink cables to the customer network on the replacement Telco switch.

20. Management Server: Disable tftp

Execute the commands that disable tftp transfer.

```
$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd stopXinetdService
 service tftp force yes
Login on Remote: platcfg
Password of platcfg: <platcfg_password>
1
$
```

Ensure that the tftp service is not running by executing the following command. A zero is expected.

```
$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd getXinetdService
 service tftp
Login on Remote: platcfg
Password of platcfg: <platcfg_password>
0
$
```

If a 1 is returned, repeat this step until getXinetdService returns a zero.

21. Management Server: Remove the iptables rule to allow TFTP

```
$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet
--table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp
--dport 69 -j ACCEPT"
```

22. Management Server: Verify the firewall is configured properly

Execute the following command to check the firewall:

```
$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT
--domain=10platnet --table=filter
Persist    Domain     Table      Chain      Match
-----------------------------------------
```

3.1.3 C-Class Enclosure Switch - netConfig Procedures

3.1.3.1 Configure Cisco 3020 Switch (netConfig)

This procedure will configure 3020 switches from the PM&C server using templates included with an application.

Prerequisites:

- It is essential that PM&C is installed. In addition, complete these procedures:
- *3.1.1 Configure netConfig Repository*
- *3.5.1 Configure Initial OA IP*
- *3.5.2 Configure Initial OA Settings Using the Configuration Wizard*

Conditional Prerequisite:

If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using *3.1.2.1 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

   Log in 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 *3.1.3.1 Step 7*.

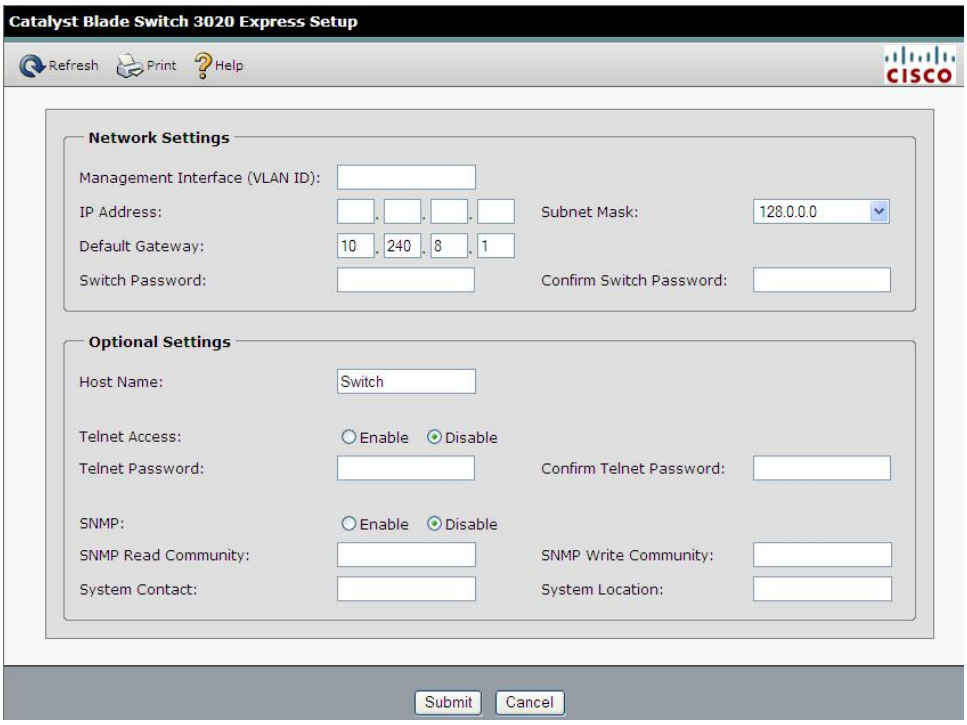
   If the switch has been previously configured using netConfig or previous attempts at initialization have failed, use netConfig to reset the switch to factory defaults by executing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> setFactoryDefault
```

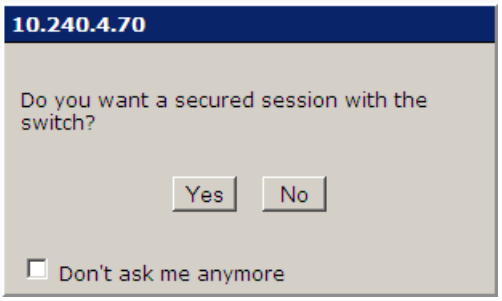
   If the above command failed, use Internet Explorer to navigate to <enclosure_switch_ip_address>.

   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**.

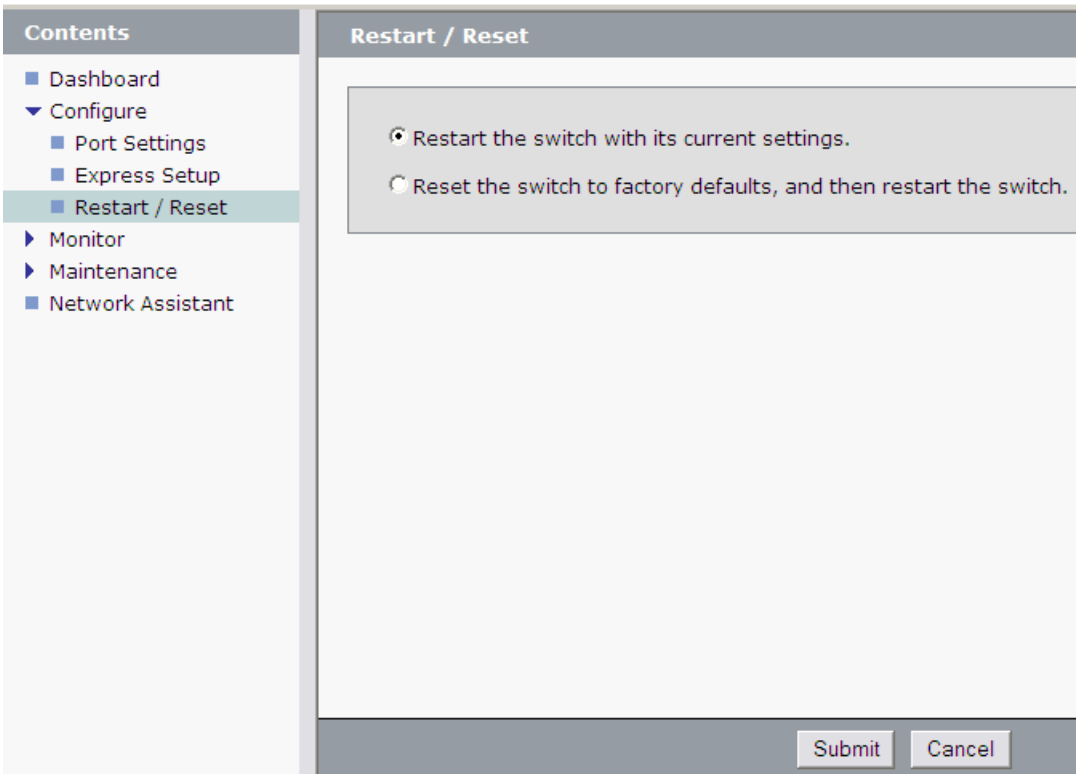


   If you are prompted with "Do you want a secured session with the switch?", click on **No**.



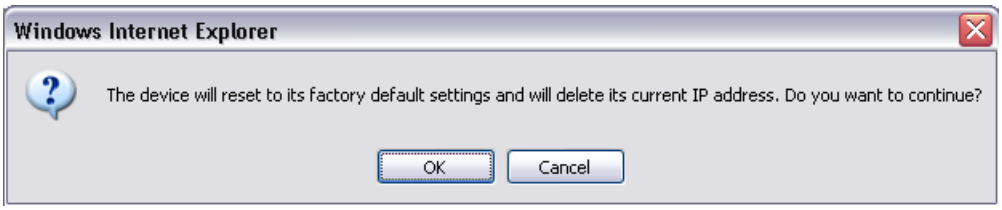
Then a new Catalyst Blade Switch 3020 Device Manager will be opened.

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: Validate XML file.

   Note: This script validates the XML file to a limited extent:

   - Verifies the file is valid XML
   - Verifies all required options for commands are present
   - Verifies all provided options for commands are valid options
   - Verifies SOME but not all option values

   Validate the XML file before executing it by performing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --file=3020_configure.xml --testRun >
/dev/null
```

If nothing is returned then the XML file is valid to the extent defined in the note above. Along with a brief description, errors will return a string indicating the line location of the fault in the XML file.

10. 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.

11. 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.

12. 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.

13. Perform *3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* 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 /var/TKLC/smac/image/<FW_image>
```

3.1.3.2 Replace a Failed 3020 Switch (netConfig)

The procedure describes all of the required steps to configure a replacement 3020 switch.

Prerequisite:

Prerequisites for this procedure are to follow the prerequisites for procedures referenced in the steps of this procedure. Also, it is assumed that the user can determine which switch is the failed switch.

Fill in the appropriate value from [2].

Variable	C3020
<IOS_image_file>	

Needed Material:

- HP MISC firmware ISO image

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. Replace switch

   Replace the failed switch with the replacement switch.

2. Install cables

   Install all cables in the new switch. Be sure all cables are placed in the same ports in the replacement switch as they were used on the failed switch.

3. Virtual PM&C: Move firmware image

   Firmware version must be identical between mating switches, to check the firmware on the mate switch use the following command:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getFirmware
   ```

   Move the appropriate FW image from the switch backup directory to the TFTP directory by performing the following command:

   For a PM&C System:

   ```
   $ sudo /bin/mv -i <switch_backup_directory/<FW_image> /var/TKLC/smac/image/
   ```

   For a non-PM&C System:

   ```
   $ sudo /bin/mv -i <switch_backup_directory/<FW_image> /var/lib/tftpboot/
   ```

   Note: If the file does not exist on the server, copy it from the firmware media.

4. Apply configuration

   Perform *3.1.3.1 Configure Cisco 3020 Switch (netConfig)*, steps 3-9 then 12, replacing the values for the switch being replaced.

5. Virtual PM&C: Restore the switch to the latest known good configuration.

   Navigate to the <switch_backup_user> home directory.

```
$ cd ~<switch_backup_user>
```

   Verify your location on the server

```
$ /bin/pwd
/home/<switch_backup_user>
```

6. Virtual PM&C: Copy the switch backup files to the current directory

```
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup*
/home/<switch_backup_user>
```

   Get a list of the file copied over.

   Note: 'switch1A' is shown as an example.

```
$ /bin/ls -l
switch1A-backup     switch1A-backup.info     switch1A-backup.vlan
```

7. Virtual PM&C: Verify switch is initialized

   Verify switch is at least initialized correctly and connectivity to the switch by verifying hostname.

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

   Note: The value beside 'Hostname:' should be the same as the <switch_hostname> variable.

8. Virtual PM&C: Issue the restore command

```
$ cd ~<switch_backup_user>
$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname>
restoreConfiguration service=ssh_service filename=<switch_hostname>-backup
```

9. Virtual PM&C: Verify Connectivity

   Perform *3.1.3.1 Configure Cisco 3020 Switch (netConfig)*, step 10.

10. **Virtual PM&C:** Cleanup FW

    Remove the FW images from the users' home directory and TFTP directory with the following command:

```
$ sudo rm ~admusr/<fw_image>
$ sudo rm /var/TKLC/smac/image/<fw_image>
```

3.1.3.3 Configure HP 6120XG Switch (netConfig)

This procedure will configure the HP 6120XG switches from the PM&C server and the command line interface using templates included with an application.

Prerequisites:

- It is essential that PM&C is installed. In addition, complete these procedures:
- *3.5.2 Configure Initial OA Settings Using the Configuration Wizard*
- *3.1.1 Configure netConfig Repository*
- *3.5.1 Configure Initial OA IP*
- This procedure requires the reader to issue commands on the switch command line interface.

Conditional Prerequisites: If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches need to be configured using *3.1.2.1 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 to ask for assistance.

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.

Note: The HP 6120XG switch requires router advertisements for learning the IPv6 default route. No manual IPv6 default route can be configured on this switch.

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 the 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.

   Note: Note that the files that are created in this step can be prepared ahead of time using the NAPD.

```
$ 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
```

7. Virtual PM&C: Apply include-credentials command to the switch

   Login to the switch using SSH

```
$ /usr/bin/ssh <username>@<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, contact My Oracle Support

9. Virtual PM&C: Validate XML file.

   Note: This script validates the XML file to a limited extent:

   - Verifies the file is valid XML
   - Verifies all required options for commands are present
   - Verifies all provided options for commands are valid options
   - Verifies SOME but not all option values

   Validate the XML file before executing it by performing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --file=6120XG_[single,LAG]Uplink_configure.xml
 --testRun > /dev/null
```

   If nothing is returned then the XML file is valid to the extent defined in the note above. Along with a brief description, errors will return a string indicating the line location of the fault in the XML file.

10. 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, contact My Oracle Support

11. 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.

12. 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.

13. Virtual PM&C: Repeat steps for each HP 6120XG

    For each HP 6120XG, repeat steps 3-12.

14. Perform *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch* for each switch configured in this procedure.

15. Virtual PM&C: Clean up FW file

    Remove the FW file from the tftp directory.

```
$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>
```

3.1.3.4 Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch (netConfig)

The procedure describes all of the required steps to configure a replacement HP (6120XG, 6125G, 6125XLG) switch.

Prerequisite: Prerequisites for this procedure are to follow the prerequisites for procedures referenced in the steps of this procedure. It is also assumed the user can determine which switch is the failed switch.

Variable	HP6120XG	HP6125G	HP6125XLG
<IOS_image_file>			

Needed Material:

- HP MISC firmware ISO image

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. Replace switch

Replace the failed switch with the replacement switch.

2. Virtual PM&C: Move firmware image

   Firmware version must be identical between mating switches, to check the firmware on the mate switch use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getFirmware
```

   Move the appropriate FW image from the switch backup directory to the backup user directory by performing the following command:

```
$ sudo /bin/cp -i <switch_backup_directory/<FW_image> ~<switch_backup_user>/
```

   Note: If the FW image does not exist on the server, copy it from the FW media. Change FW image file permissions:

```
$ sudo /bin/chmod 644 <FW_image>
```

3. Initialize Switch

   - For a 6125G:

     Perform *3.1.3.5 Configure HP 6125G Switch (netConfig)*, steps 3-4, 6 (init.xml only), and then perform Step 8. Return to this procedure, and continue with the next step.

   - For a 6125XLG:

     Perform *3.1.3.6 Configure HP 6125XLG Switch (netConfig)* steps 3-4, 6 (init.xml only), and then perform step 8. Return to this procedure, and continue with the next step.

   - For a 6120XG:

     Perform *3.1.3.3 Configure HP 6120XG Switch (netConfig)*, step 3, then steps 4-6 (init.xml only), and step 8. Return to this procedure, and continue with the next step.

4. Virtual PM&C: Copy the switch backup files to the user's home directory

```
$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup*
~<switch_backup_user>/
```

5. Virtual PM&C: Prepare to issue the restore command

   Prepare to issue the restore command by executing the following commands.

```
cd ~<switch_backup_user>
$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*
```

6. Virtual PM&C: Perform only if restoring a 6120XG switch otherwise skip to the next step.

   Some features enabled on a 6120XG may not restore properly if they reference a port channel which doesn't currently exist on the switch ahead of the restore operation. Identify any portchannels that need to be created on the switch according to the backup file and create them before restoring the configuration:

```
$ sudo /bin/cat <switch_hostname>-backup | /bin/grep "^trunk"
```

Reference the following example:

```
$ sudo /bin/cat <switch_hostname>-backup | /bin/grep "^trunk"
trunk <int list> Trk<id> LACP
trunk <int list> Trk<id> Trunk
$
```

If any port-channels are found, then for each portchannel identified by the above command, use the "netConfig setLinkAggregation" command to create it and the "netConfig showConfiguration" command to verify its configuration.

For example, If an "LACP" port channel was found, add the port-channel by executing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation
id=<id>  addPort=tenGE<int list> mode=active
```

If a "Trunk" port-channel was found (as labeled after the "Trk<id>"), add the port-channel by executing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation
id=<id>  addPort=tenGE<int list> mode=static
```

Verify the port-channels were added to the running configuration by executing the following command:

```
$ sudo  /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 showConfiguration |
 grep "^trunk"
trunk <int list> Trk<id> LACP
trunk <int list> Trk<id> Trunk
$
```

7. Virtual PM&C: Issue the restore command

   For all switch types and configurations found, use netConfig to restore the configuration by executing the following command:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname>
   restoreConfiguration service=ssh_service filename=<switch_hostname>-backup
   ```

   Note: This will cause the switch to reboot. It will take approximately 120-180 seconds before connectivity is restored.

8. Install Cables

   Install all cables in the new switch. Be sure all cables are placed in the same ports in the replacement switch as they were used on the failed switch.

9. Virtual PM&C: Verify connectivity

   - For a 6125G:

     Refer to *3.1.3.5 Configure HP 6125G Switch (netConfig)*, step 12.

   - For a 6125XLG:

     Refer to *3.1.3.6 Configure HP 6125XLG Switch (netConfig)*, step 11.

   - For a 6120XG:

Refer to *3.1.3.3 Configure HP 6120XG Switch (netConfig)*, steps 10-11.

Note: For the 6120XG, apply QoS policy and verify connectivity.

10. Virtual PM&C: Cleanup FW

    Remove the FW images from the users' home directory and TFTP directory with the following command:

```
$ sudo rm ~admusr/<fw_image>
$ sudo rm /var/TKLC/smac/image/<fw_image>
```

3.1.3.5 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.

Prerequisites:

- It is essential that PM&C is installed. In addition, complete these procedures:
- *3.1.1 Configure netConfig Repository*
- *3.5.1 Configure Initial OA IP*
- *3.5.2 Configure Initial OA Settings Using the Configuration Wizard*
- This procedure requires the reader to issue commands on the switch command line interface.

Conditional Prerequisites: If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches need to be configured using *3.1.2.1 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 Application physical Site Survey and related IP/Network Site survey. 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.

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 in to 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, login to 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 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 *F.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
```

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, contact My Oracle Support

10. Virtual PM&C: Execute Appendix *L.1 Downgrade 6125G Switch Firmware* to verify the existing firmware version and downgrade if required.
11. Virtual PM&C: Validate XML file.

    Note: This script validates the XML file to a limited extent:

    - Verifies the file is valid XML

- Verifies all required options for commands are present
- Verifies all provided options for commands are valid options
- Verifies SOME but not all option values

Validate the XML file before executing it by performing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --file=6125G_configure.xml --testRun >
/dev/null
```

If nothing is returned then the XML file is valid to the extent defined in the note above. Along with a brief description, errors will return a string indicating the line location of the fault in the XML file.

12. Virtual PM&C: Configure the switch

    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.

13. Virtual PM&C: Add the IPv6 default route (IPv6 network only)

    For IPv6 management networks, the enclosure switch requires an IPv6 default route to be configured. Apply the following command using netConfig:

    ```
    $ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addRoute network=::/0
     nexthop=<mgmtVLAN_gateway_address>
    ```

14. 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.
    ```

15. Virtual PM&C: Repeat steps for each HP 6125G

    For each HP 6125G, repeat *3.1.3.5 Step 4* - *3.1.3.5 Step 14*.

16. Perform *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch* for each switch configured in this procedure.

17. **Virtual PM&C:** Clean up FW file

    Remove the FW file from the tftp directory.

    ```
    $ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>
    ```

3.1.3.6 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.

Prerequisites:

- It is essential that PM&C is installed. In addition, complete these procedures:
- *3.5.1 Configure Initial OA IP*
- *3.5.2 Configure Initial OA Settings Using the Configuration Wizard*
- *3.1.1 Configure netConfig Repository*
- This procedure requires the reader to issue commands on the switch command line interface.

Conditional Prerequisites: If the aggregation switches are provided by Oracle, then the Cisco 4948/4948E/4948E-F switches need to be configured using *3.1.2.1 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 Application physical Site Survey and related IP/Network Site survey. 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.

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 supported by Oracle, login to 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, login to 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 *F.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, contact My Oracle Support

10. Virtual PM&C: Validate XML file.

    Note: This script validates the XML file to a limited extent:

    - Verifies the file is valid XML
    - Verifies all required options for commands are present
    - Verifies all provided options for commands are valid options
    - Verifies SOME but not all option values

    Validate the XML file before executing it by performing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --file=6125XLG_configure.xml --testRun >
/dev/null
```

    If nothing is returned then the XML file is valid to the extent defined in the note above. Along with a brief description, errors will return a string indicating the line location of the fault in the XML file.

11. 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.

12. Virtual PM&C: Add the IPv6 default route (IPv6 network only)

For IPv6 management networks, the enclosure switch requires an IPv6 default route to be configured. Apply the following command using netConfig:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addRoute network=::/0
 nexthop=<mgmtVLAN_gateway_address>
```

13. 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.
```

14. For HP 6125XLG switches connected by 4x1GE LAG uplink perform Utility procedure *3.1.4.9 Configure Speed and Duplex for 6125XLG LAG Ports (netConfig)*. Otherwise, for deployments with 10GE uplink, continue to the next step.

15. Virtual PM&C: Repeat steps for each HP 6125XLG

For each HP 6125XLG, repeat *3.1.3.6 Step 4* - *3.1.3.6 Step 14*.

16. 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 *3.1.3.6 Step 14*.

For HP 6125XLG switches uplinking with 4x1GE LAG to product Cisco 4948/E/E-F aggregation switches, perform Utility Procedure *3.1.4.10 Configure Speed and Duplex for LAG Ports for Cisco 4948/E/E-F (netConfig)*, to match speed and duplex settings from *3.1.3.6 Step 14*.

Otherwise, for deployments with 10GE uplink, continue to the next step.

17. Perform *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch* for each switch configured in this procedure.

3.1.4 Utility Procedures

3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch

This procedure should be executed after every change to a switch configuration or after completing *3.1.3.3 Configure HP 6120XG Switch (netConfig)*, *3.1.3.5 Configure HP 6125G Switch (netConfig)*, *3.1.3.6 Configure HP 6125XLG Switch (netConfig)*, or *3.1.2.3 Configure HP 5900 Aggregation Switches (PM&C Installed) (netConfig)*, or *3.1.2.4 Configure Cisco 9372TX-E Aggregation Switches (PM&C Installed) (netConfig)*.

Prerequisites:

- *3.6.1 IPM Management Server* must be completed
- *3.7.2 Installing TVOE on the Management Server* must be completed
- *3.7.3 TVOE Network Configuration* must be completed
- *3.7.4 Deploy PM&C Guest* must be completed

Procedure Reference Tables:

Variable	Value
<switch_name>	hostname of the switch
<switch_backup_user>	admusr
<fw_image>	FW file used in firmware upgrade/switch replacement/ or initial install.

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
```

Then change directory ownership:

```
$ sudo /bin/chown –R pmacd:pmacbackup /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 ~<switch_backup_user>/<switch_name>-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 -l /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup*
ll P2-Switch1-backup*
-rw-r----- 1 root root 11910 Jul 8 10:20 <switch_name>-backup
-rw------- 1 admusr admgrp 69 Jul 8 10:20 <switch_name>-backup.info
$ sudo /bin/cat /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup
$
```

5. Repeat *3.1.4.1 Step 2* - *3.1.4.1 Step 4* for each HP or Cisco switch to be backed up.
6. Delete FW files:

   Delete the firmware off the system by performing the following command:

```
$ sudo /bin/rm -f ~<switch_backup_user>/<fw_image>
```

   For Cisco 9372TX-E switches only, execute the following command:

```
$ sudo /bin/rm -f <switch_backup_directory>/<fw_image>
```

3.1.4.2 Configure SNMP Communities and Trap Servers

It is essential that all switches have been configured successfully using:

- *3.1.3.1 Configure Cisco 3020 Switch (netConfig)* and/or
- *3.1.3.3 Configure HP 6120XG Switch (netConfig)* and/or
- *3.1.3.5 Configure HP 6125G Switch (netConfig)* and/or
- *3.1.3.6 Configure HP 6125XLG Switch (netConfig)* and/or
- *3.1.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)*

Variable	Value
<switch_name>	See Application Documentation and step 2
<switch_platform_username>	See Application Documentation
<community string>	See Application Documentation
<snmp_server_ip>	See Application Documentation

1. Virtual PM&C: Log in to the PM&C Guest
2. Virtual PM&C: Determine which devices require SNMP configuration.
   1. Use the command netConfig to list the devices in its repository.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
Devices:
```

```
Device: 6120XG_IOBAY3
    Vendor:   HP
    Model:    6120
    Access:   Network: 10.240.8.9
    Init Protocol Configured
    Live Protocol Configured

Device: C3020_IOBAY1
    Vendor:   Cisco
    Model:    3020
    Access:   Network: 10.240.8.7
    Init Protocol Configured
    Live Protocol Configured

Device: cClass-switch1A
    Vendor:   Cisco
    Model:    4948E
    Access:   Network: 10.240.8.3
    Access:   OOB:
            Service: console_service
            Console: cClass-sw1A-console
    Init Protocol Configured
    Live Protocol Configured
```

2. Determine which devices should have the community string added/removed.

   Note: Refer to application documentation to determine which switches to add/remove the community string, making a note of the DEVICE NAME of each switch. This will be used as <switch_name>. In the example output above, DEVICE NAME = 6120XG_IOBAY3, C3020_IOBAY1 and cClass-switch1A.

3. Virtual PM&C: Configure the community string

   Using the information from *3.1.4.2 Step 2*, use these commands to add or remove the community string.

   - To ADD a community string:

```
$sudo /usr/TKLC/plat/bin/netConfig addSNMP --device=<switch_name>
community=<community_string>  uauth=RO
```

   - To DELETE a community string:

```
$sudo /usr/TKLC/plat/bin/netConfig deleteSNMP --device=<switch_name>
community=<community_string>
```

4. Virtual PM&C: Configure the SNMP trap server

   Using the information from *3.1.4.2 Step 2*, use these commands to add or remove a trap server.

   - To ADD a trap server:

     1. For the 6120XG:

```
$ sudo /usr/TKLC/plat/bin/netConfig addSNMPNotify --device=<switch_name>
host=<snmp_server_ip>  version=2c auth=<community_string> traplvl=not-info
```

2. For all other devices:

```
$ sudo /usr/TKLC/plat/bin/netConfig addSNMPNotify --device=<switch_name>
host=<snmp_server_ip>  version=2c auth=<community_string>
```

- To DELETE a trap server:

1. For the 6120XG:

```
$ sudo /usr/TKLC/plat/bin/netConfig deleteSNMPNotify --device=<switch_name>
host=<snmp_server_ip>  version=2c auth=<community_string> traplvl=not-info
```

2. For all other devices:

```
$ sudo /usr/TKLC/plat/bin/netConfig deleteSNMPNotify --device=<switch_name>
host=<snmp_server_ip>  version=2c auth=<community_string>
```

5. Virtual PM&C: Verify the SNMP configuration

   Verify the switch has been configured with the appropriate SNMP communities and trap servers:

```
$ sudo /usr/TKLC/plat/bin/netConfig getSNMP --device=<switch_name>

SNMP Community: "test"
```

```
$ sudo /usr/TKLC/plat/bin/netConfig listSNMPNotify --device=<switch_name>

Notification:  = (
Password change
Login failures
Port-Security
Authorization Server Contact
DHCP-Snooping
Dynamic ARP Protection
Dynamic IP Lockdown
)

Host:  = (
10.240.8.4
10.240.8.6
)
```

6. Virtual PM&C: Backup the switch configuration.
   - For Cisco: Perform *3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)*.
   - For 6120XG: Perform *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch*.
7. Virtual PM&C: Repeat *3.1.4.2 Step 3* - *3.1.4.2 Step 6* for each device.

3.1.4.3 Configure QoS (DSCP and/or CoS) on HP 6120XG Switches

Prerequisites:

- It is essential that all switches have been configured successfully using *3.1.3.3 Configure HP 6120XG Switch (netConfig)*

Variable	Value
<switch_name>	See Application Documentation and step 2
<dscp value>	See Application Documentation (if present)
<cos value>	See Application Documentation (if present)
<switch_platform_username>	See Application Documentation
<Vlanid>	See Application Documentation

1. Virtual PM&C: Login to the PM&C Guest

   Login to the PM&C Guest.

2. Virtual PM&C: Determine which devices require QoS Policies

   Use netConfig to list the devices in its repository and determine which devices should be configured with QoS.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
Devices:
Device: 6120XG_IOBAY3
Vendor: HP
Model: 6120
Access: Network: 10.240.8.9
Init Protocol Configured
Live Protocol Configured
Device: C3020_IOBAY1
Vendor: Cisco
Model: 3020
Access: Network: 10.240.8.7
Init Protocol Configured
Live Protocol Configured
Device: cClass-switch1A
Vendor: Cisco
Model: 4948E
Access: Network: 10.240.8.3
Access: OOB:
Service: console_service
Console: cClass-sw1A-console
Init Protocol Configured
Live Protocol Configured
```

   Note: Refer to application documentation to determine which switches or pairs of switches to configure with QoS, making a note of the DEVICE NAME of each 6120XG switch. These will be referred to as <switch_name> in the following steps

3. Virtual PM&C:Add DSCP and/or CoS Policy.

   Using the information from the previous step, use one of the following commands to configure DSCP and/or CoS marking on the device.

   For DSCP and CoS Marking:

```
$ sudo /usr/TKLC/plat/bin/netConfig addQOS --device=<switch_name> vlan=<vlanid>
 dscp=<dscp value> cos=<cos value> name=<user defined name>
```

For DSCP Marking Only:

```
$ sudo /usr/TKLC/plat/bin/netConfig addQOS --device=<switch_name> vlan=<vlanid>
 dscp=<dscp value> name=<user defined name>
```

For CoS Marking Only:

```
$ sudo /usr/TKLC/plat/bin/netConfig addQOS --device=<switch_name> vlan=<vlanid>
 cos=<cos value>
```

4. Virtual PM&C: Verify the QoS configuration on the switch
   Verify the QoS configuration:

```
$ sudo /usr/TKLC/plat/bin/netConfig getQOS --device=<switch_name> vlan=<vlanid>
```

   Example Output:

```
$ sudo /usr/TKLC/plat/bin/netConfig getQOS --device=6120XG_IOBAY3 vlan=2

Policy:  = (
  VLAN priorities
  VLAN ID Apply rule  | DSCP   Priority
2       DSCP        | 000011 3
)
```

5. Virtual PM&C: Repeat steps 3-4 for each Policy
   Repeat steps 3-4 for each policy that needs to be applied to the switch.
6. Backup the Switch.
   Execute the *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch* procedure.
7. Virtual PM&C: Repeat steps 3-6 for each switch.
   Repeat steps 3-6 for each switch identified in step 2.

3.1.4.4 Configure Port Mirroring

Prerequisites:

- It is essential that all switches have been configured successfully using:
  - *3.1.3.1 Configure Cisco 3020 Switch (netConfig)* and/or
  - *3.1.3.3 Configure HP 6120XG Switch (netConfig)* and/or
  - *3.1.3.5 Configure HP 6125G Switch (netConfig)* and/or
  - *3.1.3.6 Configure HP 6125XLG Switch (netConfig)* and/or
  - *3.1.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)*

Variable	Value
<switch_name>	See Application Documentation and *3.1.4.4 Step 2*
<switch_model>	Fill in appropriate value from *3.1.4.4 Step 2*
<switch_IP>	Fill in appropriate value from *3.1.4.4 Step 2*

<srcInterface>	See Application Documentation
<destInterface>	See Application Documentation
<switch_platform_username>	See Application Documentation
<srcVlanid>	See Application Documentation

1. Virtual PM&C: Log into the PM&C Guest
2. Virtual PM&C: Determine the port mirror source devices.

   Use netConfig to list the devices in its repository and determine which devices should be configured with port mirroring.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
Devices:

Device: 6120XG_IOBAY3
    Vendor: HP
    Model: 6120
    Access: Network: 10.240.8.9
    Init Protocol Configured
    Live Protocol Configured

Device: C3020_IOBAY1
    Vendor: Cisco
    Model: 3020
    Access: Network: 10.240.8.7
    Init Protocol Configured
    Live Protocol Configured

Device: 6125G_IOBAY5
    Vendor:   HP
    Model:    6125
    Access:   Network: 10.240.8.12
    Access:   OOB:
    Service: oa_service
    Console: 5
    Init Protocol Configured
    Live Protocol Configured

Device: cClass-switch1A
    Vendor: Cisco
    Model: 4948E
    Access: Network: 10.240.8.3
    Access: OOB:
    Service: console_service
    Console: cClass-sw1A-console
    Init Protocol Configured
    Live Protocol Configured
```

   Note: Refer to application documentation to determine which switches to configure source monitoring devices, making a note of the DEVICE NAME, MODEL and IP ADDRESS of each switch. These will be used as <switch_name>,<switch_model>,<switch_IP> in future steps and the model will determine the command.

3. Virtual PM&C: Configure port mirroring.

   Using the information from *3.1.4.4 Step 2*, use the following command to configure port mirroring. Pay close attention to the device model.

For VLAN Monitoring (Cisco Devices Only):

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addPortMirror session=1
 vlan=<srcVlanid> destInterface=<mirrorPort> direction=both
```

For Port Mirroring:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addPortMirror session=1
 sourceInterface=<srcInterface> destInterface=<mirrorPort> direction=both
```

Note: The interface option allows for more than one source interface. The value can be entered as a single interface ex: GE1 (1Gb port) or tenGE1 (10Gb port) or it can be entered as a range of interfaces separated by commas and dashes ex: GE1-5,GE7,tenGE9-10.

Note: The only direction supported by the HP switches is 'both.' If the direction option is used on an HP switch, it will be ignored and 'both' is applied.

VLAN Example:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=C3020_IOBAY1 addPortMirror session=1
 vlan=2 destInterface=GE10 direction=both
```

Port Example:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY3 addPortMirror session=1
 sourceInterface=tenGE1,tenGE3 destInterface=tenGE2
```

4. Virtual PM&C: Verify the Port Mirroring configuration on the switch.
   Verify that the port monitoring session is configured:

```
$ sudo /usr/TKLC/plat/bin/netConfig getPortMirror session=1 --device=6120XG_IOBAY3

Session: 1
  Direction: both
  Source: tenGE2
  Destination: tenGE1,tenGE3
```

```
$ sudo /usr/TKLC/plat/bin/netConfig getPortMirror session=1 --device=6125G_IOBAY4

Session: 1
  Direction: both
  Source: GE1
  Destination: GE22
```

   Note: Output from the command above may vary slightly from one device type to another.

5. Virtual PM&C: Backup the switch configuration

   For Cisco:

   Perform the *3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* procedure.

   For HP:

   Perform the *3.1.4.1 Backup HP (6120XG, 6125G, 6125XLG, 5900AF, 9372TX-E) Switch* procedure.

6. Virtual PM&C: Repeat steps *3.1.4.4 Step 3* - *3.1.4.4 Step 5* for each monitor source device.

3.1.4.5 SwitchConfig to netConfig Repository Configuration

This procedure will configure the netConfig repository with the necessary services and previously configured switches from a single management server for use with the c-Class platform.

Prerequisites:

- *3.6.1 IPM Management Server*,
- *3.7.2 Installing TVOE on the Management Server*,
- *3.7.3 TVOE Network Configuration*,
- *3.7.4 Deploy PM&C Guest*, and
- *3.7.5 Setup PM&C* are required to be completed before this procedure is attempted.
- Application management network interfaces must be configured on the management servers prior to executing this procedure.
- Application username and password for creating switch backups must be configured on the management server prior to executing this procedure.

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.

Variable	Serial Port
<serial console type> u=USB, c=PCIe>	u=USB, c=PCIe

Fill in the appropriate value for this site:

Variable	Value
<switch_hostname>	Fill in the appropriate value for this site:
<switch_platform_username>	See referring application documentation
<switch_platform_password>	See referring application documentation
<switch_console_password>	See referring application documentation
<switch_enable_password>	See referring application documentation
<management_server1A_mgmtVLAN_ip_address>	
<management_server1B_mgmtVLAN_ip_address>	
<pmac_mgmtVLAN_ip_address>	
<switch_mgmtVLAN_id>	
<switch1A_mgmtVLAN_ip_address>	
<mgmt_Vlan_subnet_id>	
<netmask>	
<switch1B_mgmtVLAN_ip_address>	
<switch_Internal_VLANS_list>	
<switch_mgmtVlan_id>	

<management_server_mgmtInterface>	
<management_server1A_iLO_ip>	
<management_server1B_iLO_ip>	

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>	Initial password as provided by Oracle

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

Note: Uplinks must be disconnected from the customer network before executing this procedure. One of the steps in this procedure describes 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]
- Application specific documentation (documentation that referred to this procedure)
- Template xml files on the application media

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. Management server iLO: Login and launch the integrated remote console.

   On Server1A login to iLO in IE using password provided by application:

   ```
   http://<management_server1A_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.

   If not already done so, login as admusr.

2. Management Server: Procedure pre-check - verify hardware type

   Certain steps in this procedure require enabling and disabling ethernet interfaces. This procedure supports DL360 and DL380 servers. The interfaces that are to be enabled and disabled are different for each server type.

   To determine the interface name, on the server, execute the following command:

   ```
   $ /bin/cat /proc/net/bonding/bond0 | grep Interface
   Slave Interface: eth01
   Slave Interface: eth02
   $
   ```

Note the slave interface names of ethernet interfaces to use in subsequent steps. The first line will be the value for <ethernet_inteface_1> and the second line will be the value for <ethernet_interface_2> .

For example, from the sample output provided, <ethernet_inteface_1> would be eth01 . If the output from the above command is not successful, refer back to the application documentation.

3. Management Server: Procedure pre-check - determine Platform version

   On each management server, determine the Platform version of the system by issuing the following command:

```
$ /usr/TKLC/plat/bin/appRev
```

   If the following is shown in the output, the Platform version is 7.2:

```
Base Distro Release: 7.2.x.x.x_x.x.x
```

   The values of x-x.x.x do not matter. The value of 7.2 shows the platform version. If the command shows a Base Distro Release version lower than 7.2, or fails to execute, stop this procedure and refer back to application procedures. It is possible the wrong version of TVOE/TPD is installed.

4. Management Server: Procedure pre-check - verify virtual PM&C is installed

   PM&C is required to be installed prior to this procedure being attempted. 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. Refer to application documentation or contact My Oracle Support.

5. Virtual PM&C: 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: 7.2.0.0.0_88.6.0

Checking Platform Revision for remote TPD installation...
The remote machine is running:
        Product Name: TVOE
 Base Distro Release: 7.2.0.0.0_88.6.0
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 PMAC 6.3.
- Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

6. Virtual PM&C: Login to the console of the virtual PM&C.

   Note: On a TVOE host, If you launch the virsh console, that is, "$ **`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.

   From management server1A, log into the console of the virtual pmac instance found in *3.1.4.5 Step 4*.

```
$ 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 another 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. Refer to application documentation or contact My Oracle Support.

7. Virtual PM&C: Verify PM&C release version.

   Verify the PM&C release version.

```
$ /usr/TKLC/plat/bin/appRev
```

If the following is shown in the output, the PM&C version is 5.0:

```
Product Name: PMAC
Product Release: 5.0.0_x.x.x
```

If the output does not contain "Product Name: PMAC" or does not contain a PMAC version of 5.0 or higher, then stop this procedure and refer back to the application instructions.

8. Virtual PM&C: Setup netConfig repository with necessary tftp information.

   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.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service
Service type [ssh, conserver, oa, tftp]? tftp
TFTP host IP? <pmac_mgmtVLAN_ip_address>
Directory on host? /var/TKLC/smac/image/
Add service for tftp_service successful
```

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

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=tftp_service
```

   and check the output, which will be similar to the one shown below (Note: only the tftp service info has been shown in this example. If the previous step and this step were done correctly, both the console_service and tftp_service entries would show up)

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=tftp_service
Services:
Service Name: tftp_service
Type: tftp
Host: 10.240.8.4
Options:
dir: /var/TKLC/smac/image
$
```

9. Virtual PM&C: Setup 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 with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as answer must be entered EXACTLY as they are shown here.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service
Service type [ssh, conserver, oa, tftp]? ssh
Service host? <pmac_mgmtVLAN_ip_address>
SSH username? <switch_backup_user>
SSH password?: <switch_backup_user_password>
Verify Password: <switch_backup_user_password>
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: 10.250.62.85
Options:
password: C20F7D639AE7E7
user: admusr
$
```

10. Virtual PM&C: Setup netConfig repository with Aggregation switch information.

    Note: If there are no aggregation switches in this deployment, skip to the next step.

    Use netConfig to create a repository entry for switch1A and switch1B. 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.

    Note: The model can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact My Oracle Support.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor [Cisco, HP]? Cisco
Device Model [3020, 4948, 4948E,4948E-F]? <device_model>
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation)  address for
 management?: <switch_mgmt_ip_address>/<prefix>
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=switch1A
```

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

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
Device: switch1A
Vendor: Cisco
Model: 4948E
FW Ver: 0
Access: Network: 10.240.64.34
Access: OOB:
Service: console_service
Console: switch1A_console
Init Protocol Configured
Live Protocol Configured
$
```

11. Virtual PM&C: Setup netConfig repository with switch information.

Note: If there are no 3020s in this deployment, skip to the next step.

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, stop now and contact My Oracle Support.

Note: The device name must be 20 characters or less

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor [Cisco, HP]? Cisco
Device Model [3020, 4948, 4948E,4948E-F]? 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: <FW_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 listDevices
```

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

Note: Only the switch1B info has been shown in this example. If the previous step and this step were done correctly, both switch1A and switch1B entries would show up.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
Devices:
Device: C3020_IOBAY1
Vendor: Cisco
Model: 3020
Access: Network: 10.240.8.7
Init Protocol Configured
Live Protocol Configured
[admusr@pmac5000101 ~]$
```

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

12. Virtual PM&C: setup netConfig repository

Note: If there are no 6120s in this deployment, skip to the next step.

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, stop now and contact My Oracle Support.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor [Cisco, HP]? HP
Device Model [6120, 6125, 6125XLG]? 6120
What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for
management?: <switch_mgmt_ip_address>/<prefix>
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
```

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:

Note: If the previous step and this step were done correctly, both switch1A and switch1B entries would show up.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
Device: 6120XG_IOBAY1
Vendor: HP
Model: 6120
FW Ver: 0
Access: Network: 10.240.8.10
Init Protocol Configured
Live Protocol Configured
[admusr@pmac5000101 ~]$
```

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

13. Perform the 'switchconfig to netConfig migration procedure' for all switches in the system.

3.1.4.6 Cisco Switch switchconfig to netConfig Migration

This procedure configures a Cisco switch to migrate from switchconfig to netConfig.

Needed Materials:

- HP MISC firmware ISO image
- Release Notes of the *HP Solutions Firmware Upgrade* [2],
- Application specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application media.

Variable	Serial Port
<switch1A_serial_port>	ttyS4
<switch1B_serial_port>	ttyS5

In the following tables, fill in the blanks with the appropriate value for this site:

Variable	Value
<switch_platform_username>	See referring application documentation
<switch_platform_password>	See referring application documentation
<switch_console_password>	See referring application documentation
<switch_enable_password>	See referring application documentation
<pmac_mgmtVLAN_ip_address>	
<switch_mgmtVLAN_id>	
<mgmt_Vlan_subnet_id>	
<netmask>	
<switch_Internal_VLANS_list>	
<switch_mgmtVlan_id>	
<management_server_mgmtInterface>	

<management_server1A_iLO_ip>	
<management_server1B_iLO_ip>	
<switch_mgmt_IP_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>	Initial password as provided by Oracle

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. Virtual PM&C: Verify network connectivity to the switch

   For each switch, verify network reachability.

```
# /bin/ping -w3 <switch_mgmt_IP_address>
```

2. Virtual PM&C: Login to the switch

   Login to the switch using Telnet

```
# /usr/bin/telnet <switch_mgmt_IP_address>
```

3. Switch CLI: Apply netConfig required commands:

   From the switch CLI, apply the following commands required by netConfig:

```
Switch# config t
Switch(config)# hostname <switch_name>
Switch(config)# no service config
Switch(config)# service password-encryption
Switch(config)# crypto key generate rsa usage-keys label sshkeys modulus 768
Switch(config)# aaa new-model
Switch(config)# aaa authentication login onconsole line
Switch(config)# username <switch_platform_username> secret
<switch_platform_password>
Switch(config)# enable secret <switch_enable_password>
Switch(config)# line vty 0 15
Switch(config-line)# no password
Switch(config-line)# transport input ssh
Switch(config)# exit
Switch(config)# line console 0
Switch(config-line)# login authentication onconsole
Switch(config-line)# password <switch_console_password>
Switch(config)# exit
Switch(config)# ip ssh version 2
Switch(config)# no ip http server
Switch(config)# no ip http secure-server
Switch(config)# no ip domain lookup
Switch(config)# end
Switch# write memory
```

4. **Switch CLI:** Reload the switch and verify configuration

   Reload the switch and verify the configuration from *3.1.4.6 Step 3*. If a command was not applied, repeat *3.1.4.6 Step 3*.

   ```
   Switch# reload
   ```

   If prompted, answer yes.

5. Virtual PM&C: Verify netConfig connectivity.

   Perform the following netConfig command to verify that netConfig can communicate with the switch.

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_name>
   ```

   Hostname: <switch_name>

6. Backup the Configuration

   Perform the *3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* procedure and then return to this procedure and continue with *3.1.4.6 Step 7* of this procedure

7. Reset to factory defaults

   - For the 4948-series switches, perform the following command:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig setFactoryDefault --device=<switch_name>
   ```

   - For the 3020-series switches, perform Step 4 of the *3.1.3.2 Replace a Failed 3020 Switch (netConfig)* procedure.

8. Restore the Configuration

   - For 4948-series switches: Perform Steps 6-22 of the *3.1.2.5 Replace a Failed 4948/4948E/4948E-F Switch (PM&C Installed) (netConfig)* procedure.
   - For 3020 switches: Perform Steps 5-10 of the *3.1.3.2 Replace a Failed 3020 Switch (netConfig)* procedure.

9. Virtual PM&C: Repeat *3.1.4.6 Step 2* - *3.1.4.6 Step 8* for each switch being migrated.

3.1.4.7 HP 6120XG switchconfig to netConfig Migration

This procedure configures a 6120XG switch to migrate from switchconfig to netConfig.

Needed Materials:

- HP MISC firmware ISO image
- HP Solutions Firmware Upgrade Pack Release Notes
- 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 My Oracle Support section of this document.

1. Management Server: Verify network connectivity to 6120XG switches

For each 6120XG switch, verify reachability.

```
$ /bin/ping -w3 <enclosure_switch_IP>
```

2. Management Server: Login to the Switch

   Login to the 6120XG switch using SSH/Telnet

```
$ /usr/bin/ssh manager@<enclosure_switch_IP>
```

   If the above command fails, log in using telnet:

```
$ /usr/bin/telnet <enclosure_switch_IP>
```

3. Switch CLI: Apply netConfig required commands:

   From the 6120XG CLI, apply the following commands required by netConfig:

```
Switch# config
Switch(config)# hostname <switch_name>
Switch(config)# no password all
Password protection for all will be deleted, continue [y/n]? y
Switch(config)# include-credentials
```

   Note: If prompted after 'include-credentials' answer yes to both questions.

```
Switch(config)# password manager user-name <platform_username> plaintext
<platform_enable_password>
Switch(config)# console flow-control none
Switch(config)# ip ssh listen oobm
Switch(config)# ip ssh filetransfer
Switch(config)# no tftp client
Switch(config)# no tftp server
Switch(config)# no telnet-server
Switch(config)# end
Switch# write memory
```

4. Switch CLI: Reload the switch and verify configuration

   Reload the switch and verify the configuration from step 3. If a command was not applied, repeat step 3.

```
Switch# reload
```

   If prompted, answer yes.

5. Management Server: Verify netConfig connectivity.

   Perform the following netConfig command to verify netConfig can communicate with the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig getFirmware --device=<switch_name>
Version: Z.14.32
Image: Secondary
```

6. Backup the Configuration

   Perform the *3.1.2.9 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* procedure and then return to this procedure and continue with *3.1.4.7 Step 7* of this procedure.

7. **Restore the Configuration**

   Perform steps 3-8 of the *3.1.2.5 Replace a Failed 4948/4948E/4948E-F Switch (PM&C Installed) (netConfig)* procedure and continue with *3.1.4.7 Step 8* of this procedure.

8. Verify the Configuration

   Once each HP 6120XG has finished booting from the previous step, verify network reachability and configuration.

```
[admusr@localhost ~]$ /bin/ping -w3 <enclosure_switch_IP>
[admusr@localhost ~]$ /usr/bin/ssh
<switch_platform_username>@<enclosure_switch_IP> Switch# show run
```

   Inspect the output of show run, and ensure that it is configured as per site requirements

3.1.4.8 Configuring DSCP Marking Using iptablesADM

Note: DSCP marking set using the QOS procedure *3.1.4.3 Configure QoS (DSCP and/or CoS) on HP 6120XG Switches* may conflict/overwrite marking set using the steps below.

iptableAdm uses a native iptables command with additional TPD driven arguments.

Generic command for DSCP marking:

```
$ sudo /usr/TKLC/plat/bin /iptablesAdm insert --table=mangle --type=rule
--protocol=[ipv4|ipv6] --domain=<domain> --chain=<chain> --match='-p
[tcp|udp|icmp] -j DSCP --set-dscp [DSCP value]' –-location=<number> --persist=yes
```

Where

<table> - For DSCP marking, the table will always = mangle

<domain> - User initiated name for a set of iptables rules. Valid names start with a two-digit number and then an alphanumeric value; such as 25example. NOTE: the domain sets the order of operation.

<match> - This is the native iptables command string.

<chain> - Native iptables set of rules. For the mangle table valid values are: PREROUTING, OUTPUT, FORWARD, INPUT and POSTROUTING.

Example 1

Use this command to mark a locally generated outgoing icmp packet with the value of 18:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm insert --table=mangle --type=rule
--protocol=ipv4 --domain=<domain> --chain=POSTROUTING --match='-p icmp -j DSCP
--set-dscp 18' --location=1 --persist=yes
```

- If no domain has been previously setup this command will create the domain.
- If persist=yes then the rule is placed in /etc/sysconfig/iptables or /etc/sysconfig/ip6tables

The resulting user defined rule can be viewed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm show --type=rule --protocol=ipv4
--table=mangle
```

The resulting user defined rule can be removed with the command:

```
$ sudo /sbin/iptablesAdm delete --table=mangle --type=rule --protocol=ipv4
--domain=<domain> --chain=POSTROUTING --match='-p icmp -j DSCP --set-dscp 18'
```

Note: Either the --match'<native iptables command string>' or the --location=<number> can be used to delete a rule.

Example 2

Use this command to mark an outgoing packet leaving via the ssh port with the DSCP value 12:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm insert --table=mangle --type=rule
--protocol=ipv4 --domain=<domain> --chain=POSTROUTING --match='-p tcp --sport
22 -j DSCP --set-dscp 12' --location=1 --persist=yes
```

The resulting user defined rule can be viewed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm show --type=rule --protocol=ipv4
--table=mangle
```

The resulting user defined rule can be removed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --table=mangle --type=rule
--protocol=ipv4 --domain=<domain> --chain=POSTROUTING --match='-p tcp --sport
22 -j DSCP --set-dscp 12' --location=1 --persist=yes
```

Example 3

Use this command to mark all outbound traffic on the bond1 interface with a DSCP value of 25:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm insert --type=rule --protocol=ipv4
--domain=<domain> --chain=OUTPUT --table=mangle --match='-o bond1 -j DSCP
--set-dscp 25' --location=1 --persist=yes
```

The resulting user defined rule can be viewed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm show --type=rule --protocol=ipv4
--table=mangle
```

The resulting user defined rule can be removed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --type=rule --protocol=ipv4
--domain=<domain> --chain=OUTPUT --table=mangle --match='-o bond1 -j DSCP
--set-dscp 25'
```

3.1.4.9 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.

Prerequisites:

- *3.1.1 Configure netConfig Repository*
- *3.1.3.6 Configure HP 6125XLG Switch (netConfig)*

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> getLinkAggregation

Interface:
  LAG1:
    Active Link State: Up
    Mode: Active
```

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


Interface:
  LAG1:
    Active Link State: Up
    Description: ISL to P3-Switch2
    LAG Interfaces:
      tenGE17: Bundled
      tenGE18: Bundled
      tenGE19: Bundled
      tenGE20: Bundled
    Link State: Up
    Mode: Active
    MTU: 10000
    Type: trunk
    Untagged Vlan: 1
    Vlan Membership: 1-4094
```

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

Interface:
  tenGE1:
    Active Link State: Up
    Description: Ten-GigabitEthernet1/1/5 Interface
    Duplex: full
    Link State: Up
    Media Type: N/A
    MTU: Unknown
    Speed: 1000
```

```
    Type: trunk
    Untagged VLAN: 1
    VLAN Membership: 1-4094
```

3.1.4.10 Configure Speed and Duplex for LAG Ports for Cisco 4948/E/E-F (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.

Prerequisites:

- *3.1.1 Configure netConfig Repository*
- *3.1.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)*
- *3.1.3.6 Configure HP 6125XLG Switch (netConfig)*

1. Virtual PM&C: List configured link aggregation groups on the Cisco 4948/E/E-F. Identify the LAG(s) connected to a 6125XLG enclosure switch. In this example, the switch has 8 link aggregation groups configured, but LAG id 2 is identified to be connected to a 6125XLG by 4x1GE LAG uplink.

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> getLinkAggregation

Interface:
  LAG1:
    Active Link State: Up
    Mode: Active
LAG2:
    Active Link State: Up
    Mode: Active
LAG3:
    Active Link State: Up
    Mode: Active
LAG4:
    Active Link State: Up
    Mode: Active
LAG5:
    Active Link State: Up
    Mode: Active
LAG6:
    Active Link State: Up
    Mode: Active
LAG7:
    Active Link State: Up
    Mode: Active
LAG8:
    Active Link State: Up
    Mode: Active
```

2. Virtual PM&C: Get the list of interfaces configured for the LAG. In the following example, LAG id 2 is inspected, and is shown to include interfaces GE9-12.

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> getLinkAggregation
 id=2
```

```
Interface:
  LAG2:
    Active Link State: Up
    Description: ISL to cxeny(en2)-sw2
    LAG Interfaces:
      GE9: Bundled
      GE10: Bundled
      GE11: Bundled
      GE12: Bundled
    Link State: Up
    Mode: Active
    MTU: 10000
    Type: trunk
    Untagged Vlan: 1
    Vlan Membership: 1-6
```

3. Virtual PM&C: Set the speed to 1000 and duplex to full for all LAG interfaces identified in the previous step. Speed should be set to 1000 Mbps. Duplex should be set 'full'. In this example, speed and duplex are configured on the interfaces highlighted by the previous step, GE9-12.

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> setSwitchport
interface=GE9-12 speed=1000 duplex=full
```

4. Virtual PM&C: Inspect the switch LAG port configurations and verify speed and duplex are set as shown in this example:

```
[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> getSwitchport
interface=GE9-12

Interface:
  GE9:
    Active Link State: Up
    Description: ISL_to_cxeny(en2)-sw2
    Duplex: full
    Link State: Up
    Media Type: N/A
    MTU: Unknown
    Speed: 1000
    Type: trunk
    Untagged VLAN: 1
    VLAN Membership: 1-6
<output for remaining interfaces removed to save space>
```

5. Repeat Steps *3.1.4.10 Step 2* - *3.1.4.10 Step 4* for each LAG id identified in *3.1.4.10 Step 1*.

3.2 Brocade Switch - SwitchConfig Procedures

3.2.1 Configure Brocade Switches

This procedure will configure names, user passwords and NTP settings for Brocade switches and back up the configuration to the management server hosting PM&C.

Prerequisites:

- *3.5.1 Configure Initial OA IP*,
- *3.7.2 Installing TVOE on the Management Server*,
- *3.7.3 TVOE Network Configuration*, and
- *3.7.4 Deploy PM&C Guest*

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. OA shell: Login to the active OA

   Login to 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 BayNumber:  1
 OA Role:       Active
 root@10.240.17.51's password:
```

   If the **`OA Role`** is not **`Active`**, login into the other OA the enclosure system

2. OA shell: Login to the Brocade switch console

   Run the following command to get Brocade switches bay IDs:

```
> show interconnect list

 OA-001F296DB1BB> show interconnect list
 BayInterconnect Type Manufacturer Power Health  UIDManagement  IP
--- ---------------- ------------------- ------- --------- --- -
1 Ethernet      Cisco Systems, Inc.  On    OK      Off 10.240.4.70
2 Ethernet      Cisco Systems, Inc.  On    OK      Off 10.240.4.71
3 Fibre  ChannelBROCADE              On    OK      Off 10.240.4.50
4 Fibre  ChannelBROCADE              On    OK      Off 10.240.5.51
5 [Absent]
6 [Absent]
7 [Absent]
8 [Absent]
Totals: 4 interconnect modules installed, 4 powered on.

# connect interconnect <bay_id_number>

NOTICE: This pass-thru connection to the integrated  I/O
console is provided for convenience and does not supply additional access control.

For security reasons, use the password features of the integrated switch.

Connecting to integrated switch 4 at 9600,N81...
Escape character is '<Ctrl>_' (Control + Shift + Underscore)
Press [Enter] to display the switch console:
```

Press **Enter Enter** (Enter twice) and log in as root user.

```
swd77 console login: root
Password:
Change  passwords for switch default accounts now.
Use Control-C to exit or press 'Enter' key to proceed.
```

Press **Enter** to see the prompt.

3. Brocade switch console : Set root user password

```
swd77:root> passwd root
Changing password for root
Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully
Saving password to stable storage.
Password saved to stable storage successfully.
```

4. Brocade switch console : Set factory user password

```
swd77:root> passwd factory
```

5. Brocade switch console : Set admin user password

```
swd77:root> passwd admin
```

6. Brocade switch console : Set user user password

```
swd77:root> passwd user
```

7. Brocade switch console : Set switch name for the FC switch

   Run the following command, the bay id number is the same as the one used in step 1 to connect:

```
swd77:root> switchName bay<bay_id_number>
Committing configuration...
Done.
```

8. **Brocade switch console :** Set chassis name for the FC switch

   Use the enclosure name used during the OA setup, prepended by alphabetical character. (e.g. c505_05_01)

```
swd77:root> chassisName <chassis_name>
```

   Note: The chassis name must begin with alphabetical character.

9. Brocade switch console : Set NTP server on the FC switch

```
swd77:root> tsclockserver <NTP_server_ip>
Updating Clock Server configuration...done.
Updated with the  NTPservers
```

Check if the change was applied with:

```
swd77:root> tsclockserver
Active  NTPServer       10.250.32.10
Configured  NTPServer List  10.250.32.10
```

10. Brocade switch console : Backup configuration

```
swd77:root> configUpload
Protocol (scp, ftp, local) [ftp]: scp
Server Name or IP Address [host]: <PM&C_ip>
User Name [user]: pmacadmin
File Name [config.txt]: /var/TKLC/smac/backup/<chassis_switch_bay>
Section (all|chassis [all]):
pmacadmin@<ip>‘s password:

configUpload complete: All config parameters are uploaded
```

where **<chassis_switch_bay>** would be **500_05_01_bay3** for instance

11. Brocade switch console : Logout

```
swd77:root> logout
```

Press **control + shift + underscore** and then **D** to logout from FC switch console.

12. Repeat for second Brocade switch

Repeat step 2-11 for the second Brocade switch.

13. OA : Logout

```
> exit
```

3.2.2 Upgrade Brocade Switch Firmware

This procedure will describe how to upgrade firmware for the Brocade switches. The procedure covers either 4/24 or 8/24 Brocade switches.

Prerequisites:

- *3.5.1 Configure Initial OA IP*

Needed material:

- HP MISC firmware ISO image
- *HP Solutions Firmware Upgrade Pack* Upgrade Guide
- *HP Solutions Firmware Upgrade Pack* Release Notes

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

The minimum supported HP Solutions Firmware Upgrade Pack for PMAC 6.3 is release 2.2.10. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the HP Solutions Firmware Upgrade Pack Release Notes for important information on firmware upgrades

and follow the procedures in the HP Solutions Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

3.2.3 Configure Zones in Brocade Switches

This optional procedure should be applied on both Brocade switches that are part of the same enclosure. Zone settings have to be the same for both switches.

Prerequisites:

- *3.2.1 Configure Brocade Switches* has been completed.
- Knowing the network cabling and SAN requirements by blade server is required.

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. General guide

   This procedure is optional. Skipping this procedure will allow switches to connect to all ports.

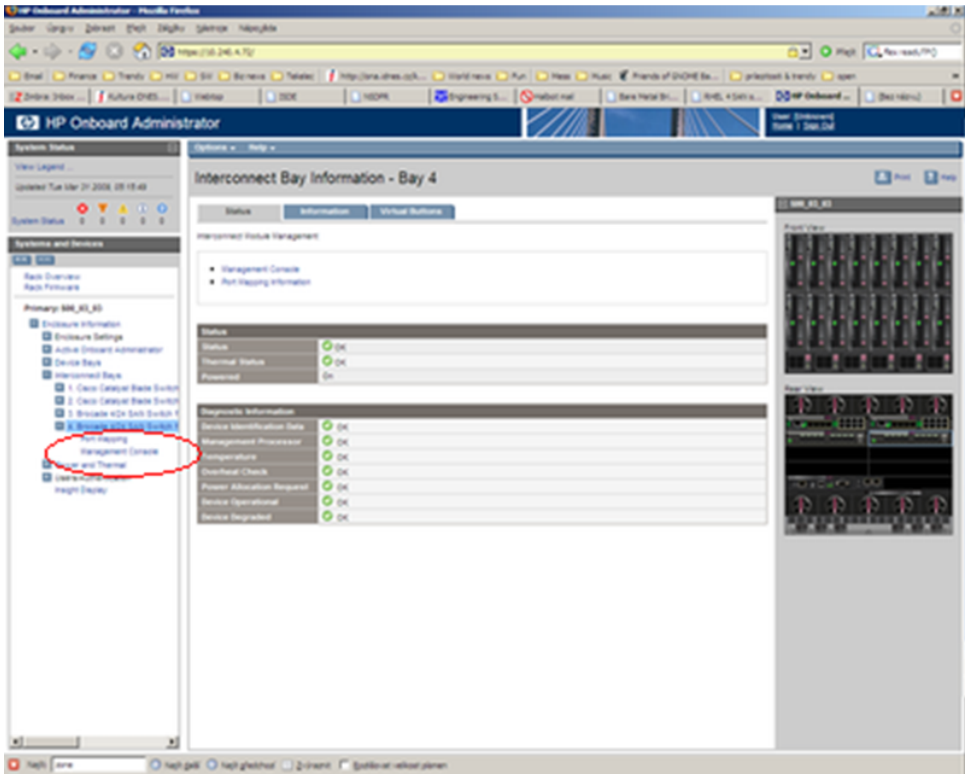
   Note: This procedure should be used with requirements provided by the application. There are general guidelines typically used, but the application documentation is the authoritative source:

   - The rules for the zone configuration: There should be one zone per one storage array in the Fibre Channel Switch
   - Identical zones need to be created in each Brocade in the same enclosure
   - The members of such zone will be all ports from the management storage array and all servers that need access to it.
   - Be sure to create zones for all management storage array controllers. If a Brocade port is not in a zone, then it cannot communicate.
   - After configuring specific zones create another "catch-all" zone that covers the rest of the devices.

2. OA GUI: Log into the Fibre Channel switch

   Log into the OA select the Fibre Channel switch

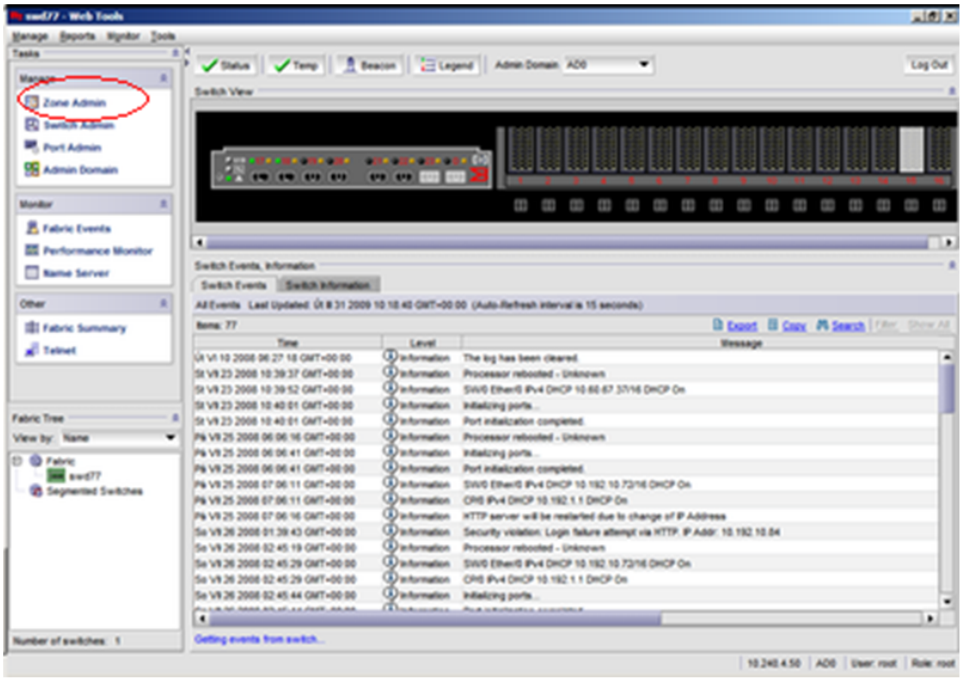
   Select **Enclosure Information** > **Interconnect Bays** > **Brocade ...** > **Management Console**



Fibre Channel console will be loaded. Login as administrative user.

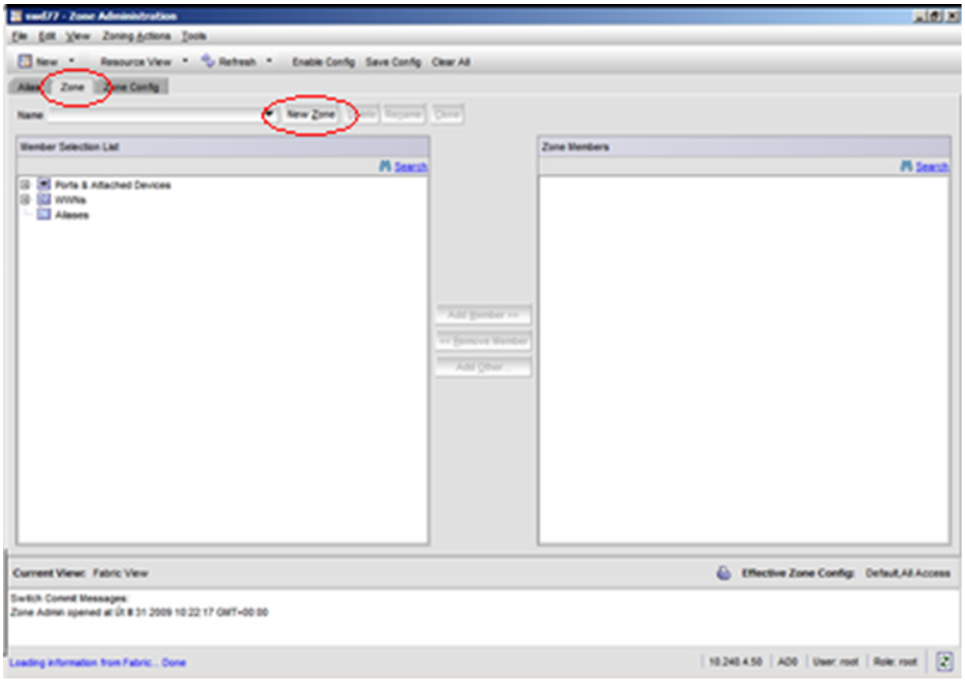
3. Fibre Channel switch console: Navigate to Zone Admin

   Navigate to **Zone Admin.**



4. Fibre Channel switch console: Create new zone

   Select **Zone** tab.



   Click on **New Zone.**

   Type in an appropriate name and click **OK**.

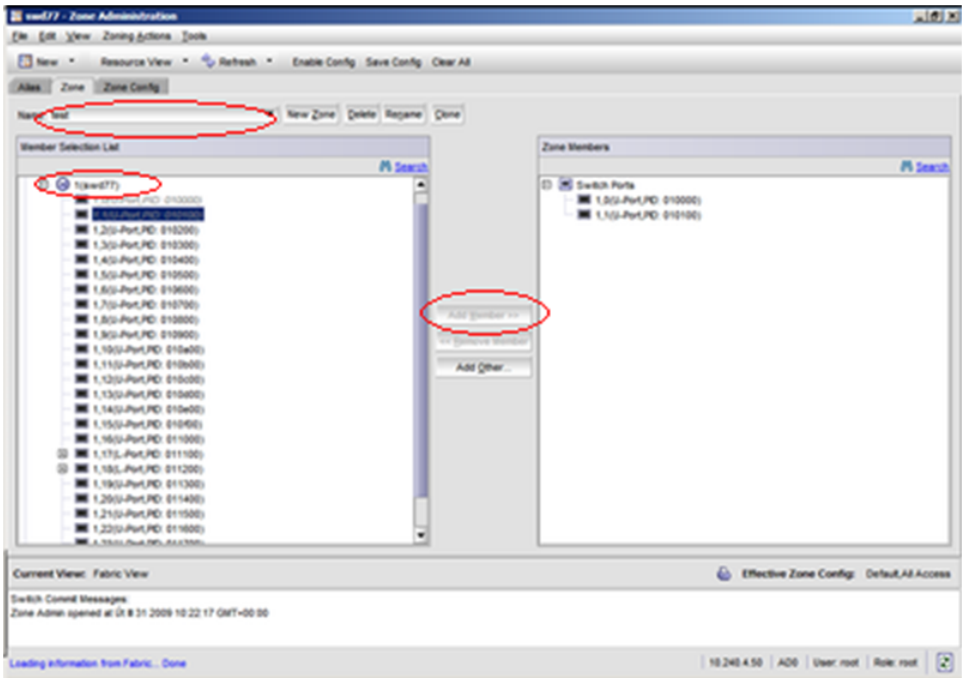
5. Fibre Channel switch console : Add port members into the zone

   In the popup menu choose the zone where ports should be added.

   Expand the **Ports and Attached Devices** twice. Select the appropriate ports under `Ports and Attached Devices`.

   A single Brocade port should be just in a single zone.

   Press the **Add Member** button.

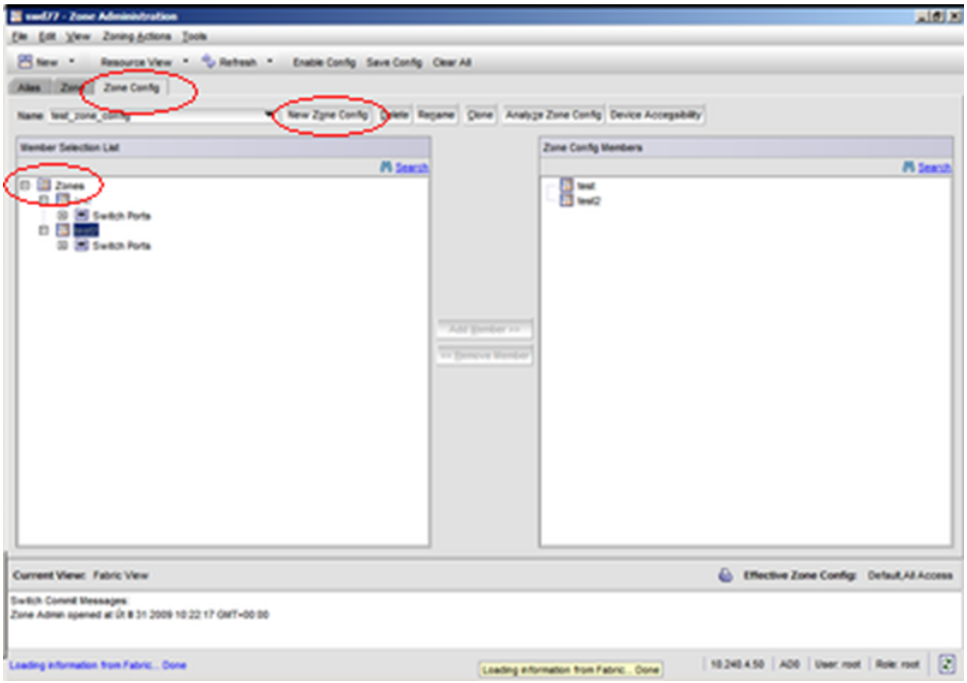


Then create “catch-all“ zone that covers all the remaining devices (blade servers and ports) that are not in the zones specified above.

6. Fibre Channel switch console : Create Zone Config

   Click on the **Zone Config** tab.

   To create a new zone config click on the **New Zone Config** button.

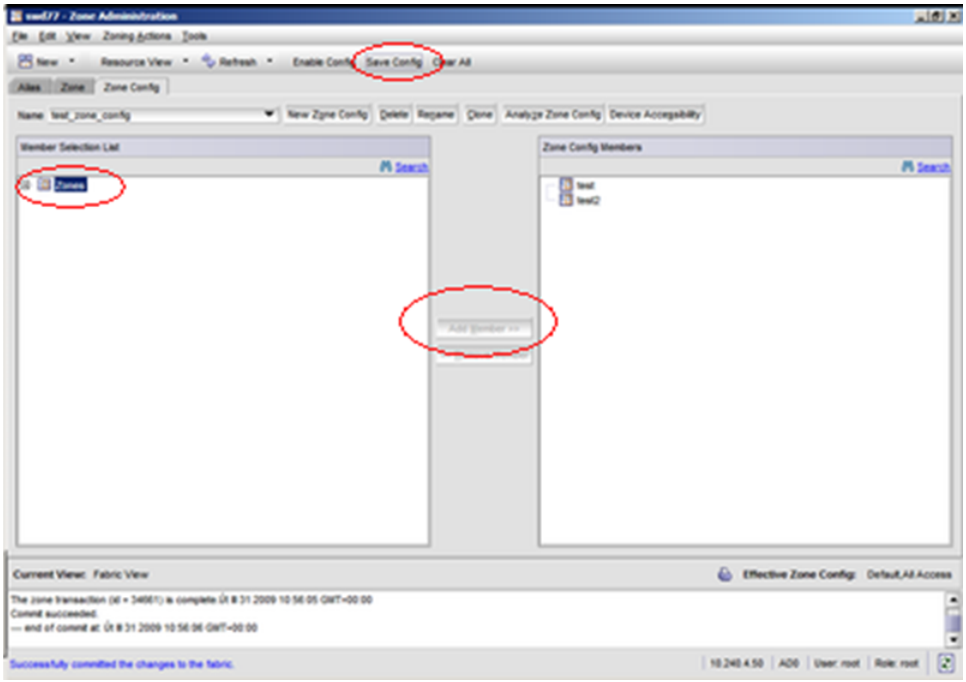


Enter appropriate name such as "Production_Zone_Config" and click **OK**.

7. Fibre Channel switch console : Add Zones into Zone Config

   Expand the **Zones** Selection List.

   Select all desired zones and press **Add Member** button.



   Press **Save Config** and then **Yes**.

   Observe the status at the bottom of the screen. Make sure that the "`Successfully committed the changes to the fabric`" message is displayed in blue at the bottom of the window.

8. Fibre Channel switch console : Enable Zone Config

   Press **Enable Config**

   Use the pull down menu to select the Zone Config to apply.

   Press **OK**

   Press **Yes**

   Observe the status at the bottom of the screen. Make sure `Successfully committed the changes to the fabric` appears in blue at the bottom of the window.

9. Repeat on the second switch

   Repeat steps 2-8 on second switch in the same enclosure. The two switches should have identical configurations.

3.2.4 Configure Brocade Switch SNMP Trap Target

This procedure will configure SNMP settings for Brocade switches.

Prerequisites:

- *3.2.1 Configure Brocade Switches* has been completed.
- Knowing the network cabling and SAN requirements by blade server is required.

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. OA: Login to Brocade switch console

   Login to OA via ssh as root user. Run the following command to get Brocade switches bay IDs:

```
> show interconnect list
OA-001F296DB1BB> show interconnect list
Bay Interconnect Type Manufacturer Power Health UIDManagement IP
--- ----------------- ------------------- ------- --------- --- -
1 Ethernet      Cisco Systems, Inc.  On    OK      Off 10.240.4.70
2 Ethernet      Cisco Systems, Inc.  On    OK      Off 10.240.4.71
3 Fibre Channel BROCADE              On    OK      Off 10.240.4.50
4 Fibre Channel BROCADE              On    OK      Off 10.240.5.51
5 [Absent]
6 [Absent]
7 [Absent]
8 [Absent]
Totals: 4 interconnect modules installed, 4 powered on.
```

   Run:

```
# connect interconnect <bay_id>
```

   This will connect the user to the FC switch console. Press **Enter** twice and log in as admin user.

   Note: The switch will be configured to reject SNMP sets and gets. Only the hosts listed in step 4 will be able to receive traps.

2. Brocade switch console: Set the SNMP parameters to the default values

```
swd77:admin> snmpconfig --default snmpv1
*****
This command will reset the agent's SNMPv1 configuration back to factory default
*****

SNMPv1 community and trap recipient configuration:
 Community 1: Secret C0de (rw)
  No trap recipient configured yet
 Community 2: OrigEquipMfr (rw)
  No trap recipient configured yet
 Community 3: private (rw)
  No trap recipient configured yet
 Community 4: public (ro)
  No trap recipient configured yet
 Community 5: common (ro)
  No trap recipient configured yet
 Community 6: FibreChannel (ro)
  No trap recipient configured yet

*****
Are you sure? (yes, y, no, n): [no] yes
```

3. Brocade switch console: Set security level (to disable SNMP sets and gets)

```
swd77:admin> snmpconfig --set seclevel
```

See output. A prompt for security level will appear:

Select 1 and press **Enter**.

```
Select SNMP GET Security Level
 (0 = No security, 1 = Authentication only, 2 =
Authentication and Privacy, 3 = No Access): (0..3) [0] 1
```

Select 3 and press **Enter**.

```
Select SNMP SET Security Level
 (0 = No security, 1 = Authentication only, 2 =
Authentication and Privacy, 3 = No Access): (3..3) [3] 3
```

Verify settings:

```
swd77:admin> snmpconfig --show seclevel
```

4. Brocade switch console:

Set SNMP trap recipient IP addresses

```
swd77:admin> snmpconfig --set snmpv1
 SNMPcommunity and  traprecipient configuration:
Community (rw): [Secret Code] <new_password_rw>
Trap Recipient's IP address : [0.0.0.0
Community (rw): [OrigEquipMfr] <new_password_rw>
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private] <new_password_rw>
Trap Recipient's  IP address : [0.0.0.0]
Community (ro): [public] <new_password>
Trap Recipient's IP address : [0.0.0.0] <trap_recipient_ip>
Trap recipient Severity level : (0..5) [0] 2
Trap recipient Port : (0..65535) [162]
Community (ro): [common] <new_password>
Trap Recipient's IP address : [0.0.0.0] <trap_recipient_ip>
Trap recipient Severity level : (0..5) [0] 2
Trap recipient Port : (0..65535) [162]
Community (ro): [FibreChannel] <new_password>
Trap Recipient's IP address : [0.0.0.0]
Committing configuration...done.
```

Replace the passwords in the following examples with the appropriate passwords provided by the application. If only one trap recipient is required, set the IP address to 0.0.0.0.:

Verify the settings:

```
swd77:admin> snmpconfig --show snmpv1
```

5. Brocade switch console: Set access control

Set access control to make sure the right hosts get access. If only one trap recipient is required, set the IP address to 0.0.0.0.:

```
swd77:admin> snmpconfig --set accessControl
 SNMPaccess list configuration:
Access host subnet area : [0.0.0.0] <trap_recipient_ip>
Read/Write? (true, t, false, f): [true] f
Access host subnet area : [0.0.0.0] <trap_recipient-ip>
Read/Write? (true, t, false, f): [true] f
Access host subnet area : [0.0.0.0]
Read/Write? (true, t, false, f): [true] f
Access host subnet area : [0.0.0.0]
Read/Write? (true, t, false, f): [false] f
Access host subnet area : [0.0.0.0]
Read/Write? (true, t, false, f): [false] f
Access host subnet area : [0.0.0.0]
Read/Write? (true, t, false, f): [false] f
Committing configuration...done.
```

Verify the settings are correct:

```
swd77:admin> snmpconfig --show accessControl
```

6. Brocade switch console:

   Set system location

   Set the system location so it is clear where the trap originates from:

```
swd77:admin> snmpconfig --set systemGroup
Customizing  MIB-II system variables ...

At each prompt, do one of the following:
o <Return> to accept current value,
o enter the appropriate new value,
o <Control-D> to skip the rest of configuration, or
o <Control-C> to cancel any change.

To correct any input mistake:
<Backspace> erases the previous character,
<Control-U> erases the whole line,
sysDescr: [Fibre Channel Switch.]
sysLocation: [End User Premise.]
<e.g Cab7enclosure1iobay3>
sysContact: [Field Support.]
authTrapsEnabled (true, t, false, f): [true]
Committing configuration...done.
```

   Verify the settings are correct:

```
swd77:admin> snmpconfig --show systemGroup
```

7. Brocade switch console: Log out

```
swd77:aadmin> logout
```

8. Configure settings for the other Brocade switch

   Repeat steps 1 through 7 on the other Brocade switch in the enclosure.

3.3 SAN Storage Arrays Procedures

3.3.1 Set IP on Fibre Channel Disk Controllers

This procedure will set IP address for fibre channel disk controllers.

Note: This procedure needs to be executed only for one of the two controllers.

Needed material:

General:

- Serial access cable that ships with the given controller and laptop running Microsoft Windows with USB port are required for console access.

P2000:

- If setting IP address for P2000, the user may need to install the P2000 MSAUSB driver on the laptop, use the HP MISC firmware ISO image and follow *B.1 P2000 MSA USB Driver Installation*.
- If setting IP address for P2000, the user may need the Release Notes of the HP Solutions Firmware Upgrade Pack [2].

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

Disk array serial console: Configure IP address on Fibre Channel Disk Controller

Connect to the disk array serial console with following settings:

- 115200 bps, 8 data bits, no parity, 1 stop bit, no flow control

Proprietary cable that ships with the controller is required for console access

The user may have to log in using the manage username and the corresponding password. Once at the prompt (#), execute the following commands:

```
# set network-parameters ip <controller_A_IP_address> netmask <netmask> gateway
 <gateway_IP_address> controller a

# set network-parameters ip <controller_B_IP_address> netmask <netmask> gateway
 <gateway_IP_address> controller b
```

To verify the values were entered correctly, run the following command and check the output:

```
# show network-parameters
```

Since the user is currently logged in at the cli, execute the following command at this time to make sure the expansion disk arrays will be identified correctly:

```
# rescan
```

3.3.2 Configuring Fibre Channel Disk Controllers

This procedure will configure security and user settings for fibre channel disk controllers.

Prerequisite: *3.3.1 Set IP on Fibre Channel Disk Controllers* 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)*.

1. Login to the Fibre Channel Disk Controller

   Login to Fibre Channel Disk Controller via ssh as a manage user.

   Output similar to the following will appear:

```
login as: manage
 manage@10.240.5.186's password: <manage_password>
 HPStorageWorks MSA2012fc
System Name: Platform IXP MSA2012fc
System Location: 500.07 U17 Brocade Ports 17 and 18
Version: W420R45

#
```

2. Fibre Channel Disk Controller: Disable http

```
# set protocols http disabled
```

3. Fibre Channel Disk Controller: Disable telnet

```
# set protocols telnet disabled
```

4. Fibre Channel Disk Controller: Disable ftp

```
# set protocols ftp disabled
```

5. Fibre Channel Disk Controller: Delete ftp user

```
# delete user ftp
```

6. Fibre Channel Disk Controller Delete admin user

   Note: This step only required if device is a P2000 G3 array

```
# delete user admin
```

   This account is an additional management account added by HP and is not needed

7. Fibre Channel Disk Controller: Change password for manage account

```
# set password manage
```

   Use the appropriate password provided by the application documentation.

8. Fibre Channel Disk Controller: Change password for monitor account

```
# set password monitor
```

Use the appropriate password provided by the application documentation.

9. Fibre Channel Disk Controller: Set NTP and timezone

```
# set controller-date <month> <day> <hh>:<mm>:<ss> <year> <time-zone> ntp enabled
 ntpaddress <PM&C_management_network_IP>
```

where

month: **jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec**

day: 1-31

hh: 0-23

mm: 0-59

ss: 0-59

year: four-digit number

time-zone: offset from Universal Time (UT) in hours (e.g.: -7)

For example:

```
# set controller-date sep 22 13:45:0 2007 -7 ntp enabled
ntpaddress 69.10.36.3
```

Check the time settings:

```
# show  controller-date
# show ntp-status
```

10. Fibre Channel Disk Controller: Verify settings:

Verify service and security protocols status:

```
# show protocols
```

Verify user settings:

```
# show users
```

11. Fibre Channel Disk Controller: Configure SNMPtrap host

```
# set snmp-parameters enable crit add-trap-host <target_IP>
```

This will enable delivery of critical events to the target destination.

12. Fibre Channel Disk Controller: Logout

Logout from the Fibre Channel Disk Controller console.

```
# exit
```

3.3.3 Configuring Advanced Settings on MSA2012fc Fibre Channel Disk Controllers

This procedure configures advanced settings on each MSA2012fc controller.

Prerequisites:

- *3.3.1 Set IP on Fibre Channel Disk Controllers* and
- *3.3.2 Configuring Fibre Channel Disk Controllers* have been completed.

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)*.

1. Fibre Channel Disk Controller GUI: Login to the Fibre Channel disk controller

   Login to Fibre Channel Disk Controller GUI as a manage user using https:

   ```
   https://<fibre_channel_disk_controller_IP>
   ```

2. Fibre Channel Disk Controller GUI: Navigate to system configuration

   Navigate to **MANAGE** > **GENERAL CONFIG** > **System configuration**

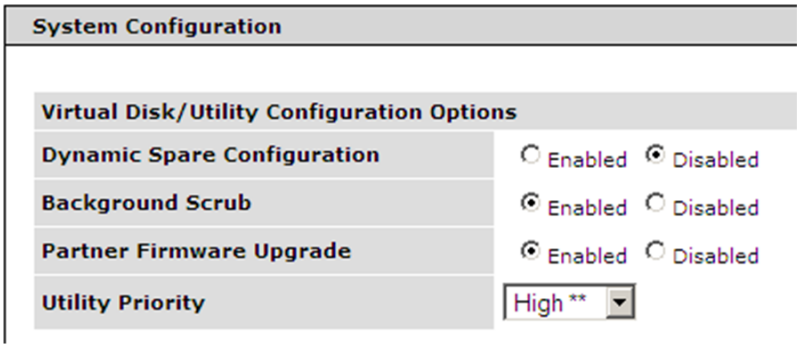
3. **Fibre Channel Disk Controller GUI:** Change advanced settings

   Make sure that:

   `Dynamic Spare Configuration` is disabled

   `Background Scrub` is enabled

   `Partner Firmware` Upgrade is enabled

   Press **Change System Configuration.**

4. Fibre Channel Disk Controller GUI: Verify advanced settings

   Verify that the following message appears above the System Configuration area:

5. **Fibre Channel Disk Controller GUI:** Logout

   Logout by pressing the **LOG OFF** button on the left hand side.

3.3.4 Configuring Advanced Settings on P2000 Fibre Channel Disk Controllers

This procedure configures advanced settings on each P2000 controller.

Prerequisites:

- *3.3.1 Set IP on Fibre Channel Disk Controllers* and
- *3.3.2 Configuring Fibre Channel Disk Controllers* have 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)*.

1. Login to fibre channel disk controller

   Connect to Fibre Channel Disk Controller via ssh as a manage user.

   Output similar to the following will appear:

```
login as: manage
manage@10.240.4.205's password: <manage_password>
 HPStorageWorks  MSAStorage P2000G3  FC/iSCSI
System Name: Uninitialized Name
System Location: Uninitialized Location
Version: L100R010

#
```

2. **Fibre Channel Disk Controller:** Configure advanced settings

```
# set advanced-settings dynamic-spares disabled
Info: Command completed successfully. - Parameter 'dynamic-spares' was set to
'disabled'.
Success: Command completed successfully. - The settings were changed successfully.

# set advanced-settings background-scrub enabled
Info: Command completed successfully. - Parameter
'background-scrub' was set to 'enabled'.
Success: Command completed successfully. - The settings
were changed successfully.

# set advanced-settings partner- firmware-upgrade enabled
Info: Command completed successfully. - Parameter
'partner-firmware-upgrade' was set to 'enabled'.
Success: Command completed successfully. - The settings
were changed successfully.
```

3. Fibre Channel Disk Controller: Verify advanced settings

```
# show advanced-settings
```

4. Fibre Channel Disk Controller: Logout

   Logout from the Fibre Channel Disk Controller console.

```
# exit
```

3.3.5 Upgrade Firmware on MSA 2012fc Disk Controllers

This procedure will upgrade the firmware of the MSA 2012fc disk controllers.

Prerequisites:

- *3.3.3 Configuring Advanced Settings on MSA2012fc Fibre Channel Disk Controllers* has been completed.

Needed material:

- HP MISC firmware ISO image
- *HP Solutions Firmware Upgrade Pack* Upgrade Guide
- *HP Solutions Firmware Upgrade Pack* Release Notes

Note: Only the A controller needs to have the steps in this section executed; B controller will be upgraded automatically after the A controller.

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

The minimum supported HP Solutions Firmware Upgrade Pack for PMAC 6.3 is release 2.2.10. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the HP Solutions Firmware Upgrade Pack Release Notes for important information on firmware upgrades and follow the procedures in the HP Solutions Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

3.3.6 Upgrade Firmware on MSA P2000 Disk Controllers

This procedure will upgrade the firmware of the MSA P2000 disk controllers.

Prerequisites:

- *3.3.4 Configuring Advanced Settings on P2000 Fibre Channel Disk Controllers* has been completed.

Needed material:

- HP MISC firmware ISO image
- *HP Solutions Firmware Upgrade Pack* Upgrade Guide
- *HP Solutions Firmware Upgrade Guide* Release Notes

Note: Only the A controller needs to have the steps in this section executed; the B controller will be upgraded automatically after the A controller. This will also upgrade any I/O modules of P2000 JBOD enclosures cascaded from the P2000 controller being upgraded.

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

The minimum supported HP Solutions Firmware Upgrade Pack for PMAC 6.3 is release 2.2.10. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the HP Solutions Firmware Upgrade Pack Release Notes for important information on firmware upgrades and follow the procedures in the HP Solutions Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

3.3.7 Replacing a Failed Disk in MSA 2012Fc Array

The MSA 2012fc arrays should be configured with spare disks. The designation and the type of spare should always be recorded for future reference.

When a disk fails, the system looks for a dedicated spare first in order to reconstruct the vdisk. If it does not find a properly sized dedicated spare, it looks for a global spare. A properly sized vdisk spare is one whose capacity is equal to or greater than that of the largest disk in the vdisk. A properly sized global spare is one whose capacity is equal to or greater than that of the largest disk in the disk array. Ideally, the disk that failed in the first place should still be physically replaced by a new disk and designated as the dedicated spare or a global spare, the decision depends on what kind of spare was used to reconstruct the vdisk.

If no properly sized spares are available, the vdisk reconstruction does not start automatically. To start reconstruction manually, replace each failed disk by appropriately sized disk and then add each new disk as a dedicated spare.

During the vdisk reconstruction, you can continue to use the vdisk. When a spare replaces a disk in a vdisk, the spare's icon in the enclosure view changes to match the other disks in that vdisk.

The array can indicate that a failure has occurred in several ways:

- SNMPtrap will be sent (if controller is configured to send SNMP traps (it should be)).
- Failed drive will have amber LED illuminated.
- If you log in to the diskcontroller, a pop up will be shown which indicates which disk(s) failed.

Prerequisites:

- *3.3.1 Set IP on Fibre Channel Disk Controllers* and
- *3.3.2 Configuring Fibre Channel Disk Controllers* have been completed.

Note: The vdisk reconstruction can take hours or days to complete, depending on the vdisk RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop reconstruction only by deleting the vdisk.

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. Fibre channel disk controller GUI: Login

   Login to Fibre Channel Disk Controller GUI using https as a manage user.

   ```
   https://<fibre_channel_disk_controller_IP>
   ```

2. Fibre Channel Disk Controller GUI: Clear metadata

   If the replacement disk has been used in another MSA2012fc array, it will have metadata stored on it. This data must be cleared before the disk can be used in the new array. The disks which need their metadata to be cleared will be in a "Leftover" or "L" state.

   Navigate to **MANAGE** > **UTILITIES** > **disk drive utilities** > **clear metadata**.

   Select the disk(s) that are in an "L" state

   Click **Clear Metadata for Selected Disk Drives** button

3. Fibre Channel Disk Controller GUI: Add a global spare disk

If you choose to add a global spare to reconstruct a vdisk, navigate to **MANAGE** > **VIRTUAL DISK CONFIG** . Click on **global spare menu** and then on **add global spares**.

Select the disk that was replaced by clicking the check box on it. It should be the bright green with an "A" on it.

Click the **Add Global Spares** button towards the bottom of the screen.

Verify that the color of the disk changes and a "G" appears on the disk. If there is a problem, new popup will explain the failure. Popups must be allowed for this message to be seen.

4. Fibre Channel Disk Controller GUI: Add a dedicated spare disk

   If you choose to add a dedicated spare to reconstruct a vdisk, navigate to **MANAGE** > **VIRTUAL DISK CONFIG** . Click on **vdisk configuration** and then on **add vdisk spares**

   Select the appropriate vdisk at the top of the page. You should see that the disk that was replaced should be bright green with an "A" ("A" means Available) on it.

   After ensuring the disk is in the correct enclosure, select the disk by clicking the check box on it.

   Click the **Add Vdisk** Spares button towards the bottom of the screen. The disk changes from a state "A" to being the same shade of blue (grey) as the rest of the disks in the enclosure. If there is a problem a popup will explain the failure. Popups must be allowed for this message to be seen.

   Log off of the disk controller by clicking **LOG OFF**.

3.3.8 Replacing a Failed Disk in MSA P2000 Disk Array

The MSA P2000 arrays should be configured with spare disks. The designation and the type of spare should always be recorded for future reference.

When a disk fails, the system looks for a dedicated spare first in order to reconstruct the vdisk. If it does not find a properly sized dedicated spare, it looks for a global spare. A properly sized vdisk spare is one whose capacity is equal to or greater than that of the largest disk in the vdisk. A properly sized global spare is one whose capacity is equal to or greater than that of the largest disk in the disk array. Ideally, the disk that failed in the first place should still be physically replaced by a new disk and designated as the dedicated spare or a global spare, the decision depends on what kind of spare was used to reconstruct the vdisk

If no properly sized spares are available, the vdisk reconstruction does not start automatically. To start reconstruction manually, replace each failed disk by appropriately sized disk and then add each new disk as a dedicated spare.

During the vdisk reconstruction, you can continue to use the vdisk. When a spare replaces a disk in a vdisk, the spare's icon in the enclosure view changes to match the other disks in that vdisk.

The array can indicate that a failure has occurred in several ways:

- SNMPtrap will be sent (if controller is configured to send SNMP traps (it should be)).
- Failed drive will have amber LED illuminated.
- If you log into the diskcontroller, a pop up will be shown which indicates which disk(s) failed.

Prerequisites:

- *3.3.1 Set IP on Fibre Channel Disk Controllers* and
- *3.3.2 Configuring Fibre Channel Disk Controllers* have been completed.

Note: The vdisk reconstruction can take hours or days to complete, depending on the vdisk RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop reconstruction only by deleting the vdisk.

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. Fibre channel disk controller GUI: Login

   Login to Fibre Channel Disk Controller GUI using https as a manage user.

   ```
   https://<fibre_channel_disk_controller_IP>
   ```

2. Fibre Channel Disk Controller GUI: Clear metadata

   If the replacement disk has been used in another P2000 array, it will have metadata stored on it. This data must be cleared before the disk can be used in the new array. The disks which need their metadata to be cleared will be in a **LEFTOVR** state.

   To clear metadata from leftover disks:

   In the **Configuration View** panel, right-click the system and then select **Tools** > **Clear Disk Metadata**.

   In the main panel, select the disk(s) that are in an **LEFTOVR** state

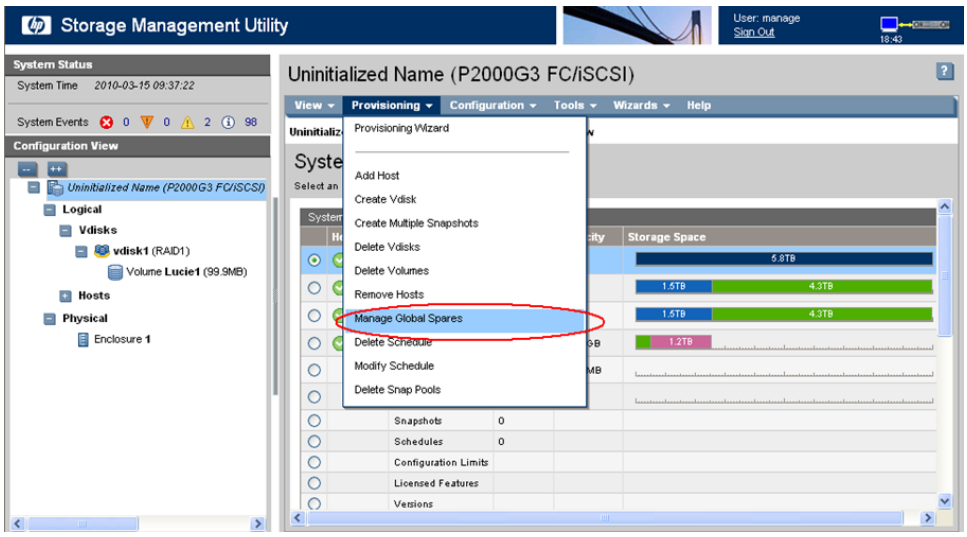
   Click **Clear Metadata**.

   When processing is complete a success dialog appears.

   Click **OK**.

3. Fibre Channel Disk Controller GUI: Add a global spare disk

   If you choose to add a global spare to reconstruct a vdisk, in the **Configuration View** panel, right-click the system . Then in the right hand side blue bar menu click **Provisioning** and select **Manage Global Spares**



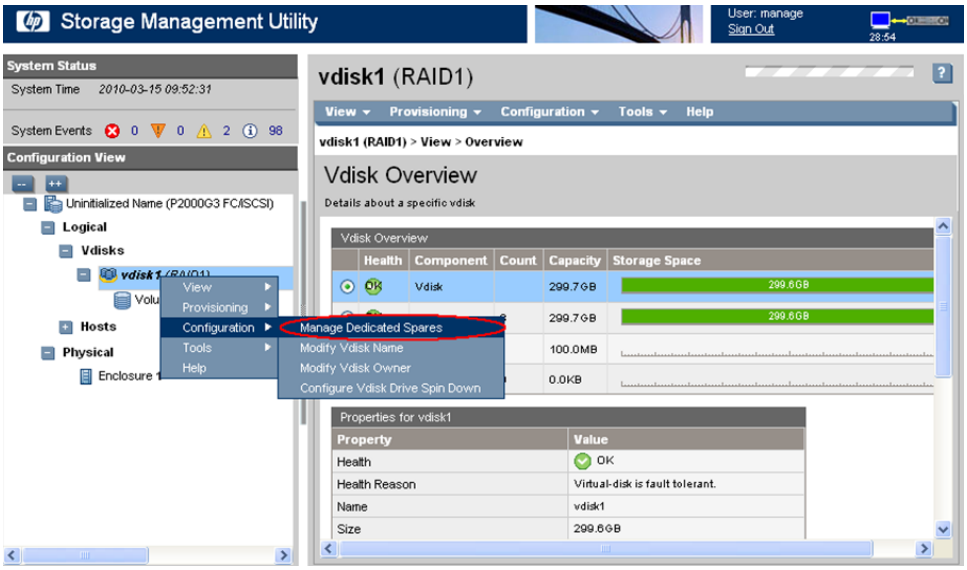
Switch to **Graphical** representation if needed . Select the disk that was replaced by clicking the check box on it. It should be labeled with an **AVAIL** on it.

Click the **Modify Spares** button .

Verify that the color of the disk changes to blue and a **GLOBALSP** appears on the disk. If there is a problem, new popup will explain the failure. Popups must be allowed for this message to be seen.

4. Fibre Channel Disk Controller GUI: Add a dedicated spare disk

If you choose to add a dedicated spare to reconstruct a vdisk, in the **Configuration View** panel, right-click appropriate vdisk and navigate to **Configuration > Manage Dedicated Spares**



Switch to **Graphical** representation if needed . After ensuring the disk is in the correct enclosure, select the replaced disk by clicking the check box on it. It should be labeled with an **AVAIL** on it.

Click the **Modify Spares** button .

Verify that the color of the disk changes to green and SPARE appears on the disk. If there is a problem, new popup will explain the failure. Popups must be allowed for this message to be seen.

Log off of the disk controller by clicking **Log off**.

3.4 Blade Server Procedures

3.4.1 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.

Prerequisites:

- TPD has to have been installed on the server

Needed Materials:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- HP Solutions Firmware Upgrade Pack 2.x.x Upgrade Guide
- Release Notes of the HP Solutions Firmware Upgrade Pack [2]
- USB Flash Drive (4GB or larger and formatted as FAT32) if upgrading with USB 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.

The minimum supported HP Solutions Firmware Upgrade Pack for PMAC 6.3 is release 2.2.10. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the HP Solutions Firmware Upgrade Pack Release Notes for important information on firmware upgrades and follow the procedures in the HP Solutions Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

3.4.2 Confirm/Upgrade Blade Server BIOS Settings

This procedure will provide the steps to confirm and update the BIOS boot order on the blade servers.

Prerequisite: *3.4.1 Upgrade Blade Server Firmware* 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)*.

3.4.2.1 BIOS Settings for HP Systems

For instructions on configuring Gen9 BIOS settings, refer to [1] TPD Initial Product Manufacture Software Installation Procedure, E53017.

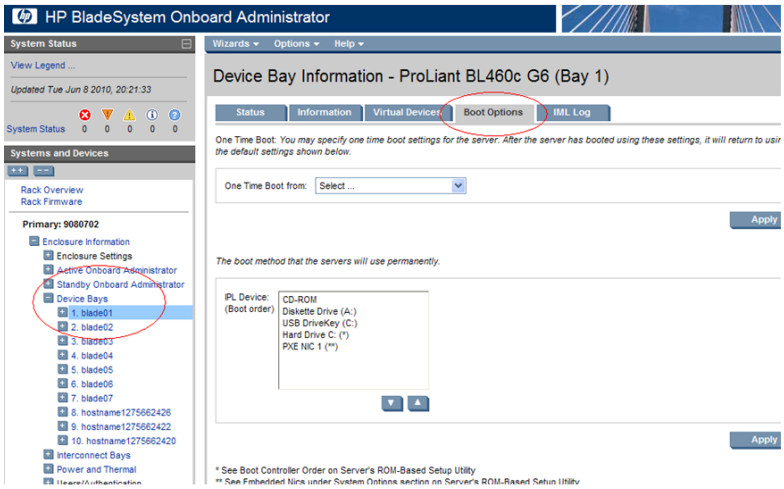
1. OA Web GUI: Login

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

2. OA Web GUI: Navigate to device Bay Settings

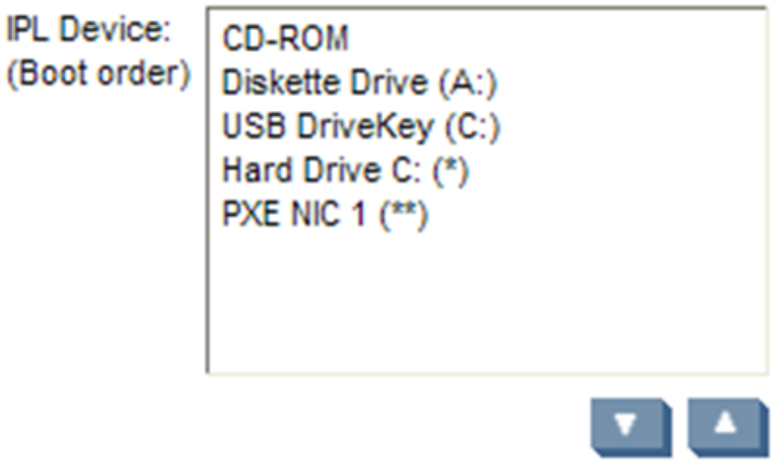
   Navigate to **Enclosure Information** > **Device Bays** > **<Blade 1>**

Click on **Boot Options** tab.



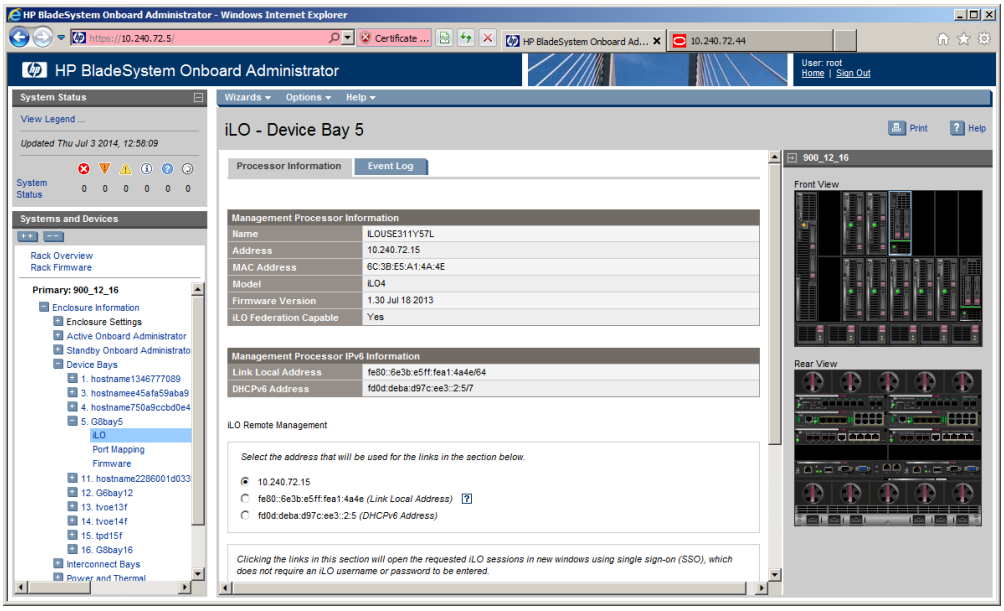
3. OA Web GUI: Verify/update Boot device Order

   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**



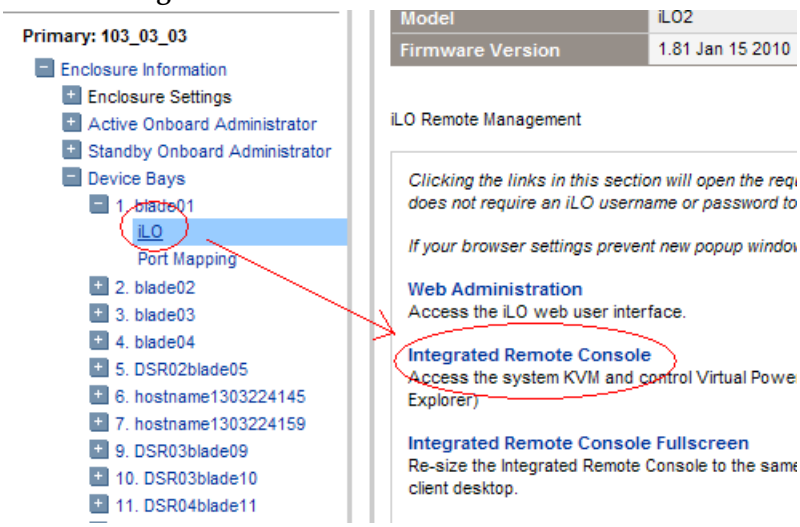
4. OA Web GUI: Access the Blade iLO

a) Navigate to **Enclosure Information** > **Device Bays** > **<[device]>** > **iLO**.



In **iLO Remote Management**, select the address from the radio buttons. If you are presented with the option to select from multiple addresses, choose the appropriate static address.

b) 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.

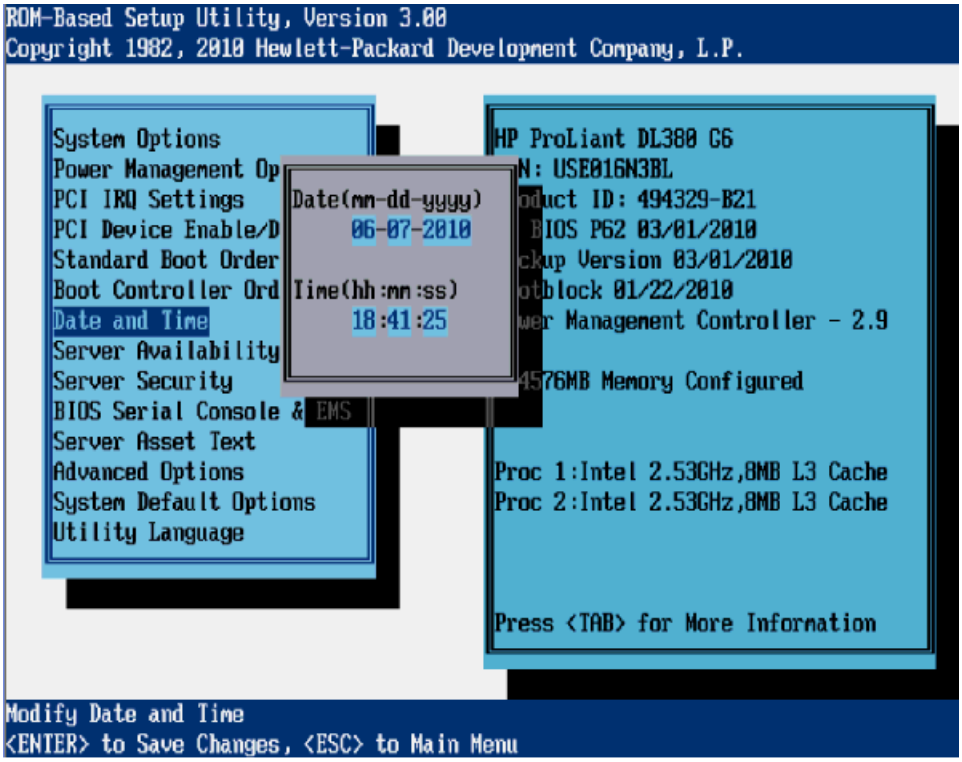
5. Server iLO: Restart the blade and access the BIOS

You might be prompted with a certificate security warning, just press continue.

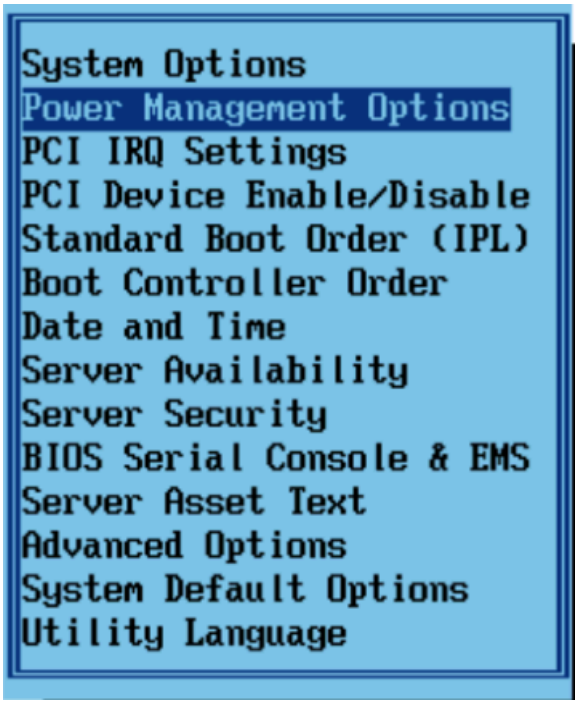
Once a prompt is displayed, login onto the blade using the "admusr" username.

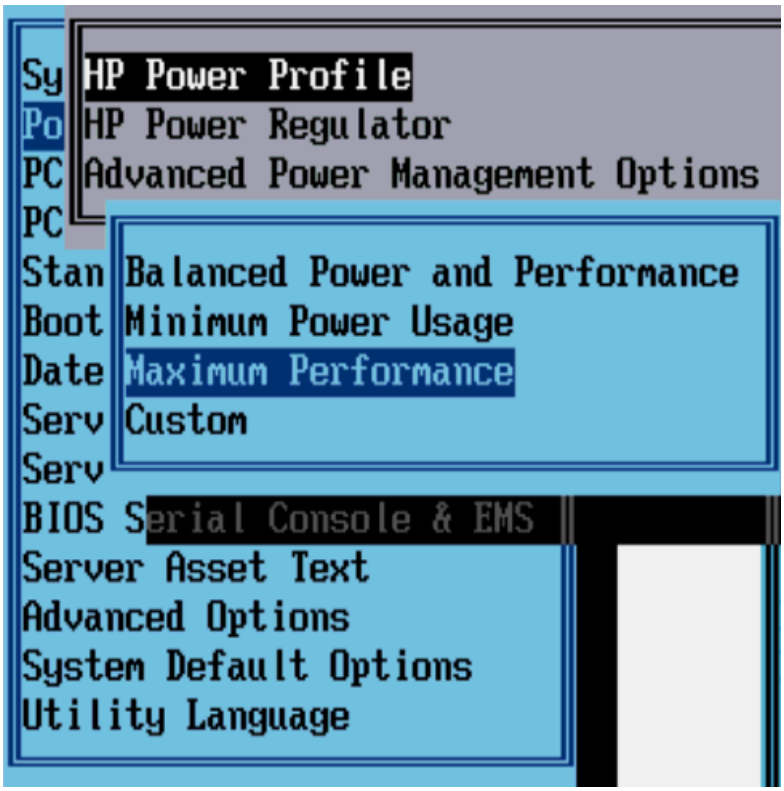
Once logged in, Reboot the server (using the "reboot" command) and after the server is powered on, as soon as you see <F9=Setup> in the lower left corner of the screen, press **F9** to access the BIOS setup screen.

6. Server iLO: 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. **OA Web GUI:** Repeat for the remaining blades

   Repeat Steps 2 through 6 for the remaining blades. Once done, exit out of the OA GUI.

3.4.2.2 BIOS Settings for Oracle Sun Systems

For all TPD supported Oracle servers, the Energy Performance should be set to "Performance", and on the Oracle X4-2 servers, you must set UEFI Configuration Synchronization so that "Synchronization Late" is Disabled. If this step is not performed the server may reboot a second time after POST on some reboots. This can be especially bothersome when trying to do a one-time boot to USB or CD/DVD-ROM.

Note: In the following steps, unless stated otherwise, "X5-2" refers to all versions of the X5-2 server that is supported by TPD. For example the Netra X5-2 Server, Oracle X5-2 Server, Oracle X5-2M Server, etc. Likewise, the same applies for X6-2 servers.

The following steps describe configuring the BIOS Power Management and UEFI setting appropriately.

1. Oracle ILOM: Connect and Login

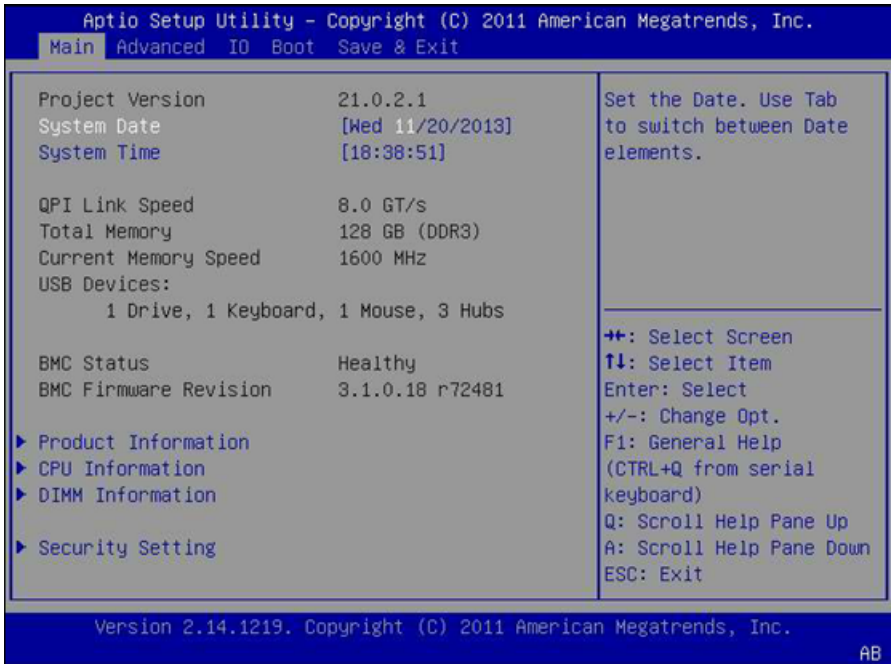
   Connect to the ILOM as described in *F.1 How to Access a Server Console Remotely*. Once connected, login.

2. Oracle ILOM: Reboot and press F2

   Reboot the server using the "reboot" command. After the server is powered on, monitor the middle of the screen for the message <Press F2 to run Setup>. Press F2 to access the BIOS setup screen.

3. Oracle ILOM: Update the date and time

   When the process completes and the BIOS Main menu is presented, the date and current UTC time should be set.



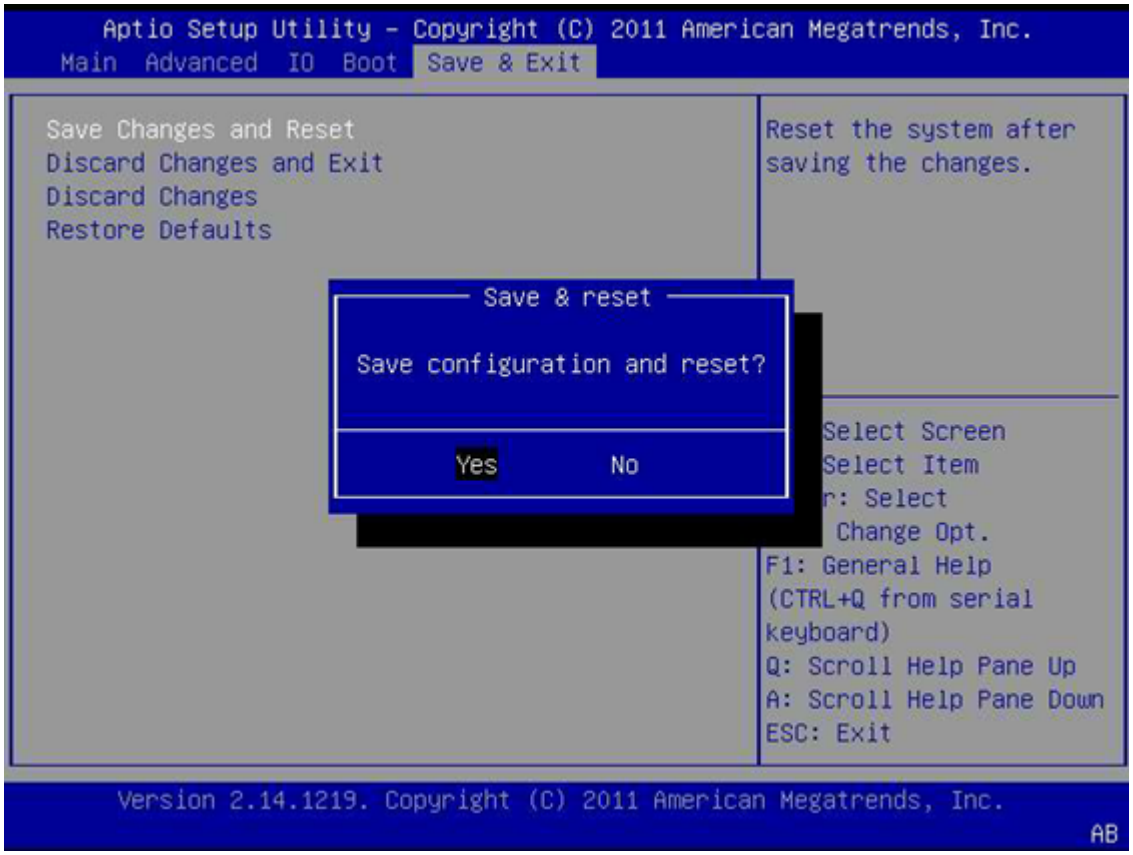
4. Oracle ILOM: Go to the **Advanced** menu.

   Note: If the server is an X5-2 or X6-2, skip this step and proceed with step 6.

5. Oracle ILOM: Select **Processors**.
6. Oracle ILOM: Select **CPU Power Management Configuration**.
7. Oracle ILOM: If the **Energy Performance** field is not set to **[Performance]**, select **Energy Performance** and press <Enter>.

   Note: For X5-2s and X6-2s, set **ENERGY_PERF_BIAS_CFG** mode to **PERF**. Press <Enter> and skip to step 9.

8. Oracle ILOM: In the resulting menu, select the **Performance** option and press <Enter>.
9. Oracle ILOM: Press the <Escape> key once on the X5-2 and X6-2 or two times on all other Oracle systems to return to return to the **Advanced** menu. Unless this is an Oracle X4-2, skip to step 14.
10. Oracle ILOM: Select **UEFI Configuration Synchronization** and press <Enter>.
11. Oracle ILOM: If **Synchronization Late** is not **[Disabled]**, press <Enter> to modify the option.
12. Oracle ILOM: In the resulting menu, select the **Disabled** option and press <Enter>.
13. Oracle ILOM: Press the <Escape> key to return to the **Advanced** menu.
14. Oracle ILOM: Navigate to the **Boot** menu.
15. Under Legacy Boot Option Priority, verify the RAID Adapter is listed first. If not, highlight it and use + key to move it to the top of the list.
16. Oracle ILOM: Select the **Exit** or **Save & Exit** menu, and press <Enter> on **Save Changes and Reset** or **Save Changes and Exit**.
17. Oracle ILOM: Answer **Yes** to the resulting prompt for confirmation.



3.4.3 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.

Prerequisites:

- *3.5.1 Configure Initial OA IP*
- *3.7.2 Installing TVOE on the Management Server*
- *3.7.3 TVOE Network Configuration*
- *3.7.4 Deploy PM&C Guest*

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 only as instructed by the application.

   Note: If using a text editor like VIM, take care to use **sudo** before the command otherwise you may not be able to save the file.

```
<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
```

3.4.4 Accessing the Server Virtual Serial Port

This procedure describes the steps to access iLO or ILOM VSP.

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. For HP Servers:

   Prerequisite: *3.4.3 Configure Blade Server iLO Password for Administrator Account* has been completed.

   a) HP iLO: Access VSP

      This procedure describes the steps how to access iLO or ILOM VSP.

      Log in via SSH to the iLO IP as the Administrator user:

```
# ssh Administrator@<ilo_ip>
Administrator@<ilo_ip>'s password:
User:Administrator logged-in to
ILOUSE8068S2T.nc.tekelec.com(10.250.36.71)
iLO Advanced 1.50 at 17:30:27 INT=4Mar 12 2008
Server Name: localhost.localdomain
Server Power: On

</>hpiLO-> vsp

Starting virtual serial port

Press 'ESC (' to return to the CLI Session
</>hpiLO-> Virtual Serial Port active: IO=0x03F8
```

      Press **Enter** to refresh the screen.

Note: press **ESC(** to escape VSP console.

2. For Oracle Servers:
   a) Oracle ILOM: Log in via SSH as the root user:

```
# ssh root@<ilom_ip>
Password:
Oracle(R) Integrated Lights Out Manager
Version 3.1.0.18 r72481
Copyright (c) 2012, Oracle and/or its affiliates. All rights reserved.
Warning: password is set to factory default
```

   b) Oracle ILOM: Connect to the virtual serial port.

```
-> start /HOST/console/
Are you sure you want to start /HOST/console (y/n)? y

Serial console started. To stop, type ESC (
```

Press **Enter** to refresh the screen.

Note: press **ESC(** to escape VSP console.

3.4.5 Configure Syscheck Default Route Ping Test

This procedure will provide the steps how configure ping test on the blade system

Prerequisite: TPD must be installed on the blade server.

Note: Repeat this test for every bladeserver in the blade system.

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

Blade Server: Configure syscheck default route test

Log in to blade server as admusr.

Enable the syscheck default router test:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net defaultroute -enable
```

Run syscheck to verify that the test is working:

```
$ sudo /usr/TKLC/plat/bin/syscheck -v net defaultroute
Running modules in class net...
OK
LOG LOCATION: /var/TKLC/log/ syscheck/fail_log
```

Restart syscheck:

```
$ sudo /sbin/initctl/syscheck restart
```

Repeat for each blade.

3.4.6 Preparing a System for Extended Power Outage

This procedure describes how to properly shut down a system for an extended period of time, such as in the event of shipment from Manufacturing to the customer site.

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. Power down all blade servers

   Refer to instructions provided by the application to correctly power down all blade servers.

2. Verify each server has shutdown
3. Fibre channel controller shell: Shutdown fibre channel switch

   Login via SSH into one controller in each MSA as the manage user.

   Run:

```
# shutdown both
```

4. Power down disk arrays

   Power down disk arrays using power switches on each array.

5. Management servers: Power off

   Login to each management server via SSH as admusr.

   Run:

```
$ sudo /sbin/shutdown -h now
```

6. Power off aggregation switches

   If the aggregation switches are provided by Oracle, power off the 4948/4948E switches.

   If the aggregation switches are provided by the customer, request that the customer follow their policies for preparing devices for an extended power outage.

3.4.7 Bringing Up a System After Extended Power Outage

This procedure describes the steps to properly power up the HP blade system.

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. Power on device cabinet

   Power on the cabinets that house the devices.

2. Power on aggregation switches

   If the aggregation switches are provided by Oracle, power on the 4948/4948E switches.

3. Power on management server

Turn on the management server by depressing the power button on the front of the server.

4. Power on disk arrays

   Turn power switches "on" on all disk arrays.

5. Power on remaining cabinets

   Power on remaining cabinets.

   Ensure all power supply LEDs are green on all equipment.

6. Power on blade servers

   Power up each blade server.

3.5 C7000 Enclosure Procedures

3.5.1 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.

Prerequisite: Onboard Administrator must be present in the OA Bay 1 location.

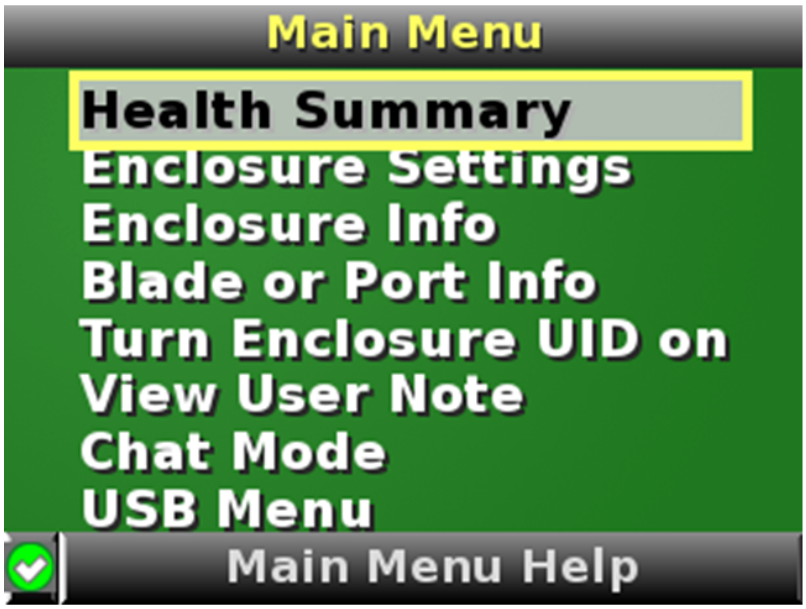
Note: The enclosure should be provisioned with two Onboard Administrators. This procedure needs to be executed only for OABay 1, regardless of the number of OA's installed in the enclosure.

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. If not already disabled, set the DHCPv6 option to **Disabled**.
      3. If not already disabled, set the SLAAC option to **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.

3.5.2 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.

Prerequisites:

- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E switches need to be configured using *3.1.2.1 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.
- In addition, the procedure *3.5.1 Configure Initial OA IP* must be completed.
- If there is any doubt whether the aggregation switches are provided by Oracle or the customer, contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* and ask for assistance.
- Both OAs are installed.

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 *3.5.8 Replacing Onboard Administrator* to learn how to correctly replace one of the Onboard Administrators.

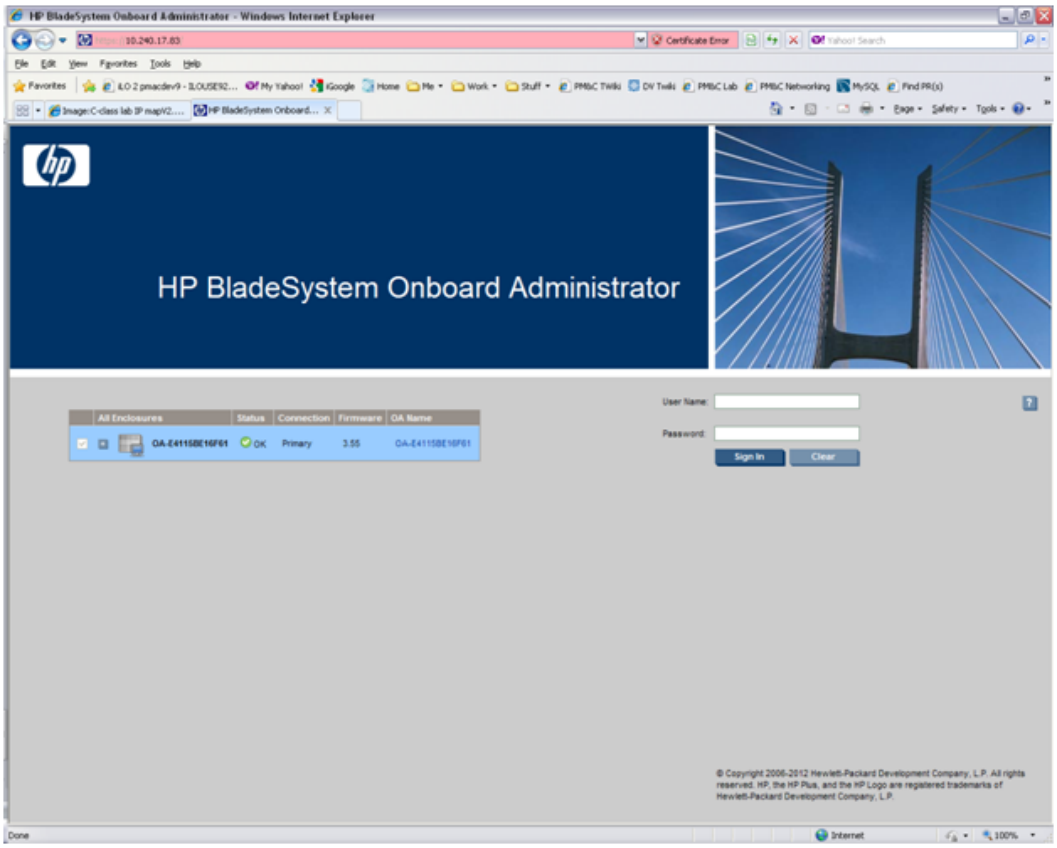
Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. OAGUI: Login

Open your web browser and navigate to the OA Bay1 IP address assigned in *3.5.1 Configure Initial OA IP*.

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

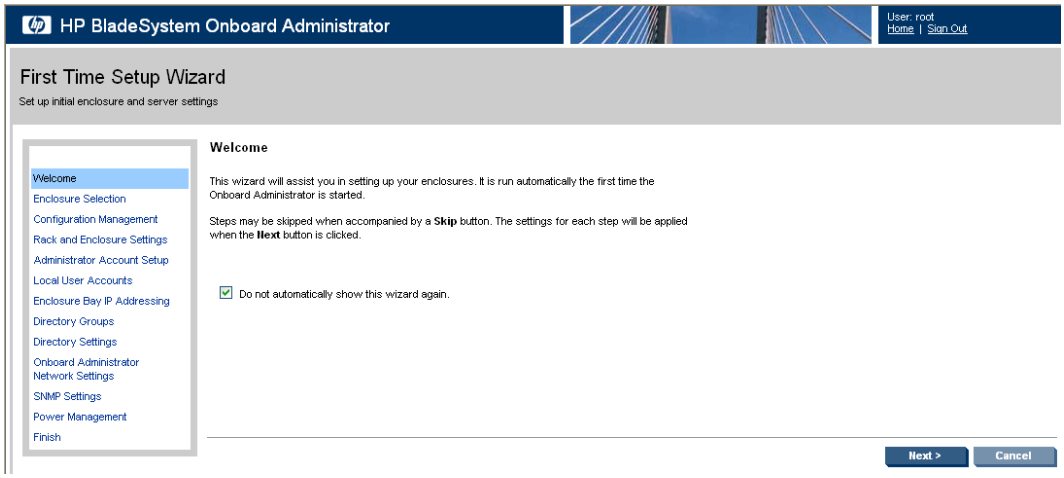
You will see the following:



Log in as an administrative user. The original password is on a paper card attached to each OA.

2. Run First Time Setup wizard

   You will see the main wizard window:

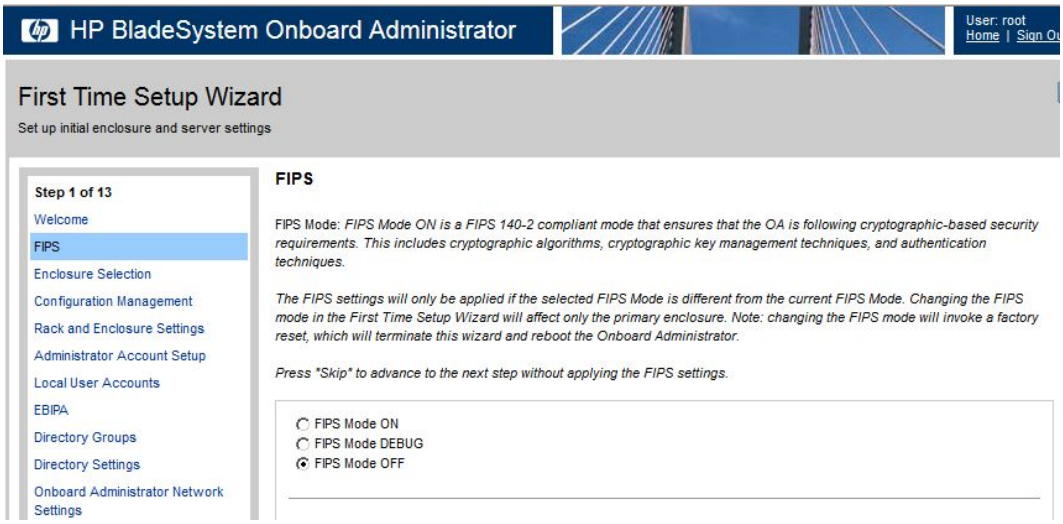


Note: If needed, navigate to **Wizards** > **First Time Setup** to get to the screen above.

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

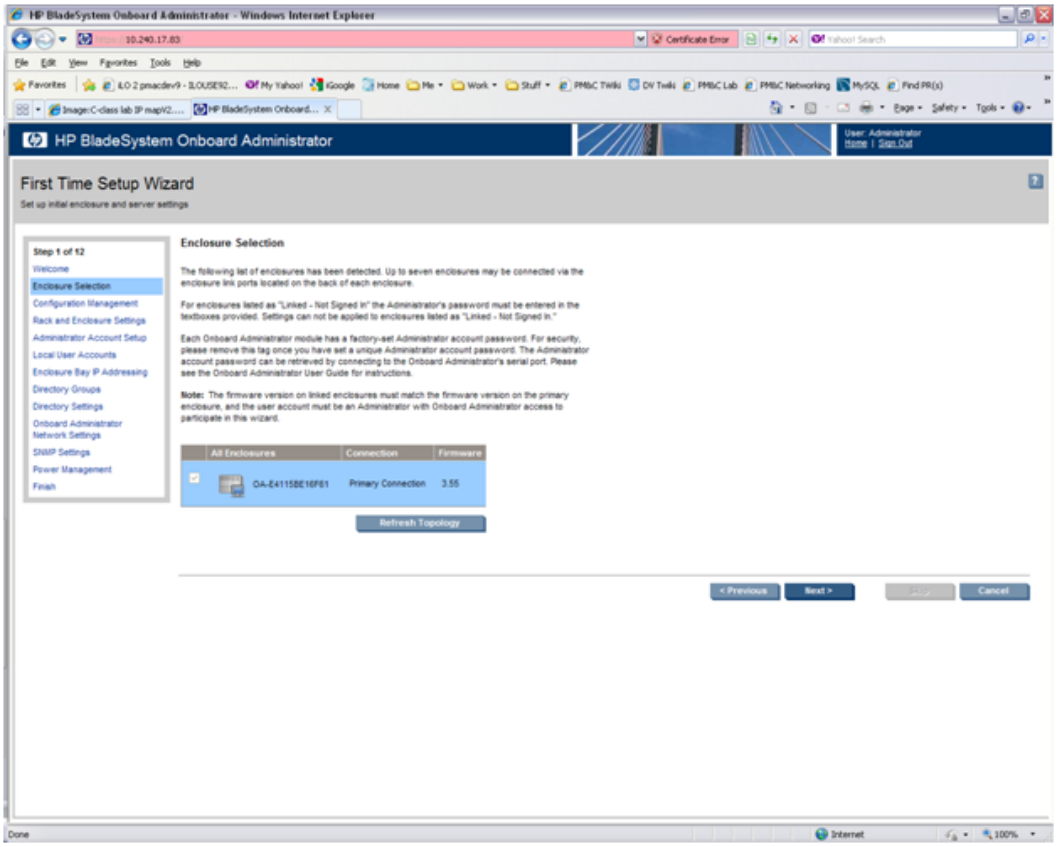
You will see **Rack and Enclosure Settings**:

3. OAGUI: FIPS
   Click on **Next**. FIPS mode is not currently supported.



4. OAGUI: Select enclosure

   Choose enclosure:



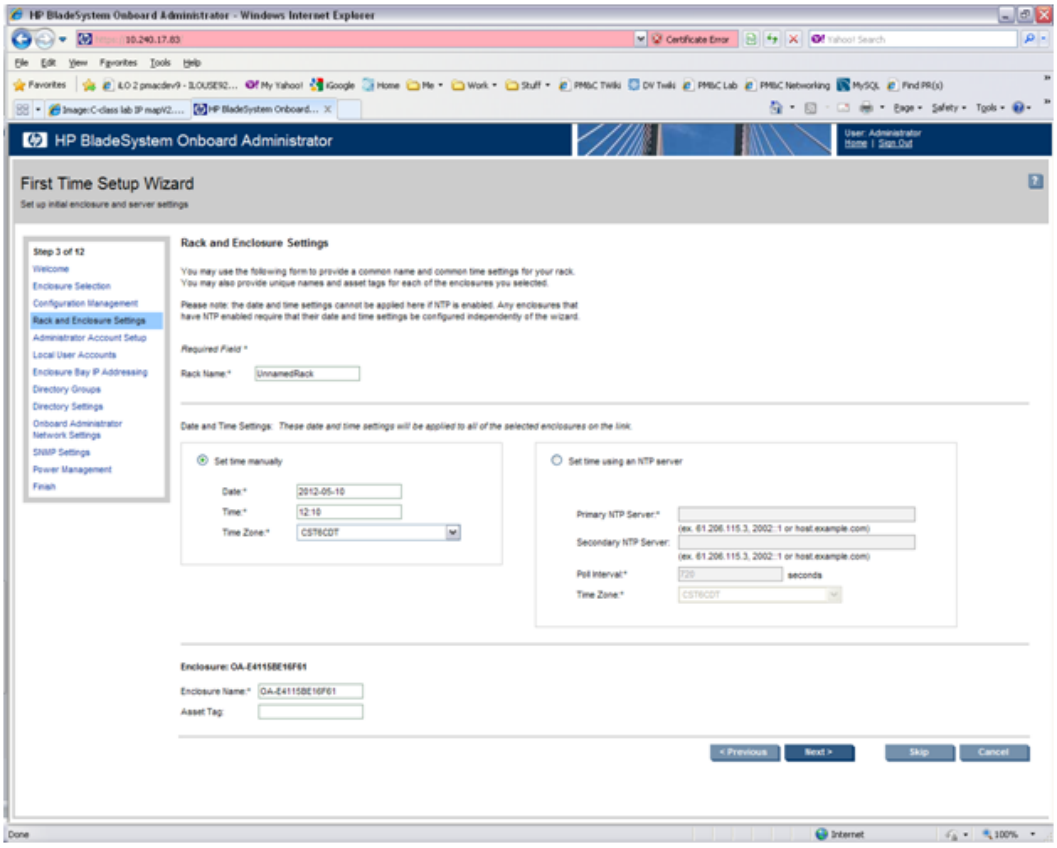
   Click on **Next**.

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>).

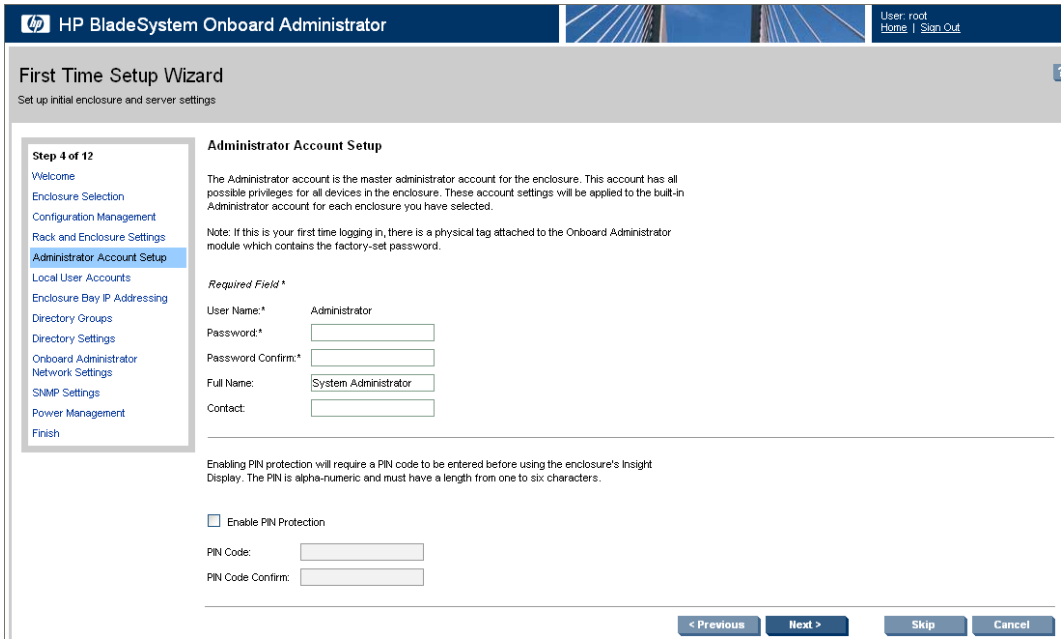
   Set **Poll interval** to **720**.

   Set **Time Zone** to UTC if the 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 **Next**.

8. OAGUI: Create pmacadmin and admusr user.

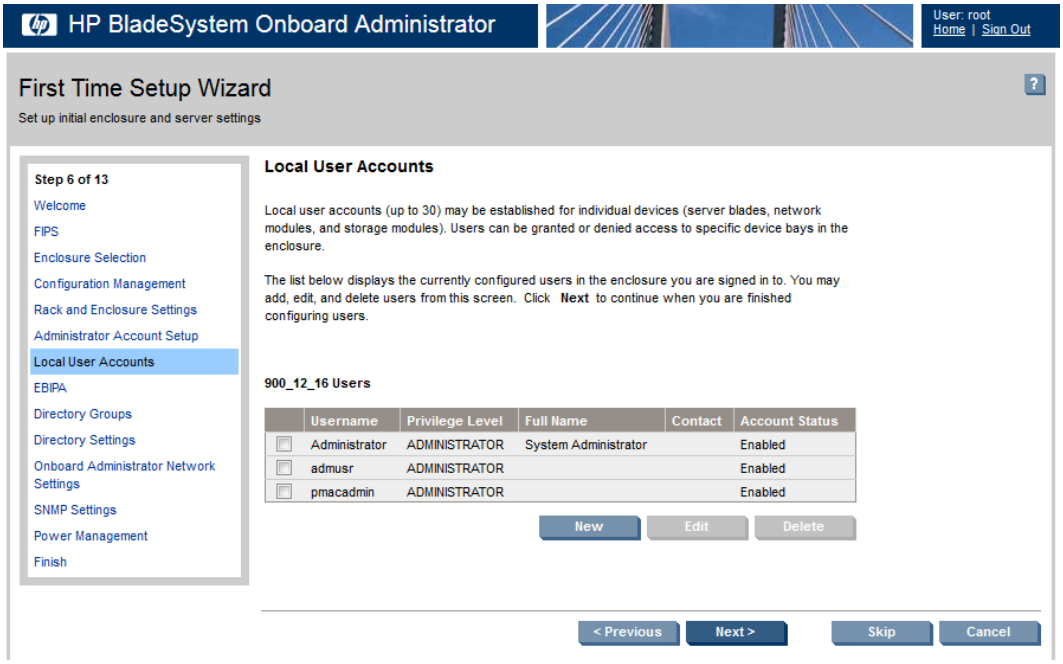
   On the **`Local User Accounts`** screen click on **New** to add **`pmacadmin`** user.

   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.

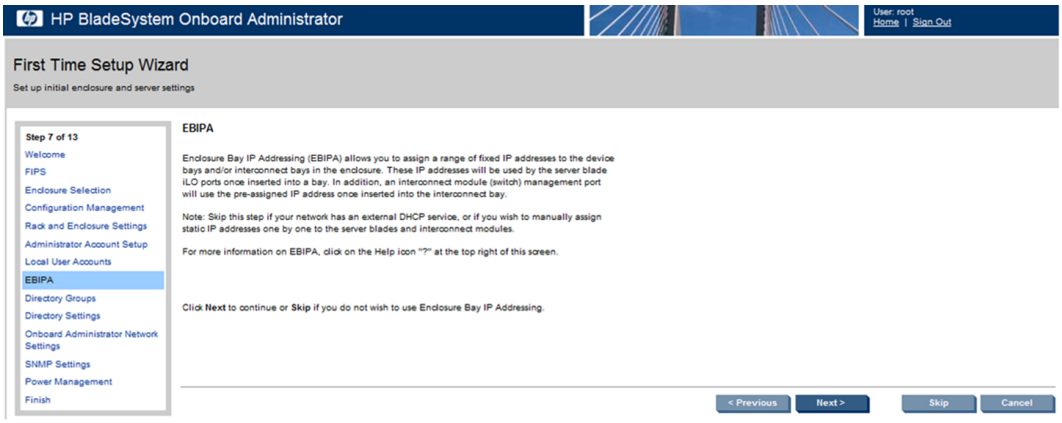


Then click **Next**.

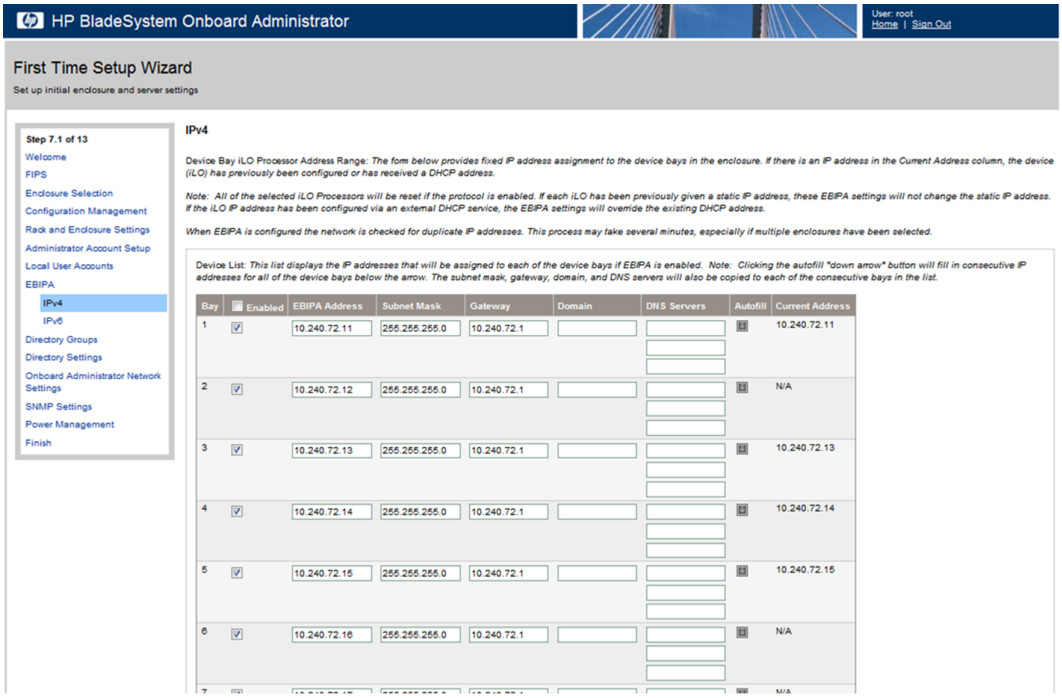
9. OAGUI: EBIPA settings

   a) On the **EBIPA Settings** (Enclosure Bay IP Addressing) screen, click **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.

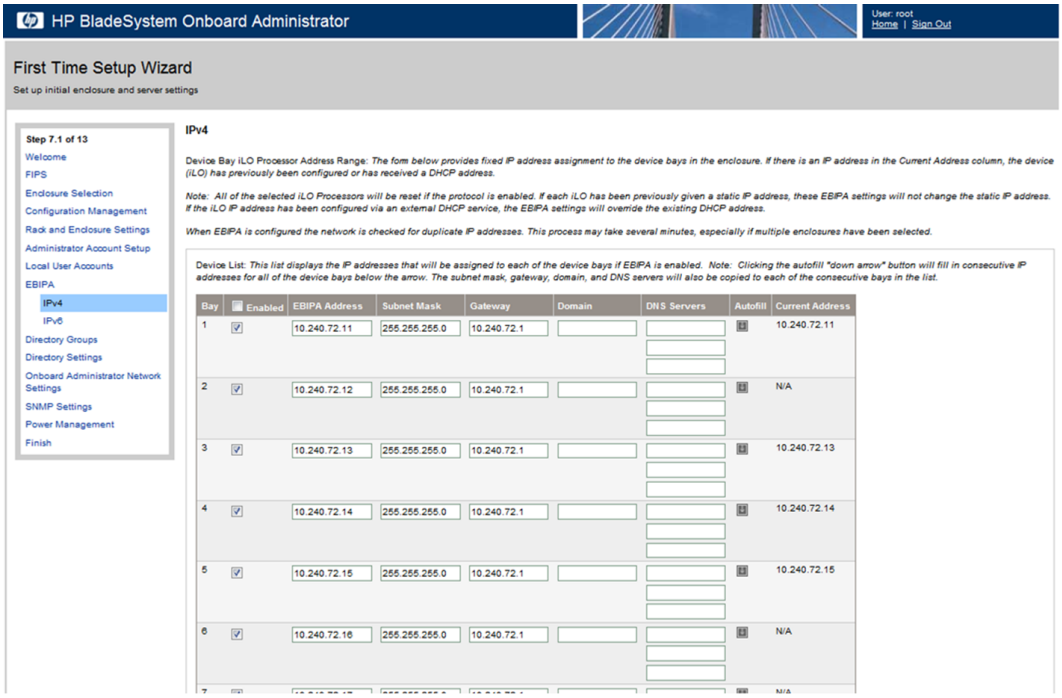
   Note: Bays 1A-16A and 1B-16B are used for double-density blades (i.e., BL2x220c) which are not supported in this release.

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.

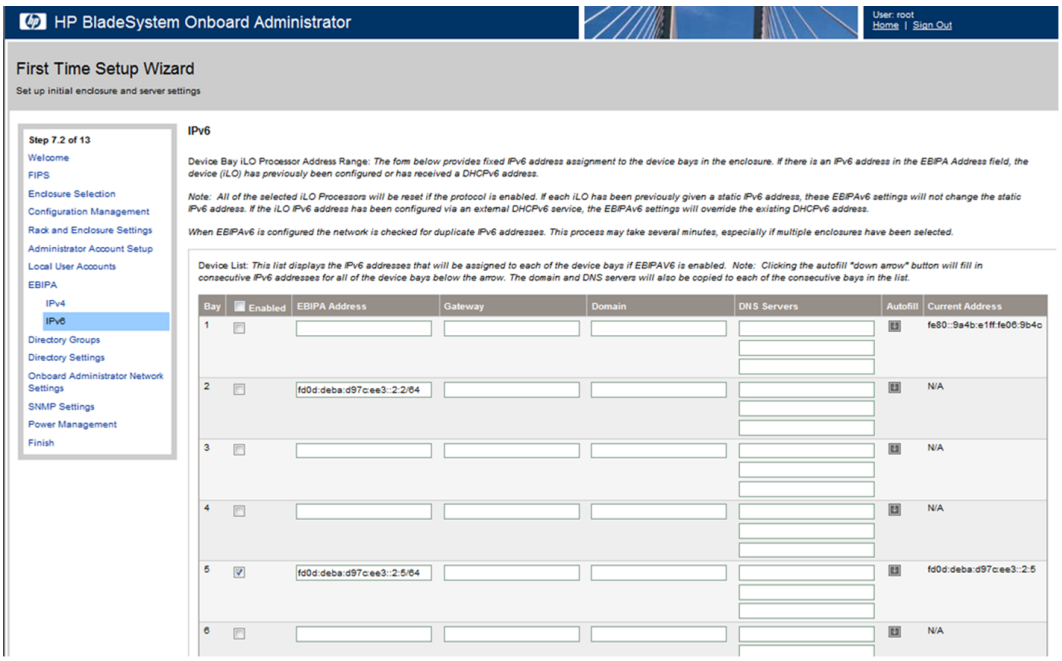
   Note: Do not use autofill as this will fill the entries for the Device Bays 1A through 16B.

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.

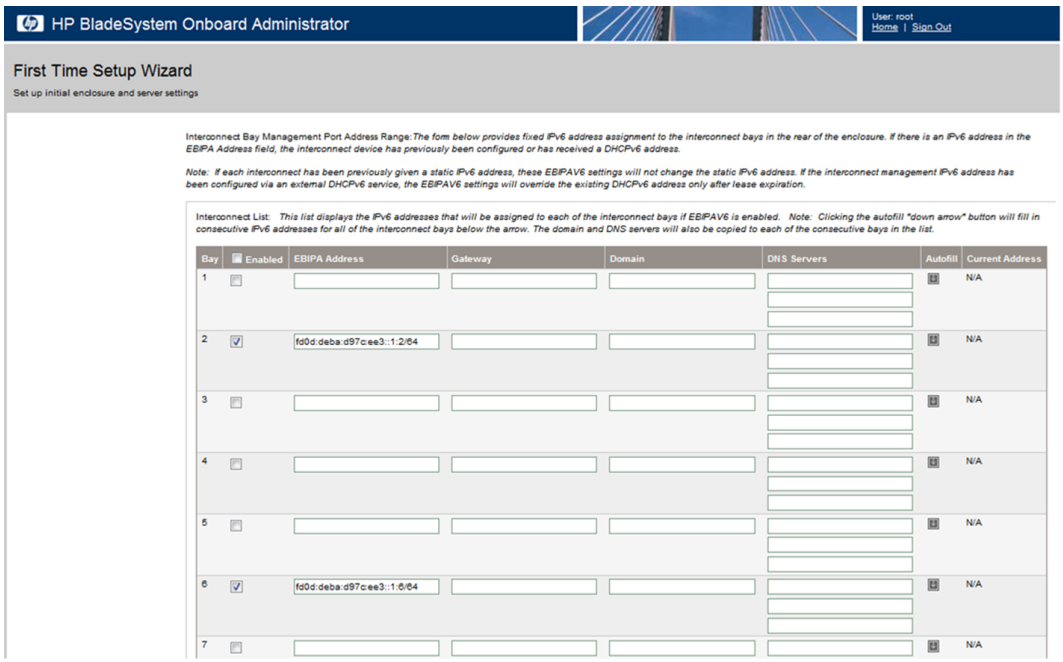
   Note: Bays 1A-16A and 1B-16B are used for double-density blades (i.e. BL2x220c) which are not supported in this release.

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**.

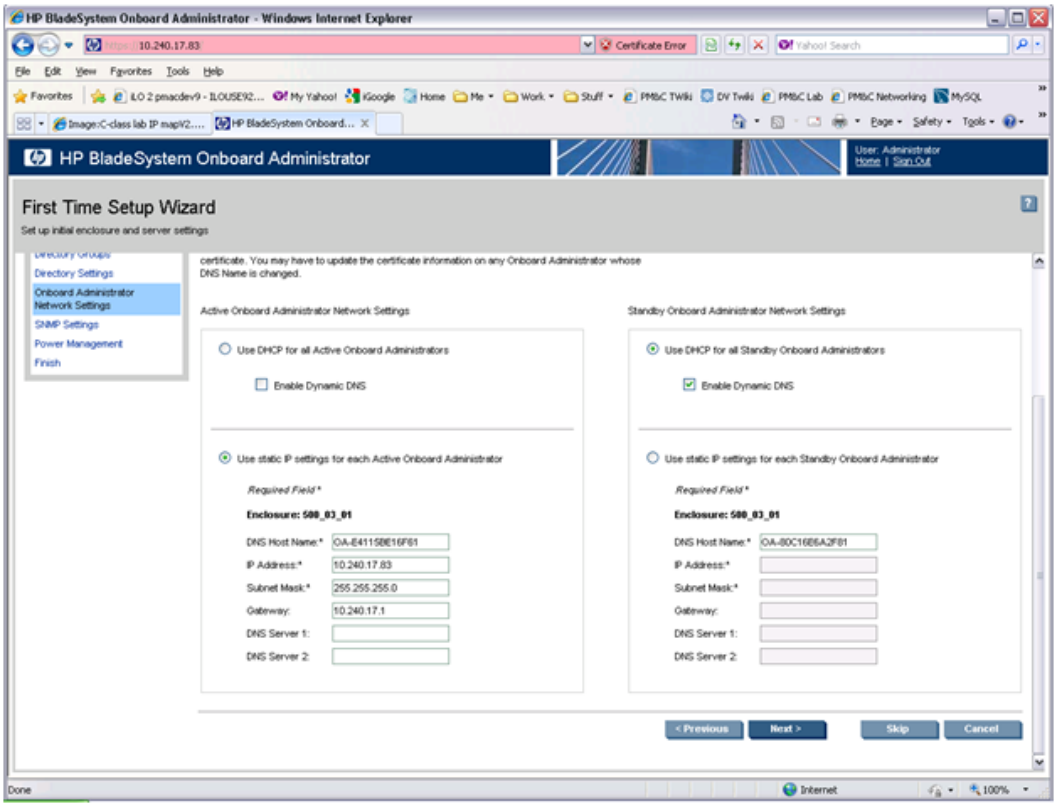
11. OAGUI: Skip Directory Settings step

    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.

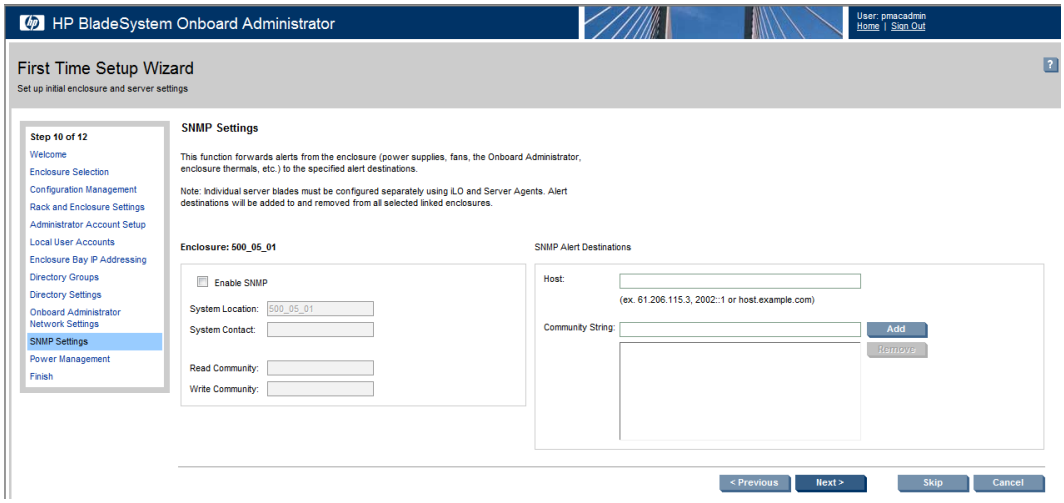


Click on **Next**.

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 *K.1 Disabling SNMP on the OA*.

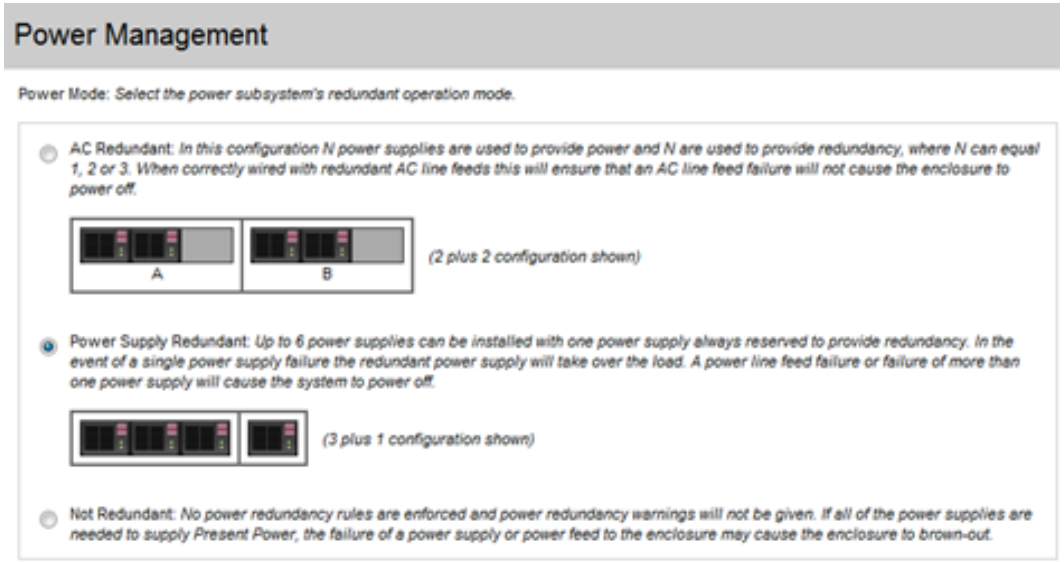


Note: This step does not set an SNMP Trap Destination. To set an SNMP Trap Destination, see *3.5.11 Add SNMP Trap Destination on OA*.

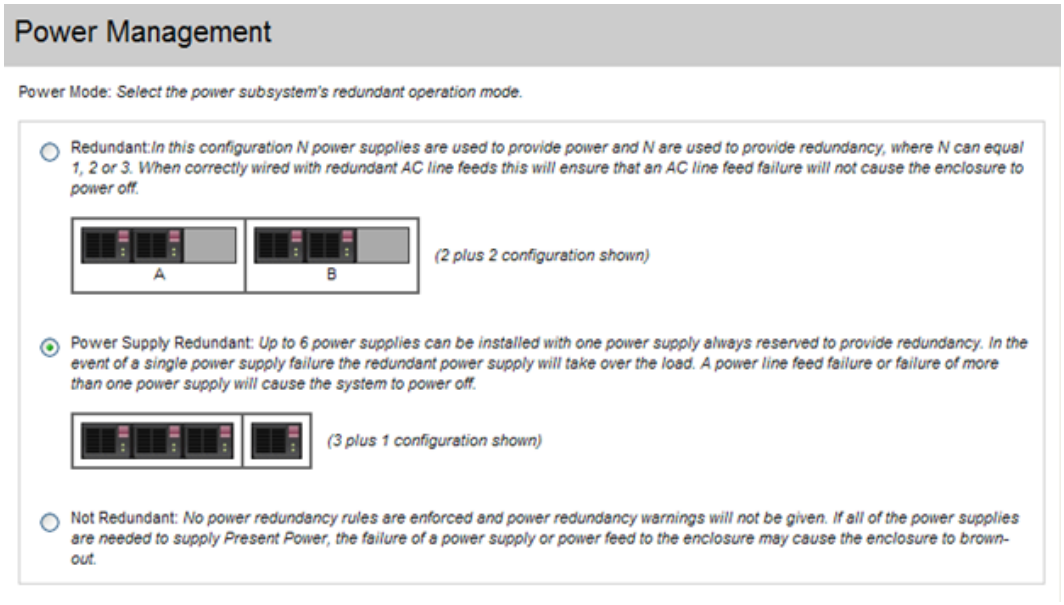
14. OA GUI: Power Management

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 **Power Supply Redundant** radio button.

AC-powered Enclosures:



DC-powered Enclosures:



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

Click on **Next**.

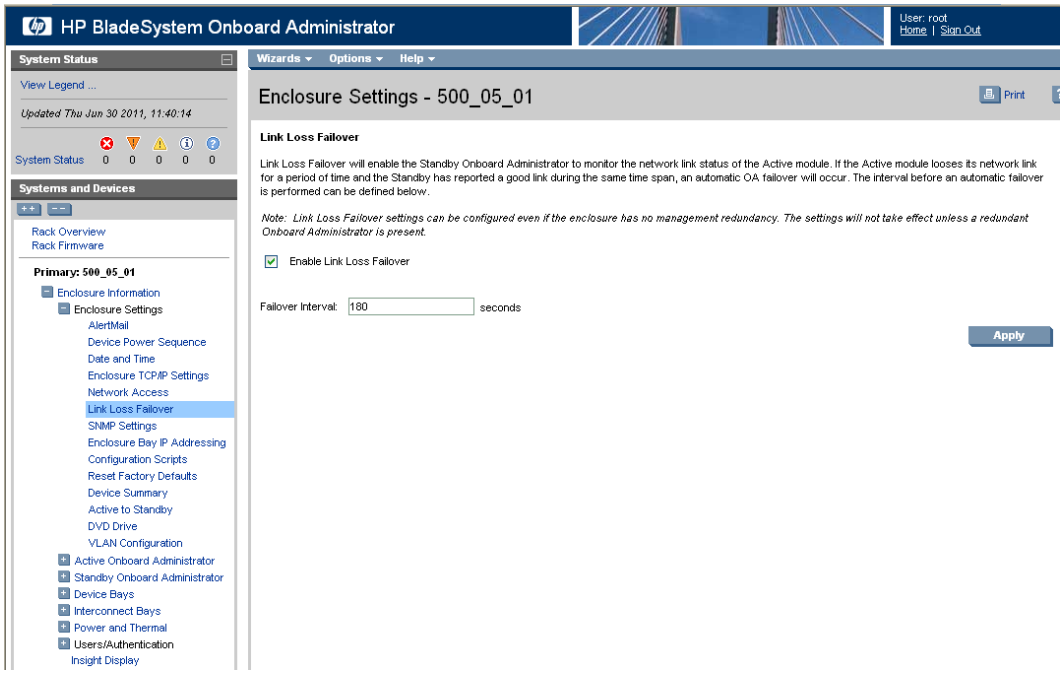
15. OAGUI: Finish First Time Setup Wizard

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** box and specify **`Failover Interval`** to be **`180`** seconds.

Click **Apply**.

3.5.3 Configure OA Security

This procedure will disable telnet access to OA.

Prerequisite: *3.5.2 Configure Initial OA Settings Using the Configuration Wizard* has been completed.

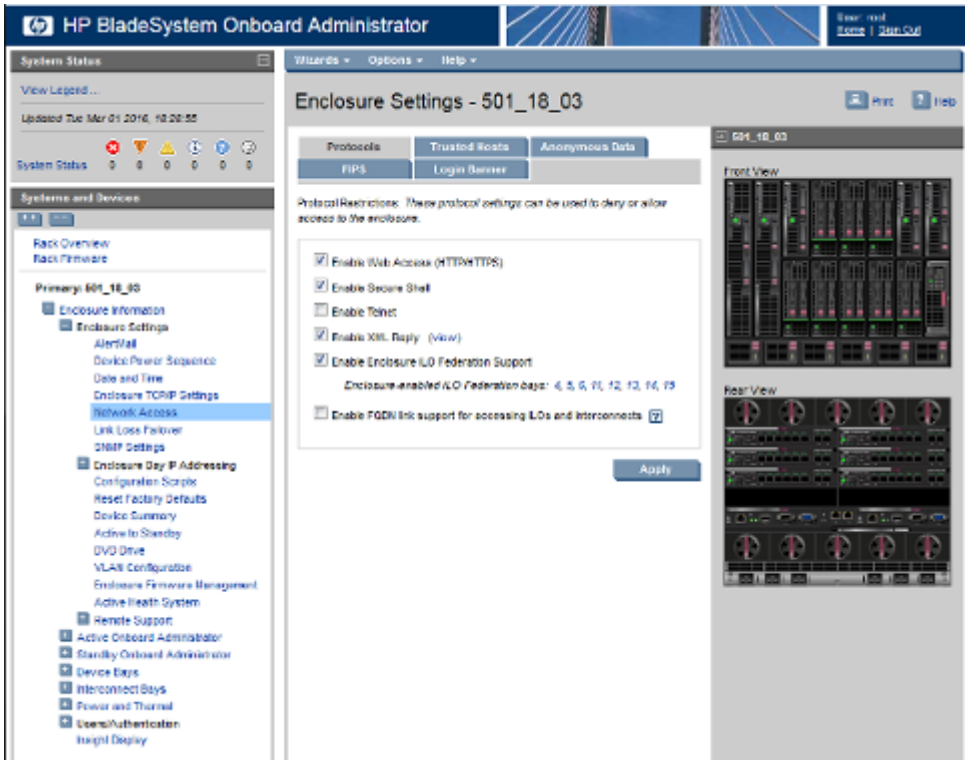
Note: If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

1. Active OAGUI: Login

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

2. OA GUI: Disable telnet

   Navigate to **Enclosure Information** > **Enclosure Settings** > **Network Access**. Uncheck the **`Enable Telnet`** checkbox.



3. OA GUI: Apply changes by clicking **Apply**.

3.5.4 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.

Prerequisites:

- Obtain any customer approval needed for OA firmware updates. This procedure can change the version of firmware installed in one or both OAs.

Needed material:

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

The minimum supported *HP Solutions Firmware Upgrade Pack* for PMAC 6.3 is release 2.2.10. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the *HP Solutions Firmware Upgrade Pack* Release Notes [2] for important information on firmware upgrades and follow the procedures in the *HP Solutions Firmware Upgrade Pack* Upgrade Guide [2] to upgrade the firmware. Software centric customers should refer to *HP Solutions Firmware Upgrade Pack* Software Centric Release Notes [3].

3.5.5 Store OA Configuration on Management Server

This procedure will backup OA settings on the management server.

Prerequisites:

- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E switches need to be configured using *3.1.2.1 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.
- In addition, *3.5.2 Configure Initial OA Settings Using the Configuration Wizard*,
- *3.7.2 Installing TVOE on the Management Server*,
- *3.7.3 TVOE Network Configuration*, and
- *3.7.4 Deploy PM&C Guest*

- 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.

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.

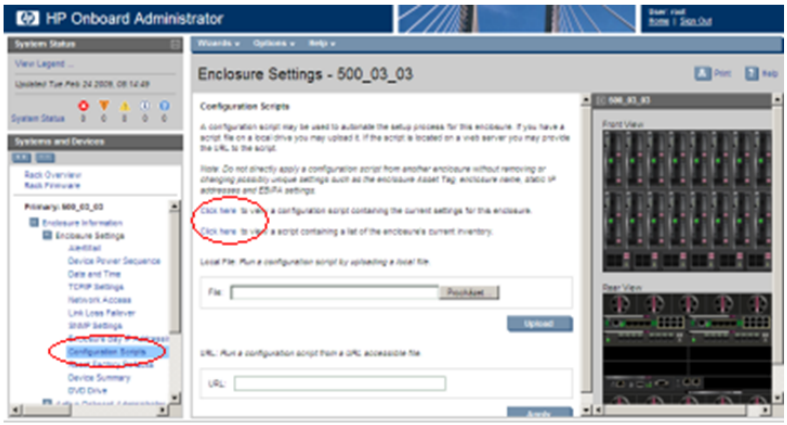
1. OA GUI: Login

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

2. OA GUI: 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
$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/OA_backups/OABackup
$ sudo /bin/chown pmacd:pmacbackup /usr/TKLC/smac/etc/OA_backups
$ sudo /bin/chown pmacd:pmacbackup /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 *A.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 /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. OA GUI: Log out

   Log out from the OA by pressing **Sign Out** at the top-right corner.

3.5.6 Restore OA Configuration from Management Server

This procedure will restore configuration backup from the management server and apply it on the OA's.

Prerequisites:

- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E switches need to be configured using *3.1.2.1 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.
- *3.5.2 Configure Initial OA Settings Using the Configuration Wizard*
- *3.7.2 Installing TVOE on the Management Server*
- *3.7.3 TVOE Network Configuration*
- *3.7.4 Deploy PM&C Guest*

It is assumed that:

- *3.5.5 Store OA Configuration on Management Server* has been performed in the past.
- *3.5.1 Configure Initial OA IP* has been completed prior to this procedure.

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.

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. Obtain configuration files

   Obtain configuration files from the management server :

   a) Log in to the PM&C server as the user admusr.

   b) Copy the OA backup file to the home directory of admusr:

```
$ sudo cp /usr/TKLC/smac/etc/OA_backups/OABackup/<backup_config_filename>
/home/admusr
```

   c) Make the file readable by admusr:

```
$ sudo chown admusr /home/admusr/<backup_config_filename>
$ sudo chmod 400 /home/admusr/<backup_config_filename>
```

   d) From the PC, use scp or WinSCP to copy the file from admusr@<PM&C IP>:/home/admusr/<backup_config_filename>

Unix Users:

```
$ scp
admusr@<pmac_management_network_ip>:/usr/TKLC/smac/etc/OA_backups/OABackup/<backup_config_filename>
 .
```

Windows Users: Refer to *A.1 Using WinSCP* to copy the file to your PC.

e) On the PM&C, remove the file copied above:

```
$ sudo rm /home/admusr/<backup_config_filename>
```

f) Log out of the PM&C server.

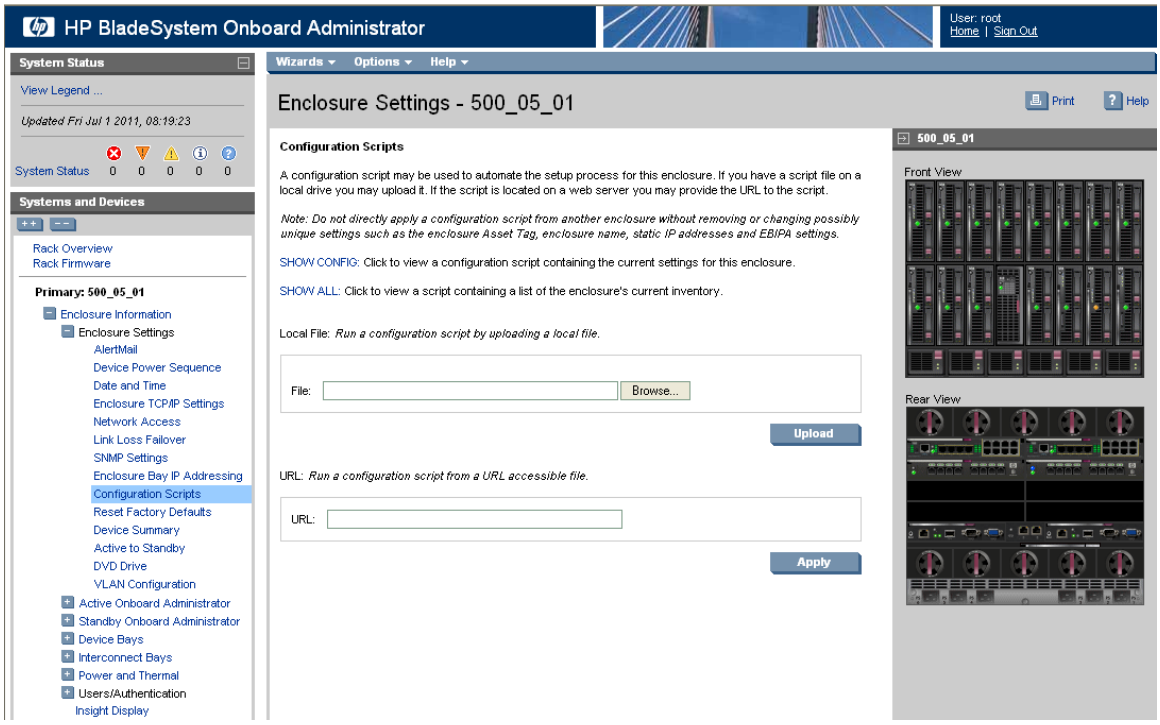
2. OA GUI: Login

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

3. OA GUI: Restore configuration

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

   Use **Local file** form to upload and run configuration script:



The restore can take up to 5-10 minutes.

A pop up appears after the restore is complete. This will contain logs from the restoration process. Check if there are any errors.

Note: If both OAs were reset to factory defaults and had to be restored from the configuration file, the configured user's passwords must be manually reset to their original values. Specifically, the pmacadmin user password so the PMAC and the OAs can communicate. See *3.5.2 Step 8*.

4. OA GUI: Log out

   Log out from the OA by pressing **Sign Out** at the top-right corner.

3.5.7 Adding a redundant Onboard Administrator to enclosure

This procedure has become obsolete with Platform 5.0.

3.5.8 Replacing Onboard Administrator

This procedure describes how to replace OA in an enclosure with Redundant OA.

Prerequisites:

- Obtain any customer approval needed for OA firmware updates. This procedure can change the version of firmware that is installed in one or both OAs.
- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E switches need to be configured using *3.1.2.1 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.
- In addition, *3.5.3 Configure OA Security* must be completed.
- 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.

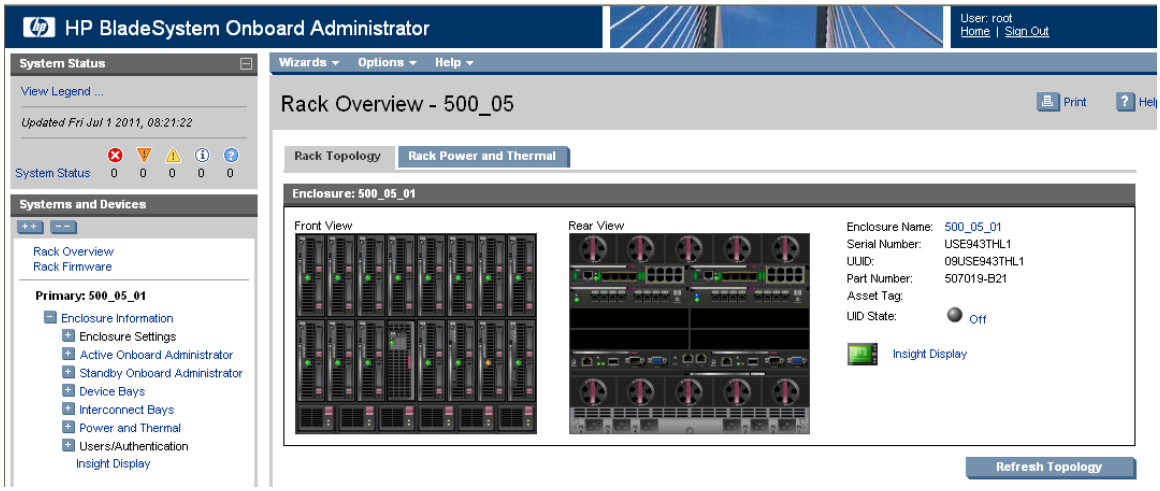
Note: The transfer of configuration occurs only from OA in Bay 1 to OA in Bay 2. Therefore in order to keep the current configuration of the system, the insertion of new OA into the OABay 1 location should be avoided.

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. OA GUI: Log into the active OA

   Navigate to the IP address of the active OA, using *C.1 Determining Which Onboard Administrator Is Active*. Log in 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:

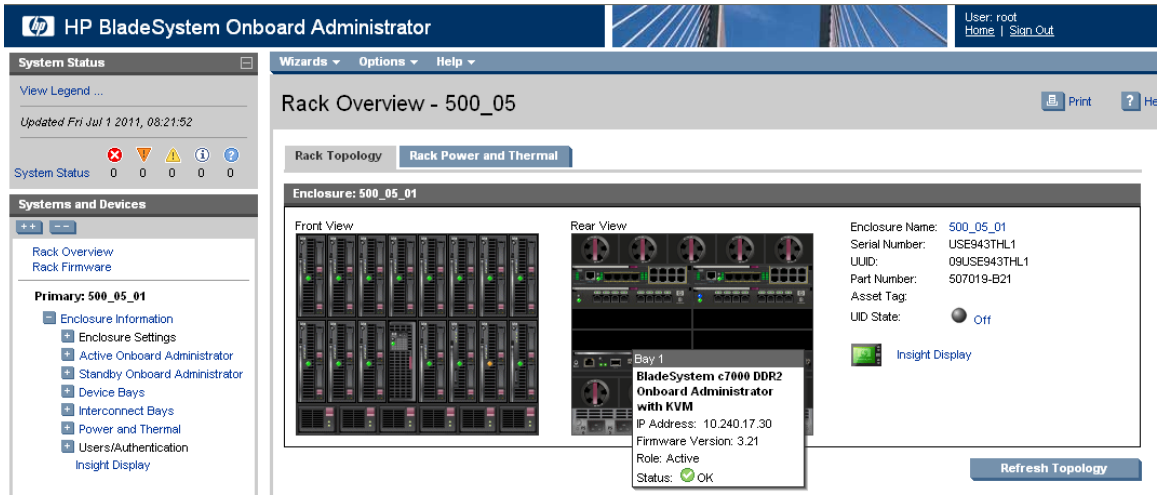
Active OA IP Address:	
Active OA Subnet Mask:	
Active OA Gateway:	

   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

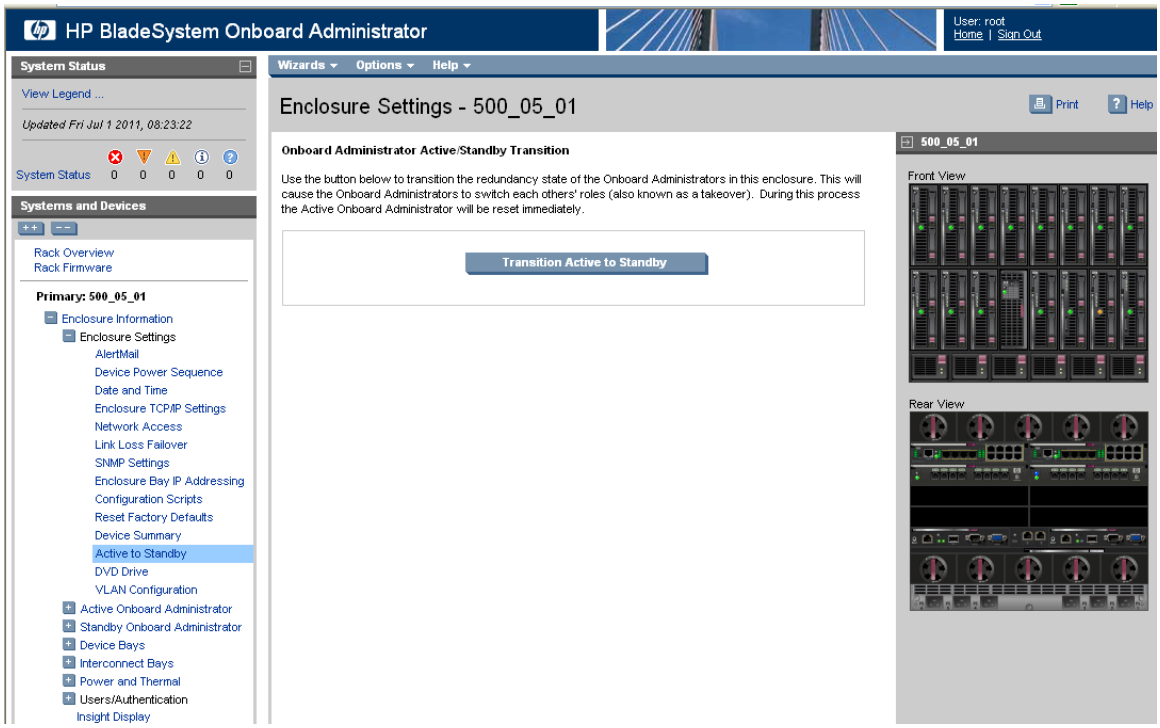
   Note the location of the active onboard administrator within the enclosure. The active OA will have the Active LED on, as in the figure below. You may also mouse over the OA and see its role.



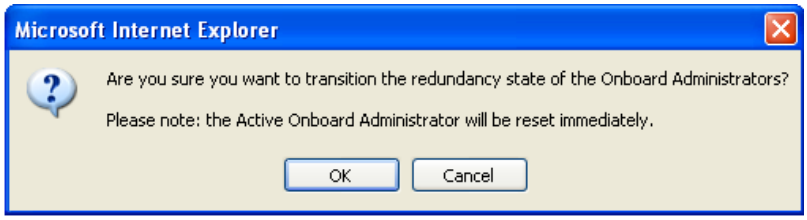
If the OA to be replaced is not the active OA for the enclosure, skip to step 5. Otherwise, continue with step 4.

4. OAGUI: Force active OA into standby mode

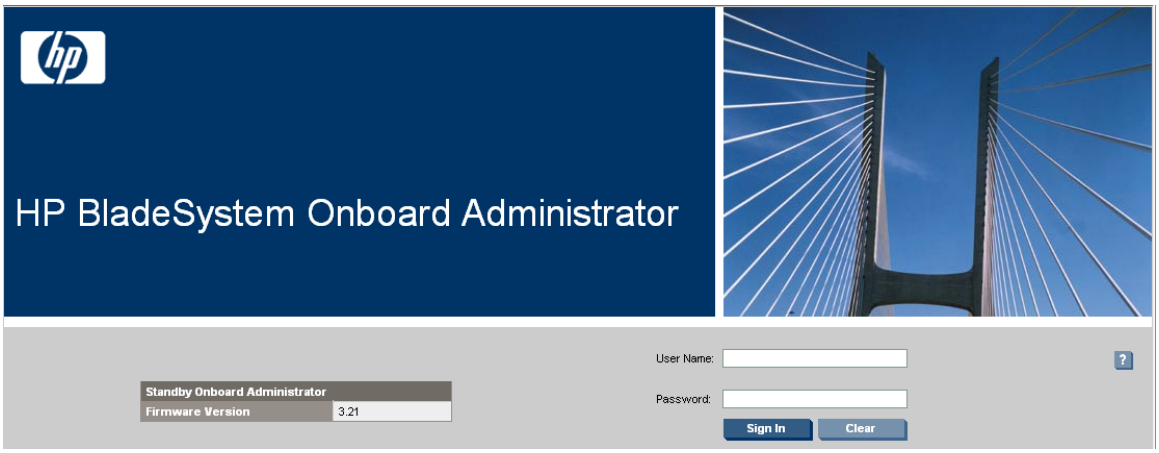
   On the left-hand side navigate to **Enclosure Information** > **Enclosure Settings** > **Active to Standby**, then click on the **Transition Active to Standby** button.



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: Log into the active OA

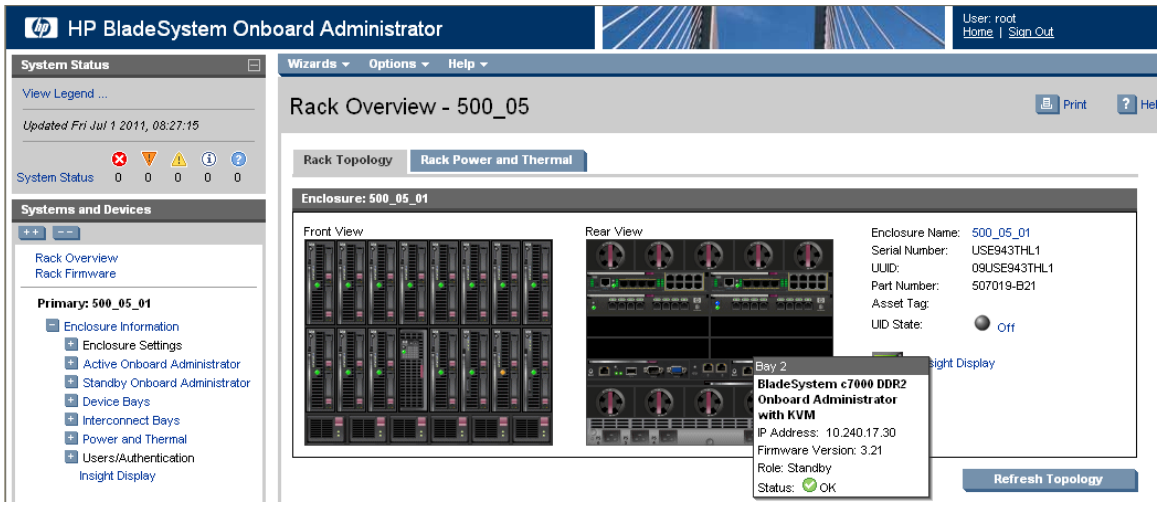
   Navigate to the IP address of the active OA, using *C.1 Determining Which Onboard Administrator Is Active*. Log in as root.

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 *3.5.1 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 *3.5.4 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.

3.5.9 Updating IPv4 Addressing

This procedure will update the IP addressing for a C7000 enclosure.

Prerequisites:

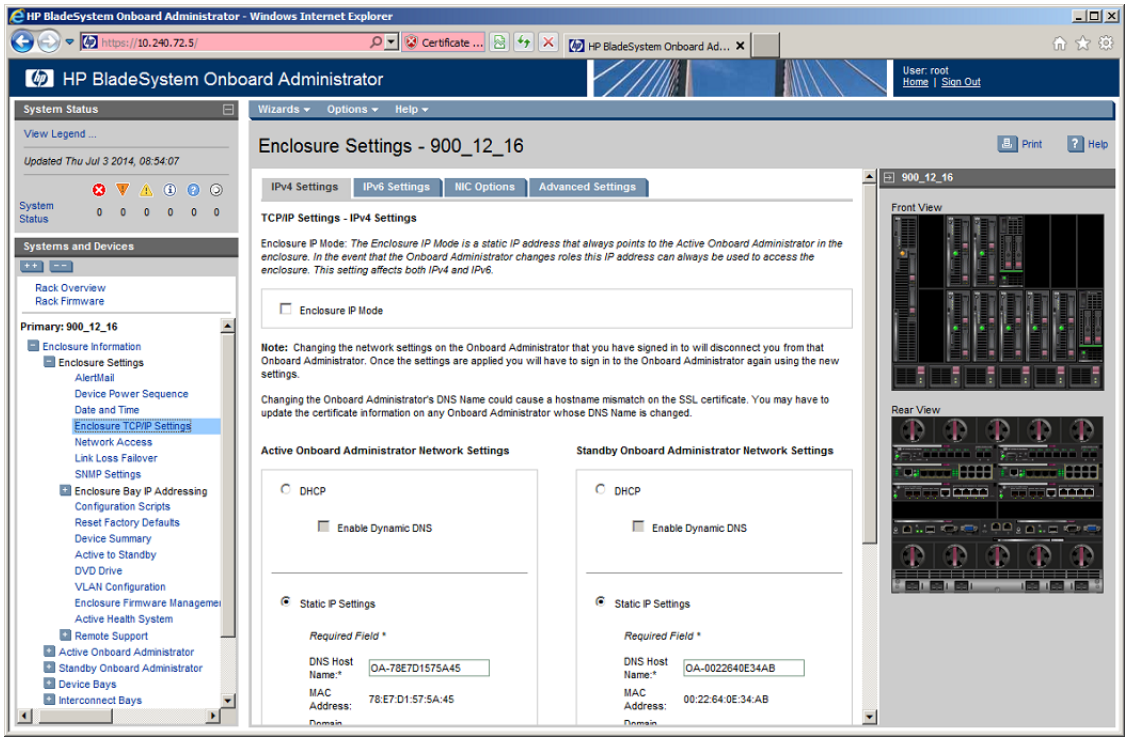
- Obtain the addressing information from the customer.
- The enclosure has been previously configured, and the PM&C GUI is reachable over the network.

1. OA GUI: Login

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

2. OA GUI: Update the IPv4 OA settings

Navigate to **Enclosure Information** > **Enclosure Settings** > **Enclosure TCP/IP Settings** and view the **IPv4 Settings** tab.



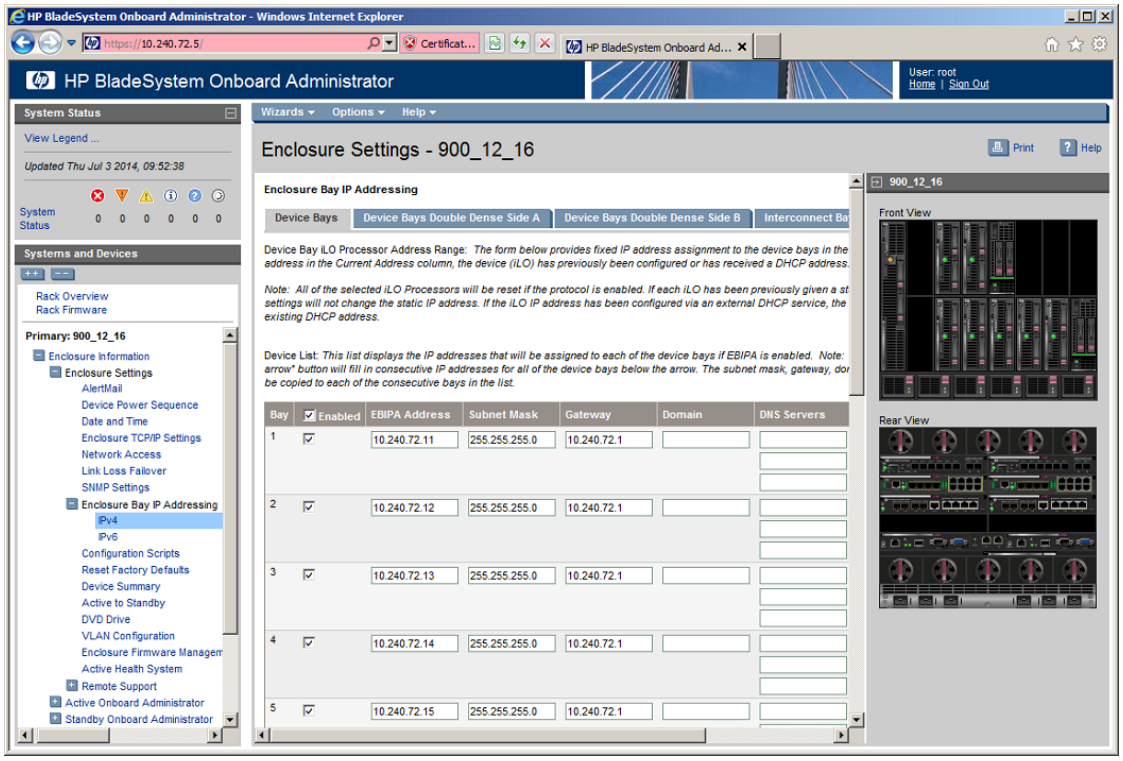
3. OA GUI: Update the static IP settings for both the Active and Standby OA. The following should be changed:

   - IP Address
   - Subnet Mask
   - Gateway

   When done, press **Apply**.

4. OA GUI: Update the IPV4 EBIPA settings.

   Navigate to the **Enclosure Information** > **Enclosure Settings** > **Enclosure Bay IP Addressing** > **IPv4** and view the **Device Bays** tab.



5. OA GUI: Update the IP settings for the device bays.

   The following should be changed:

   - EBIPA Address
   - Subnet Mask
   - Gateway

   When done, press **Apply**.

6. OA GUI: Select the **Interconnect Bays** tab and update the IP settings for the interconnect device bays.

   The following should be changed:

   - EBIPA Address
   - Subnet Mask
   - Gateway

   When done, press **Apply**.

7. OA GUI: Logout

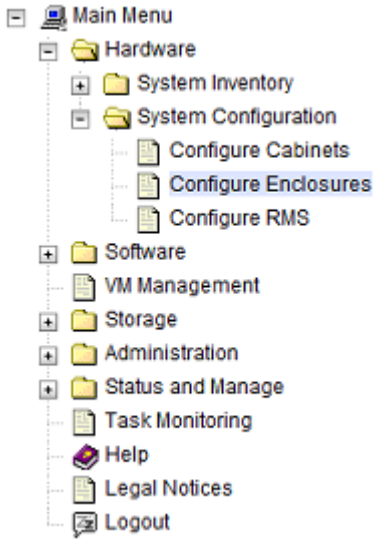
   Log out from the OA by pressing **Sign Out** at the top right corner.

8. PM&C GUI: Login
   Open your web browser and enter:

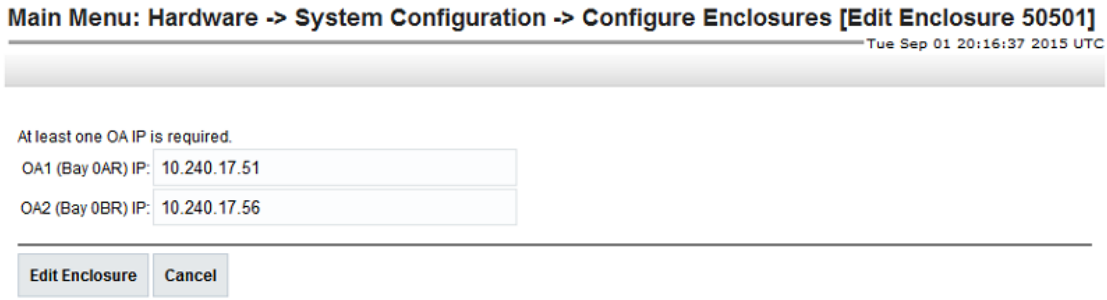
   ```
   https://<pmac_management_network_ip>
   ```

   Log in as the guiadmin user.

9. PM&C GUI: Navigate to Configure Enclosures
   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Enclosures**.

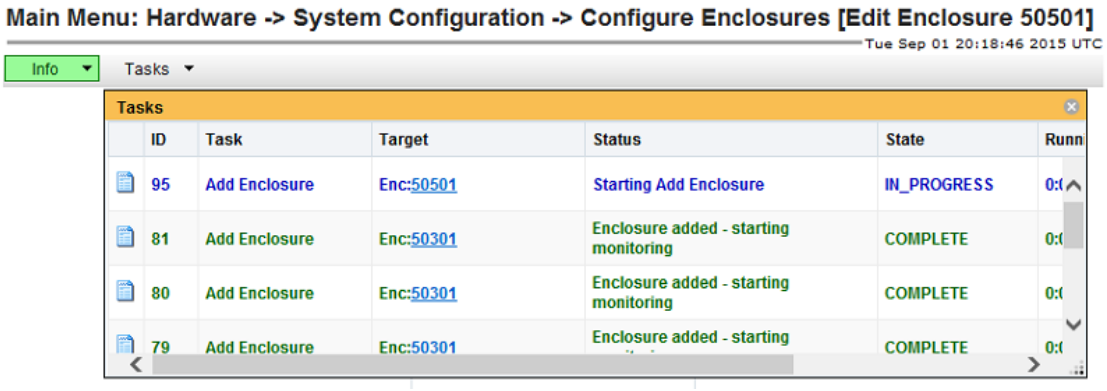


10. PM&C GUI: Select Enclosure to edit
    On the **Configure Enclosures** panel, select the enclosure that you are modifying. Then click on **Edit Enclsoure**.
11. PM&C GUI: Edit Enclosure address
    On the **Edit Enclosure** panel, update the IP addresses. Then click on **Edit Enclsoure**.



12. 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%".

3.5.10 Updating IPv6 Addressing

This procedure will update the IP addressing for a C7000 enclosure. It may be used to add IPv6 addresses or to edit existing IPv6 addresses.

Prerequisites:

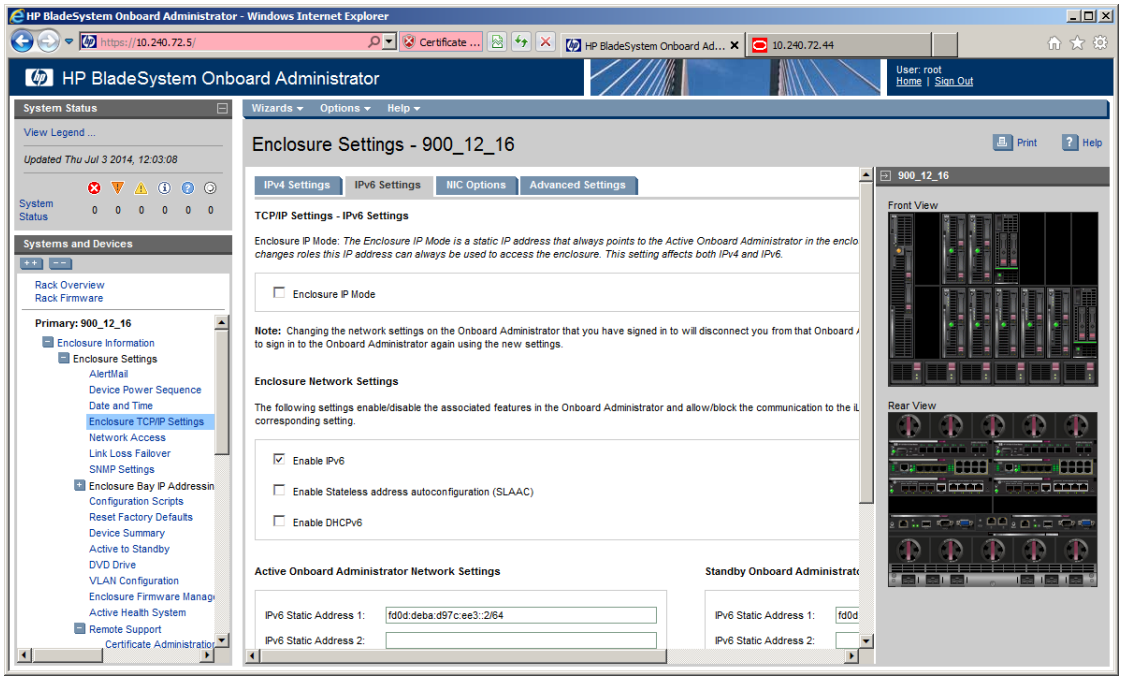
- Obtain the addressing information from the customer.
- The enclosure has been previously configured, and the PM&C GUI is reachable over the network.

1. OA GUI: Login

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

2. OA GUI: Update the IPv6 OA settings

   Navigate to **Enclosure Information** > **Enclosure Settings** > **Enclosure TCP/IP Settings** and view the **IPv6 Settings** tab.



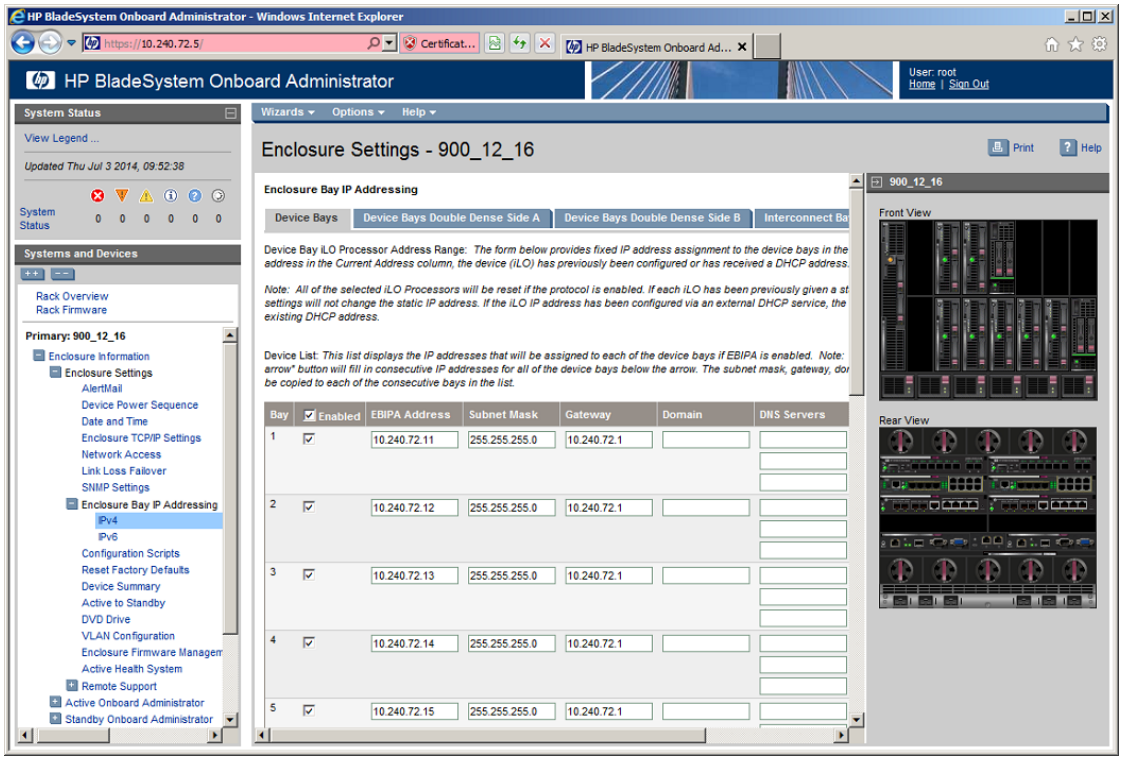
3. OA GUI: Under **Enclosure Network Settings**, verify the **Enable IPv6** checkbox is checked.
4. OA GUI: Update the static IP settings for both the Active and Standby OA. The following should be changed:

   - IPv6 Static Address 1
   - Static Default Gateway

   When done, press **Apply**.

5. OA GUI: Update the IPv6 EBIPA settings

   Navigate to **Enclosure Information** > **Enclosure Settings** > **Enclosure Bay IP Addressing** > **IPv6** and view the **Device Bays** tab.



6. OA GUI: Update the IP settings for the device bays.

   The following should be changed:

   - Verify **Enabled** is checked
   - EBIPA Address
   - Gateway

   When done, press **Apply**.

7. OA GUI: Select the **Interconnect Bays** tab and update the IP settings for the interconnect device bays.

   The following should be changed:

   - Verify **Enabled** is checked
   - EBIPA Address
   - Gateway

   When done, press **Apply**.

8. OA GUI: Logout

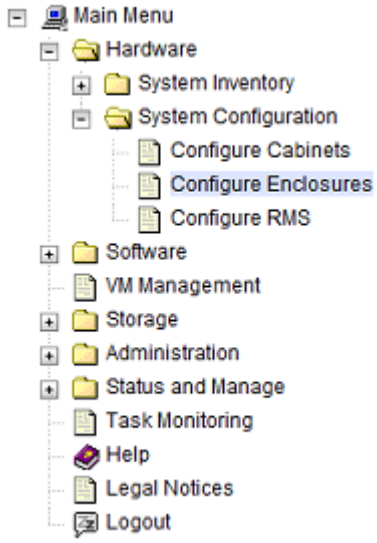
   Log out from the OA by pressing **Sign Out** at the top right corner.

9. PM&C GUI: Login
   Open your web browser and enter:

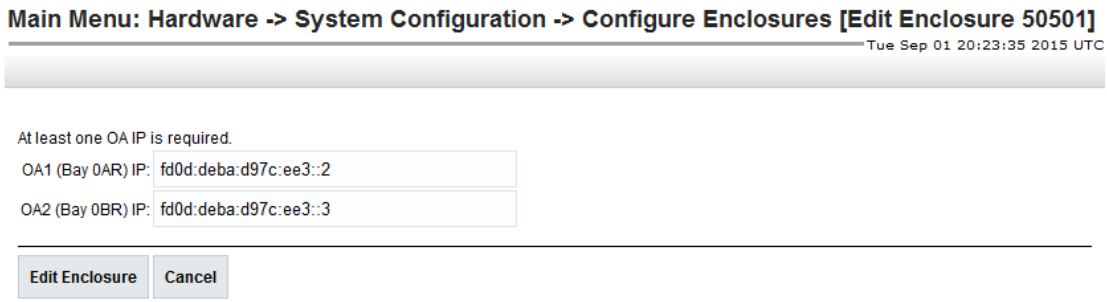
   ```
   https://<pmac_management_network_ip>
   ```

   Log in as the guiadmin user.

10. PM&C GUI: Navigate to Configure Enclosures
    Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Enclosures**.

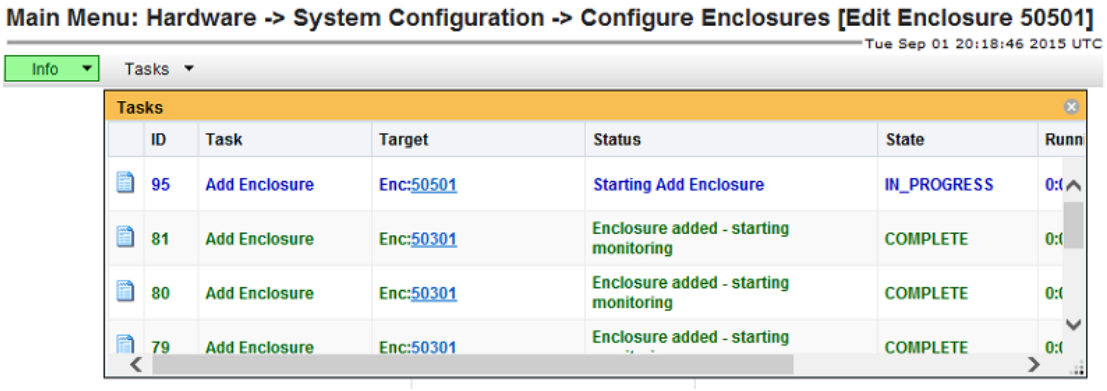


11. PM&C GUI: Select Enclosure to edit
    On the **Configure Enclosures** panel, select the enclosure you are modifying. Then click on **Edit Enclsoure**.
12. PM&C GUI: Edit Enclosure address
    On the **Edit Enclosure** panel, update the IP addresses. Then click on **Edit Enclsoure**.



13. PM&C GUI: Monitor Add Enclosure

    The Configure Enclosures page is 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%".

3.5.11 Add SNMP Trap Destination on OA

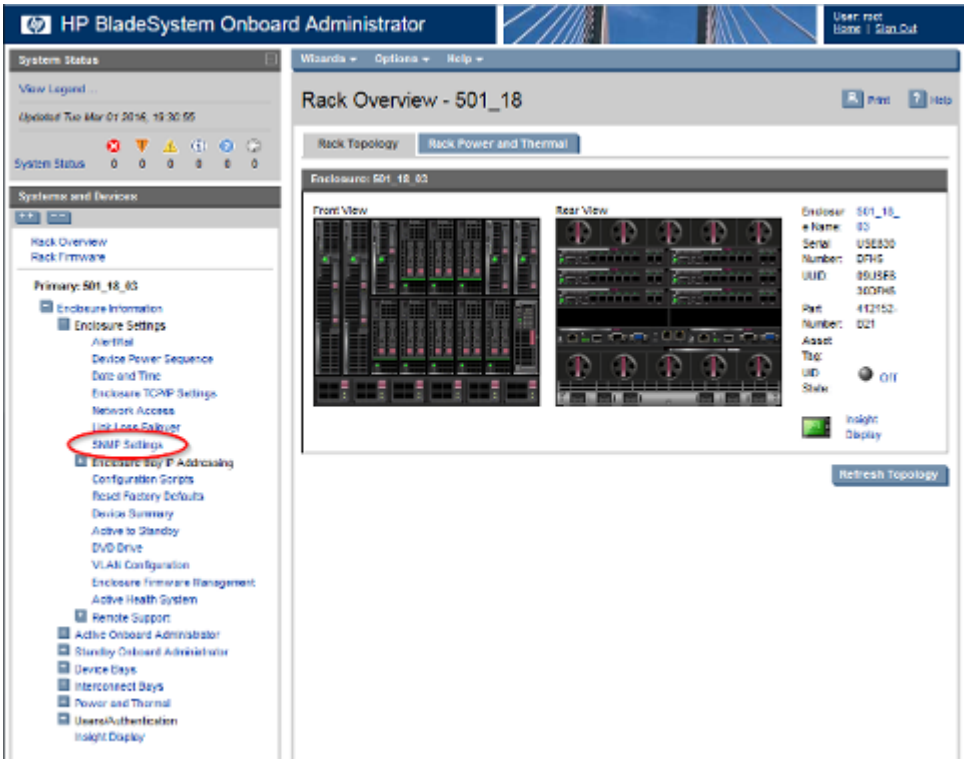
An SNMP trap destination must be added and configured using the Onboard Administrator (OA), or SNMP must be disabled. One of these actions must be completed as described in this procedure.

1. Either add an SNMP trap destination as follows, or proceed to *3.5.11 Step 2* to disable SNMP.
   a) Active OA GUI: Login

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

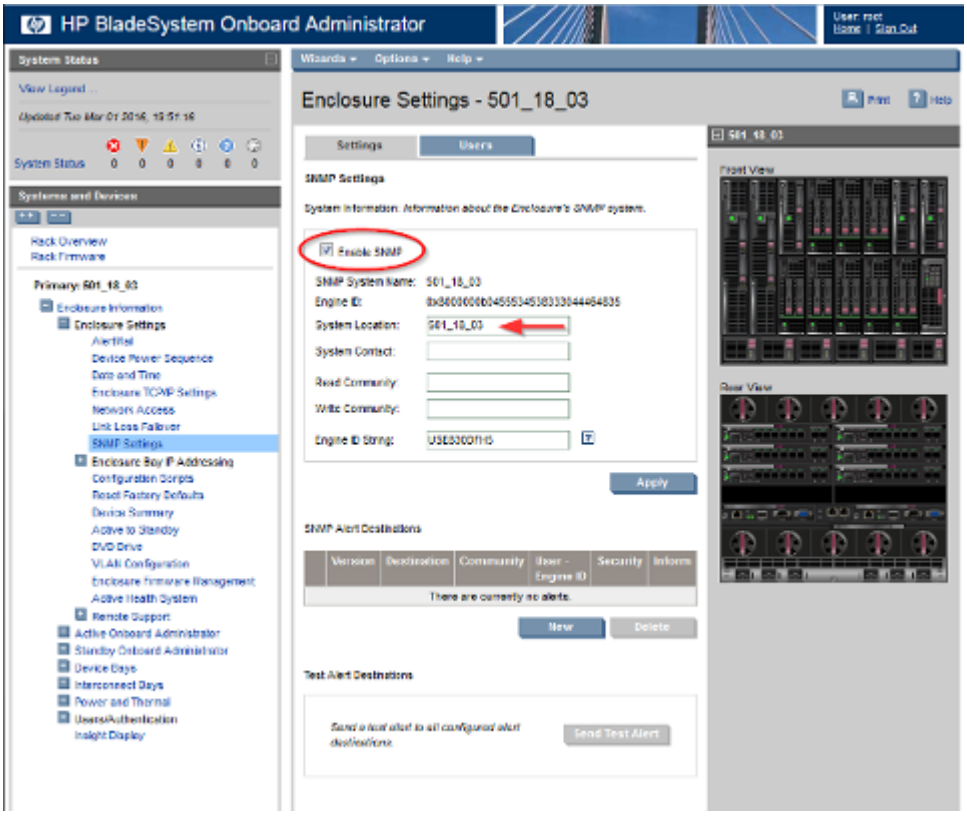
   b) OA GUI: Navigate to SNMP Settings page

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



c) OA GUI: Enable SNMP and populate System Information

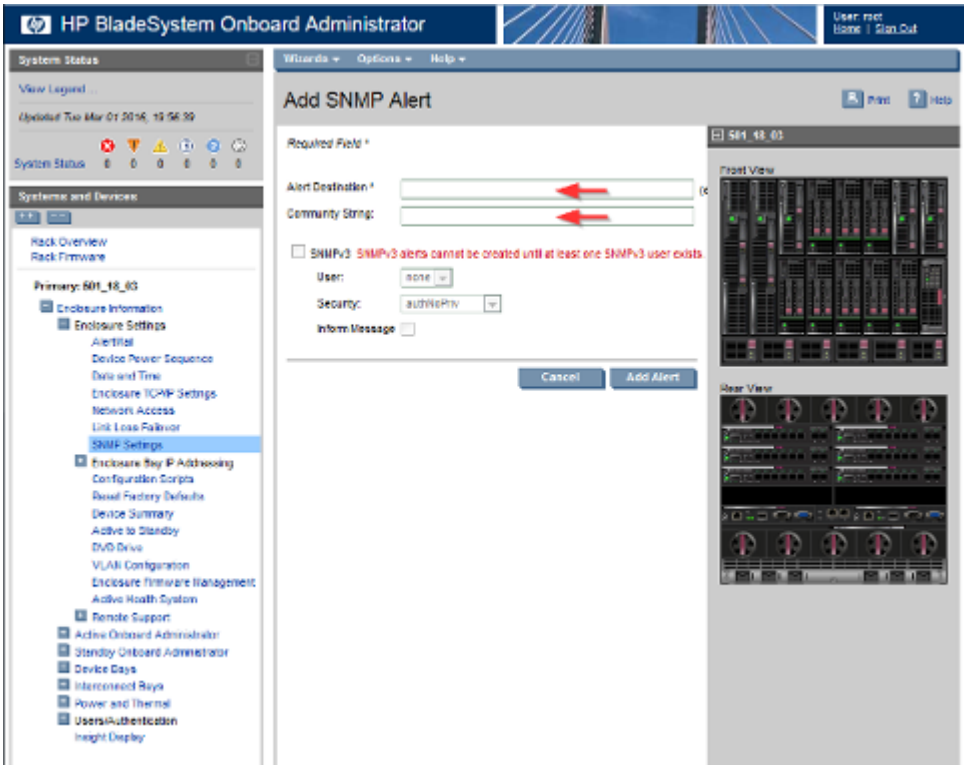
If SNMP is not already enabled, check the **Enable SNMP** checkbox. Enter the **Enclosure Name** (shown in the title bar) or your preferred name into the **System Location** box.



Do not set **Read Community** and **Write Community**. Click **Apply** to save the System Information.

d) OA GUI: Add SNMP Alert Destinations

Click **New**. The **Add SNMP Alert** page appears. Type the destination information into the **Alert Destination** box (ex. 61.206.115.3, 2002::1 or host.example.com) and type the community string into the **Community String** box.



Click **Add Alert** to add the destination to the system.

Upon successfully adding a new SNMP Alert Destination you will be returned to the SNMP Settings page.

e) Perform *3.5.11 Substep d* for each required destination.

2. To disable SNMP, follow these steps:
   a) If necessary, log in to the Active OA as instructed in *3.5.11 Substep a*.
   b) Navigate to SNMP Settings page as instructed in step *3.5.11 Substep b*.
   c) Uncheck the Enable SNMP checkbox. Click **Apply** to save the changes.

3.5.12 Delete SNMP Trap Destination on OA

This procedure will remove an SNMP trap destination from the Onboard Administrator.

1. Active OA GUI: Login

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

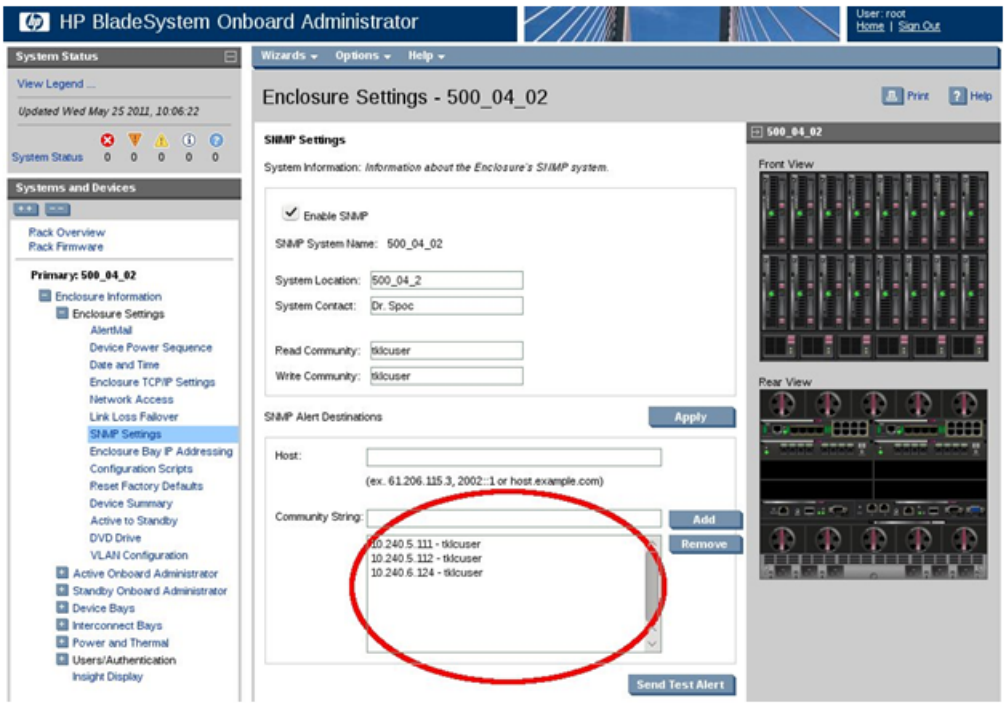
2. OA GUI: Navigate to SNMP Settings page

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

All configured SNMP trap destinations will be shown in the box in the center of the SNMP Settings page.

3. OA GUI: Remove SNMP trap destination

   Select the trap destination that will be removed and click the **Remove** button.



If no SNMP trap destinations are shown in the box in the center of the SNMP Settings page, then you might wish to disable SNMP by unchecking the **Enable SNMP** checkbox.

The SNMP trap destination has now been removed from the configuration and will no longer be listed as a configured destination. Click **Apply** to activate the configuration. The following progress meter will appear.

When the progress meter disappears the configuration has been applied.

3.6 Management Server Procedures

3.6.1 IPM Management Server

This procedure provides instructions for configuring and IPMing the DL360, DL380, or Oracle rack mount server.

Needed material:

- *TPD Initial Product Manufacture Software Installation Procedure*, E53017

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

1. Configure and IPM the DL360, DL380, or Oracle RMS

   Follow *TPD Initial Product Manufacture Software Installation Procedure* (E53017), sections 3.1 through 3.4 to configure and IPM the management server.

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

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

   Note: If you are using a serial console for installation, do not use the console=tty0 option.

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

2. Verify the initial product manufacture

   Follow section 3.5 in *Initial Product Manufacture*, E53017 to verify the IPM completed successfully.

3.6.2 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.

3.6.2.1 DL360/DL380 Server Firmware Upgrade

This procedure will upgrade the DL360 or DL380 server firmware.

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.

Prerequisites:

- *3.6.1 IPM Management Server* has been completed

Needed Material:

- HP Service Pack for ProLiant (SPP) firmware ISO image [2]
- HP MISC firmware ISO image [2] (for errata updates if applicable)
- *HP Solutions Firmware Upgrade Pack* Upgrade Guide [2]
- *HP Solutions Firmware Upgrade Pack* Release Notes [2]
- 4GB or larger USB stick if upgrading using USB media

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:

- 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.

The minimum supported HP Solutions Firmware Upgrade Pack for PMAC 6.3 is release 2.2.10. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the HP Solutions Firmware Upgrade Pack Release Notes for important information on firmware upgrades and follow the procedures in the HP Solutions Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

3.6.2.2 Oracle Rack Mount Server

This procedure will update the firmware on Oracle RMS

Needed Materials:

- Oracle Firmware Upgrade Pack 3.x.x Release Notes
- Oracle Firmware Upgrade Pack 3.x.x Upgrade Guide

The minimum supported Oracle Firmware Upgrade Pack for PMAC 6.3 is release 3.1.7. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the Oracle Firmware Upgrade Pack Release Notes for procedures on how to obtain the firmware, and then follow the procedures in the Oracle Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

3.7 PM&C Procedures

3.7.1 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 PM&C into a state where the Initialization process can begin.

- Install TVOE 3.2 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.

- 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 4 pt NICs) (G6)	DL380 (with HP 4pt Gigabit in PCI Slot 1) (Gen8, 9)	DL380 (with HP 4pt Gigabit in PCI Slot 3) (G6)	Oracle RMS (without 10GigE card)		DL380 (with HP 1Gb 4pt 331FLR Adapter) (Gen9)
						X3-2	X5-2 and X6-2	
<ethernet_ interface_1>	eth01	eth01	eth01	eth01	eth01	eth01	eth01	eth01
<ethernet_ interface_2>	eth02	eth02	eth02	eth02	eth02	eth02	eth03	eth02
<ethernet_ interface_3>		eth21		eth11	eth31	eth03	eth02	eth03
<ethernet_ interface_4>		eth22		eth12	eth32	eth04	eth04	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): _____

PM&C Interface Alias	TVOE Bridge Name	TVOE Bridge Interface
		<TVOE_Control_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

Variable	Value	Description
<NetBackup_gateway_address>		Gateway address used for routing on the NetBackup network.
<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

3.7.2 Installing TVOE on the Management Server

Install the TVOE Hypervisor platform on the Management Server.

At this point in the installation, the PM&C is not available to do an IPM using TVOE on the management server. It is necessary to physically provide the TVOE media via a USB drive.

Prerequisites:

- TVOE installation media.

Note: For more information about configuring the iLO IP address, refer to Appendix F in Initial Product Manufacture, E53017.

Install TVOE onto the Management Server.

Follow *3.6.1 IPM Management Server* to IPM the management server with TVOE.

3.7.3 TVOE Network Configuration

Prerequisites:

- *3.7.2 Installing TVOE on the Management Server*

1. TVOE Management Server iLO: Log into the management server on the remote console

   Log into the management server iLO using application provided passwords following *F.1 How to Access a Server Console Remotely*.

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

   Click on 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: Configure the control network bond for back-to-back configurations (optional)

   If the control network for the RMS servers consists of direct connections between the servers with no intervening switches (known as a "back-to-back" configuration), execute this step to set the primary interface of bond0 to <ethernet_interface_1>, otherwise 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 set --device=bond0 --onboot=yes --type=Bonding
    --mode=active-backup --miimon=100 --primary=<ethernet_interface_1>Interface
   bond0 updated
   ```

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.

```
$ 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 --type=Bridge --name=control
--bridgeInterfaces=<TVOE_Control_Bridge_Interface>
```

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

   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 untagged 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_mgmt_ip_address> --netmask=<mgmt_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>
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.

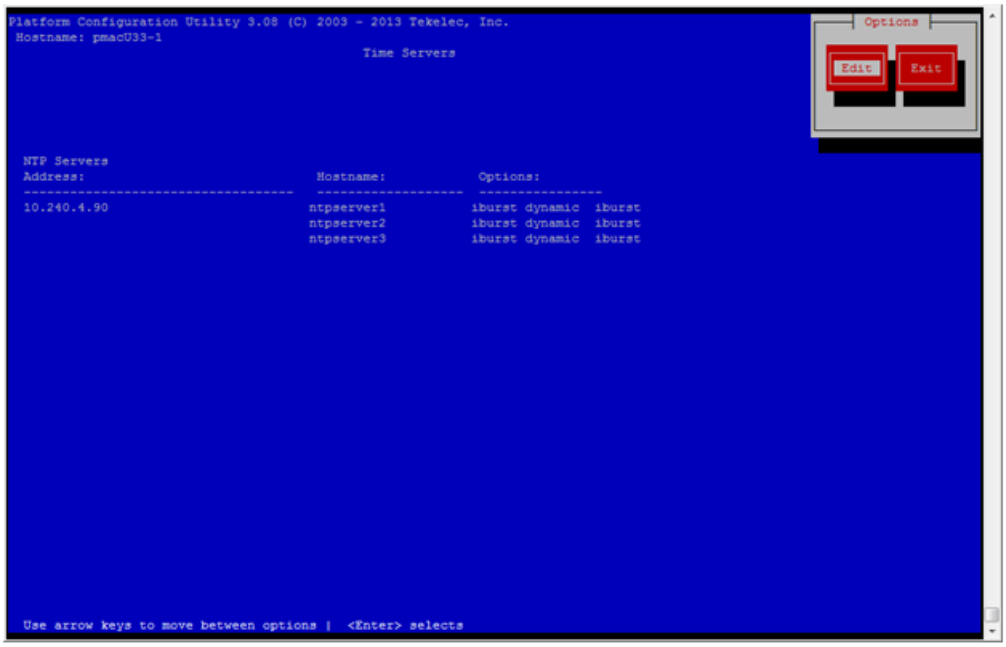
14. This step will configure NTP servers for a server based on TPD.

Note: 3 NTP Sources will be configured in this step.

a) TVOE Management Server: Log in as platcfg

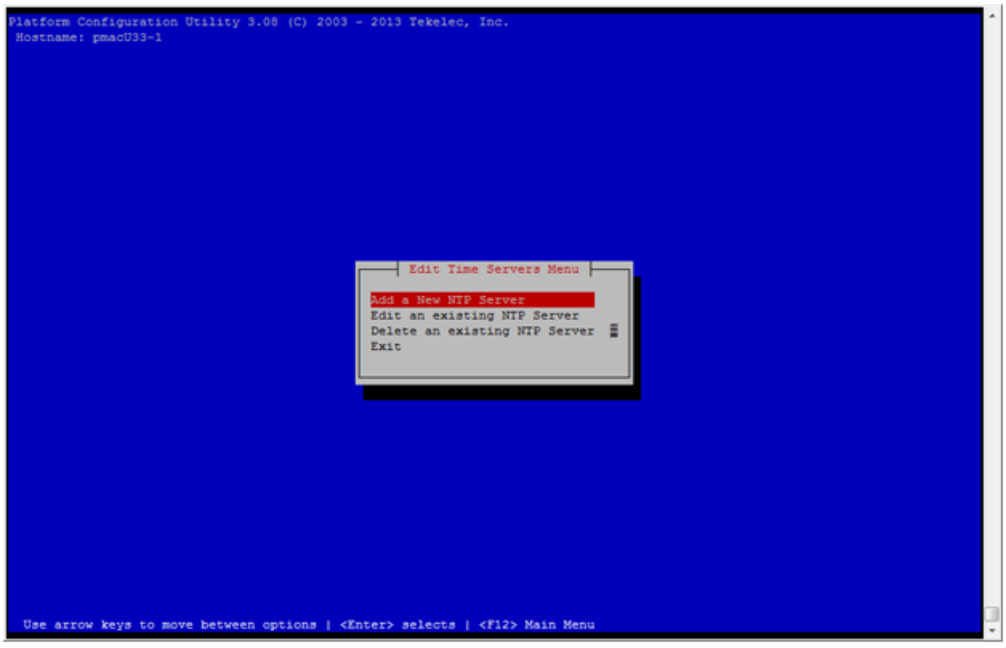
Log in as platcfg user on the server. The platcfg main menu will be shown.

b) TVOE Management 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) TVOE Management Server: Update NTP Information

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



d) TVOE Management Server: Edit NTP Information

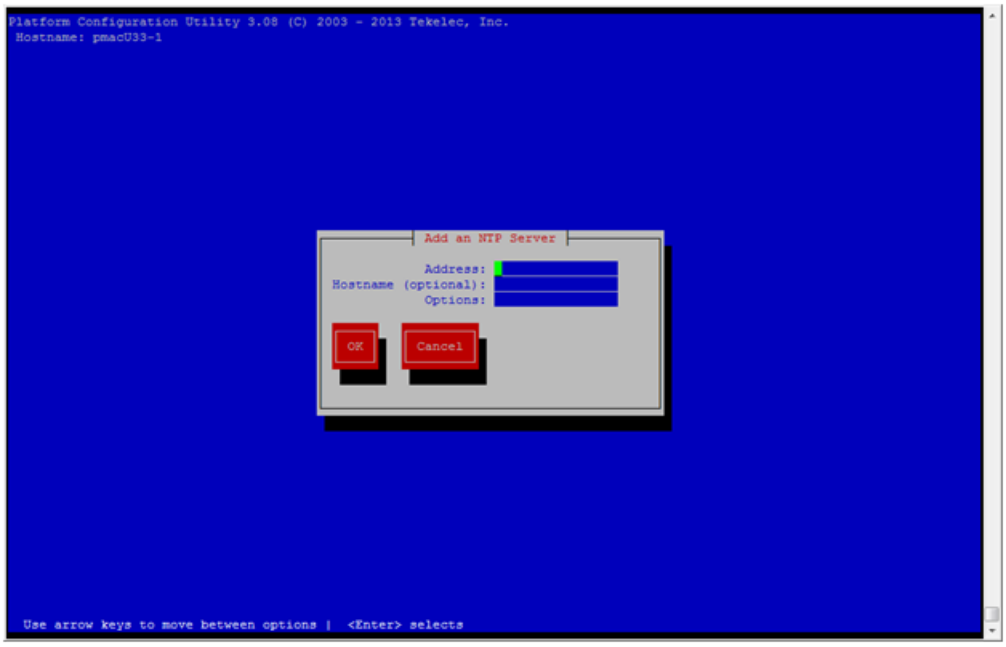
Select the appropriate **Edit Time Servers Menu** option. When all Time Server actions are complete exit the **Edit Time Servers Menu**. Remember that 3 (or more) NTP sources are required.

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

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



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

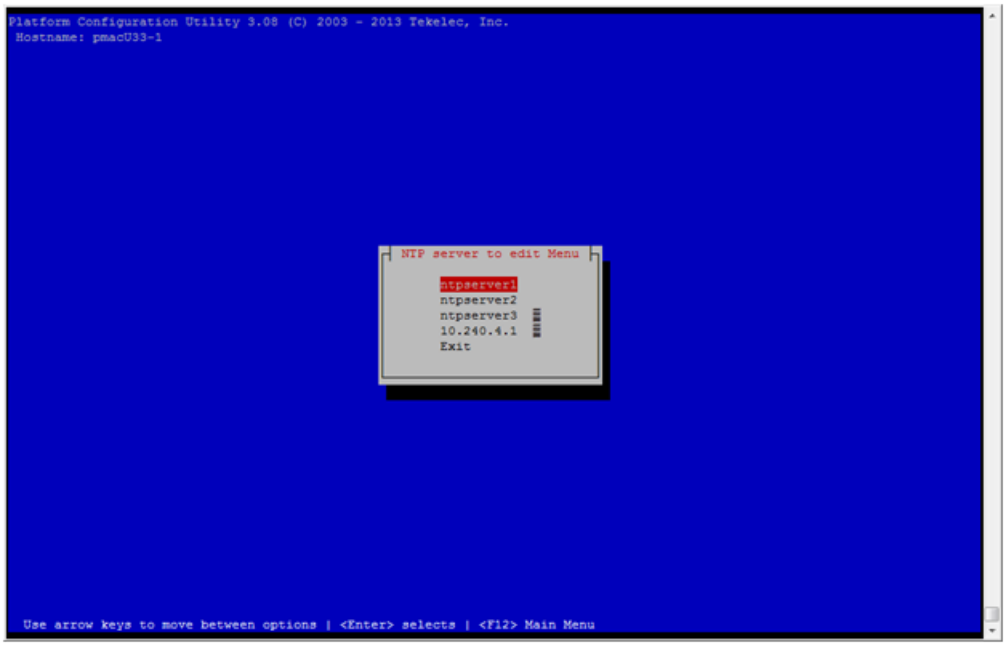
      The NTP server is added. The **Edit Time Servers Menu** is displayed.

      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

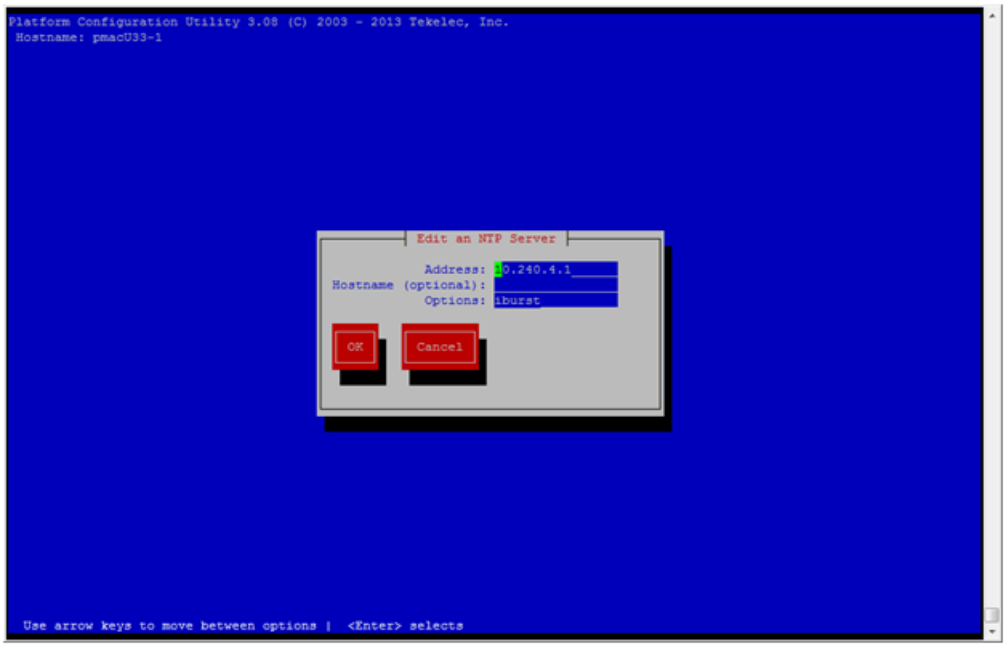
   a. TVOE Management Server: If editing an existing NTP server select **Edit an existing NTP Server**.

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



b. TVOE Management Server: Select appropriate NTP server.

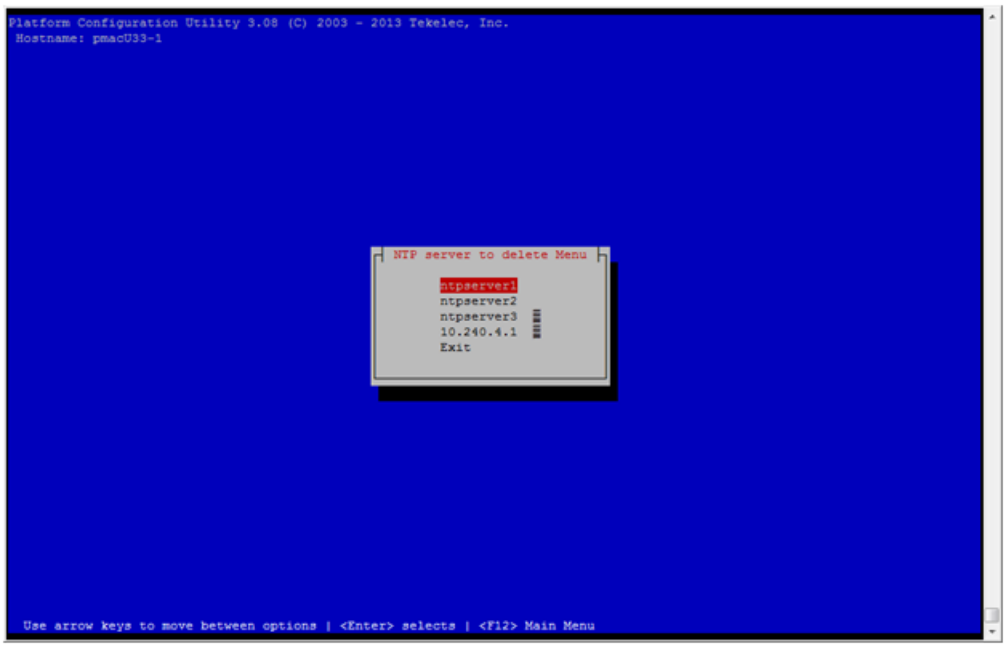
The **Edit an NTP Server** window is displayed.



3. Deleting an existing NTP Server

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

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



b. TVOE Management Server: Select appropriate NTP server.

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

e) TVOE Management Server: Restart the NTP server

f) TVOE Management Server: Exit platcfg.

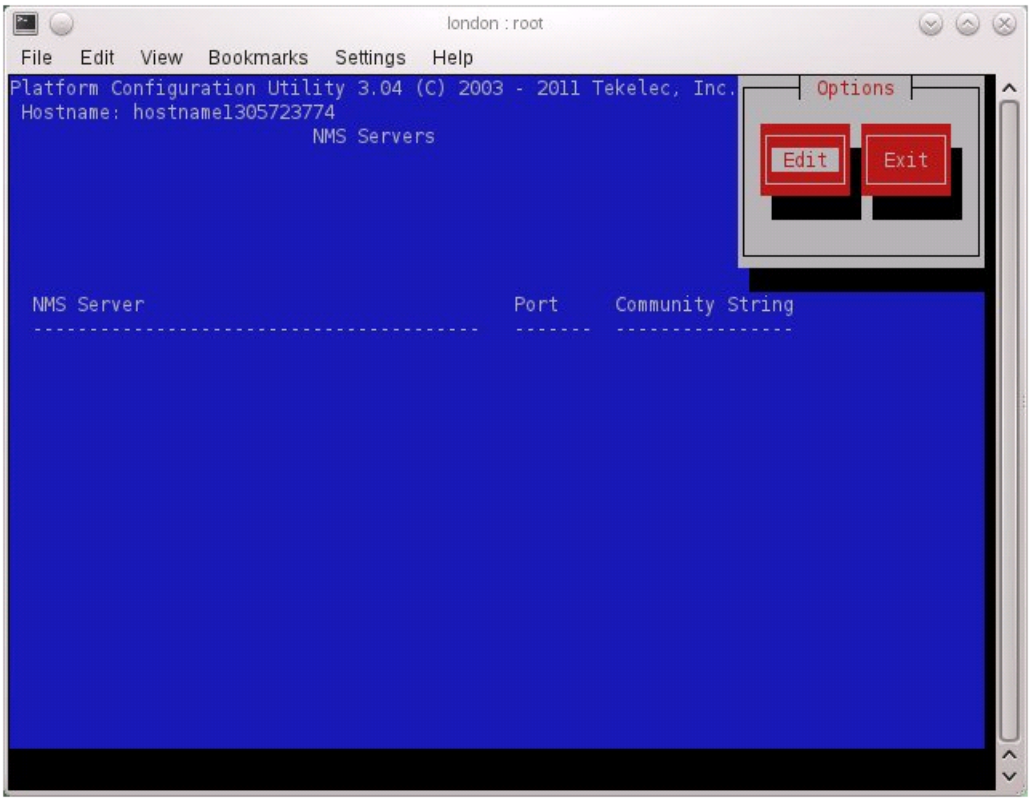
Select **Exit** on each menu until platcfg has been exited.

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) TVOE Management Server: Log in as platcfg user on the server. The platcfg main menu will be shown.

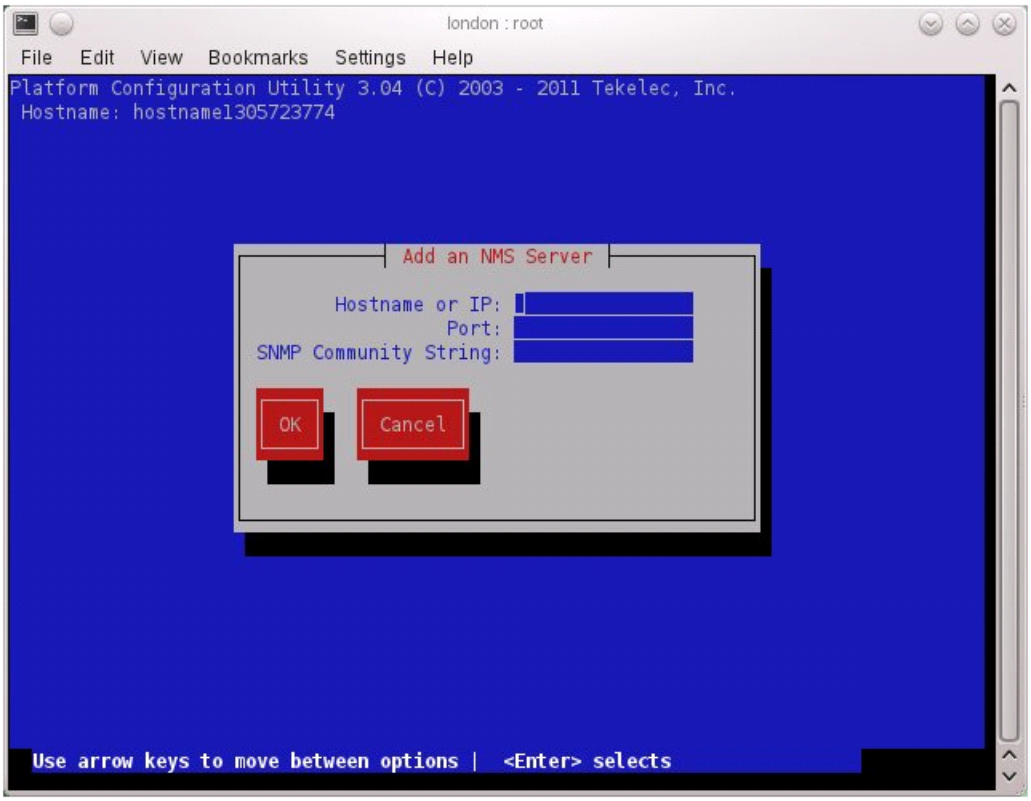
b) TVOE Management Server: Navigate to NMS server configuration page.

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.



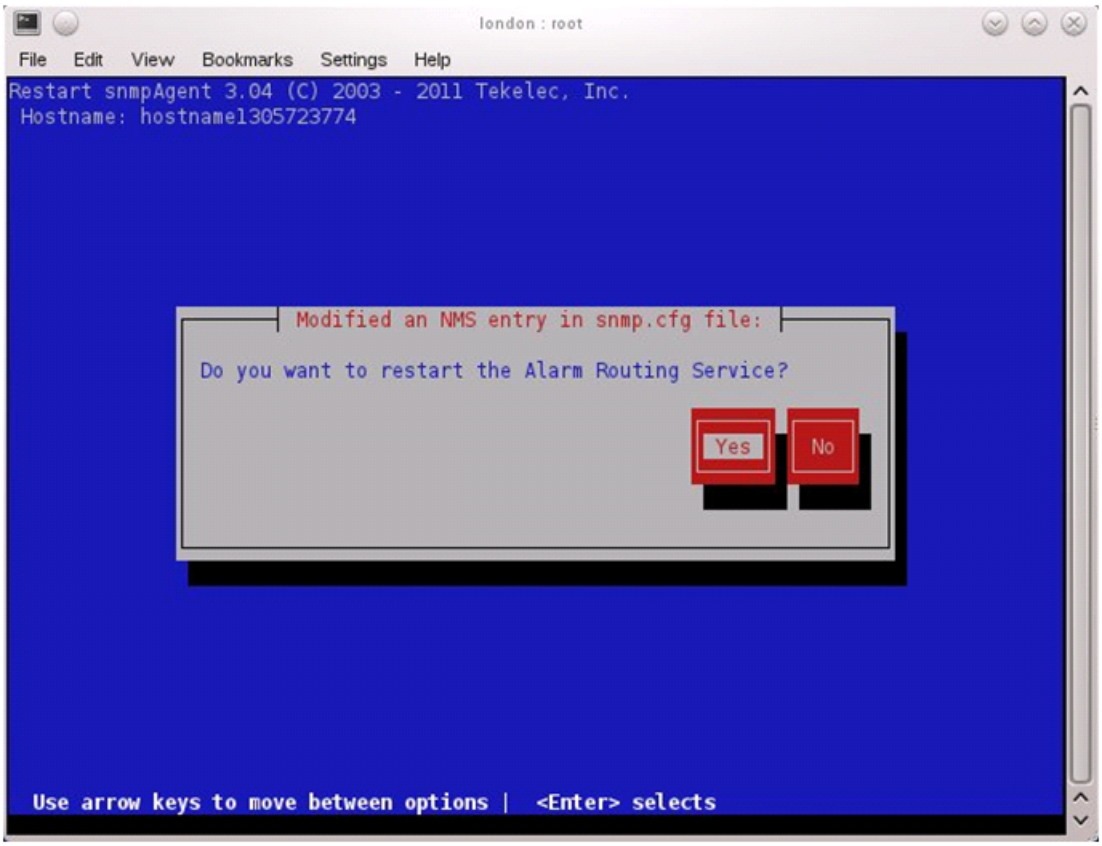
c) TVOE Management Server: Add the SNMP trap destination.

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. 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 *3.11.2 TVOE NetBackup Client Configuration*. The steps in *3.11.2 TVOE NetBackup Client Configuration* can only be performed after the Aggregation Switches in *3.1.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PM&C Installed) (netConfig)* 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.

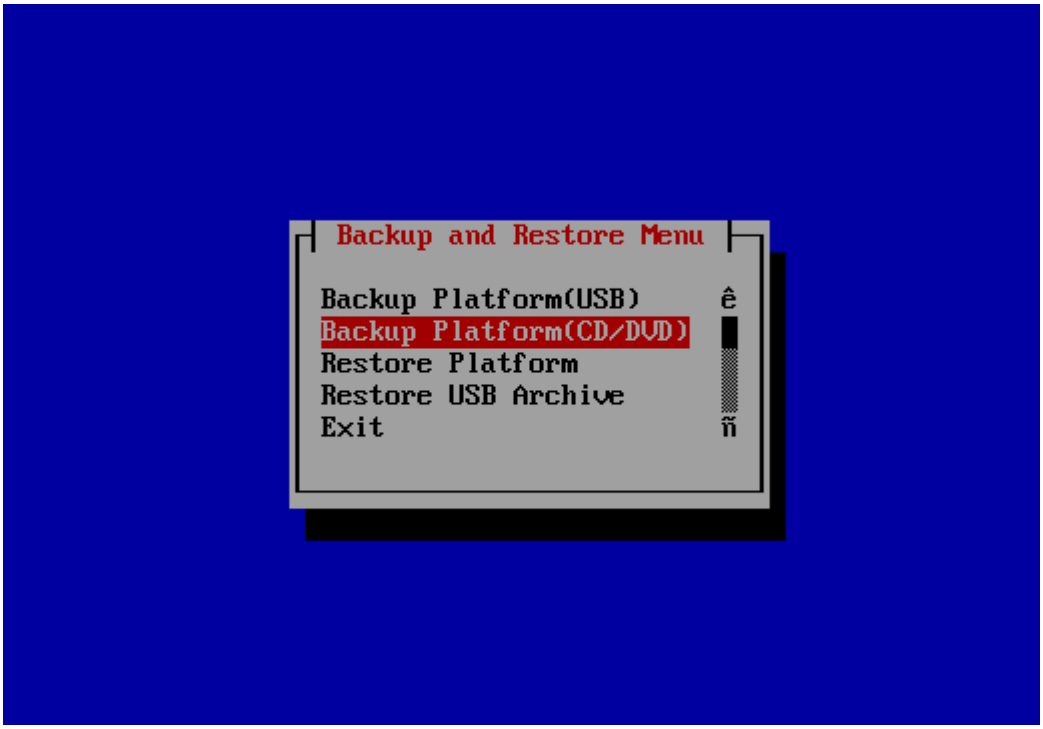
Note: The backup image is to be transferred to a customer device.

a) TVOE Management Server: Log in as platcfg user.

The platcfg "Main Menu" is presented.

b) TVOE Management Server: Navigate to the **Backup and Restore** Menu.

Select the following menu options sequentially: **Maintenance** > **Backup and Restore**. The 'Backup and Restore Menu' is presented.



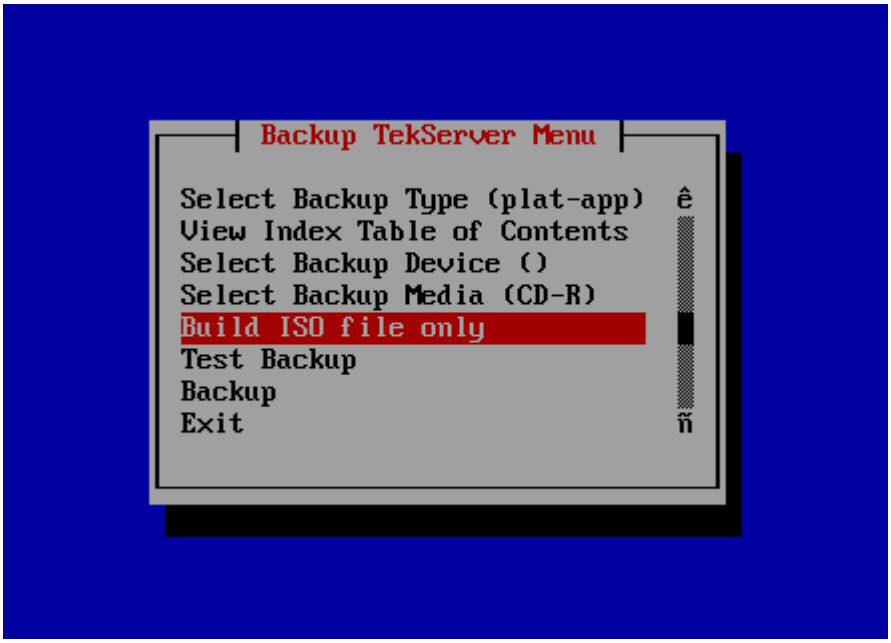
c) TVOE Management Server: Navigate to the **Backup TekServer Menu**.

Select **Backup Platform (CD/DVD)**.

Note: If this operation is attempted on a system without media (ie. the CD/DVD), a message may appear stating "No disk device available. This is normal on systems without a cdrom device." This can be ignored. Hit any key to continue.

d) TVOE Management Server: Build the backup ISO image.

Select **Build ISO file only**.



Note: The message "Creating ISO Image... This may take a while" may appear briefly.

After the ISO is created, platcfg will return to the "Backup TekServer Menu" as shown in substep d. 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"

e) TVOE Management Server: Exit platcfg

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

f) Customer Server: Log into the customer server and copy backup image to the customer server where it can be safely stored.

Note: This step assumes the network configuration is complete and the source and target servers can connect to each other. If this is not the case, skip this step for now and return to it when the network configuration is complete.

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>:/var/TKLC/bkp/* /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>:/var/TKLC/bkp/* /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 *A.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.

3.7.4 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. The media will either be physical media (USB) or a disk image (.iso file) from OSDC. The media can be stored on a USB or downloaded to the TVOE (usually /var/TKLC/upgrade). Once the PM&C media is mounted, the pmac-deploy script can be found in the upgrade directory of the media.

Prerequisites:

- *3.7.2 Installing TVOE on the Management Server*
- *3.7.3 TVOE Network Configuration*
- PM&C Installation Media

1. TVOE Management Server iLO: Log into the management server on the remote console

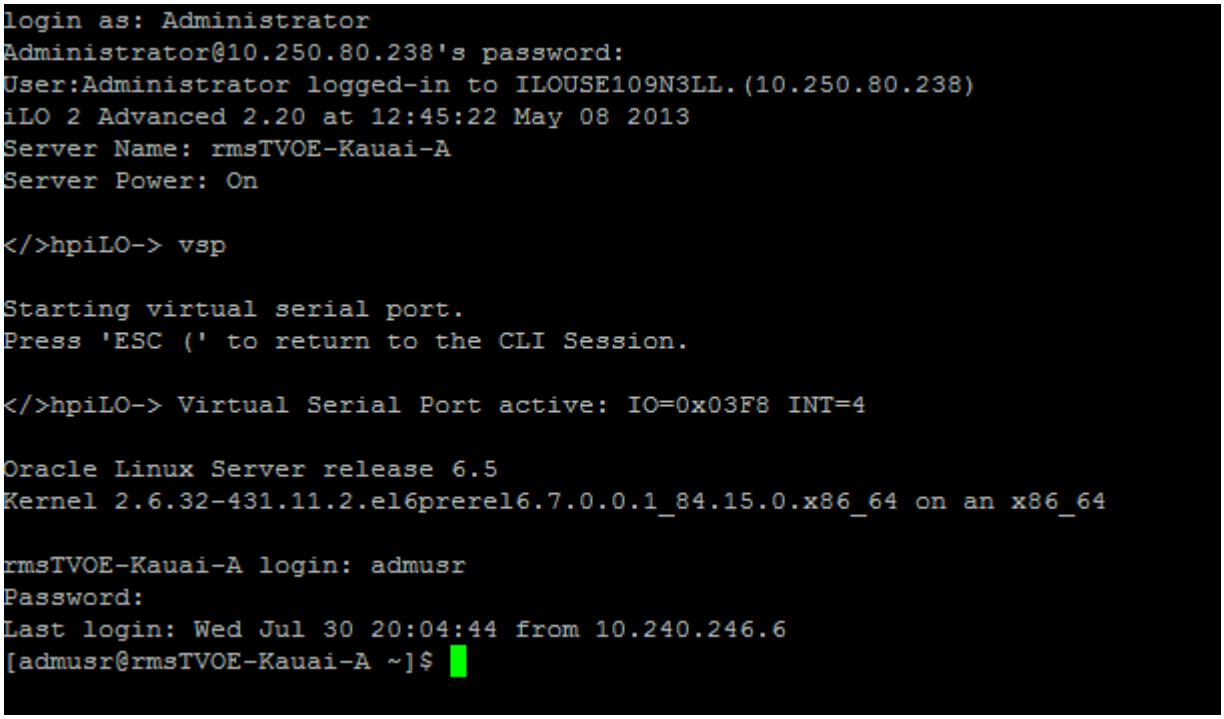
   Log into the management server iLO using application provided passwords following *F.1 How to Access a Server Console Remotely*.

   ```
   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.

   Alternatively, the user can log into the management console through PuTTY.

   a) Connect to the server using **<management_server_iLO_ip>**
   b) Start the virtual serial port by executing the **vsp** command
   c) Log into the remote server using admusr credentials.

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

   Example 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>
```

   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.

   If the version of Netbackup being installed is 7.7 or greater, the -netbackVolSize=5 must be included in the command. This will create a 5G volume instead of the standard 2G volume size. The Netbackup 7.7 client requires additional space to be installed.

```
$ 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
--netbackupVolSize=5
--bridge=<TVOE_NetBackup_Bridge>
--nic=netbackup
--isoimagesVolSizeGB=20
```

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

3.7.5 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.

Prerequisites:

- *3.7.4 Deploy PM&C Guest*

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

```
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 into the PM&C with 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 the output is not correct, then there is likely 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

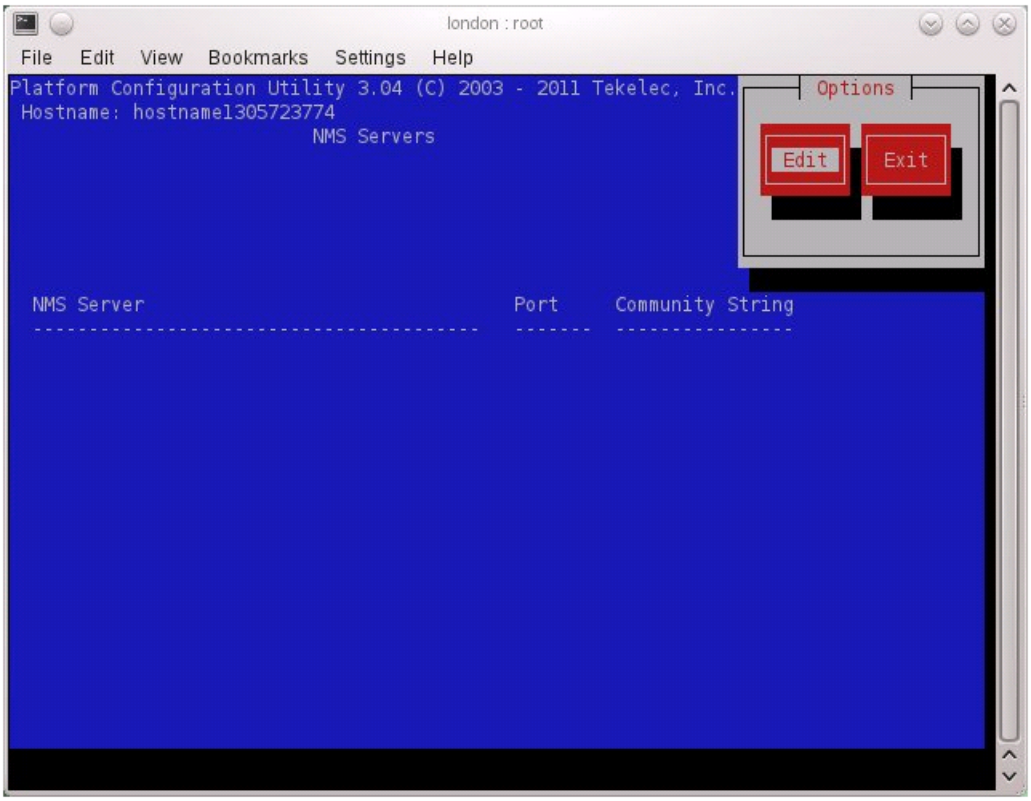
   Run:

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

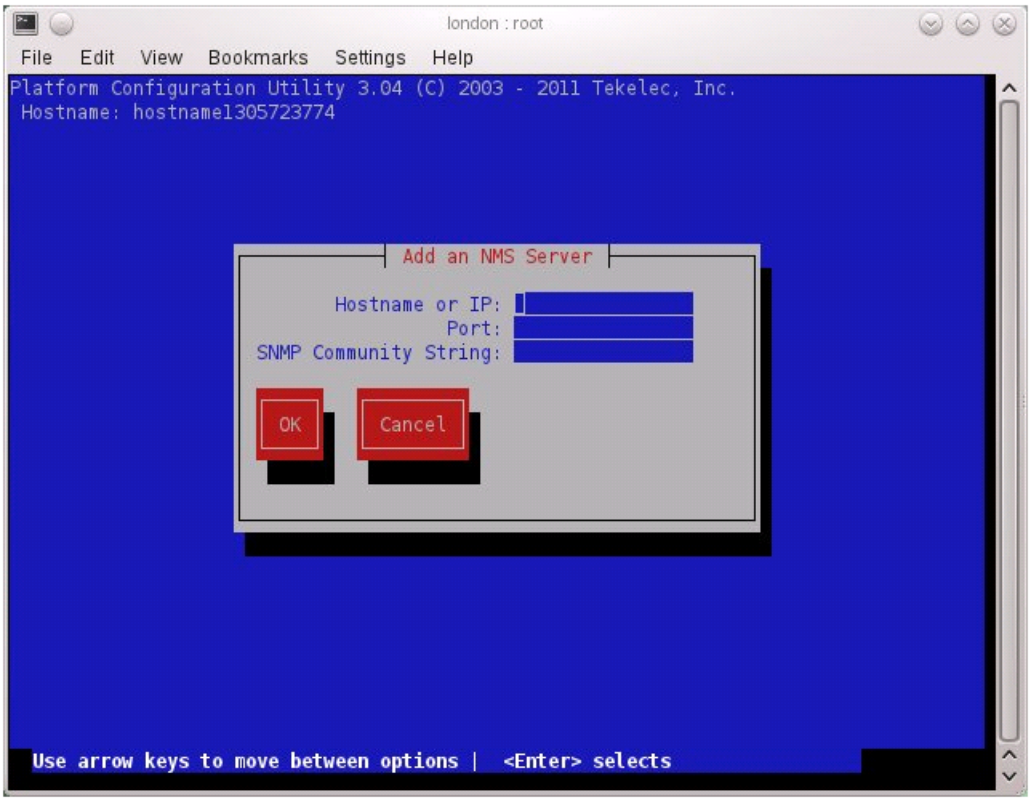
7. This step will add an SNMP trap destination to a server based on TPD. All alarm information will then be sent to the NMS located at the destination.

   1. Server: Login as user platcfg 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.

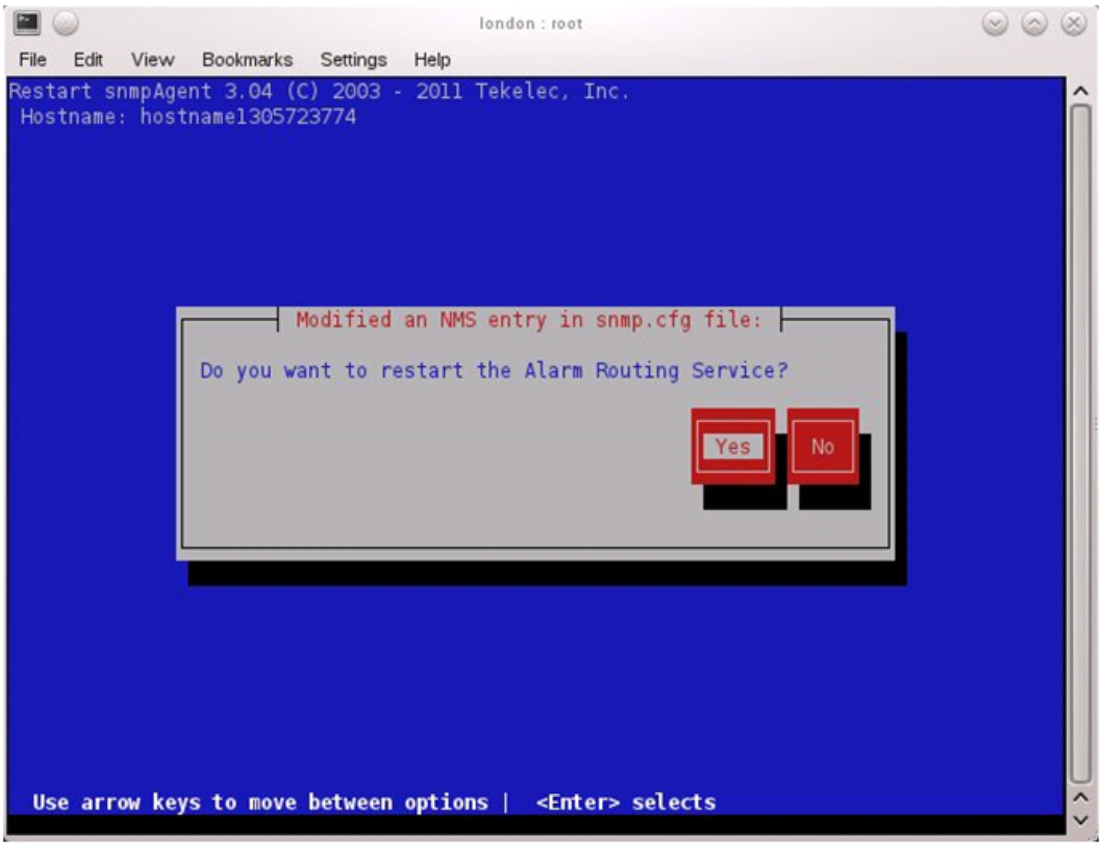


3. Server: Add the SNMP trap destination. Select **Edit** and then choose **Add a New NMS Server**. The 'Add an NMS Server' page will be displayed.



Complete the form by entering in all information about the SNMP trap destination. 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. The PM&C login prompt will be printed.

8. Log in to the PM&C as user admusr.
9. Reboot the server to ensure all processes are started with the new TimeZone.

   Run:

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

10. 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.

    Note: This is an optional step only required if needed by an Application.

    Needed Material:

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

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

    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. For each subdirectory created, set the directory's ownership. If you create multiple levels of subdirectories, set the ownership of each level separately, as shown:

```
$ sudo mkdir /usr/TKLC/smac/etc/<dir1>
$ sudo chown pmacd:pmacbackup /usr/TKLC/smac/etc/<dir1>

$ sudo mkdir /usr/TKLC/smac/etc/<dir1>/<dir2>
$ sudo chown pmacd:pmacbackup /usr/TKLC/smac/etc/<dir1>/<dir2>
```

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-xxxx-104-5.0.0_50.8.0-application-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/<path
to files>/* /<path to destination directory>
```

e) Remove the application media from the TVOE host:

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

11. 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 *3.7.5 Step 15*.

12. 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.

13. 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. Additionally, a tpdDefaultRouteNetworkError alarm may 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


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

14. 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: Mon Mar 14 16:12:33 2016
        Product Name: PMAC
     Product Release: 6.2.0.0.0_62.16.0
 Base Distro Product: TPD
 Base Distro Release: 7.2.0.0.0_88.17.0
     Base Distro ISO: TPD.install-7.2.0.0.0_88.17.0-OracleLinux6.7-x86_64.iso
            ISO name: PMACBLD-6.2.0.0.0_62.16.0.iso
                  OS: OracleLinux 6.7
```

15. Logout of the virsh console

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

16. Management Server iLO: Exit the TVOE console.

    Run:

    ```
    $ logout
    ```

    You may now close the iLO browser window.

17. If the NetBackup feature is to be configured on this PM&C, execute *3.7.27 Initialize PM&C Application using the GUI* to initialize the PM&C using the GUI and enable the NetBackup feature.

3.7.6 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.

Prerequisites:

- PM&C has been deployed and initialized, but possibly not fully configured.
- Aggregation switches have been properly configured.

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 *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 guiadmin user.

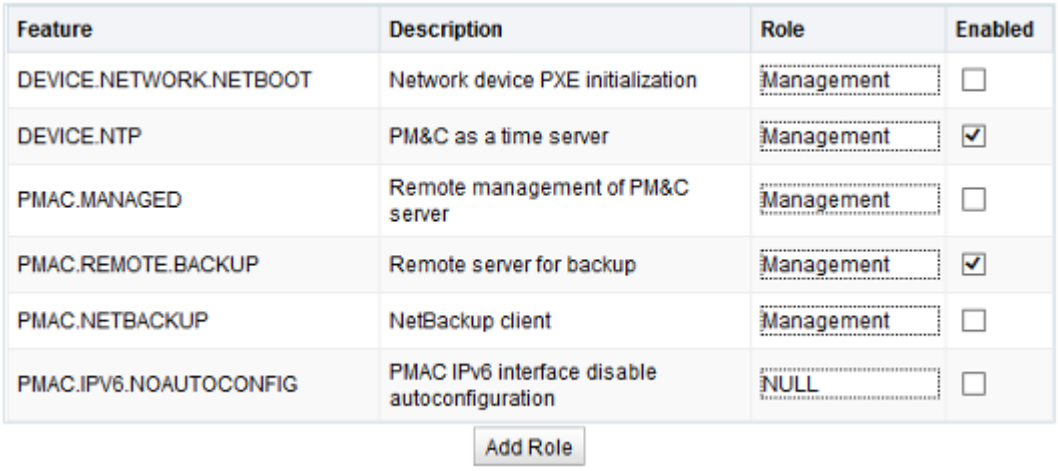
Navigate to **Main Menu** > **Administration** > **PM&C Configuration**.

2. PM&C GUI: Select a profile

   Click on "**Feature Configuration**" in the navigation pane.

3. 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:



Feature	Description	Role	Enabled
DEVICE.NETWORK.NETBOOT	Network device PXE initialization	Management	☐
DEVICE.NTP	PM&C as a time server	Management	☑
PMAC.MANAGED	Remote management of PM&C server	Management	☐
PMAC.REMOTE.BACKUP	Remote server for backup	Management	☑
PMAC.NETBACKUP	NetBackup client	Management	☐
PMAC.IPV6.NOAUTOCONFIG	PMAC IPv6 interface disable autoconfiguration	NULL	☐

Add Role

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.

4. 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.

5. PM&C GUI: Set the User Defined Site Name and the Welcome Message

   Navigate to **Main Menu** > **Administration** > **General Options**

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

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 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:
::
```

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".

3.7.7 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.

Prerequisite: The *3.7.6 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)*.

1. PM&C GUI: Login

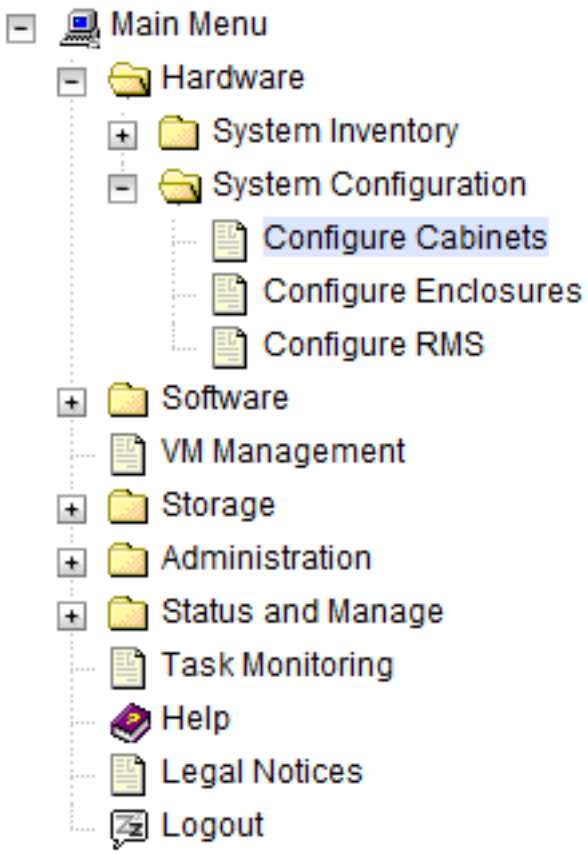
   Open your web browser and enter:

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

   Log in as the guiadmin user.

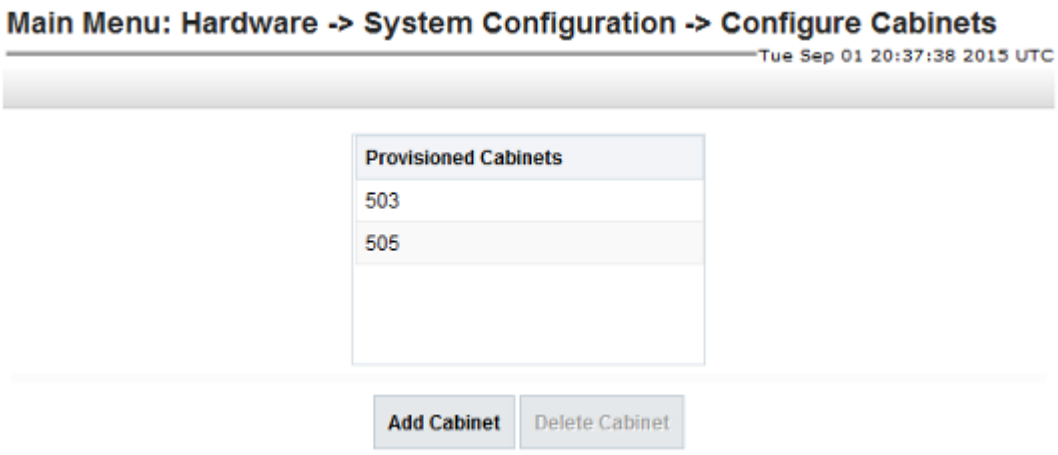
2. PM&C GUI: Navigate to Configure Cabinets

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Cabinets**.



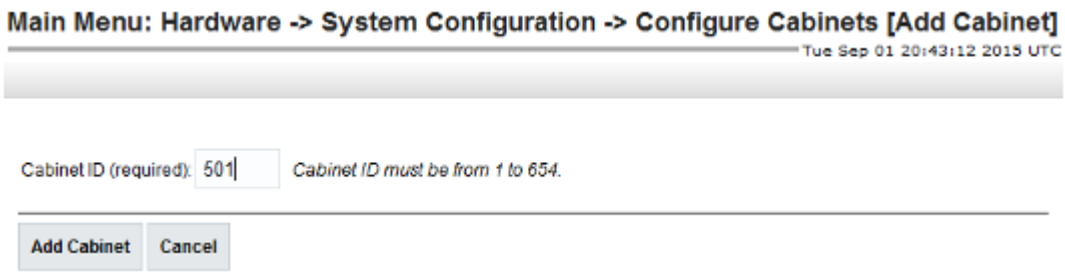
3. PM&C GUI: Add Cabinet

   On the **`Configure Cabinets`** panel, press the **Add Cabinet** button



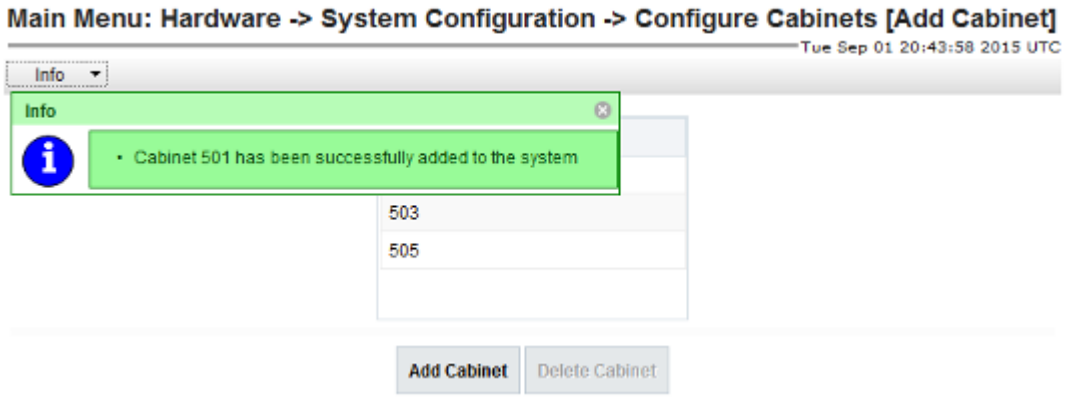
4. PM&C GUI: Enter Cabinet ID

   Enter the **`CabinetID`** and press the **Add Cabinet** button.

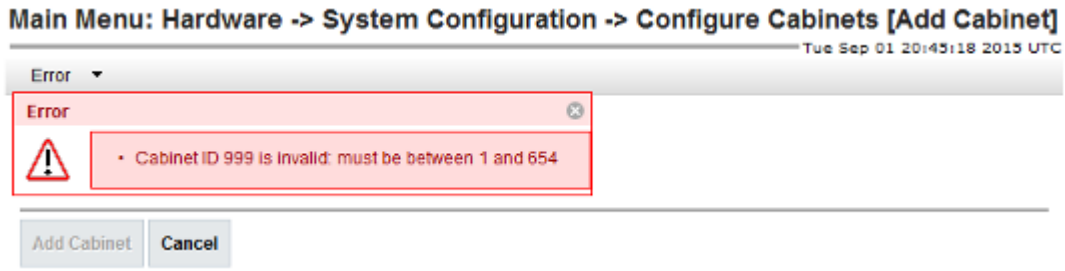


5. PM&C GUI: Check errors

   If no error is reported to the user you will see the following:

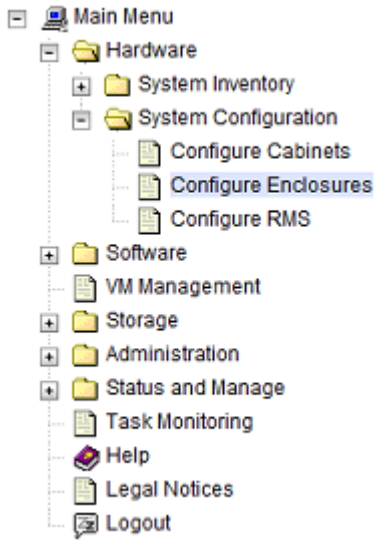


   Or you will see an error message:



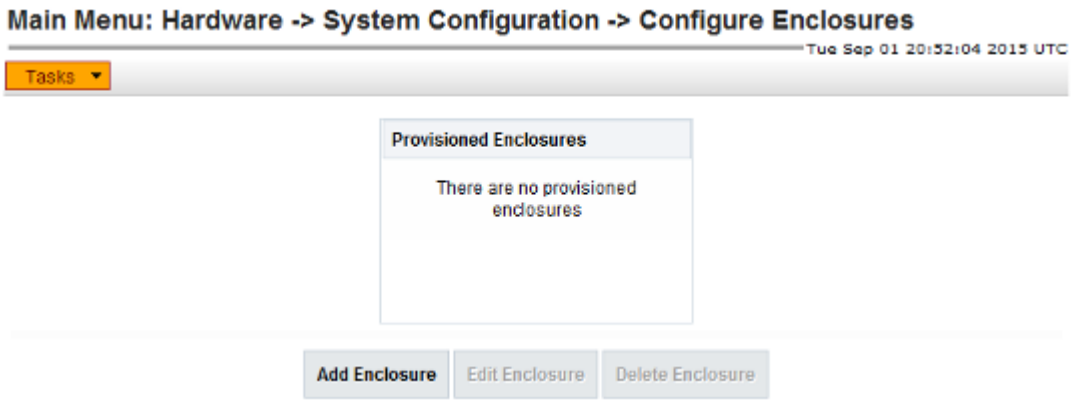
6. PM&C GUI: Navigate to Configure Enclosures

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Enclosures**.



7. PM&C GUI: Add Enclosure

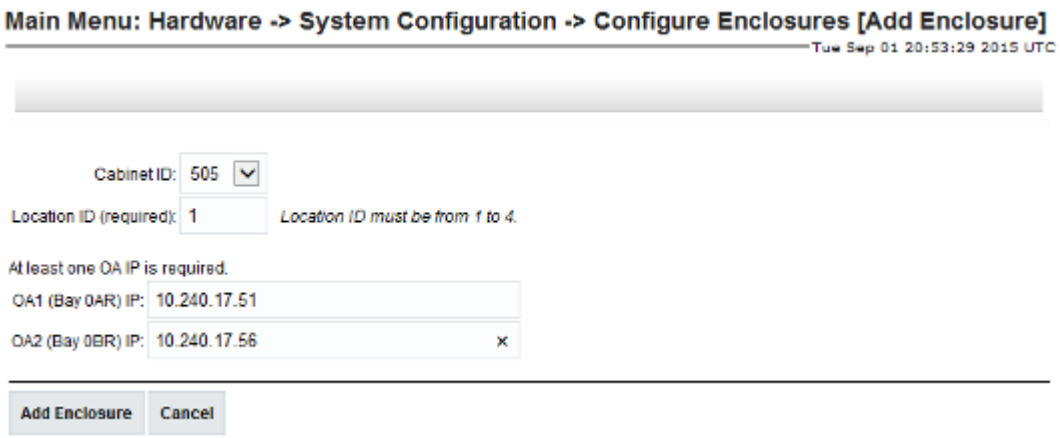
   On the **`Configure Enclosures`** panel, press the **Add Enclosure** button



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).

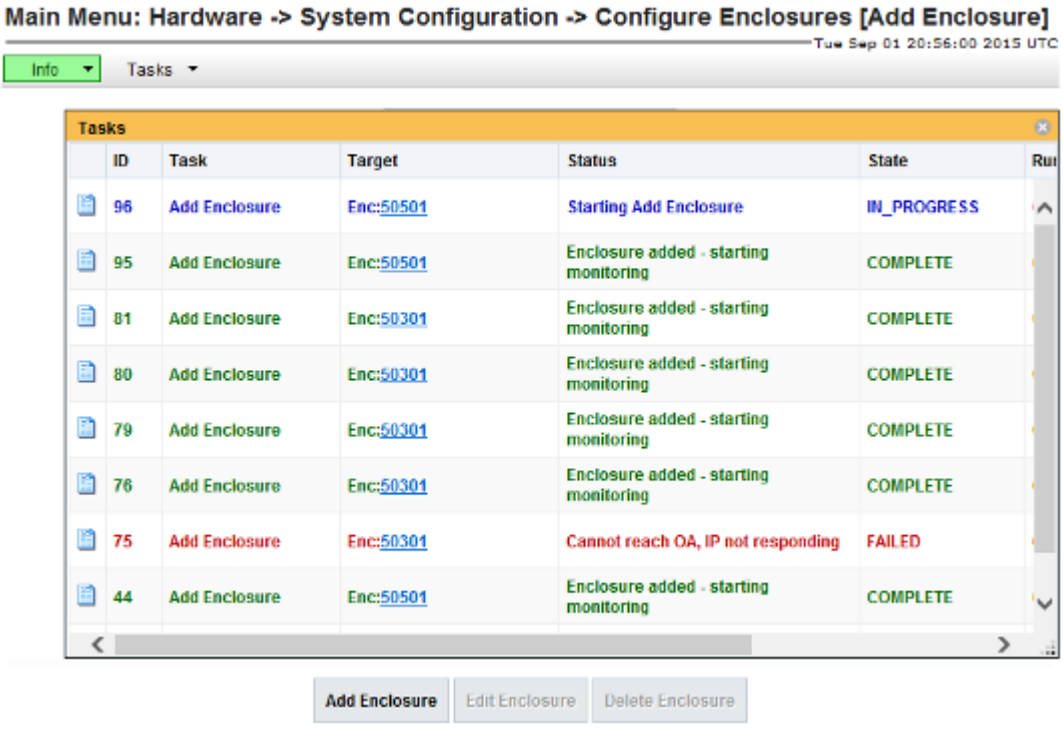
   Then click on **Add Enclosure**.



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%".

3.7.8 Edit an Enclosure in the PM&C System Inventory

This procedure provides the instructions for editing an existing enclosure configuration in the PM&C system inventory. This action is used to notify PM&C of enclosure OA IP address changes.

Prerequisite: The *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure has been completed.

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

1. PM&C GUI: Login

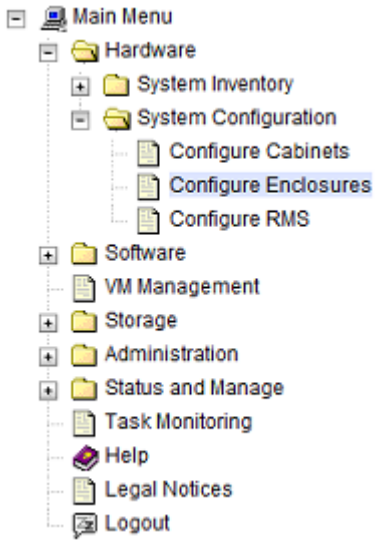
   Open your web browser and enter:

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

   Login as the guiadmin user.

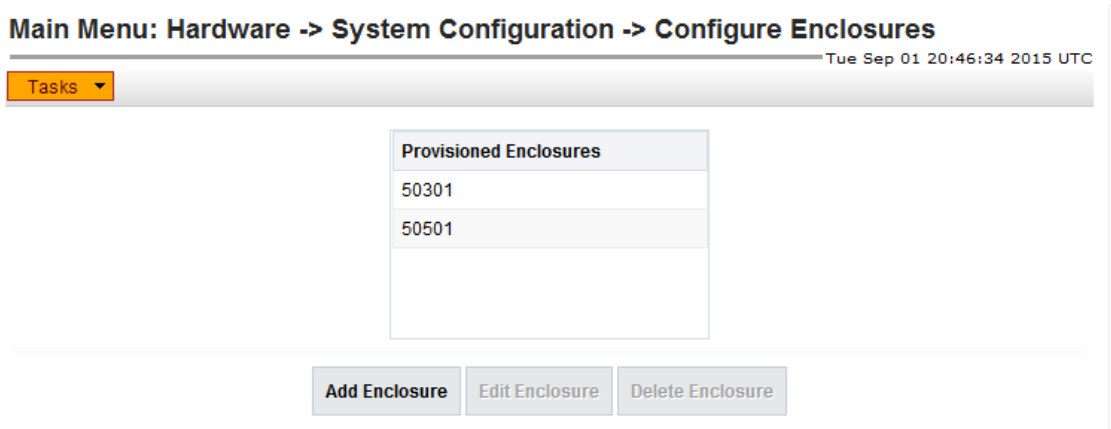
2. PM&C GUI: Navigate to Configure Enclosures

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Enclosures**.



3. PM&C GUI: Edit Enclosure

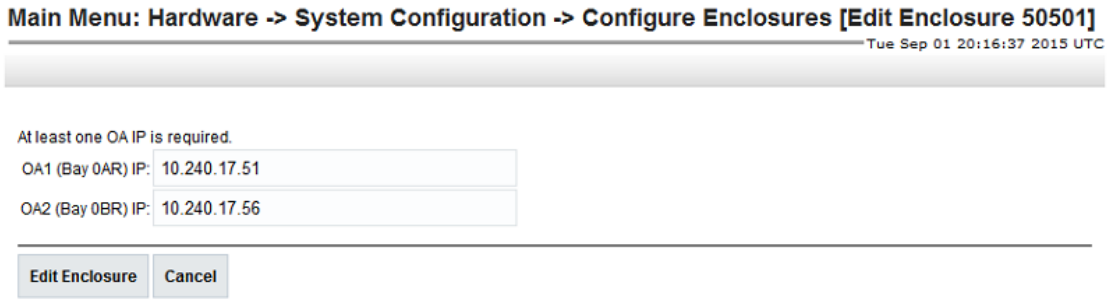
   On the **`Configure Enclosures`** panel, select a row from the list of provisioned enclosures and press the **Edit Enclosure** button



4. PM&C GUI: Modify Enclosure Details

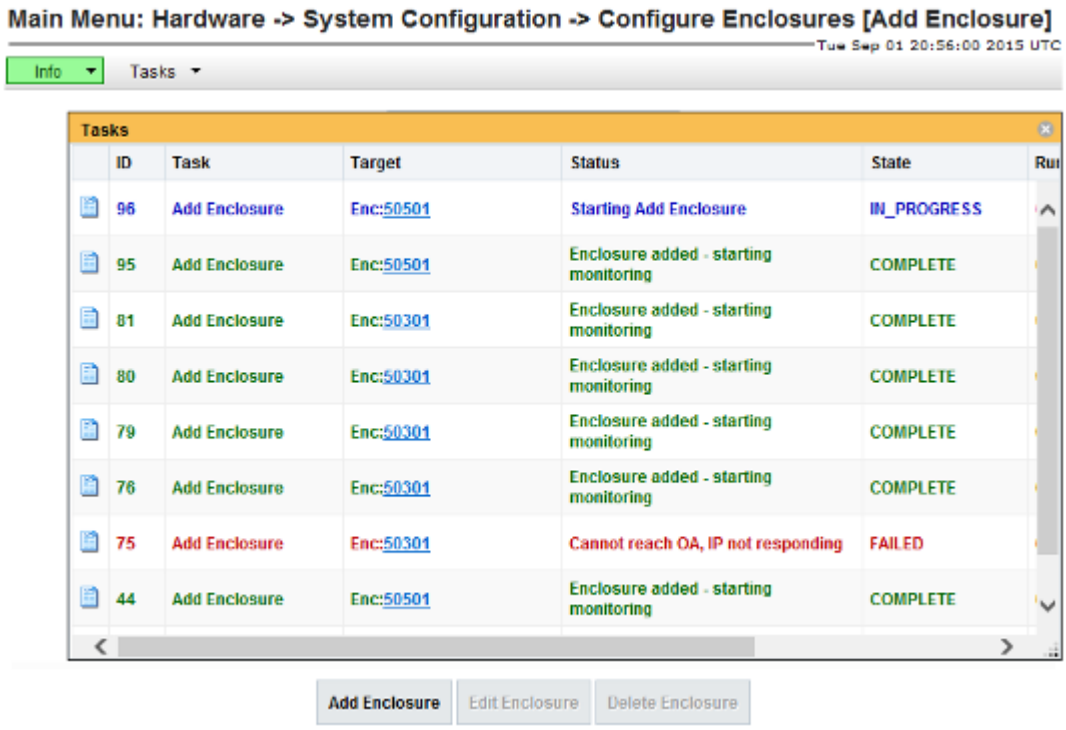
   On the **`Edit Enclosure`** panel, modify the **`OA IP`** addresses as needed.

   Press on the **Edit Enclosure** button.



5. 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%".

3.7.9 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.

Prerequisite: The *3.7.6 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)*.

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.

```
> 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>
   ```

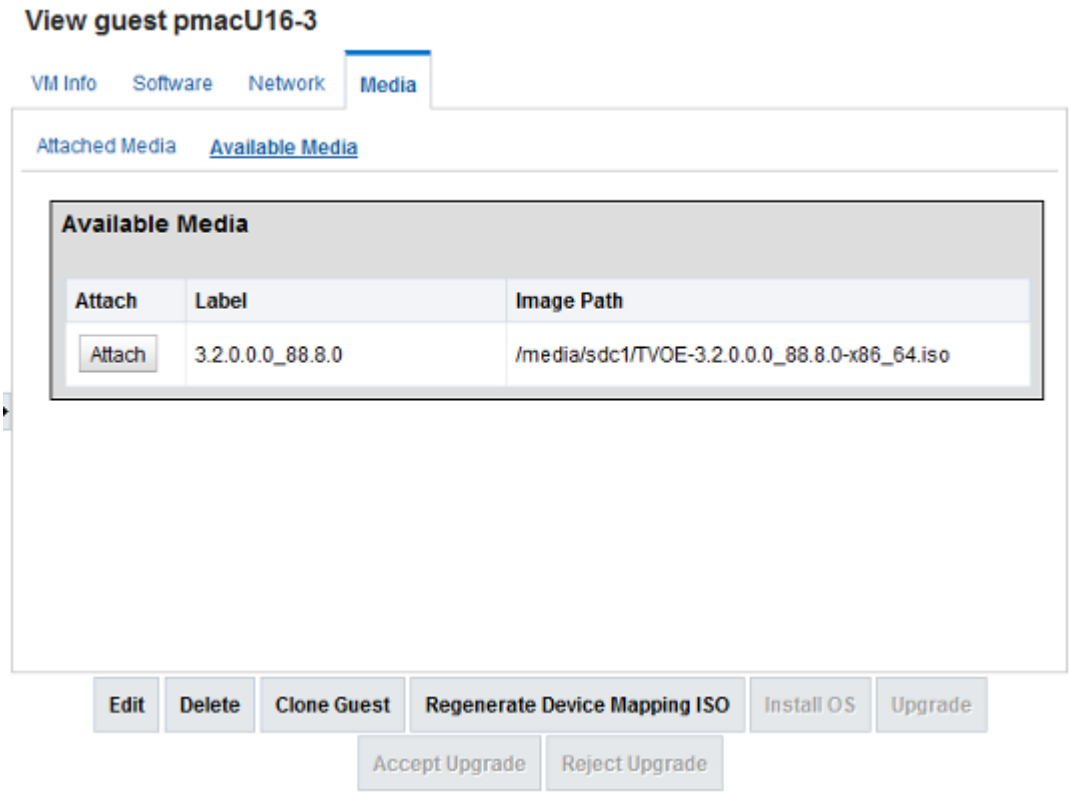
   Login as guiadmin user.

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.

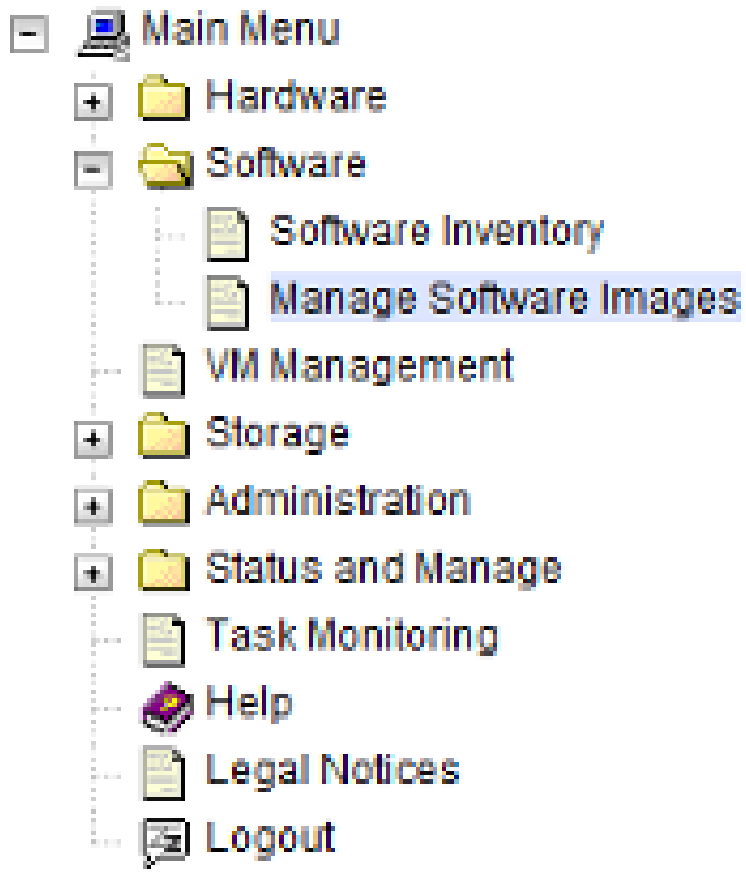
   In the PM&C GUI, navigate to **Main Menu** > **VM Management.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.

   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.

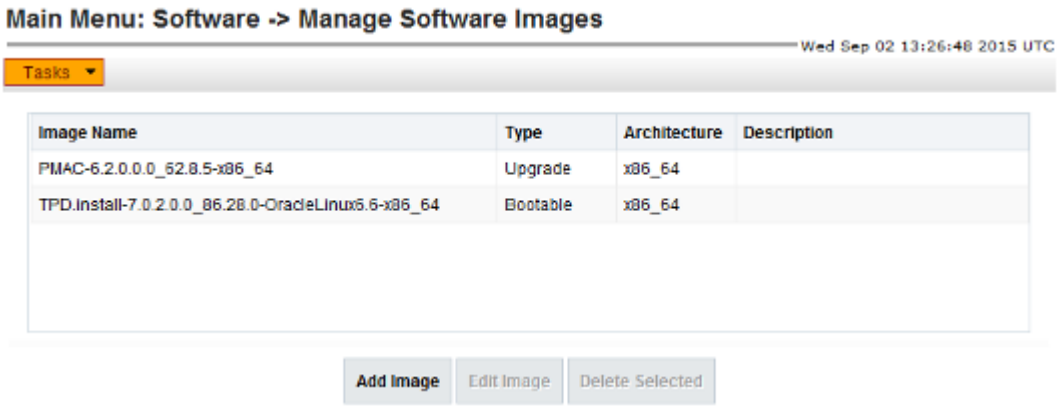


4. PM&C GUI: Navigate to Manage Software Images

   Navigate to **Main Menu** > **Software** > **Manage Software Images**



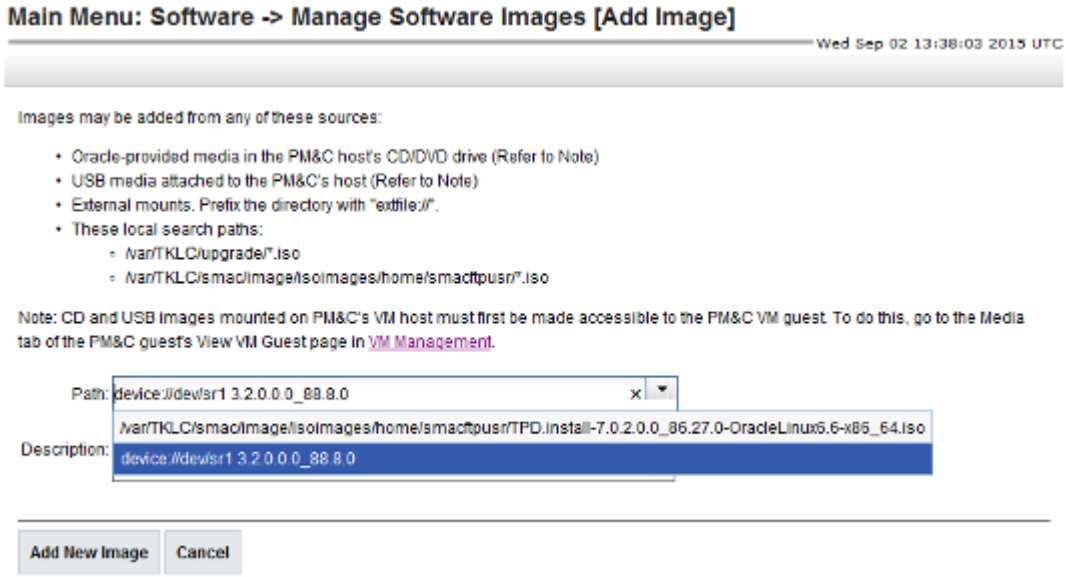
5. PM&C GUI: Add image
   Press the **Add Image** button.



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/...".

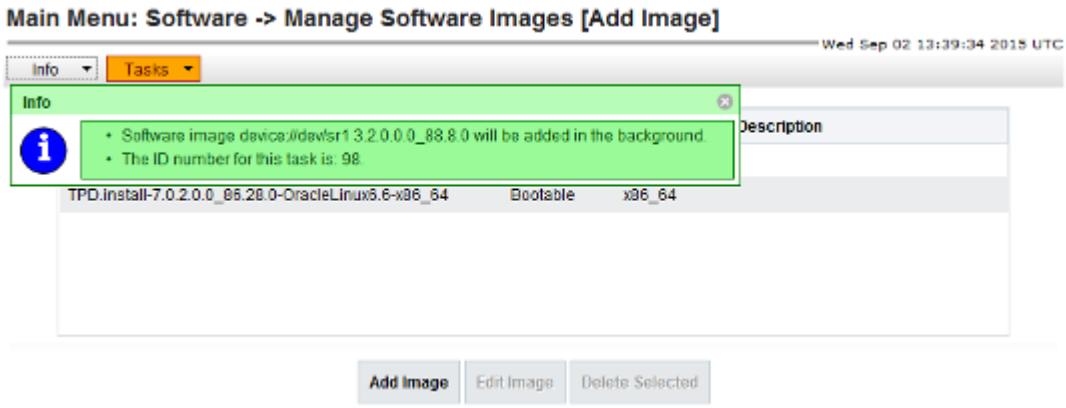
- If the image was supplied on a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest 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.



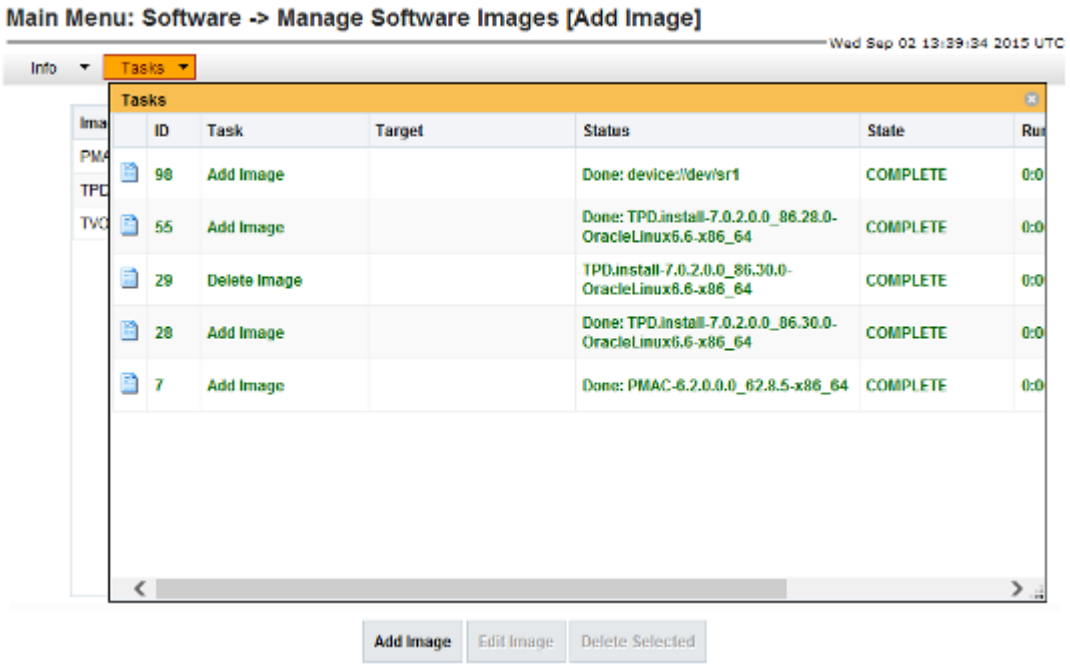
7. PM&C GUI: Monitor the Add Image status

   An Info message, accessible via the Info button, will confirm that a background task has been started to add the image:



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 or source device 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. To confirm that the new image has been attached, reload the page by reselecting the VM guest in the "VM Entities" list and select the **Media** > **Attached Media** subtab. 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.

3.7.10 IPM Servers Using PM&C Application

This procedure provides the steps for installing TPD or TVOE using an image from the PM&C image repository.

Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for IPM have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for IPM have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- A bootable image was added to the PM&C image repository using the *3.7.9 Adding ISO Images to the PM&C Image Repository* procedure.
- The BIOS settings on the servers have been verified using the *3.4.2 Confirm/Upgrade Blade Server BIOS Settings* procedure (for blade servers) or Section 3.2 of TPD Initial Product Manufacture Software Installation Procedure, E53017.

Note: If you are about to IPM as preparation for SAN configuration, follow the *3.8.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation* procedure.

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

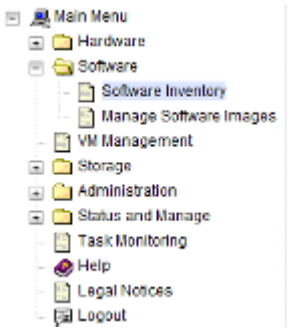
   If needed, open web browser and enter:

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

   Login as the guiadmin user.

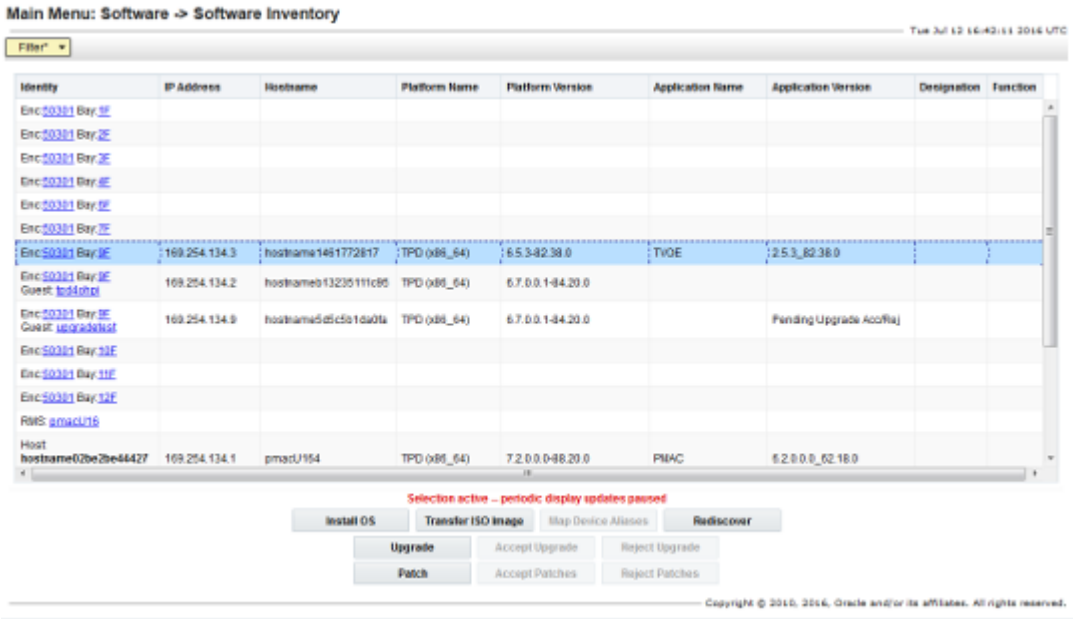
2. PM&C GUI: Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory**.

3. PM&C GUI: Select Servers

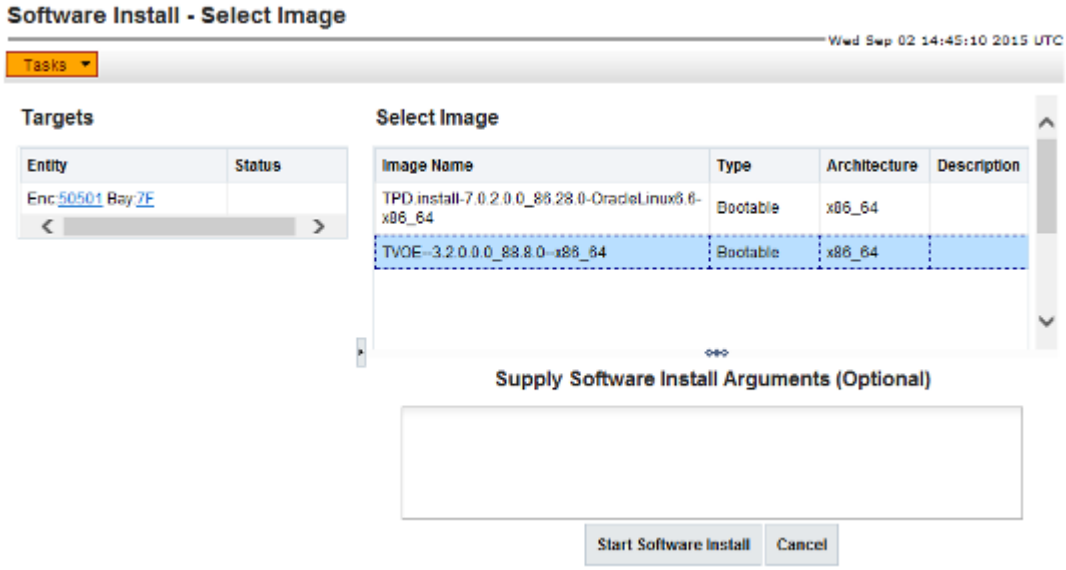
   Select the servers you want to IPM. If you want to install the same OS on more than one server, you may select multiple servers by individually Ctrl-clicking multiple rows. Selected rows will be highlighted.

   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.

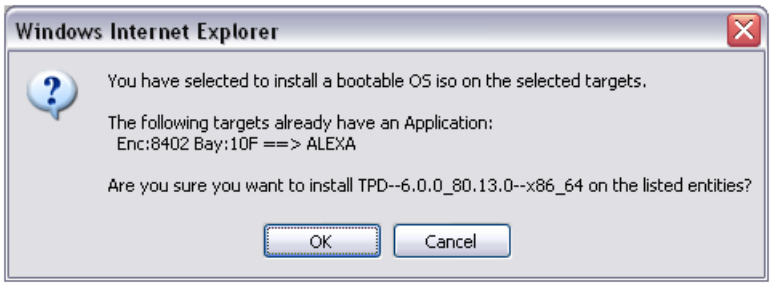
   An example of the optional installation arguments would be: if a target server to be IPM'd includes a 10G FLOM and the control bond has to be moved to it's NIC card, the user would include the optional argument 'control_if=eth05,eth06' in the 'Supply Software Install Arguments (Optional)' text area.

6. PM&C GUI: Start Install

   Press the **Start Install** button.

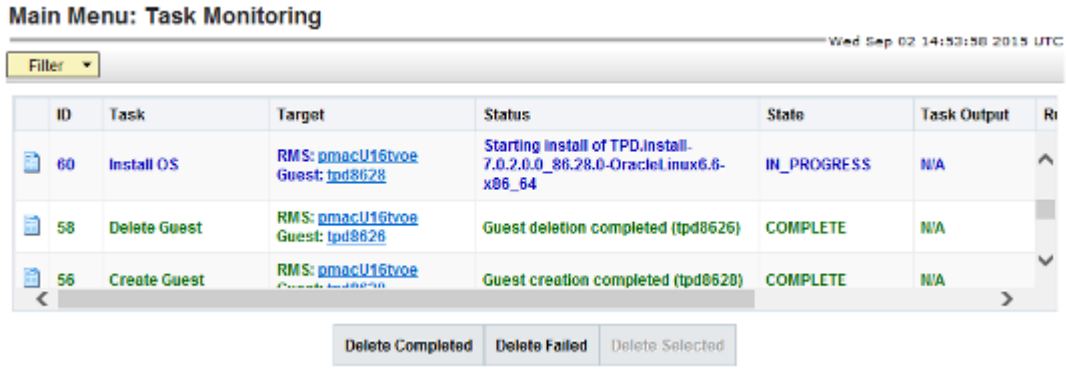
7. PM&C GUI: Confirm OS Install

   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.

3.7.11 Install/Upgrade Applications Using PM&C

This procedure provides the steps for performing an application install/upgrade using an image from the PM&C image repository.

Prerequisites:

- Enclosures containing blade servers or servers containing a TVOE host targeted for application install/upgrade have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for application install/upgrade have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- An upgradable image was added to the PM&C image repository using the *3.7.9 Adding ISO Images to the PM&C Image Repository* procedure.

Note: Firmware update is only supported for HP c-Class blades and Rack Mount Servers.

Note: Until the target servers are fully discovered by PM&C, the user will be unable to install patches on the servers (this might take up to 15 minutes after the upgrades complete).

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

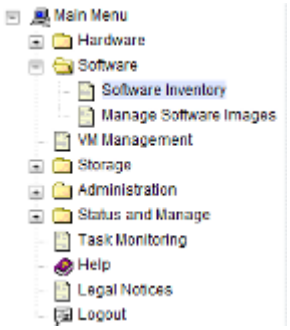
   If needed, open your web browser and enter:

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

   Login as the guiadmin user.

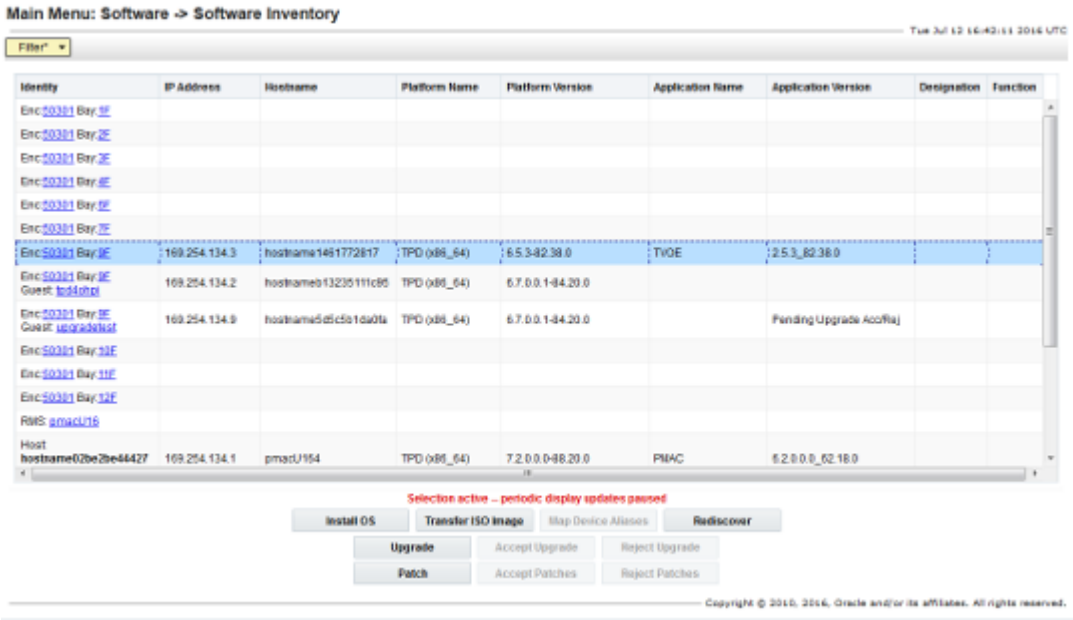
2. PM&C GUI: Navigate to the Software Inventory

Navigate to **Main Menu** > **Software** > **Software Inventory**.



3. PM&C GUI: Select Servers

   Select the servers you want to upgrade. If you want to perform an upgrade on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted in green.

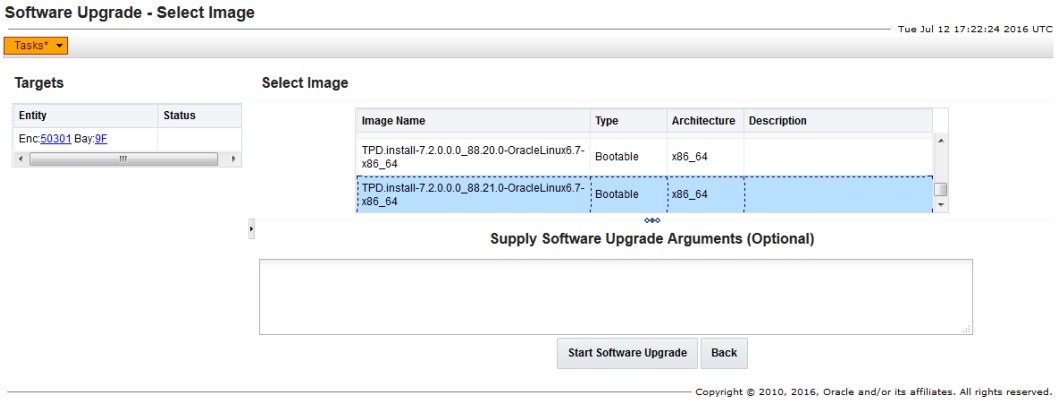


   Press the **Upgrade** button.

   Note: Until the target servers are fully discovered by PM&C, the user will be unable to start an application install or upgrade on the servers (this may take up to 15 minutes after the OS Installs complete). A server that has not yet been discovered is represented by an empty row on the Software Inventory page (no IP address, hostname, plat name, plat version, etc. is displayed).

4. PM&C GUI: Select Image

   The left side of the screen displays the servers to be upgraded. From the list of upgrade images on the right side of the screen, select the image to install on the selected servers.



5. PM&C GUI: Supply Upgrade Arguments (Optional)

   Upgrade arguments can be supplied by entering them into the text box displayed under the list of upgrade images. Each upgrade argument must be of the form **key=value** and supported by the version of TPD that the application being installed/upgraded is based on. Multiple arguments must be separated by spaces or entered on new lines. If no upgrade arguments need to be supplied for the application being installed/upgraded, leave the upgrade arguments text box empty.

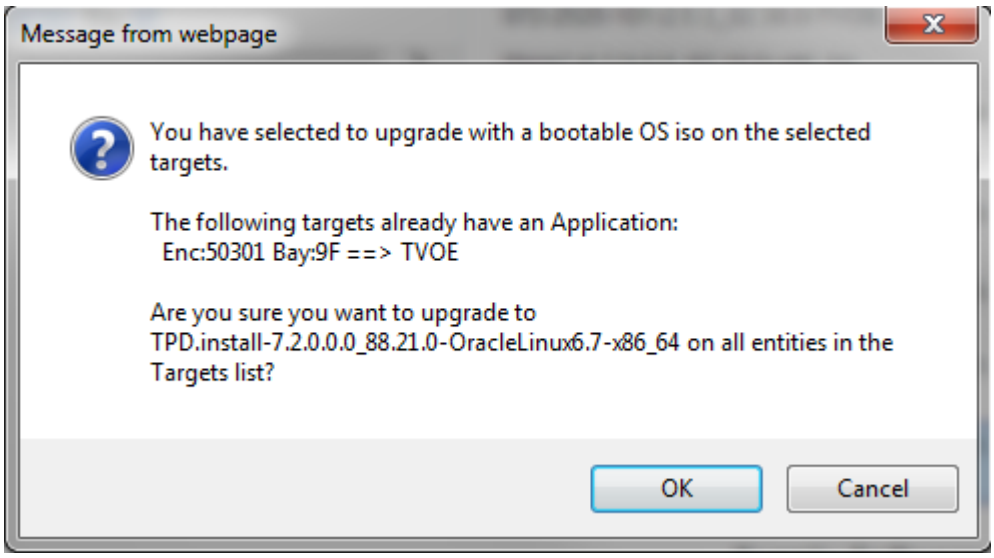
   Note: PM&C does not validate supplied firmware update arguments.

6. PM&C GUI: Start Upgrade

   Press the **Start Upgrade** button.

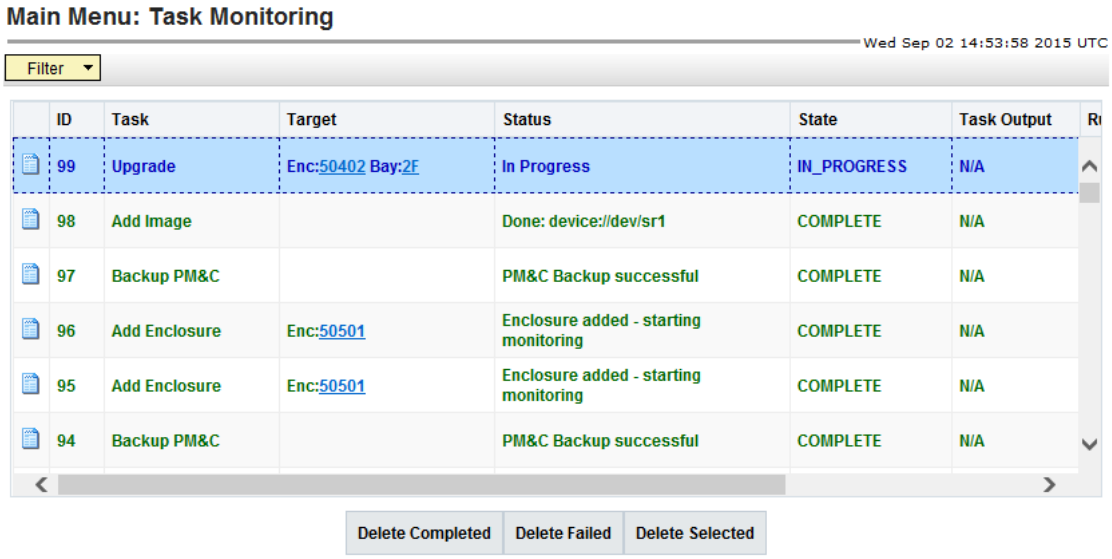
7. PM&C GUI: Confirm Upgrade

   Press the **OK** button to proceed with the upgrade.



8. PM&C GUI: Monitor Upgrade

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Upgrade background task. A separate task will appear for each server being upgraded.



When the task is complete and successful its text will change to green and its Progress column will indicate "100%".

9. PM&C GUI: Verify that the installed/upgraded application is fully functional. The application must provide the steps necessary for verifying its functionality.
10. PM&C GUI: Accept or Reject Upgrade (Platform 6.x Applications Only)

    If the application you just upgraded or installed is based on a TPD 6.x release, you must either accept or reject the upgrade. To accept an upgrade using PM&C, perform the *3.7.19 Accepting Upgrades Using PM&C* procedure. Likewise, to reject an upgrade using PM&C, perform the *3.7.20 Rejecting Upgrades Using PM&C* procedure.

3.7.12 Patch Applications Using PM&C

This procedure provides the steps for performing an application patch using an image from the PM&C image repository.

Prerequisites:

- Enclosures containing blade servers or servers containing a TVOE host targeted for application patch have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for application patch have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- A patch image was added to the PM&C image repository using the *3.7.9 Adding ISO Images to the PM&C Image Repository* procedure.
- The target servers have been IPM'd with an application based on a TPD release supported by PMAC 6.3.

Note: Until the target servers are fully discovered by PM&C, the user will be unable to install patches on the servers (this might take up to 15 minutes after the upgrades complete).

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

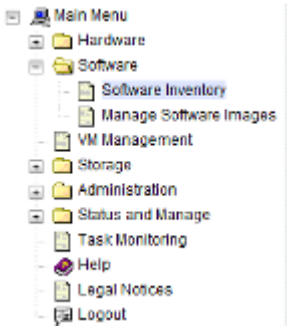
   If needed, open your web browser and enter:

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

   Login as the guiadmin user.

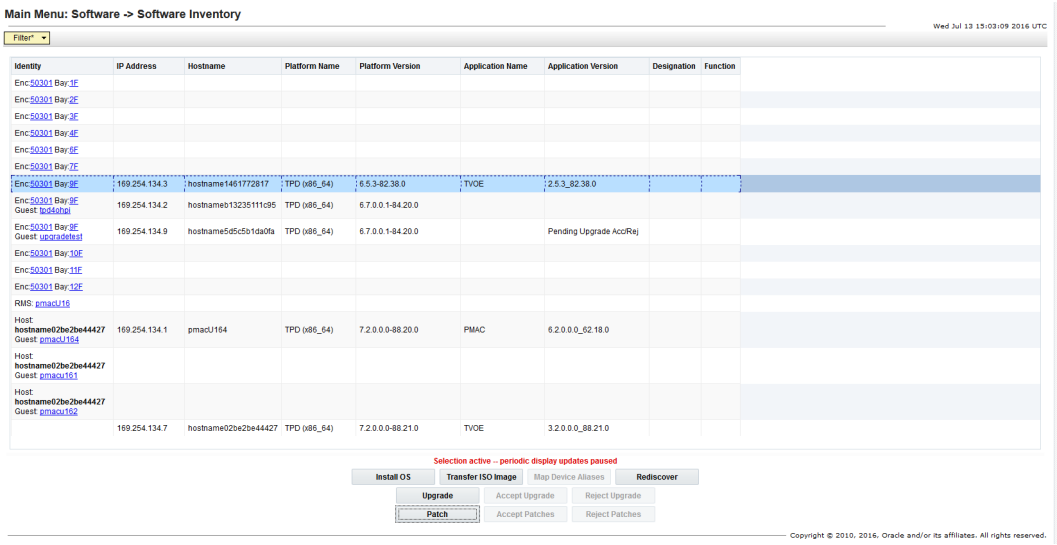
2. PM&C GUI: Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory**.



3. PM&C GUI: Select Servers

   Select the servers you want to patch. If you want to perform a patch on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted in blue.

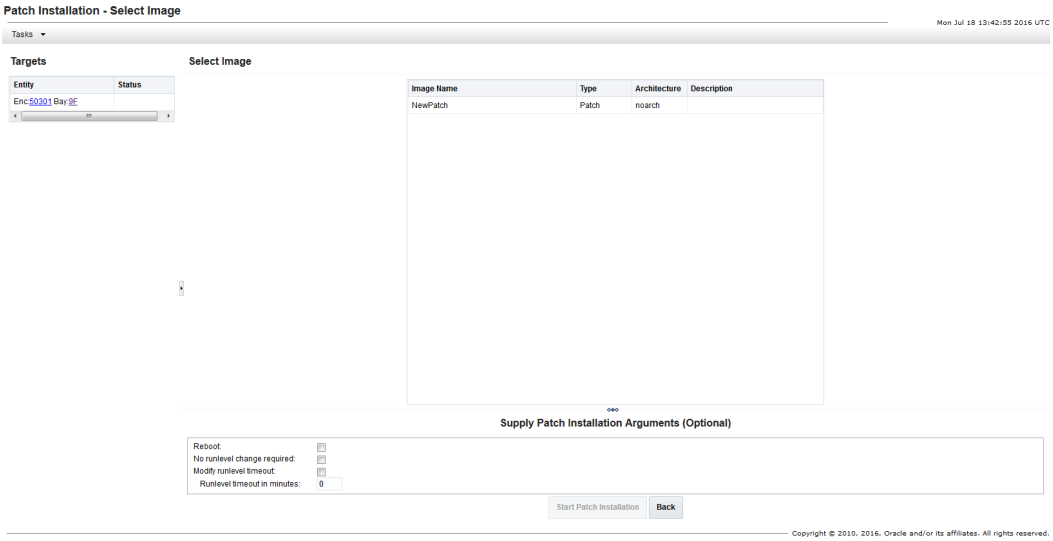


   Press the **Patch** button.

   Note: Until the target servers are fully discovered by PM&C, the user will be unable to install patches on the servers (this might take up to 15 minutes after the OS Installs complete). A server that has not yet been discovered is represented by an epty row on the Software Inventory page (no IP address, hostname, plat name, plat version, etc. is displayed).

4. PM&C GUI: Select Image

The left side of the screen displays the servers to be patched. From the list of patch images on the right side of the screen, select the image to install on the selected servers.



5. PM&C GUI: Supply Patch Installation Arguments (Optional)

   There are three optional arguments that can be specified as part of a patch. These are located on the bottom of the Select Image page.

   The first option is **Reboot**. If this is enabled, the patched server will reboot once the patch installation has completed. The second option is **No runlevel change required**. If this is enabled, the patched server will not transition from runlevel 4 to 3 prior to installing the patch. This means that applications running on the server will not be halted during the patch installation. The third option is **Modify runlevel timeout**. If this is enabled, a custom runlevel timeout can be specified in the box below this option. This timeout (in minutes) determines how long the patching process will wait for a runlevel transition from 4 to 3 before the installation is aborted.

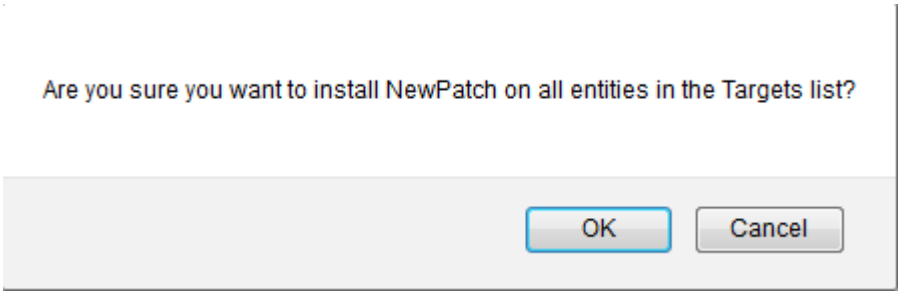
   Any of these options can be specified as the sole option. Additionally, **Reboot** and **Modify runlevel timeout** may be specified together. **No runlevel change required** cannot be specified with either of the other options.

6. PM&C GUI: Start Patch Installation

   Press the **Start Patch Installation** button.

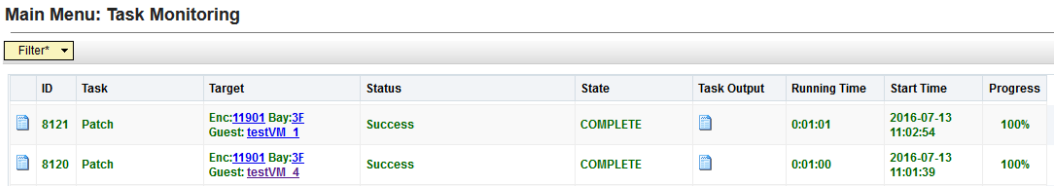
7. PM&C GUI: Confirm Patch

   Press the **OK** button to proceed with the patch.



8. PM&C GUI: Monitor Patch

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Patch background task. A separate task will appear for each server being patched.



   When the task is complete and successful, its text will change to green and its Progress column will indicate "100%".

9. PM&C GUI: Verify the Patch Installation.

   The application must provide the steps necessary for verifying that the patch is fully functional.

10. PM&C GUI: Accept or Reject Patch

    If the application you just patched is based on a TPD 7.2 or newer release, you must either accept or reject the patch. To accept a patch using PM&C, perform the *3.7.21 Accepting Patches Using PM&C* procedure. Likewise, to reject a patch using PM&C, perform the *3.7.22 Rejecting Patches Using PM&C* procedure.

3.7.13 Install PM&C on Redundant DL360 or DL380

This procedure is optional and required only if the redundant PM&C Server feature is to be deployed.

This procedure will provide the instructions for installing and configuring TVOE on a redundant DL360 or DL380 server and deploying a redundant PM&C, as well as creating the first backup from the primary PM&C.

Prerequisites:

- *3.7.9 Adding ISO Images to the PM&C Image Repository* has been completed using the TVOE media.
- *3.7.9 Adding ISO Images to the PM&C Image Repository* has been completed using the PM&C media. Make note of the PM&C Image Name; it will be used during the procedure as <PMAC_Image_Name>.
- *3.7.10 IPM Servers Using PM&C Application* has been completed on the redundant management server using the TVOE media.
- *3.7.3 TVOE Network Configuration* has been completed for the redundant management server.

Note: In the event a disaster recovery is required, refer to the recovery procedure in 909-2210-001.

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.

Note: It is assumed that the use of a redundant PM&C means the NetBackup feature is not in use.

1. Redundant Management Server iLO: Log in to the redundant management server on the remote console.

   Log in to the TVOE as admusr using *F.1 How to Access a Server Console Remotely*.

   Log in to iLO in IE using the password provided by application:

   ```
   http://<redundant_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. Primary Management Server iLO: Log in to the primary management server on the remote console.

   Log in to the primary PM&C guest as admusr using the virsh console.

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

   virsh # console pmacU17-1

   [Output Removed]

   pmacU17-1 login:
   ```

3. Primary PM&C: Export the PM&C ISO image to the Redundant Management Server's address on the control network.

   ```
   $ sudo /usr/sbin/exportfs
   <redundant_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name>
   $
   ```

4. Redundant Management Server TVOE: Mount the PM&C upgrade media from the PM&C server.

   ```
   $ sudo /bin/mount
   <primary_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name> /mnt/upgrade
   $
   ```

5. Redundant Management Server TVOE: Using the pmac-deploy script, deploy the PM&C instance using the configuration detailed by the completed NAPD. All configuration options (NetBackup or isoimagesVolSizeGB) should match the configuration of the primary PM&C.

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

   ```
   $ cd /mnt/upgrade/upgrade
   $ sudo ./pmac-deploy --guest=<Redundant_PMAC_Name>
   --hostname=<Redundant_PMAC_Name> --controlBridge=<TVOE_Control_Bridge>
   --controlIP=<Redundant_PMAC_Control_ip_address>
   --controlNM=<PMAC_Control_netmask>
   --managementBridge=<PMAC_Management_Bridge>
   --managementIP=<Redundant_PMAC_Management_ip_address>
   --managementNM=<PMAC_Management_netmask_or_prefix
   ```

```
--routeGW=<PMAC_Management_gateway_address>
--ntpserver=<Redundant_TVOE_Management_server_ip_address>
--isoimagesVolSizeGB=20
```

6. 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.
7. Redundant Management Server TVOE: Unmount the media.

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

8. Perform *3.7.5 Setup PM&C* on the Redundant PM&C.

Warning: Initialization of the redundant PM&C is to be avoided at all costs

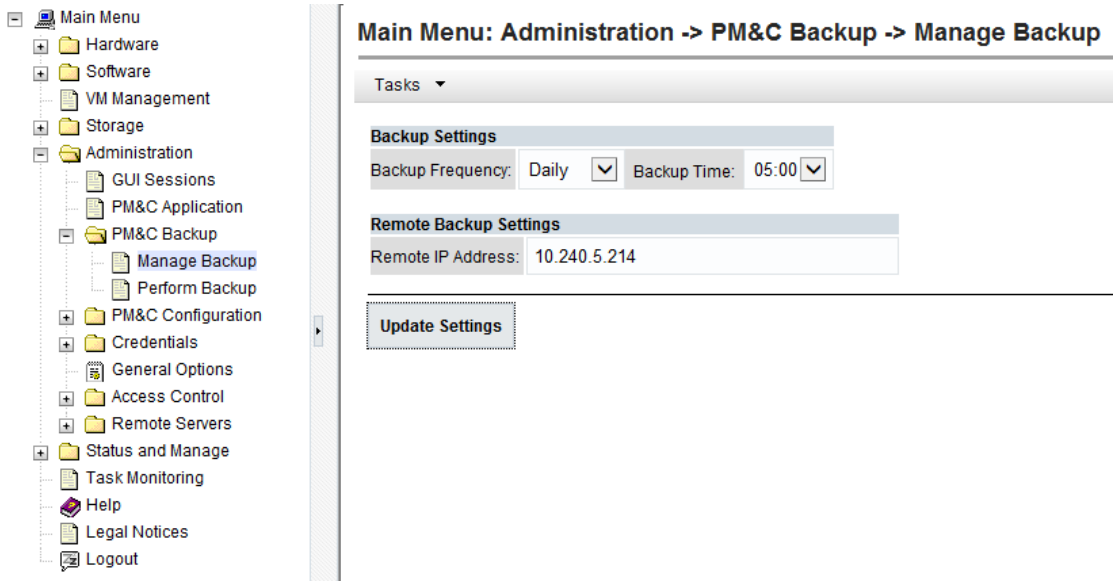
9. Primary PM&C Server GUI: Log in

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

Log in as **guiadmin** user.

10. Primary PM&C Server GUI: Configure the primary PM&C to send backups to the redundant PM&C

Navigate to **Main Menu** > **Administration** > **PM&C Backup** > **Manage Backup**



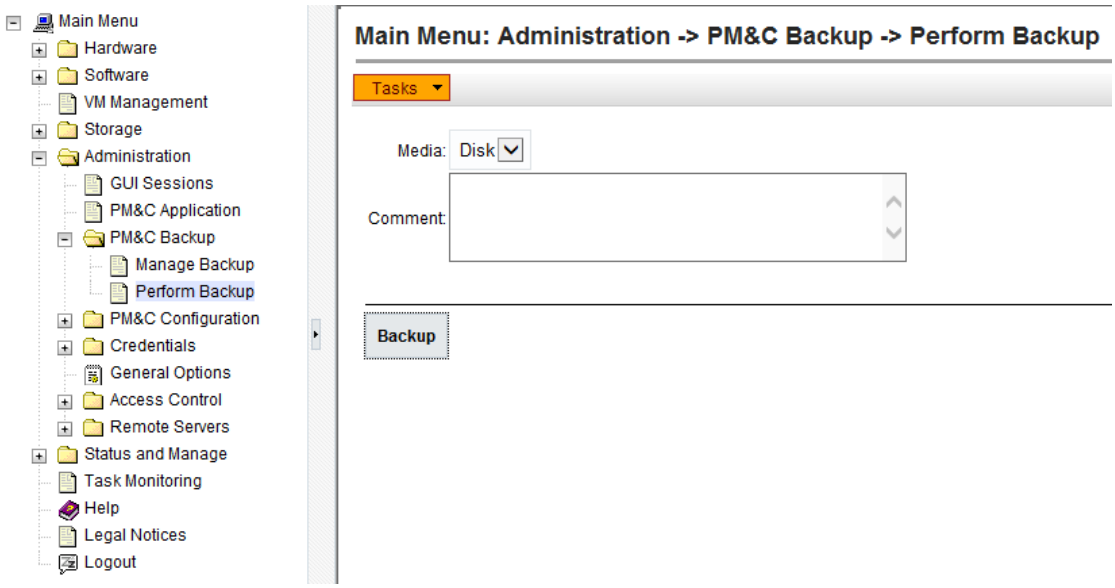
On the **Manage Backup** panel, enter the IP address of the redundant PM&C (redundant_management_server_mgmtVLAN_IP) and click on **Update Settings**.

11. Primary PM&C Server GUI: Verify update was successful

Click on the **Task Monitoring** link to monitor the Update PM&C Backup Data status. Verify the task completes successfully.

12. Primary PM&C Server GUI: Perform initial backup to the redundant PM&C server

    Navigate to **Main Menu** > **Administration** > **PM&C Backup** > **Perform Backup**.



    Select "**Remote Server**" from the drop down media, enter any desired comment and click **Backup**.

13. Primary PM&C Server GUI: Verify the backup was successful

    Click on the Task Monitoring link to monitor the Backup PM&C status. Verify the task completes successfully.

    Note: This backup copies the existing PM&C backup files and all of the images added to the PM&C image repository from the primary PM&C Server to the redundant PM&C Server.

14. Primary PM&C: Unexport the PM&C ISO image.

```
$ sudo /usr/sbin/exportfs -u
<redundant_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name>
$
```

3.7.14 Configure Management Server SNMP Trap Target

This procedure will configure SNMP settings for the Management Server.

Prerequisites:

- The *3.7.6 Configure PM&C Application* procedure has been completed.
- Knowing the IP address of the target NMS Server(s) for SNMP traps.

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. Perform the steps to add an SNMP trap destination.

   Perform the steps in *3.10.3 Add SNMP trap destination on TPD based Application*, logging into the Management Server and providing the IP address of each trap destination(s).

2. Ensure the PM&C MIB is available to the SNMP trap destination

   PM&C specific MIB files are located in the `/usr/TKLC/smac/etc/mib` directory on the Management Server.

   The file of interest is `pmacAppAlarms.mib`.

3.7.15 PM&C NetBackup Client Installation and Configuration

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

Prerequisites:

- The PM&C application must be initialized, or subsequent to the initialization configured with the NetBackup Feature enabled. Additionally the appropriate NetBackup network configuration for this system must be completed.
  - *3.7.23 Initialize PM&C Application*, or *3.7.6 Configure PM&C Application*

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

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

   Execute *3.7.24 Configure PM&C Application Guest NetBackup Virtual Disk*.

2. TVOE Management Server iLO: Log in with PM&C admusr credentials

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

   Log into 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: 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 the output is incorrect, then there is likely 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.

   Log into 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 *3.10.5 Application NetBackup Client Install Procedures*.

   Note: The following data is required to perform the *3.10.5 Application NetBackup Client Install Procedures*:

   - Netbackup support:
     - PM&C 5.7.0 supports Netbackup client software versions 7.1 and 7.5.
     - PM&C 5.7.1 through PM&C 6.3 supports Netbackup client software versions 7.1, 7.5, and 7.6.
     - PM&C 6.4 supports Netbackup client software versions 7.1, 7.5, 7.6, and 7.7.
   - The PM&C is a 64 bit application.
   - 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 *3.10.5 Application NetBackup Client Install 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.

3.7.16 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 *3.7.6 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:

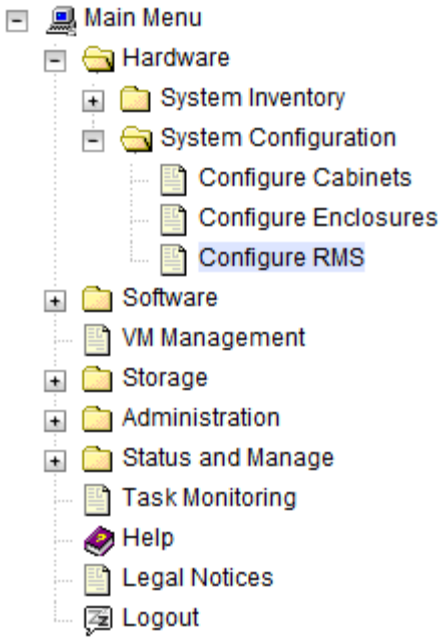
   ```
   https://<pmac_management_network_ip>
   ```

2. PM&C GUI: Configure Cabinet (optional)

   If this is a RMS installation only or a cabinet has not been previously configured, perform steps *3.7.7 Step 2* through *3.7.7 Step 5* of procedure *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* to add one or more cabinets.

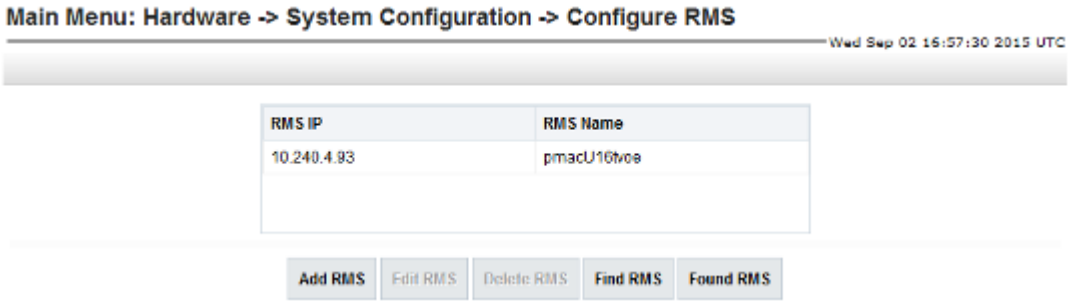
3. PM&C GUI: Configure RMS

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure RMS**



4. PM&C GUI: Add RMS

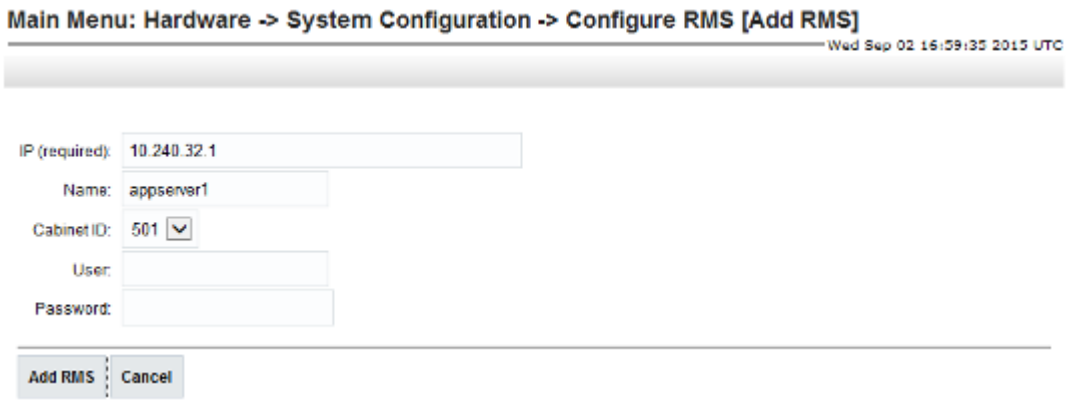
   On the Configure RMS panel, click the Add RMS button.



5. PM&C GUI: Enter information

   Enter the IP Address of the rack mount server management port (iLO) in the specified field. In the User field enter user "root" and in the Password field enter the password for the iLO root user. All the other fields are optional.

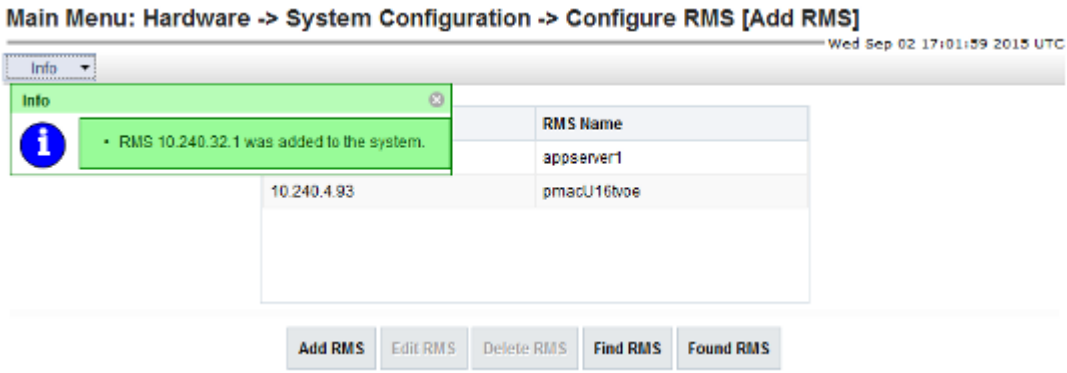
   Then click on the **Add RMS** button.



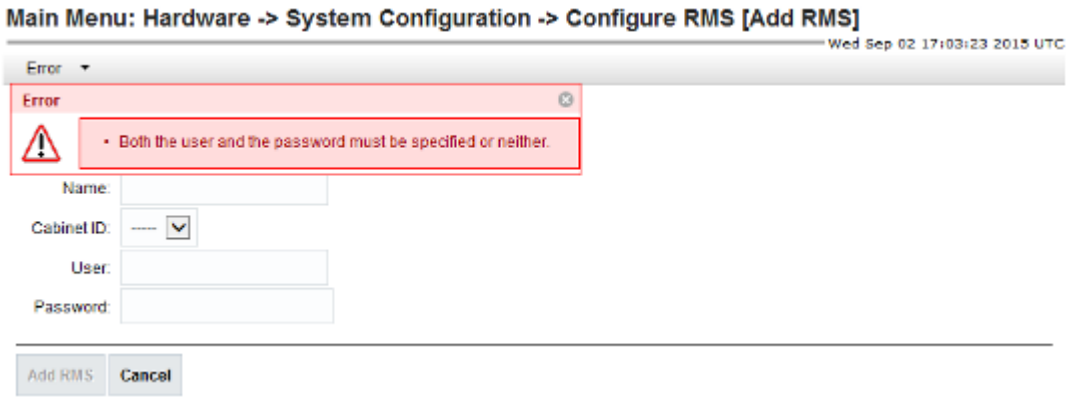
Note: If the initial iLO credentials provided by Oracle have been changed, enter valid credentials (not to be confused with OS or Application credentials) for the rack mount server management port.

6. PM&C GUI: Check errors

   If no error is reported to the user you will see the following:

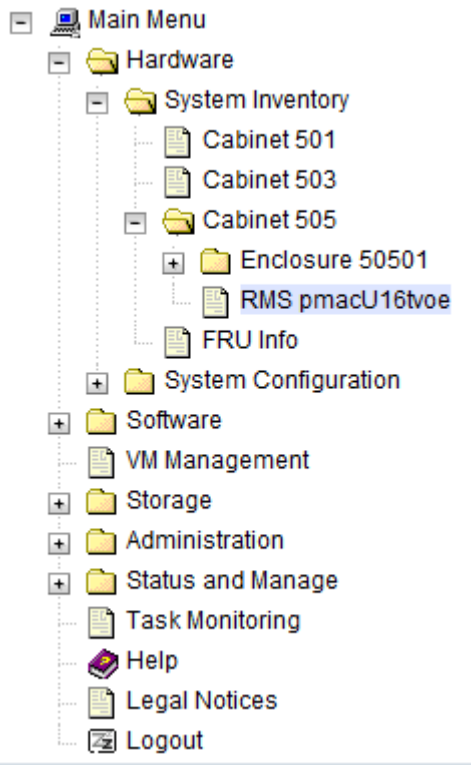


   Or you will see an error message:

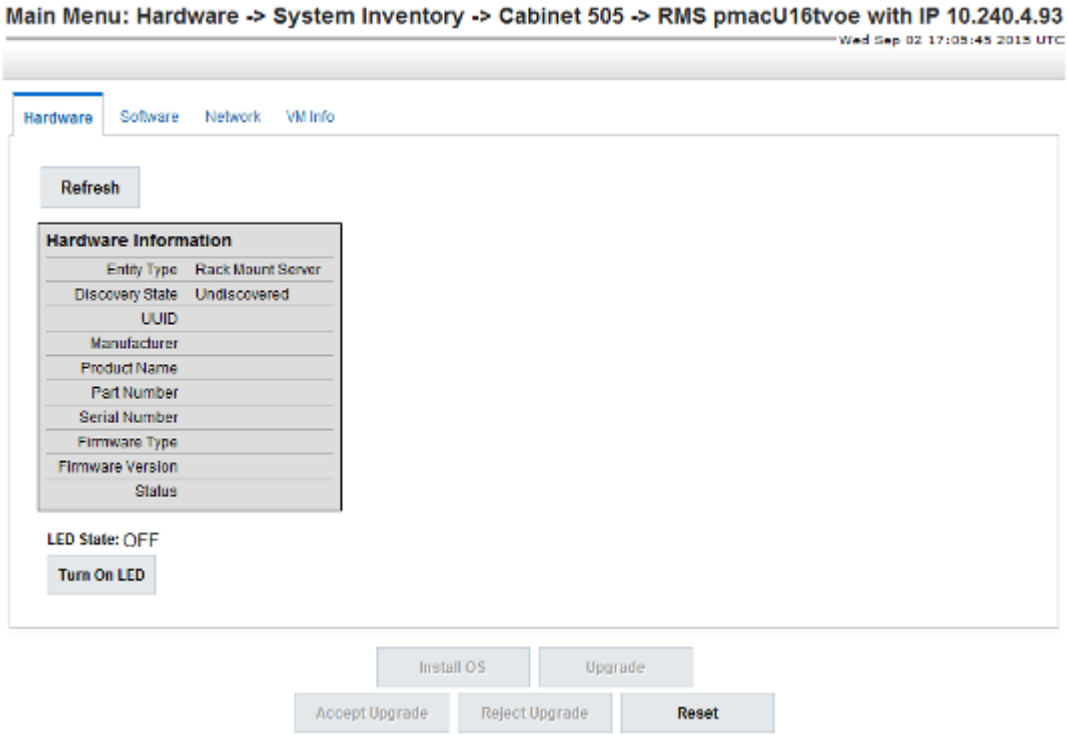


7. PM&C GUI: Verify RMS discovered

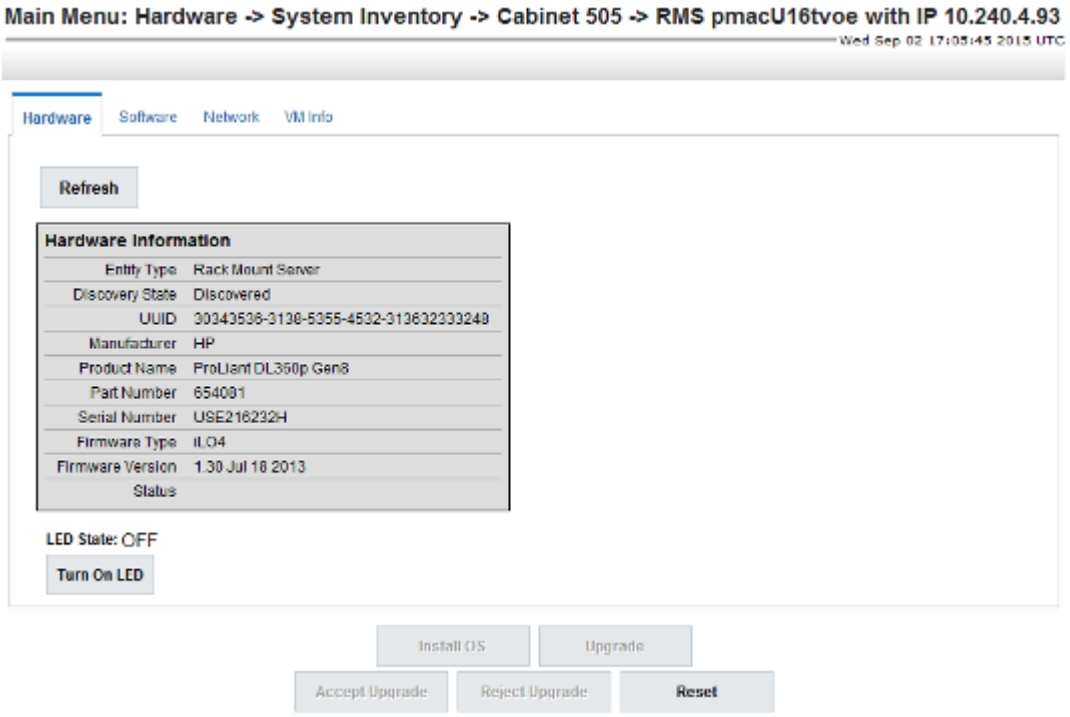
   Navigate to **Main Menu** > **Hardware** > **System Inventory** > **Cabinet xxx** > **RMS yyy** Where "xxx" is the cabinet id selected when adding RMS (or "unspecified") and "yyy" is the name of the RMS.



The RMS inventory page is displayed.



Periodically refresh the hardware information using the Refresh button until the "Discovery state" changes from "Undiscovered" to "Discovered". If "Status" displays an error, contact My Oracle Support for assistance.



3.7.17 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.

Prerequisite:

- *3.7.16 Add Rack Mount Server to the PM&C System Inventory* 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)*.

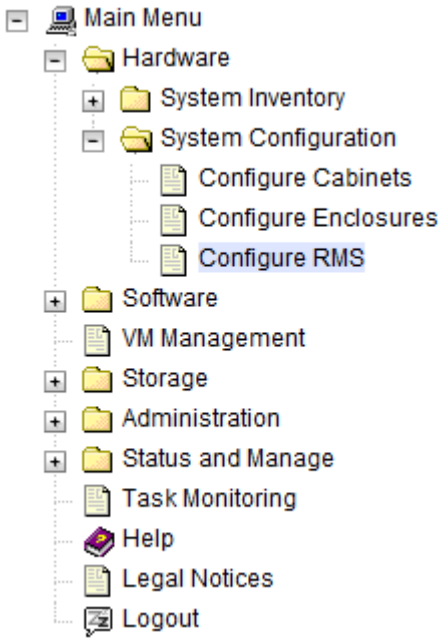
1. PM&C GUI: Login

   Open web browser and enter:

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

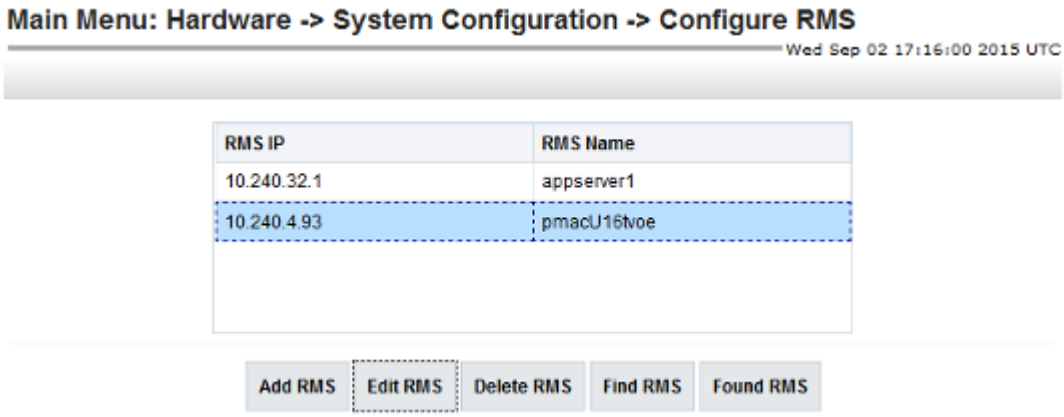
2. PM&C GUI: Configure RMS

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure RMS**.



3. PM&C GUI: Edit RMS

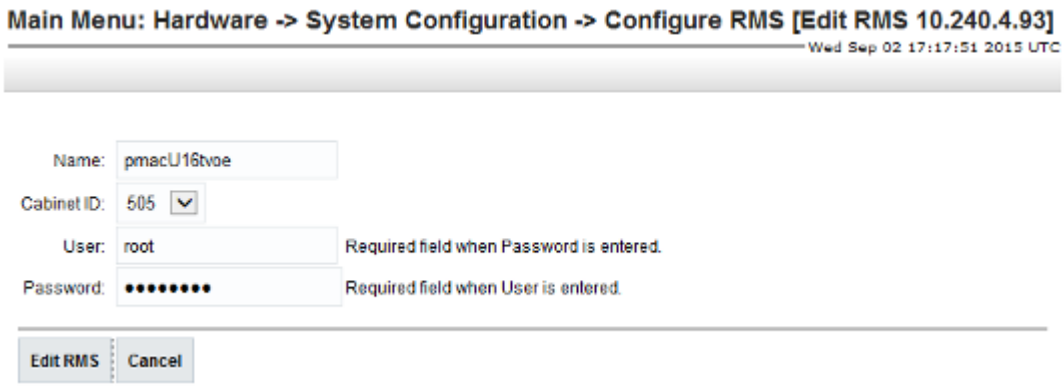
   On the Configure RMS panel, select one row in the list of rack mount servers and click the **Edit RMS** button.



4. PM&C GUI: Edit RMS

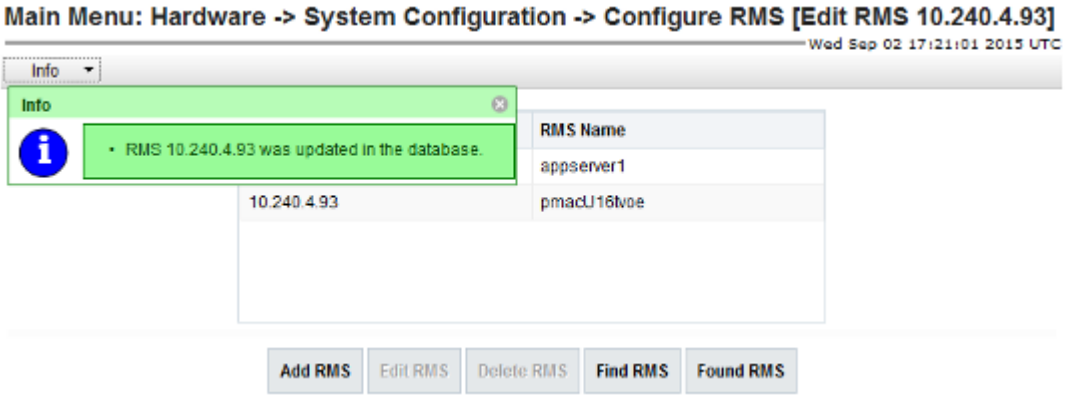
   In the Edit RMS panel, modify the field that needs to be altered.

   Then click on the **Edit RMS** button.

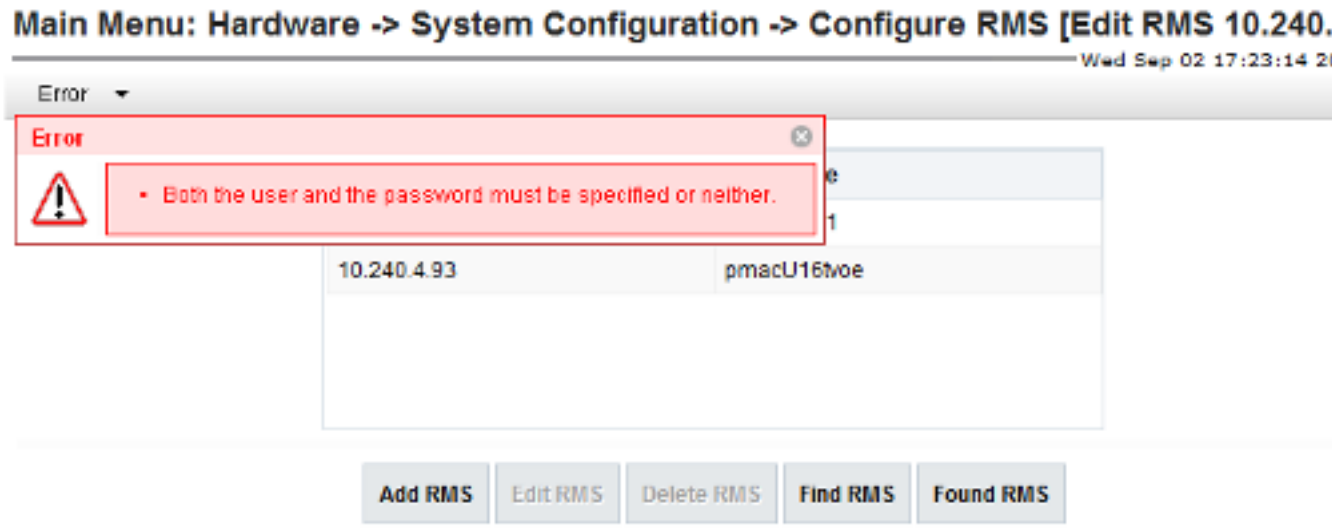


5. PM&C GUI: Check errors

   If no error is reported to the user you will see the following:



   Or you will see an error message:



3.7.18 Finding and Adding a Rack Mount Server to the PM&C System Inventory

This procedure provides instructions to find and add a rack mount server to the PM&C system inventory. This option is used to locate rack mount servers already running a Tekelec OS or within a specified IP Address range and then add those to the PM&C system inventory.

Prerequisites:

- The *3.7.6 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)*.

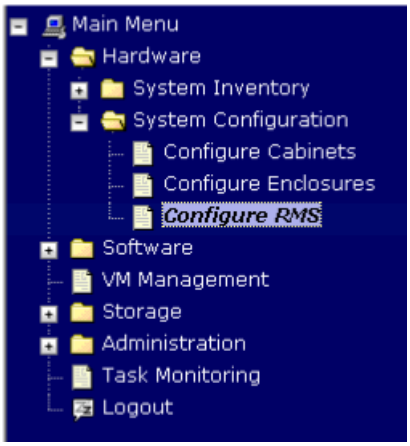
1. PM&C GUI: Login

   Open web browser and enter:

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

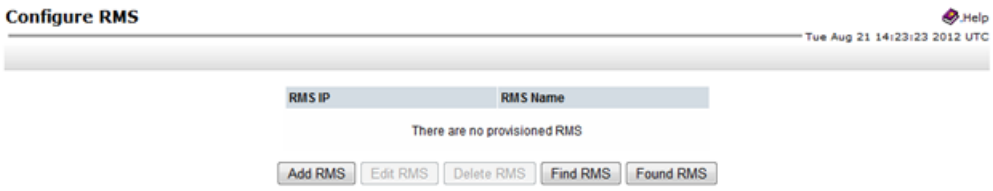
2. PM&C GUI: Configure RMS

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure RMS**

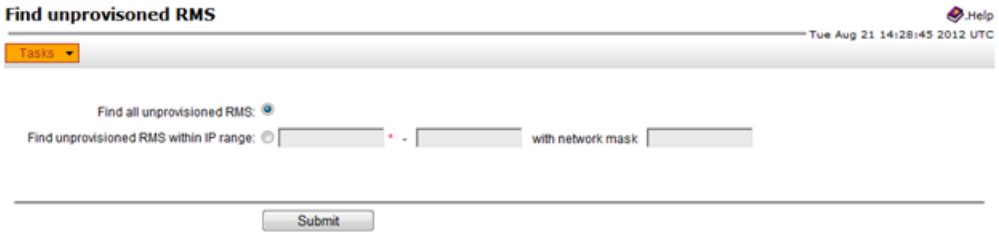
3. PM&C GUI: Find RMS

   On the Configure RMS panel, click the **Find RMS** button.

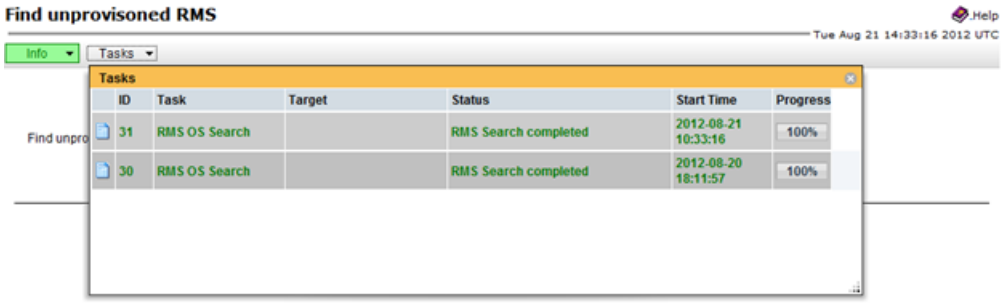
4. PM&C GUI: Find unprovisioned RMS

   On the Find unprovisioned RMS panel, click on the type of find you wish to perform. If the RMS has a Tekelec OS installed then use the default "Find all unprovisioned RMS" option. If the RMS does not have a Tekelec OS Installed then PM&C can search a range of IP Addresses for a valid Management Port (e.g. iLO) connection. Click the Submit button.



5. PM&C GUI: Monitor Find RMS

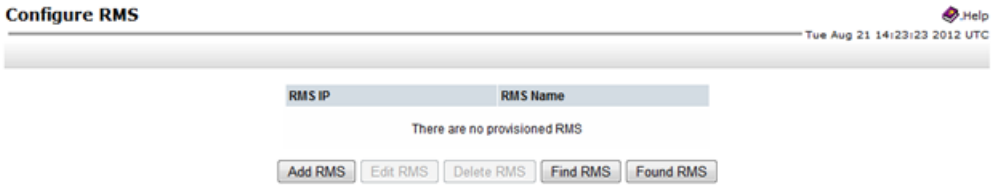
   The Find unprovisioned RMS page is then redisplayed with a new background task entry in the Tasks table. This table can be accessed by pressing the **Tasks** button located on the toolbar under the Find unprovisioned RMS heading.



   When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

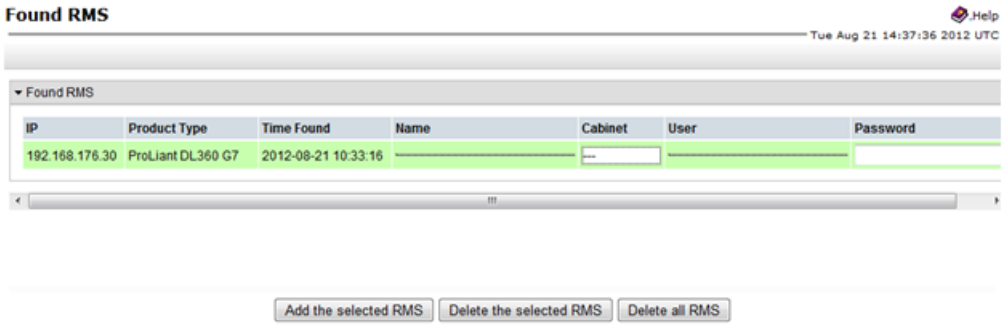
6. PM&C GUI: Found RMS

   On the Configure RMS panel, click the **Found RMS** button.



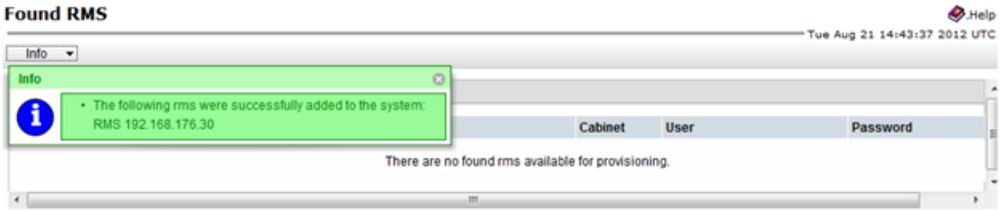
7. PM&C GUI: Add a found RMS

   On the Found RMS panel, click on one of the found RMS, enter values for any of the optional fields as needed. Press the "Add the selected RMS" button.



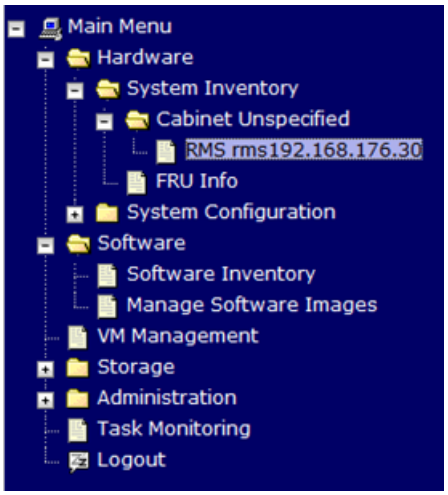
8. PM&C GUI: Check errors

   If no error is reported to the user you will see the following:

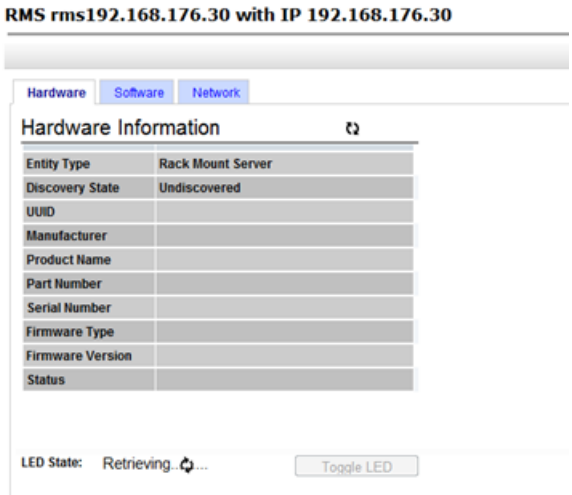


9. PM&C GUI:Verify RMS discovered

   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.

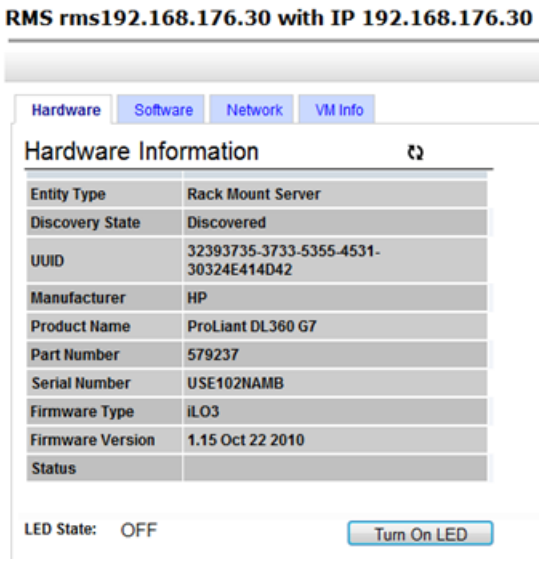


   The RMS inventory page is displayed.



   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 by referring to *1.4 My Oracle Support (MOS)*.



3.7.19 Accepting Upgrades Using PM&C

This procedure provides the steps for accepting upgrades via PM&C.

Prerequisites:

- Enclosures containing blade servers or servers containing a TVOE host targeted for accept upgrade have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for accept upgrade have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- The BIOS settings on the target servers have been verified using the *3.4.2 Confirm/Upgrade Blade Server BIOS Settings* procedure or section 3.2 of TPD Initial Product Manufacture Software Installation Procedure, E53017.
- The target servers have been upgraded with an application based on a TPD 6.x release.

Note: Until the target servers are fully discovered by PM&C, the user will be unable to accept upgrades on the servers (this might take up to 15 minutes after the upgrades complete).

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

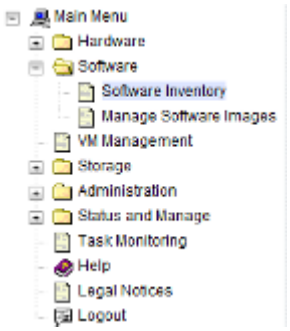
   If needed, open your web browser and enter:

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

   Login as the guiadmin user.

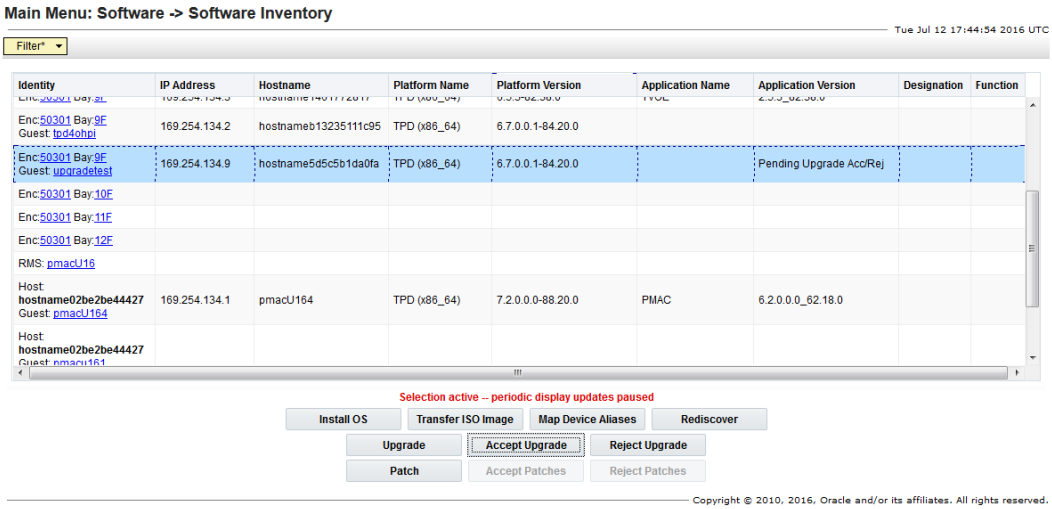
2. PM&C GUI: Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory.**



3. PM&C GUI: Select Servers

   To accept upgrades, the servers must be in the pending accept/reject upgrade state. Servers in the pending accept/reject upgrade state will have **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** displayed in their App Version column. Note that it may take up to 15 minutes for PM&C to discover and display the **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after an upgrade completes. Select the servers whose upgrades you want to accept. If you want to perform an accept upgrade on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted.

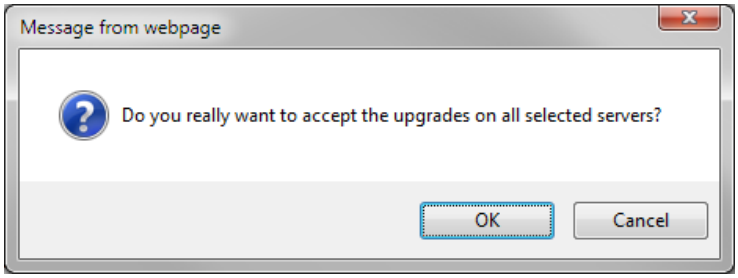


   Press the **Accept Upgrade** button

   Note: This action might result in a reboot if a migration of the file system is required.

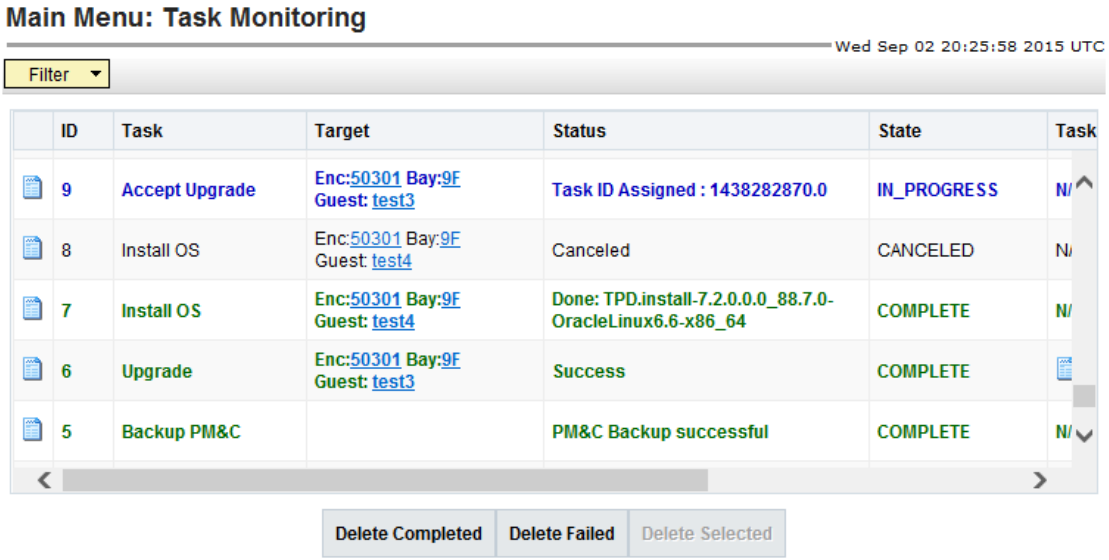
4. PM&C GUI: Confirm Accept Upgrade

   Press the **OK** button to proceed with the accept upgrade.



5. PM&C GUI: Monitor Accept Upgrade

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Accept Upgrade background task. A separate task will appear for each upgrade being accepted.



   When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

3.7.20 Rejecting Upgrades Using PM&C

This procedure provides the steps for rejecting upgrades via PM&C.

Prerequisites:

- Enclosures containing blade servers or servers containing a TVOE host targeted for reject upgrade have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for reject upgrade have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- The target servers have been upgraded with an application based on a TPD 6.x release.

Note: The image transfer is only supported for discovered entities (IP address is known).

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

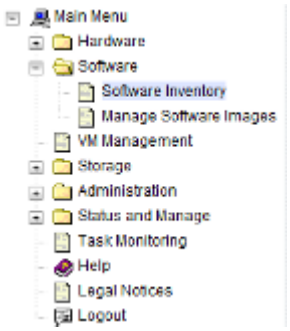
   If needed, open your web browser and enter:

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

   Login as the guiadmin user.

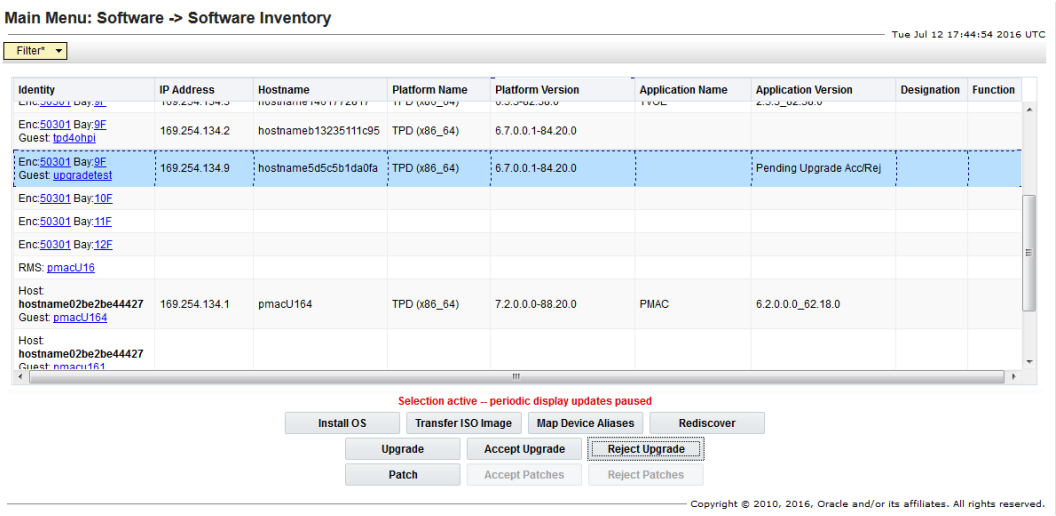
2. PM&C GUI: Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory.**



3. PM&C GUI: Select Servers

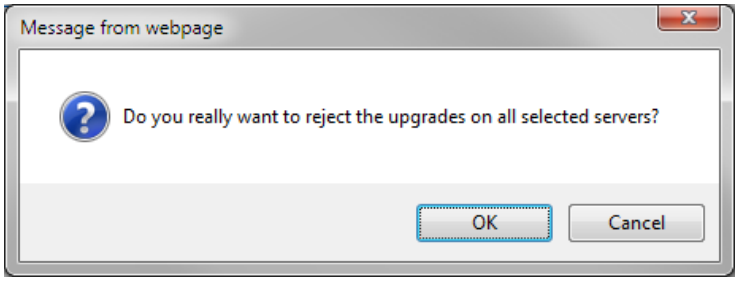
   To reject upgrades, the servers must be in the pending accept/reject upgrade state. Servers in the pending accept/reject upgrade state will have **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** displayed in their App Version column. Note that it may take up to 15 minutes for PM&C to discover and display the **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after an upgrade completes. Select the servers whose upgrades you want to reject. If you want to perform a reject upgrade on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted.



   Press the **Reject Upgrade** button.

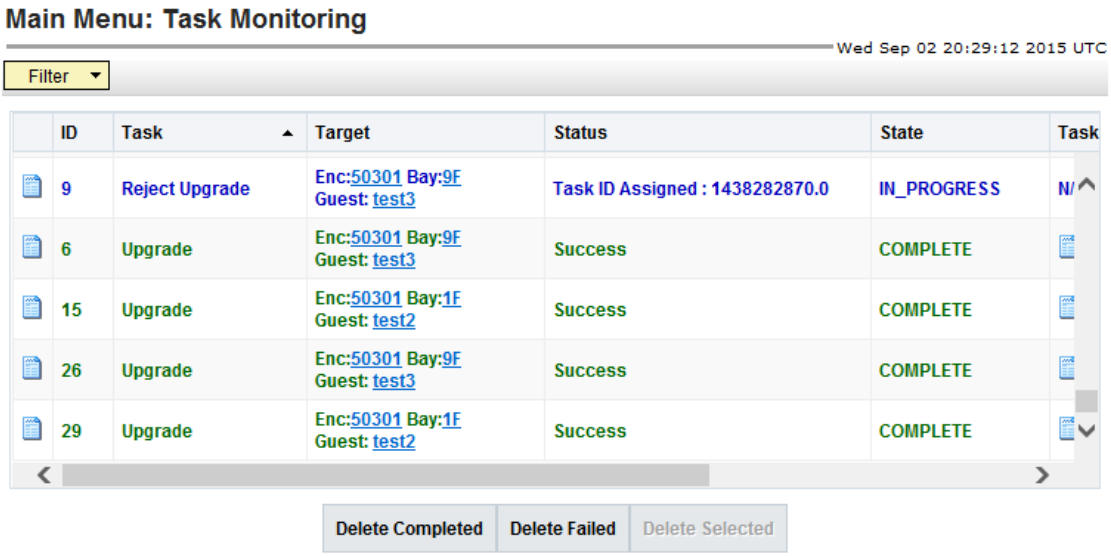
4. PM&C GUI: Confirm Reject Upgrade

   Press the **OK** button to proceed with the reject upgrade.



5. PM&C GUI: Monitor Reject Upgrade

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Reject Upgrade background task. A separate task will appear for each upgrade being rejected.



   When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

3.7.21 Accepting Patches Using PM&C

This procedure provides the steps for accepting patches via PM&C.

Prerequisites:

- Enclosures containing blade servers or servers containing a TVOE host targeted for application patch have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for application install/upgrade have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- The target servers have been patched with an application based an a TPD release supported by PMAC 6.3.

Note: Until the target servers are fully discovered by PM&C, the user will be unable to accept patches on the servers (this might take up to 15 minutes after the upgrades complete).

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

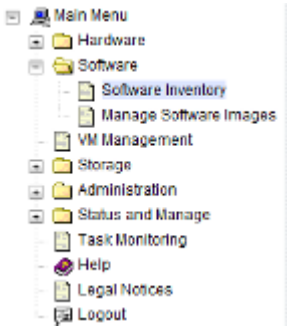
   If needed, open your web browser and enter:

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

   Login as the guiadmin user.

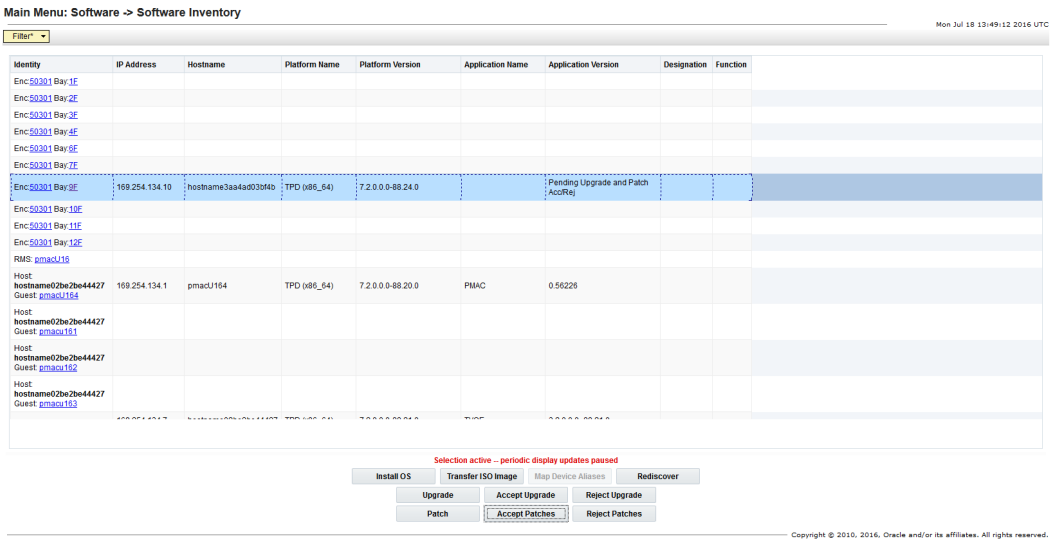
2. PM&C GUI: Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory.**



3. PM&C GUI: Select Servers

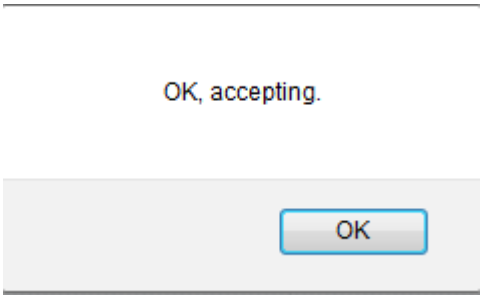
   To accept patches, the servers must be in a pending patch acc/rej state. Servers in this state will have **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** in their App Version column. Note that it may take up to 15 minutes for PM&C to discover and display the **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after a patch completes. Select the servers whose patches you want to accept. If you want to perform an accept patch on more than one server, you may select multiple servers by control-clicking multiple rows. Selected rows will be highlighted.



   Press the **Accept Patches** button.

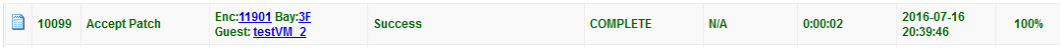
4. PM&C GUI: Confirm Accept Patch

   Press **OK** to proceed with accepting the patches.



5. PM&C GUI: Monitor Accept Patch

   Navigate to **Main Menu > Task Monitoring** to monitor the progress of the Accept Patch background task. A separate task will appear for each patch being accepted.



   When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

3.7.22 Rejecting Patches Using PM&C

This procedure provides the steps for rejecting patches via PM&C.

Prerequisites:

- Enclosures containing blade servers or servers containing a TVOE host targeted for application patch have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for application install/upgrade have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- The target servers have been patched with an application based an a TPD release supported by PMAC 6.3.

Note: Until the target servers are fully discovered by PM&C, the user will be unable to reject patches on the servers (this might take up to 15 minutes after the upgrades complete).

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

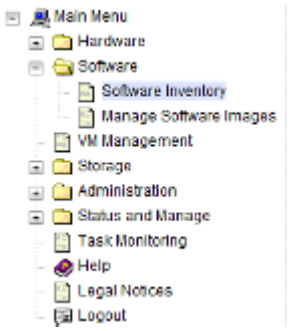
   If needed, open your web browser and enter:

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

   Login as the guiadmin user.

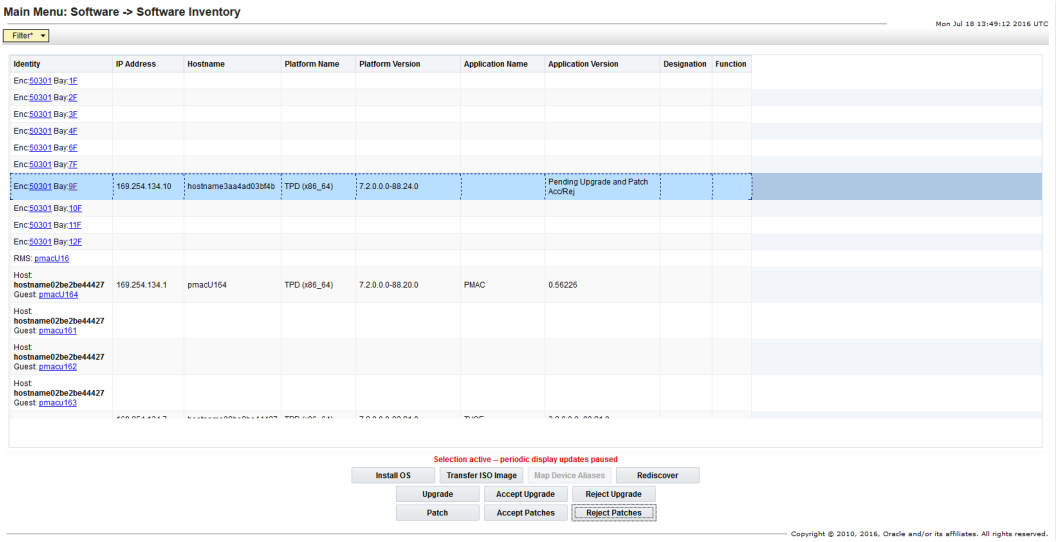
2. PM&C GUI: Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory.**



3. PM&C GUI: Select Servers

   To reject patches, the servers must be in a pending patch acc/rej state. Servers in this state will have **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** in their App Version column. Note that it may take up to 15 minutes for PM&C to discover and display the **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after a patch completes. Select the servers whose patches you want to reject. If you want to perform a reject0 patch on more than one server, you may select multiple servers by control-clicking multiple rows. Selected rows will be highlighted.



   Press the **Reject Patches** button.

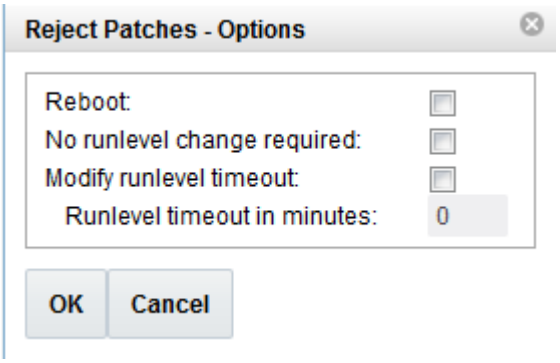
4. PM&C GUI: Reject Patches - Options

   There are three options that can be specified as part of a patch rejection.

   The first option is **Reboot**. If this is enabled, the patched server will reboot once the patch rejection has completed. The second option is **No runlevel change required**. If this is enabled, the patched server will not transition from runlevel 4 to 3 prior to rejecting the patch. This means that applications running on the server will not be halted during the patch rejection. The third option is **Modify runlevel timeout**. If this is enabled, a custom runlevel timeout can be specified in the box below this option. This timeout (in minutes) determines how long the rejection process will wait for a runlevel transition from 4 to 3 before the rejection is aborted.

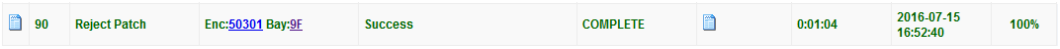
Any of these options can be specified as the sole option. Additionally, **Reboot** and **Modify runlevel timeout** may be specified together. **No runlevel change required** cannot be specified with either of the other options.

Press **OK** to proceed with rejecting the patches.



5. PM&C GUI: Monitor Reject Patch

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Reject Patch background task. A separate task will appear for each patch being rejected.



   When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

3.7.23 Initialize PM&C Application

Initialization of the PM&C application can be performed using the PM&C CLI if an initialization profile exists with the desired features. In the case where a PM&C feature needs to be enabled or modified the PM&C GUI is used to initialize the application. This procedure defines the initialization of the PM&C application and network resources.

Prerequisites:

- PM&C has been deployed and is not initialized or fully configured.
- Aggregation switches have been properly configured.

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)*.

If the PM&C application is to be initialized using the PM&C CLI, execute *3.7.26 Initialize PM&C Application using CLI*, otherwise, execute *3.7.27 Initialize PM&C Application using the GUI*.

Note: If the NetBackup feature is to be configured on this PM&C, execute *3.7.27 Initialize PM&C Application using the GUI*.

3.7.24 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: Select the "VM Info" tab and the "Virtual Disks" sub-tab. 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.

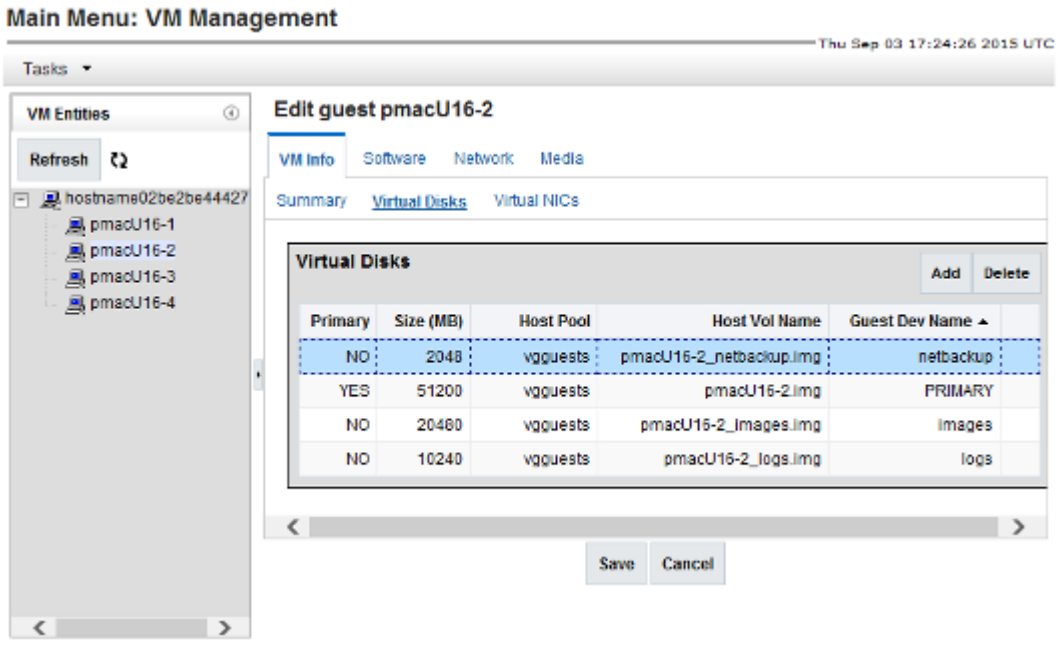
   Click "Edit" and enter the following data for the new NetBackup virtual disk.

   Note: If you are installing Netbackup 7.7 or greater, the "Size" field should be set to "5120" MB.

   - 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.

3.7.25 PM&C Guest Migrate NetBackup Client to New File System

If the Netbackup client software was installed on a PM&C application guest prior to the "NetBackup" virtual disk being required for a PM&C deploy with NetBackup, execute *3.7.24 Configure PM&C Application Guest NetBackup Virtual Disk*.

Note: The procedure above will create a new NetBackup virtual disk for the PM&C guest. The PM&C guest will be shut down and restarted. The content of the "/usr/openv" directory will be moved to the new NetBackup virtual disk, and mounted at "/usr/openv".

Note: If you are planning to upgrade to NetBackup version 7.7 or greater, execute procedure *P.1 Increase the PM&C Netbackup Filesystem Size* to increase the PM&C Netbackup filesystem Size.

3.7.26 Initialize PM&C Application using CLI

Prerequisites:

- PM&C has been deployed and is not initialized or fully configured.

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. TVOE Management Server iLO: Login with TVOE admusr credentials

   Login to the TVOE as admusr.

   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. PM&C: 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 "$ **`sudo kill -9 <PID>`**". Then execute the "virsh console X" command again. Your console session should now run as expected.

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

   ```
   virsh # list --all

   Id Name State
   ----------------------------------
   13 myTPD running
   20 pmacdev7 running

   virsh # console pmacdev7
   Connected to domain pmacdev7
   Escape character is ^]

   CentOS release 6.2 (Final)
   Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.14.0.x86_64 on an x86_64

   pmacdev7 login:
   ```

3. PM&C: Initialize the PM&C Application with the PM&C profile.

   Note: The example below uses the default PM&C profile named TVOE

   ```
   $ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE
   Profile successfully applied.
   $ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig
   Initialization has been started as a background task
   ```

4. Wait for the background task to successfully complete. The command will show "IN_PROGRESS" for a short time.

Run the following command until a "COMPLETE" or a "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:
```

5. Perform a system healthcheck on PM&C:

```
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
This command should return no output on a healthy system.
$ 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.
.
```

6. Logout of the virsh console

   Exit the virsh console session using *Appendix I, How to Exit a Guest Console Session on an iLO.*

7. Management Server iLO: Exit the TVOE console.

   Run:

```
$ logout
```

3.7.27 Initialize PM&C Application using the GUI

Note: You must be logged in as the guiadmin user to access this page.

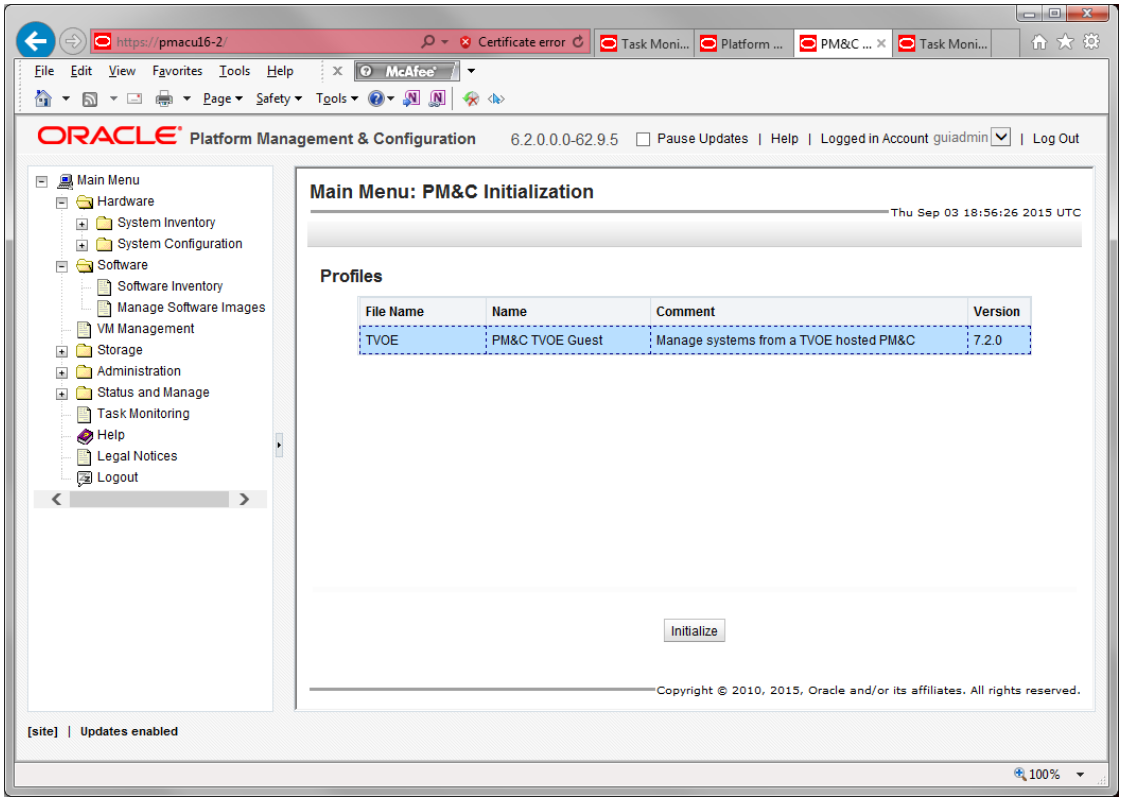
1. PM&C GUI: Load GUI and navigate to the Configuration view

   Open web browser and enter:

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

   Login as guiadmin user.

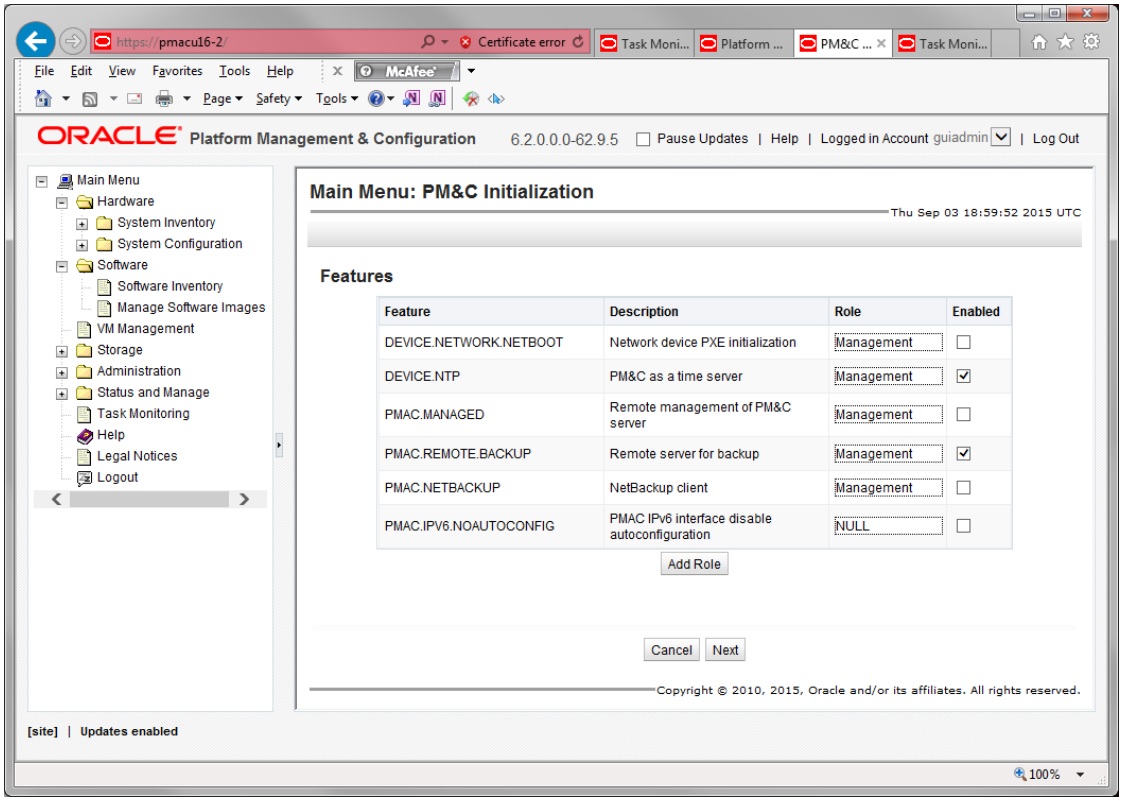
2. PM&C GUI: Select the appropriate PM&C initialization profile.
   The "PM&C Initialization" view will be presented to the operator. Select the appropriate profile.



3. PM&C GUI: Select and enable, appropriate PM&C Features, and if required add new Roles.

   Note: In this example the Features view was used to create a "NetBackup" role, and the NetBackup Feature was enabled.

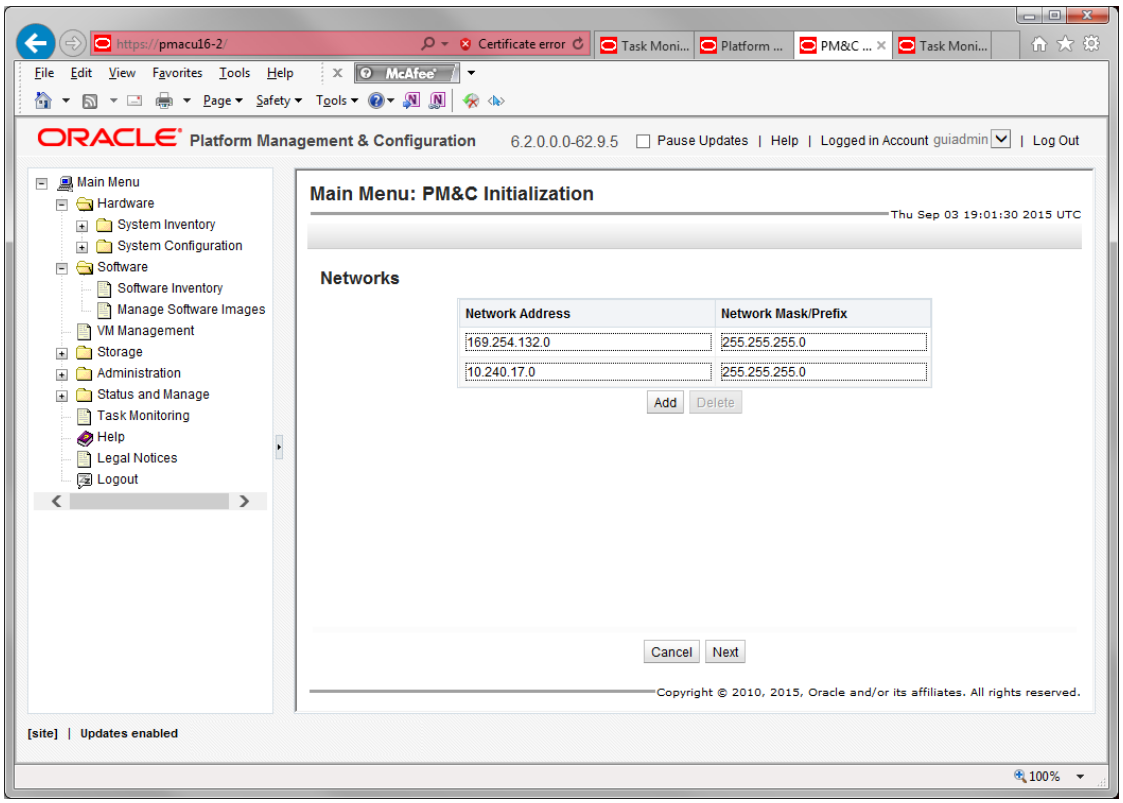
   Enable the appropriate feature and role, and click "**Next**".



4. PM&C GUI: Provision the PM&C application Networks.

   Note: In the example below the NetBackup network was provisioned and added.

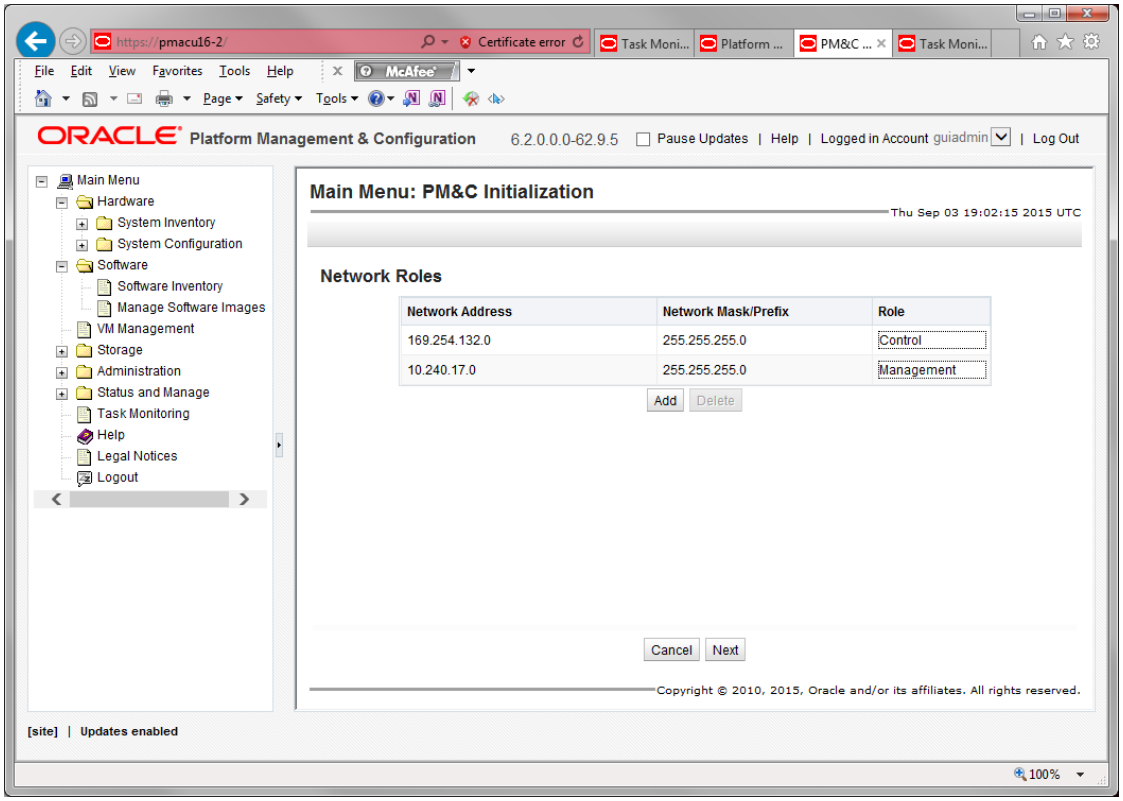
   Provision the appropriate networks and click "**Next**".



5. PM&C GUI: Provision the PM&C application Network Roles.

   Note: In the example below the NetBackup role was provisioned and added.

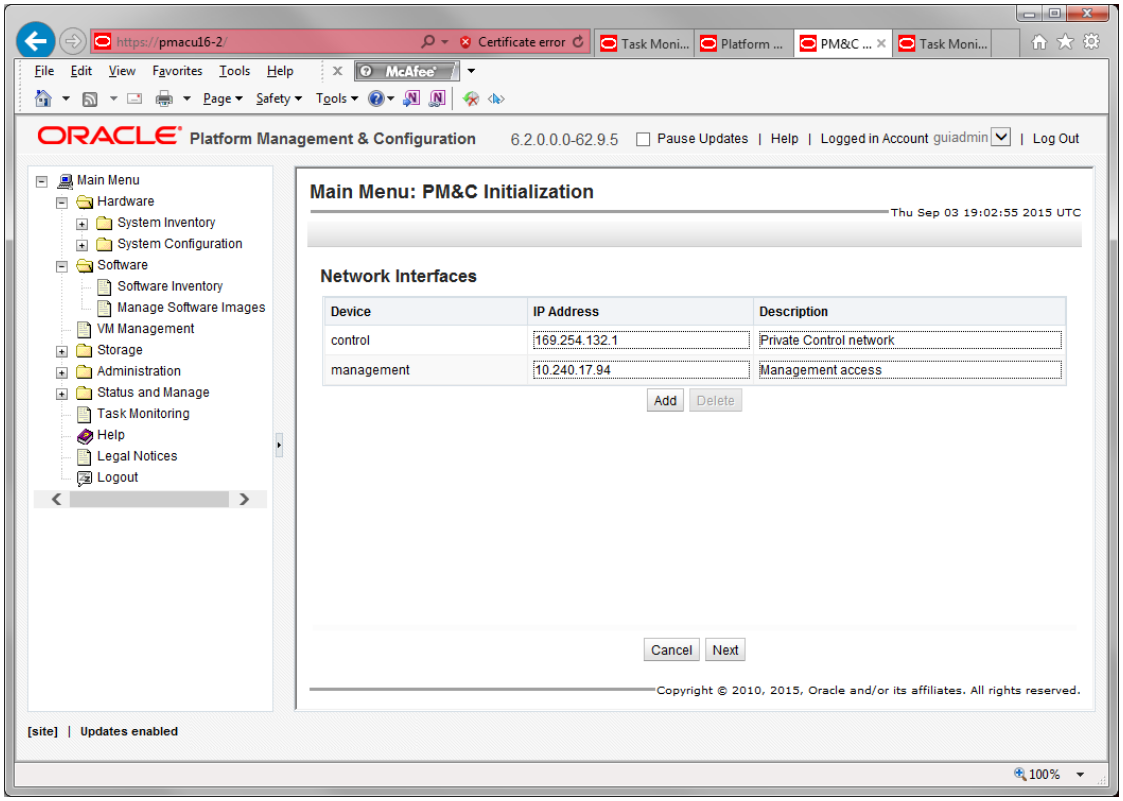
   Provision the appropriate network role and click "**Next**".



6. PM&C GUI: Provision the PM&C application Network Interfaces.

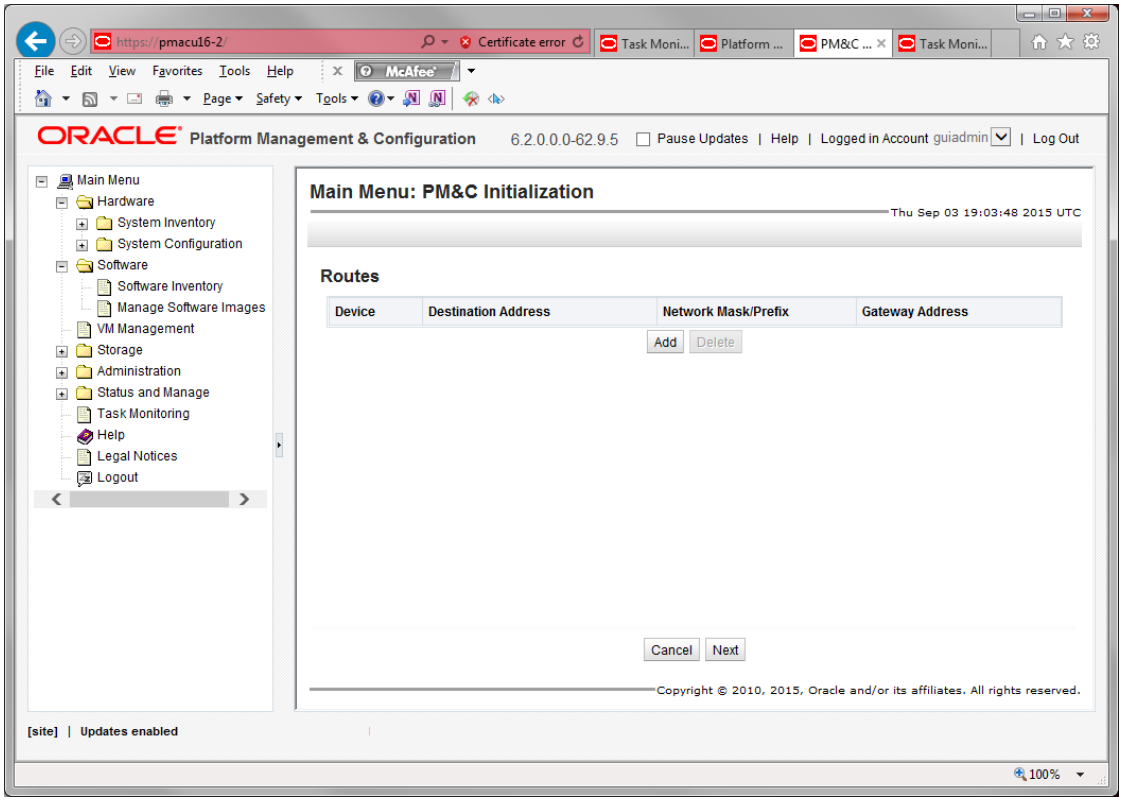
   Note: In the example below, the NetBackup interface was provisioned and added.

   Provision the appropriate interface and click "**Next**".

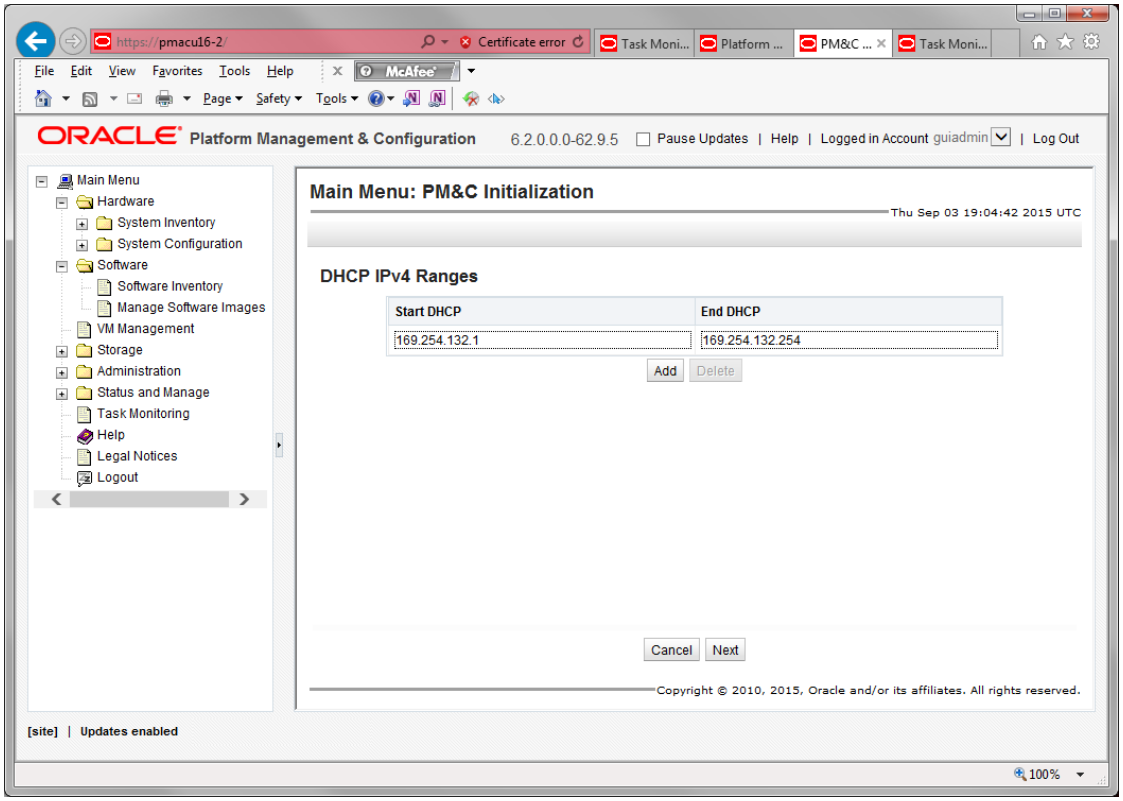


7. PM&C GUI: Provision the PM&C application Routes.

   Note: In the following example the default route and NetBackup routes were provisioned. Provision the appropriate routes and click "**Next**".

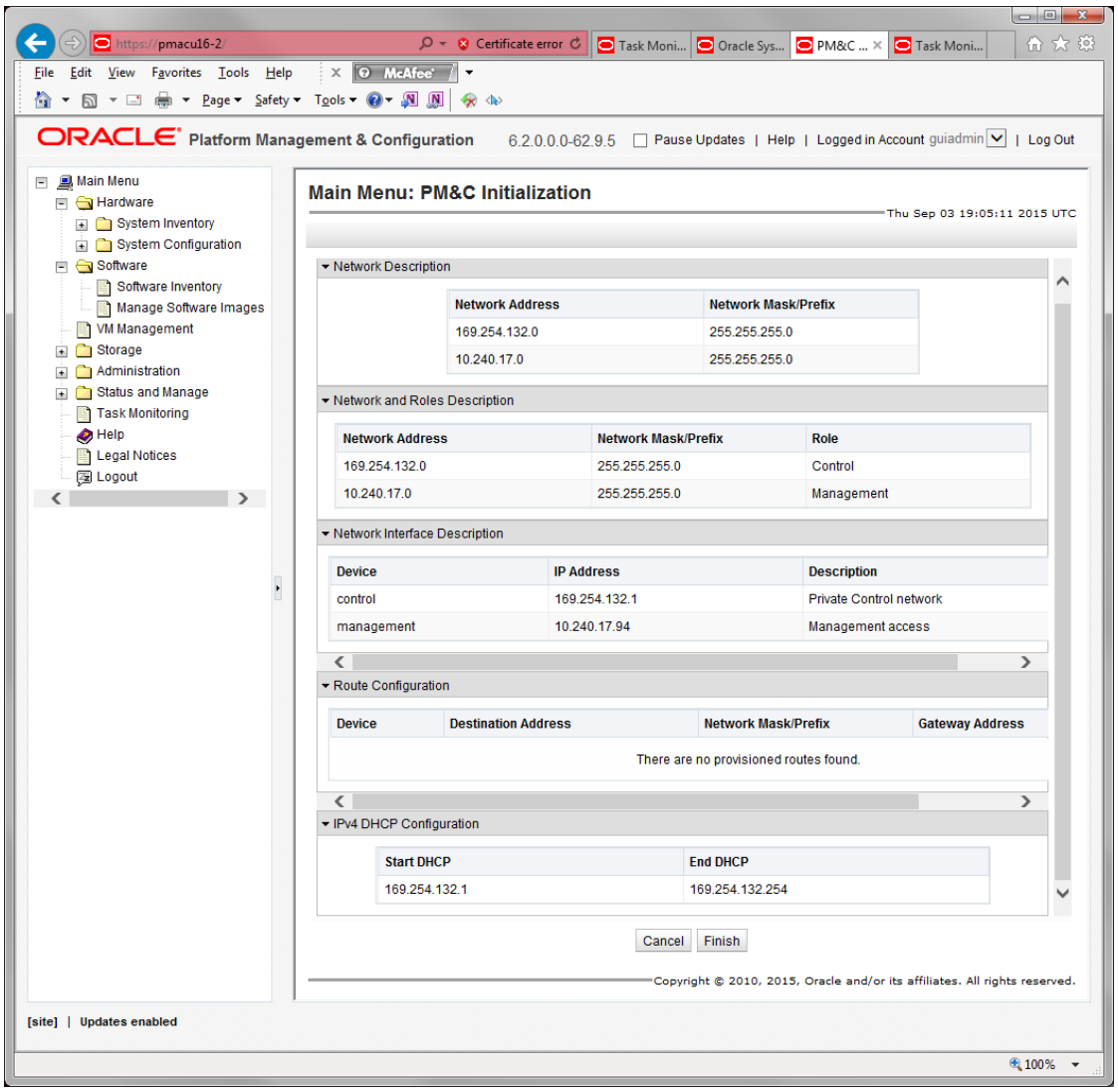


8. PM&C GUI: Provision the PM&C application DHCP Ranges.
   Provision the appropriate DHCP ranges.



9. PM&C GUI: Finish the PM&C application initialization.

   Verify the PM&C application initialization is correct on the "**Configuration Summary**" view and click **Finish**.



10. PM&C GUI: Verify the PM&C application initialization.

    Navigate to the Background Task Monitoring view and verify the "**Initialize PM&C**" task was successful.

3.7.28 Updating the TVOE Host SNMP Community String from the GUI

This section details how to use the PM&C GUI interface to update the Read Only or Read/Write SNMP Community String on all TVOE hosting servers and the PM&C Guest TPD which are known to the PM&C control network.

Note: You must be logged in as the Admin user to access this page.

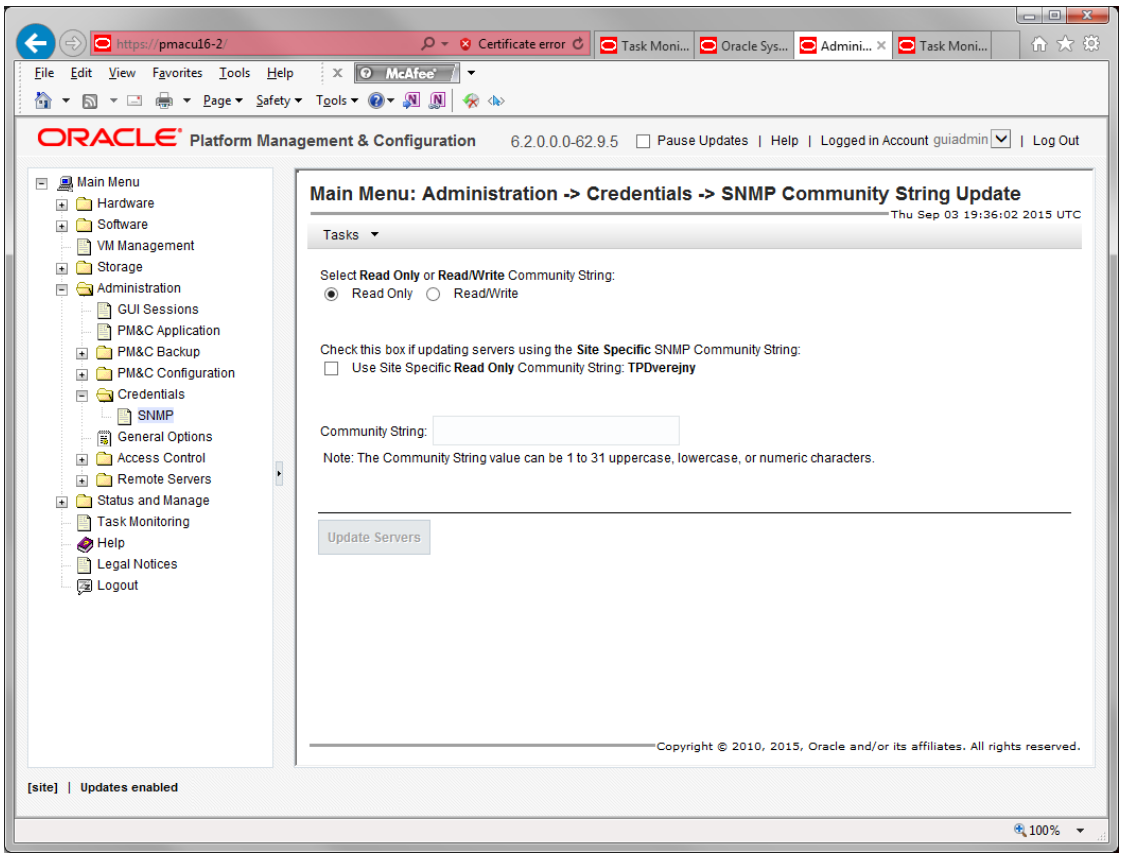
1. PM&C GUI: Load GUI and navigate to the Configuration view

   Open web browser and enter:

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

Login as guiadmin user.

2. PM&C GUI: Navigate to **Main Menu** > **Administration** > **Credentials** > **SNMP**.



3. PM&C GUI: Select the Read Only or Read/Write radio button depending on which SNMP Community String is to be updated.

   Note: In this example the Read Only radio button is selected.

4. PM&C GUI: If this the first time the SNMP Community Strings have been updated for this PM&C, leave the Use Site Specific checkbox unchecked. If this is an attempt to update one or more servers hosting the TVOE application "after" the Read Only and/or Read/Write Community String has already been updated, then select the Use Site Specific checkbox. This will disable the Community String textbox and enable the Update Servers button because the string to be used is the one stored in the PM&C database (or the one given in the GUI indicated next to the checkbox). Proceed to *3.7.28 Step 6*.

5. PM&C GUI: Enter a new Read Only Community String into the Community String textbox.

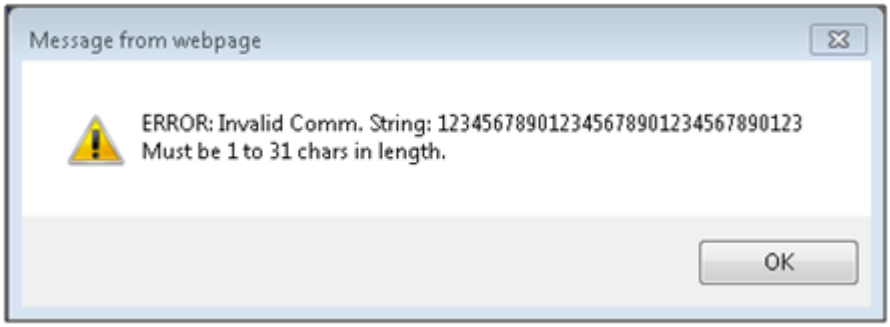
   Note: The string may only contain 1 to 31 characters in the set a-z, A-Z, and 0-9.

   Once the first character has been entered, the Update Servers button will become enabled.

6. PM&C GUI: Click on the "Update Servers" button.

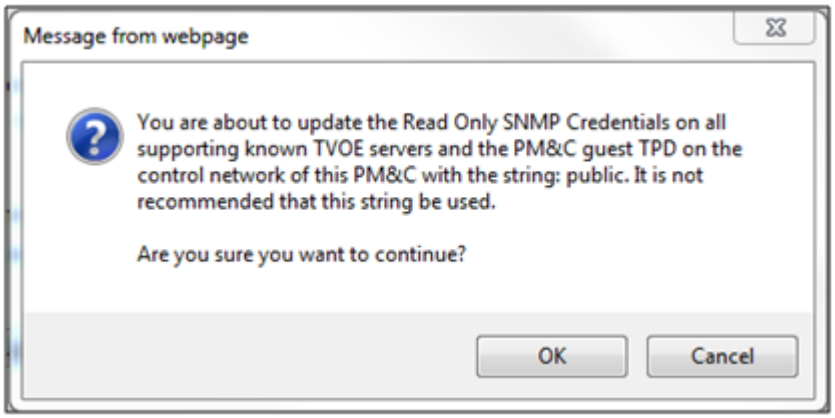
   The following error or warning messages may be displayed depending on the Community String entered into the textbox after the user clicks on the Update Servers button:

   - Invalid string length (over 31 characters)



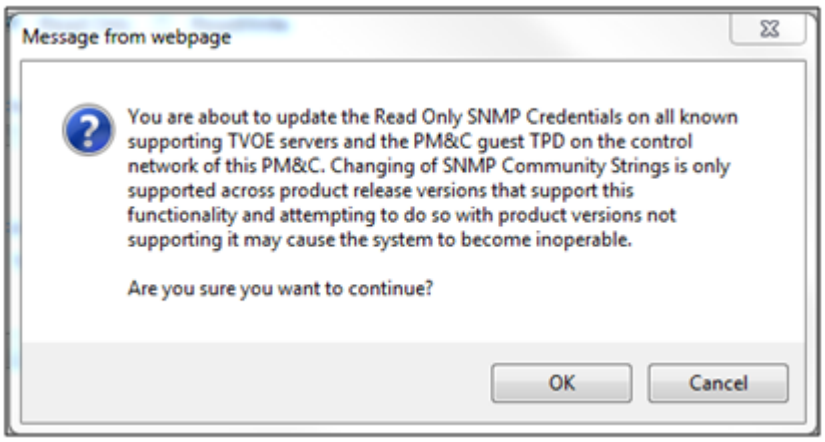
- Invalid characters (must be a-z, A-Z, 0-9)

- Use of non-recommended Community String (any mixed case combination of "public", "private", "password" , or "snmp-trap").



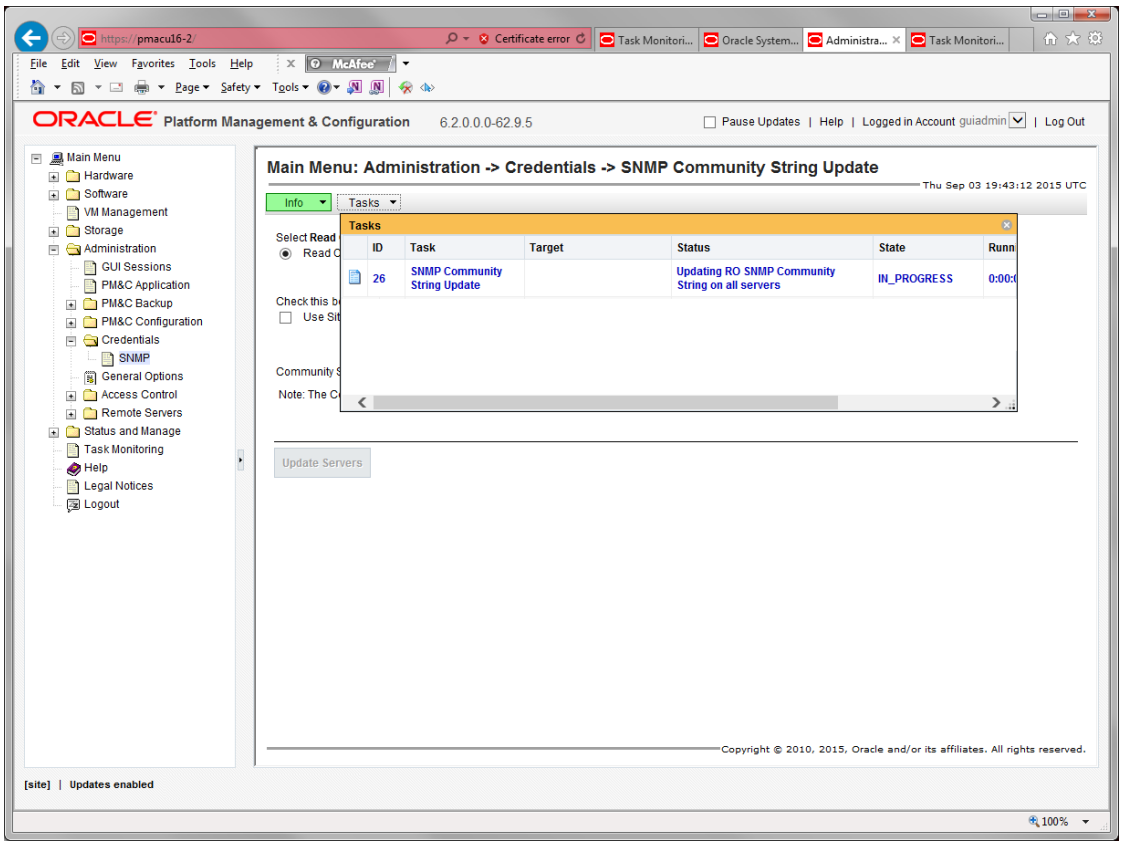
These whole words are not recommended as a standard Community String but the user is allowed to override the controls and allow these string to be set.

- Valid Community String general warning.

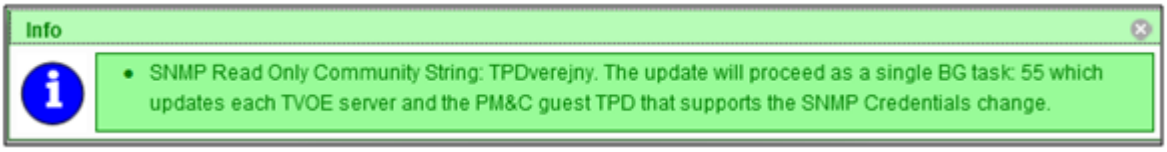


This general warning is always displayed after the Community String validation is performed to make sure the user is aware that changing these TVOE host Community Strings can cause their system to become in-operable if other components are not changed to reflect what is entered here.

Note: When this operation is initiated, all supporting TVOE hosting servers and the PM&C guest TPD on the PM&C control network will be updated. All those servers that match the existing Site Specific Community String will not be updated again until the string name is changed. Once validation is complete and the user selects OK on the general warning, a background task is created which can be monitored at the SNMP GUI page from the Tasks button or from the main menu Task Monitoring page.



The Info button can also be displayed which indicates a successful or failed update operation:



7. If the update needs to be validated, the user can enter the pmaccli command getCommStrStatus at a SSH terminal connection to the PM&C to display the status of the Community Strings on all servers on the PM&C control network.

   Execution loops over all known servers on the PM&C control network and attempts to retrieve the Read Only and Read/Write Community String. It displays the IPv4 and IPv6 for each server, the TPD release, the Application name and version, whether the servers supports the update functionality, and the status of the Community Strings for that server. All servers whose TPD instance is greater than 6.5.0_82.4.0 will be queried. It uses the values set in the PM&C database to determine the status of each Community String. The status can be either of the following:

   - Query Failed - Unable to retrieve the Read Only and Read/Write Community Strings from a given server.
   - Site Specific - Matches the current (the non-default) Read Only or Read/Write Community String stored in the PM&C database.
   - Default - Matches the default (non-editable) Read Only or Read/Write Community String stored in the PM&C database.

- Unknown - Was able to retrieve the Read Only or Read/Write Community String but it does not match what is maintained in the PM&C database. Usually indicates the Community String was updated manually from an interface other than the PM&C.
- Not Applicable - This indicates the server does not support the Update functionality and therefore the status cannot be determined. It is assumed this server matches the default values since they cannot be updated. Usually the server release is an older TPD and Application or a TVOE of < 2.5.0-82.4.0.

The output of the command includes “Server Update Supported” with a value indicating if the Update is actually supported or not. The possible values for support are:

- Supported - This indicates the TPD release is >= 6.5.0_82.4.0 and the Application name is TVOE or PMAC.
- Supported for Query Only - This indicates the TPD release is >= 6.5.0_82.4.0 and the Application name is unknown or something other than TVOE or PMAC. The Community Strings will not be updated via the PM&C but they can be queried from this command or the getHostCommStr command.
- Not Supported - This indicates the TPD release is < 6.5.0_82.4.0 and cannot be queried. In this case the Community String is set to the default values and the status is indicated as Not Applicable.

Example output:

```
pmaccli getCommStrStatus

SNMP Credentials Status Info:
================================================================================
Server IP Address (IPv4 - IPv6) : 169.254.131.6 - fe80::b699:baff:fea8:b860
Server Release Info (Host - App): TPD: 6.0.0-80.28.1 - Unknown: Unknown
Server Update Supported         : Not Supported
SNMP Read Only Community String : TPDverejny - Status: Not Applicable
SNMP Read Write Community String: TPDsoukromy - Status: Not Applicable

Server IP Address (IPv4 - IPv6) : 169.254.131.7 - fe80::1ec1:deff:fe75:df00
Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0
Server Update Supported         : Supported
SNMP Read Only Community String : newtestrol - Status: Site Specific
SNMP Read Write Community String: newtestrwl - Status: Site Specific

Server IP Address (IPv4 - IPv6) : 169.254.131.12 - fe80::5054:ff:feee:850
Server Release Info (Host - App): TPD: 6.0.0-80.28.0 - Unknown: Unknown
Server Update Supported         : Not Supported
SNMP Read Only Community String : TPDverejny - Status: Not Applicable
SNMP Read Write Community String: TPDsoukromy - Status: Not Applicable

Server IP Address (IPv4 - IPv6) : 169.254.131.14 - fe80::5054:ff:fe07:ea61
Server Release Info (Host - App): TPD: 5.0.0-72.44.0 - Unknown: Unknown
Server Update Supported         : Not Supported
SNMP Read Only Community String : TPDverejny - Status: Not Applicable
SNMP Read Write Community String: TPDsoukromy - Status: Not Applicable

Server IP Address (IPv4 - IPv6) : 169.254.131.8 - fe80::1ec1:deff:fe75:fca0
Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0
Server Update Supported         : Supported
SNMP Read Only Community String : newtestrol - Status: Site Specific
SNMP Read Write Community String: newtestrwl - Status: Site Specific

Server IP Address (IPv4 - IPv6) : 169.254.131.5 - fe80::2e76:8aff:fe50:3974
Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0
Server Update Supported         : Supported
SNMP Read Only Community String : newtestrol - Status: Site Specific
SNMP Read Write Community String: newtestrwl - Status: Site Specific

Server IP Address (IPv4 - IPv6) : 169.254.131.2 - fe80::3ed9:2bff:fef6:3e38
Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0
Server Update Supported         : Supported
SNMP Read Only Community String : testro - Status: Unknown
SNMP Read Write Community String: newtestrwl - Status: Site Specific
```

3.7.29 Configure PM&C Application Guest Isoimages Virtual Disk

This procedure allows the user to expand PM&C temporary area for importing software images using sftp in cases where PM&C already exists and larger ISO images need to be imported. The preferred method is to designate the extra space during PM&C deployment, refer to *3.7.4 Deploy PM&C Guest*.

1. PM&C GUI: Determine if the PM&C application guest is configured with a "isoimages" 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 "isoimages" device.

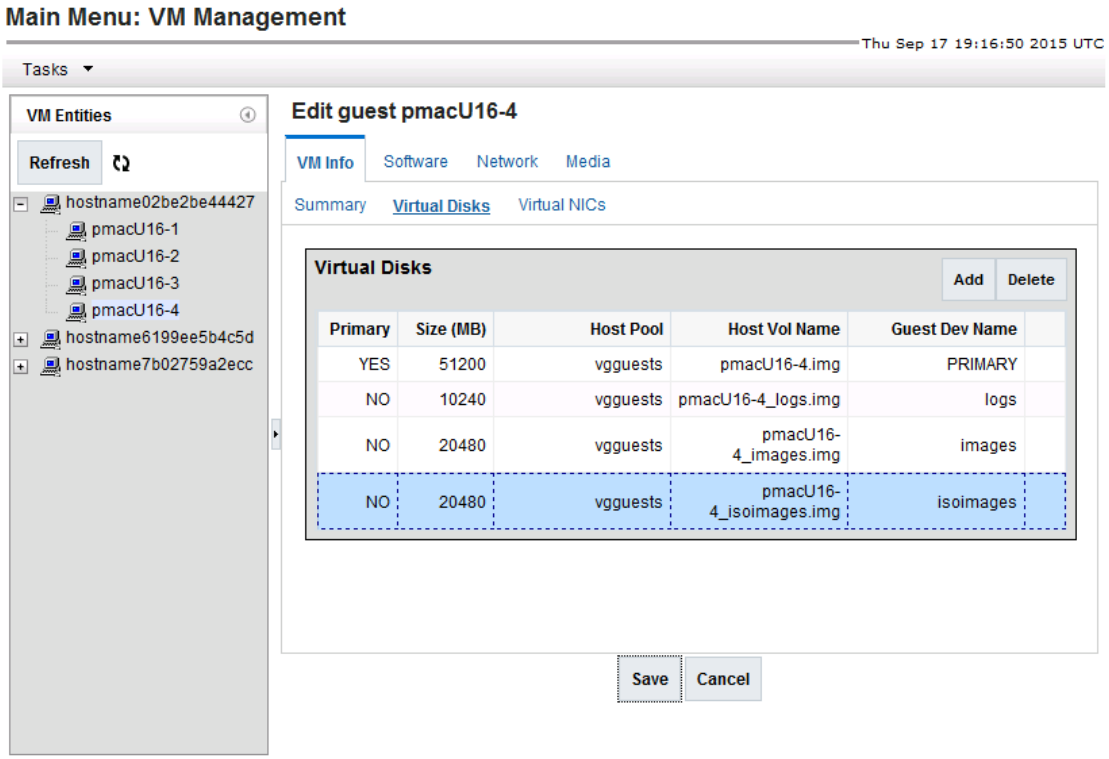
   If the "isoimages" device exists for the PM&C application guest then return to the procedure that invoked this procedure. Otherwise continue with this procedure.

3. PM&C GUI: Edit the PM&C application guest to add the "isoimages" virtual disk.

Click "Edit" and then click the "Add" button in upper corner of Virtual Disks grid. Then enter the following data for the new isoimages virtual disk.

- Size (MB): "20480"
- Host Pool: "vgguests"
- Host Vol Name: "<pmacGuestName>_isoimages.img"
- Guest Dev Name: "isoimages"

4. PM&C GUI: Verify the new isoimages 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 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.

3.7.30 Certificate Management

3.7.30.1 Set the PM&C Domain Name

For instructions on how to set the Domain Name, refer to procedure *3.7.33 Configuring PM&C Domain Name System*.

3.7.30.2 Generate a New Certificate Signing Request

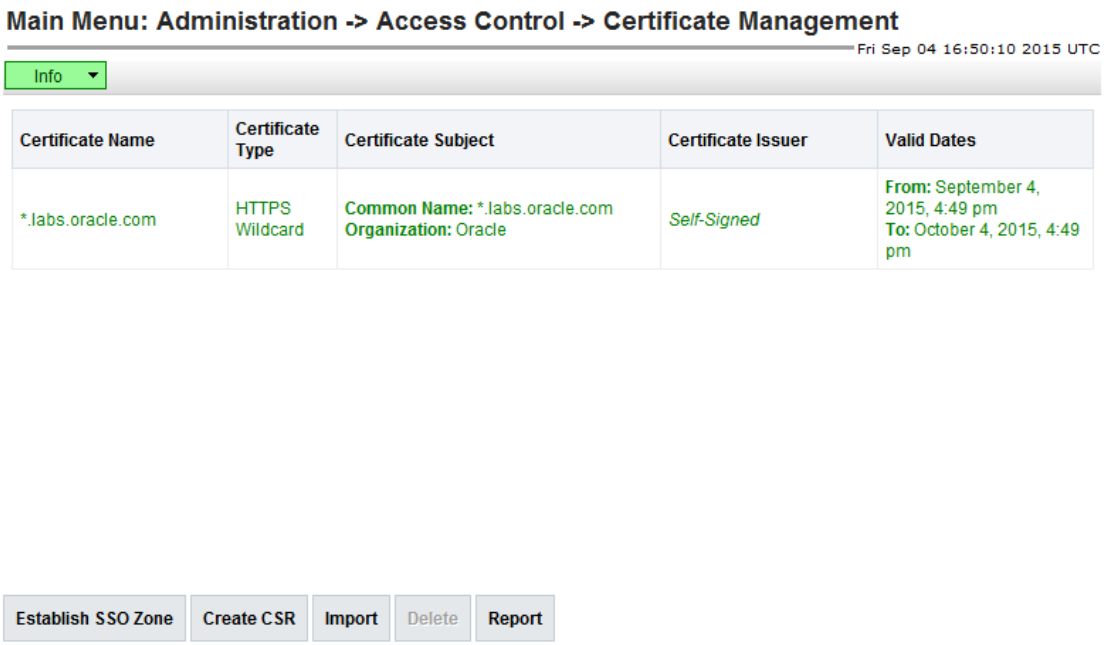
This procedure will generate a new self-signed HTTPS certificate and a Certificate Signing Request to be submitted to the customer's Certificate Authority. The CA will then provide a signed certificate that can be used to replace the self-signed certificate using the procedure *3.7.30.3 Update an HTTPS Certificate*.

Prerequisite: Procedure *3.7.30.1 Set the PM&C Domain Name*

Use this procedure if the customer does not already have an HTTPS certificate to install. Such a certificate may have been generated by a previous use of this procedure or by using the customer's own procedure. If the customer already has a certificate to install, use *3.7.30.4 Import an HTTPS Certificate* or *3.7.30.3 Update an HTTPS Certificate* instead.

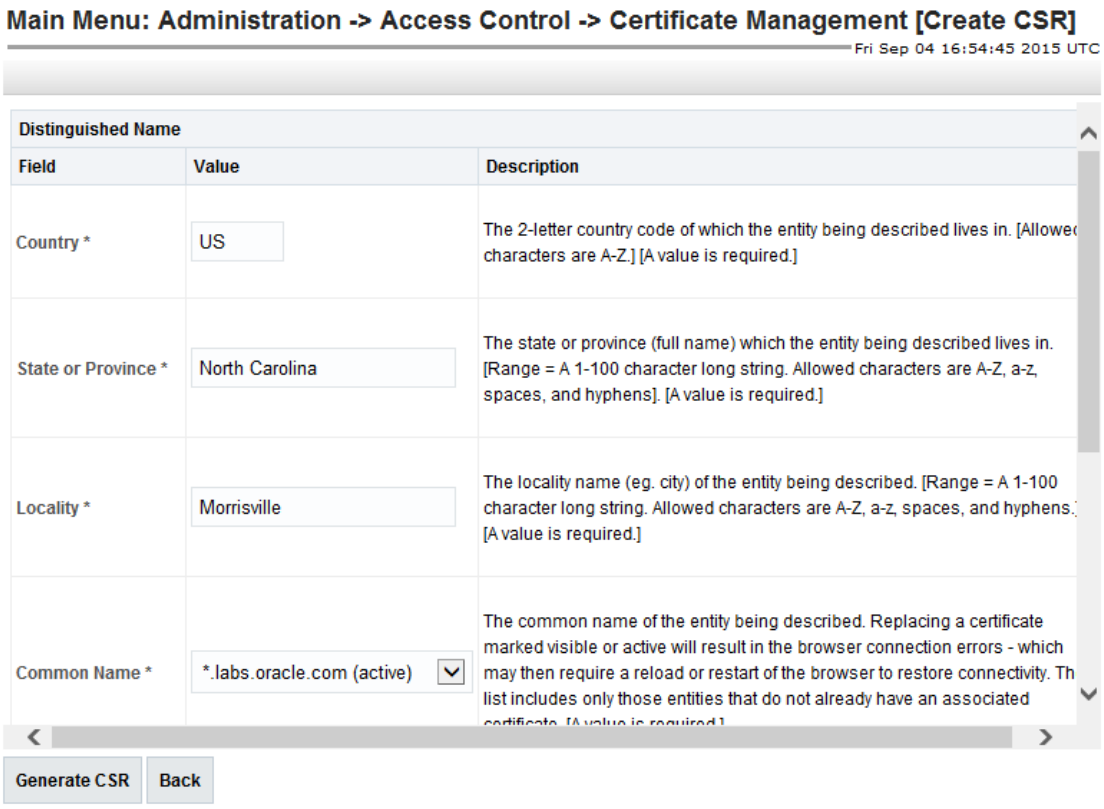
1. Login to the PM&C GUI as the guiadmin user.
2. Navigate to **Main Menu** > **Administration** > **Access Control** > **Certificate Management**

   This page will display any certificates already present on the PM&C system. A certificate currently in use by PM&C will be shown in green text.



Click the **Create CSR** button.

3. On the resulting **Create CSR** page, modify any fields as necessary to describe the system for which the new certificate will be generated. All fields are required.



The Common Name field will determine whether the new certificate will apply only to this PM&C host (e.g. "pmac1.office.company.com") or to any host in the same domain (e.g. "*.office.company.com". Use the host-specific option unless there are other hosts in the same domain sharing a single certificate.

The Common Name field will only offer names for which no certificate is already present on this PM&C. To replace an existing certificate, first delete it as instructed in *3.7.30.5 Delete an HTTPS Certificate*.

4. Click the **Generate CSR** button.

   This will create and install a new (self-signed) HTTPS certificate in PM&C and write the related Certificate Signing Request to a file. This file will be available immediately via the **Main Menu** > **Status and Manage** > **Files** screen (refer to *3.7.30.3 Update an HTTPS Certificate*).

   Because a new self-signed certificate is in use now, the user will need to re-establish the GUI session and accept the certificate.

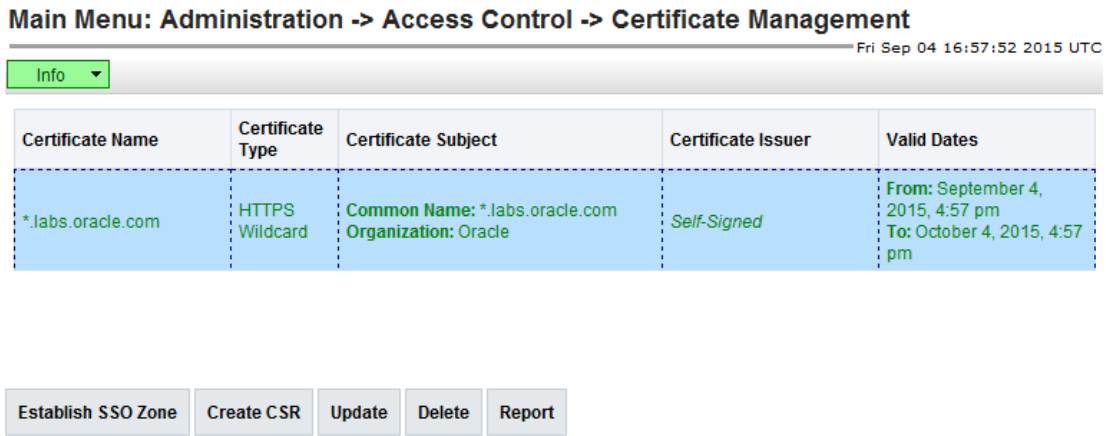
3.7.30.3 Update an HTTPS Certificate

This procedure is used to replace a self-signed certificate generated by PM&C with a CA-signed certificate provided by the customer's Certificate Authority. This will be done after these steps have been taken:

- The Procedure "Generate a new Certificate Signing Request" has been used to generate a new self-signed certificate and CSR
- The CSR has been submitted to a Certificate Authority
- The CA has provided a signed certificate

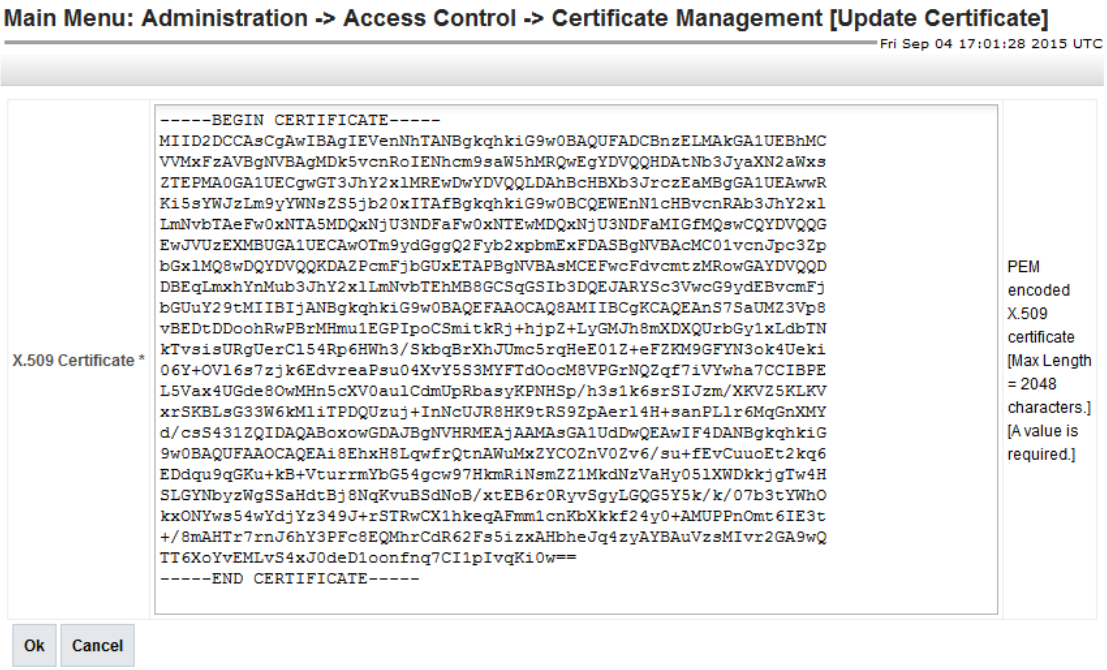
1. Login to the PM&C GUI as the guiadmin user.
2. Navigate to **Main Menu** > **Administration** > **Access Control** > **Certificate Management**.
3. Select the certificate to be updated.

   The Import button will change to an Update button.

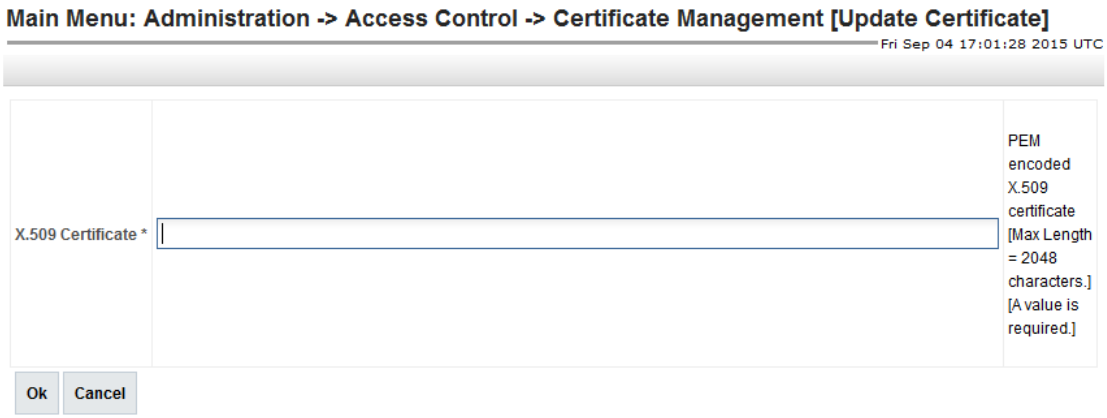


4. Click the Update button.

   This will display the certificate currently installed.



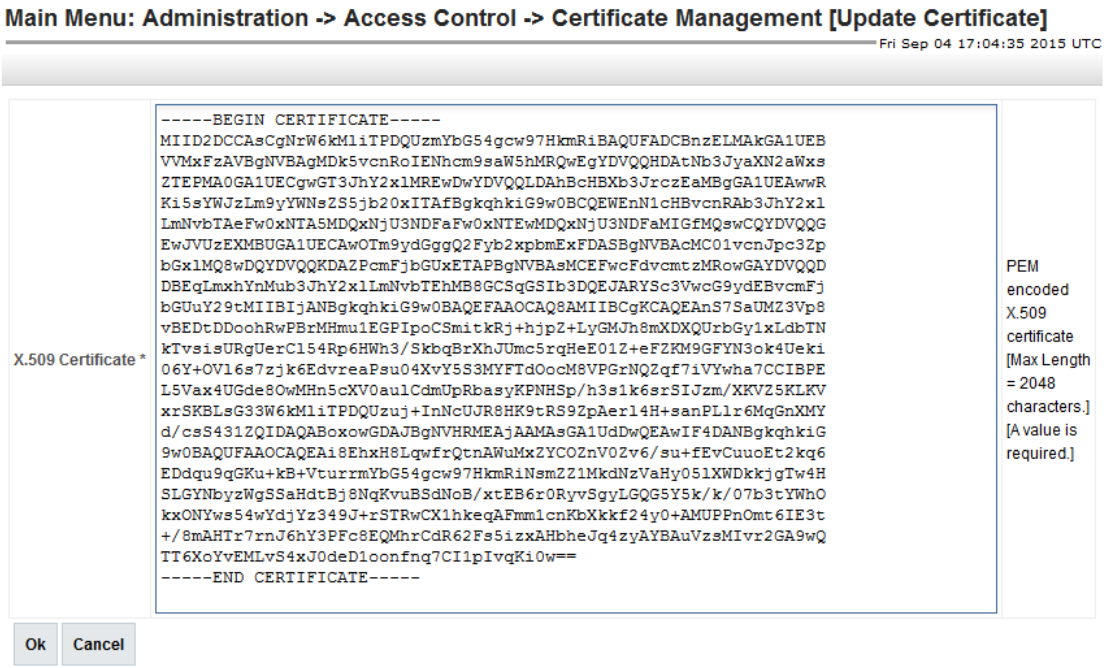
5. Select this text and delete it, but do not click the OK button yet.



6. Using an ASCII text editor on the PC, open the signed certificate provided by the Certificate Authority.
7. Copy the certificate from the editor to the "X.509 Certificate" field on the PM&C screen.

   Include the BEGIN and END lines and everything between:

```
-----BEGIN CERTIFICATE-----
<encoded certificate data>
-----END CERTIFICATE-----
```



8. Click the Ok button.

   The PM&C web server will be restarted immediately to put the updated certificate into effect. If the signing CA is not known to the browser or the PM&C was not accessed by DNS name, the user will have to re-establish the GUI session and accept the new certificate.

   Users will now be able to access the PM&C GUI without having to acknowledge and accept the server's certificate if the following conditions are met:

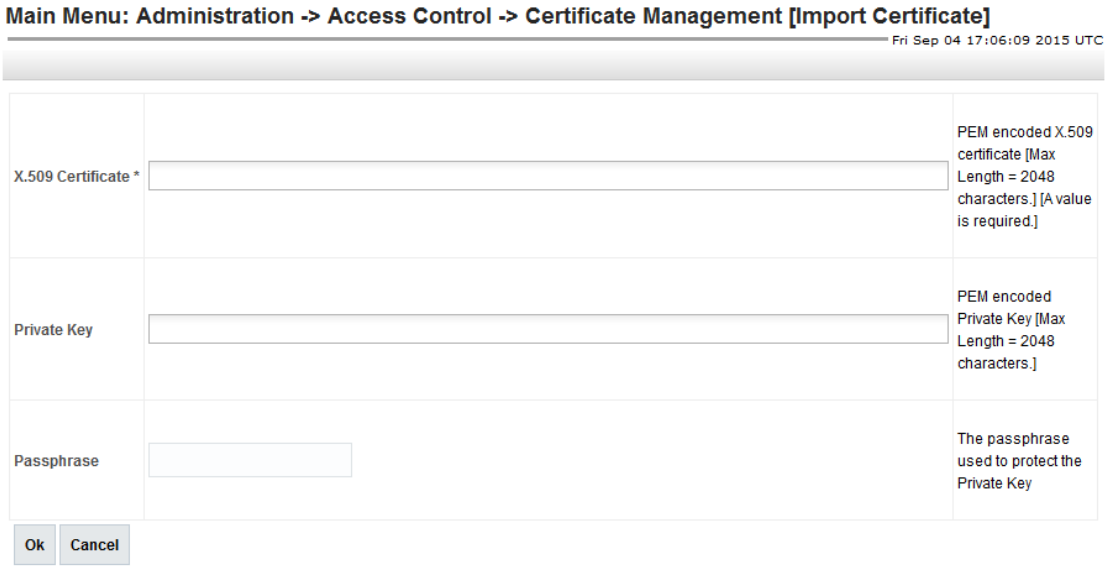
   - The PM&C is accessed by DNS name, not by IP address. This will require either a DNS server provided by the customer or configuration of the PM&C host name in the client PC's hosts file.
   - The browser recognizes the CA's signature on the certificate. This requires that the certificate be signed by a Certificate Authority known to the browser. Browsers are shipped with well-known CAs already installed, but certificates for additional CAs, such as customer-operated CAs, can be installed manually.

3.7.30.4 Import an HTTPS Certificate

This procedure is used to install a certificate and private key provided by the customer. If the key is encrypted, the customer's passphrase for the key must also be provided.

Note: The customer's passphrase is used only once to decrypt the customer's private key. The key is then re-encrypted by PM&C using its own passphrase. The customer's passphrase is not retained by PM&C.

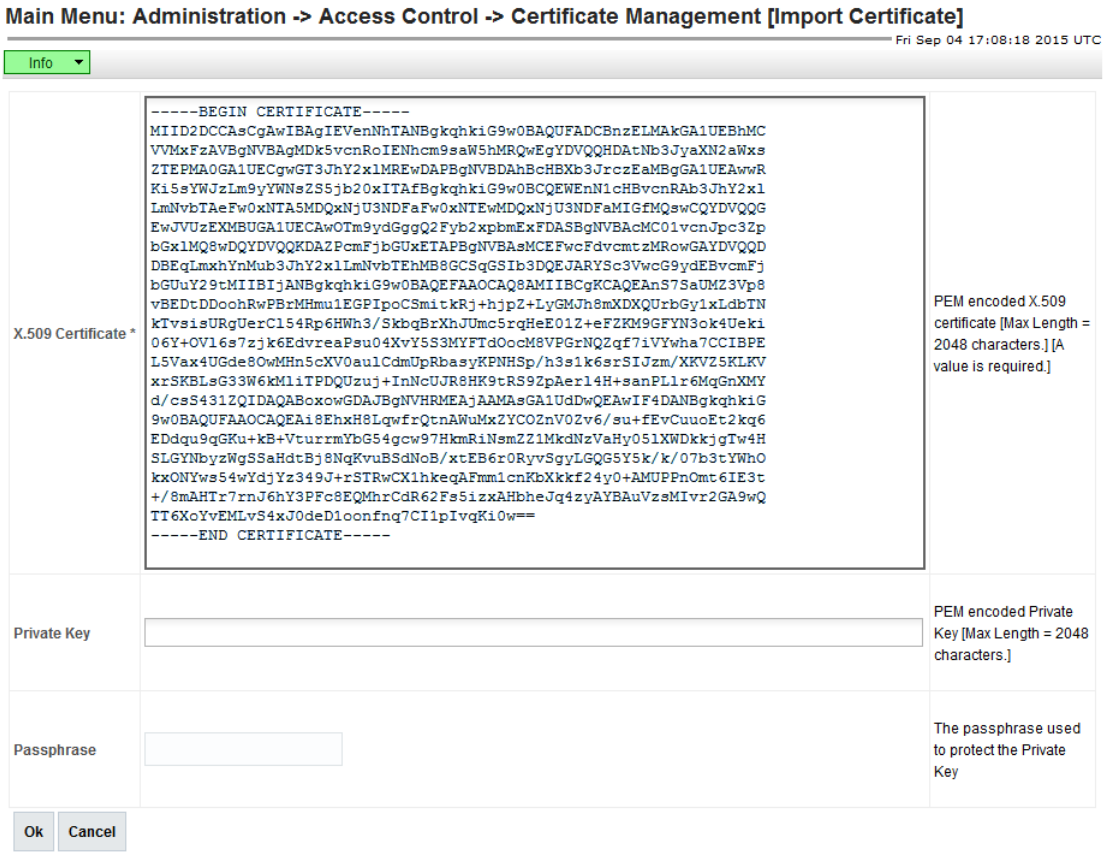
1. Login to the PM&C GUI as the guiadmin user.
2. Navigate to **Main Menu** > **Administration** > **Access Control** > **Certificate Management**.
3. Click the Import button.



4. Using an ASCII text editor on the PC, open the certificate to be imported.
5. Copy the certificate from the editor to the "X.509 Certificate" field on the PM&C screen.

   Include the BEGIN and END lines and everything between:

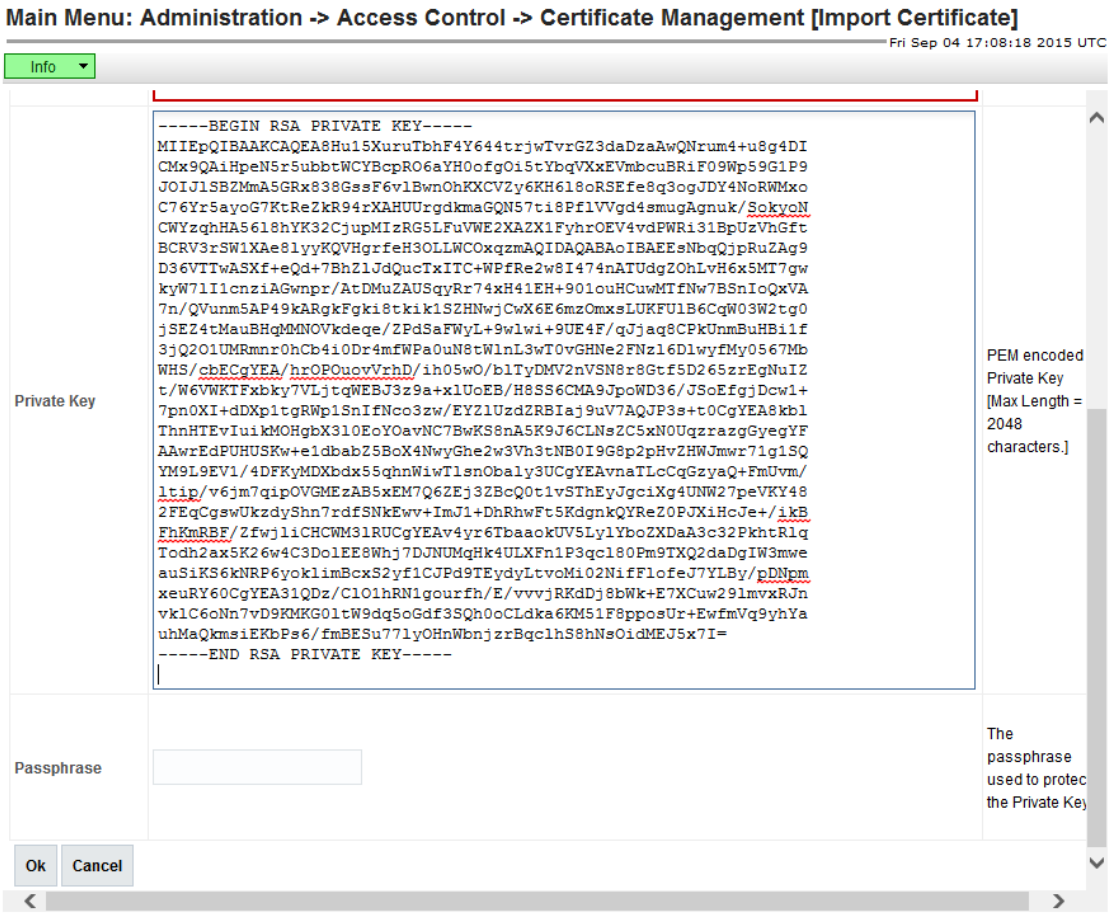
```
-----BEGIN CERTIFICATE-----
<encoded certificate data>
-----END CERTIFICATE-----
```



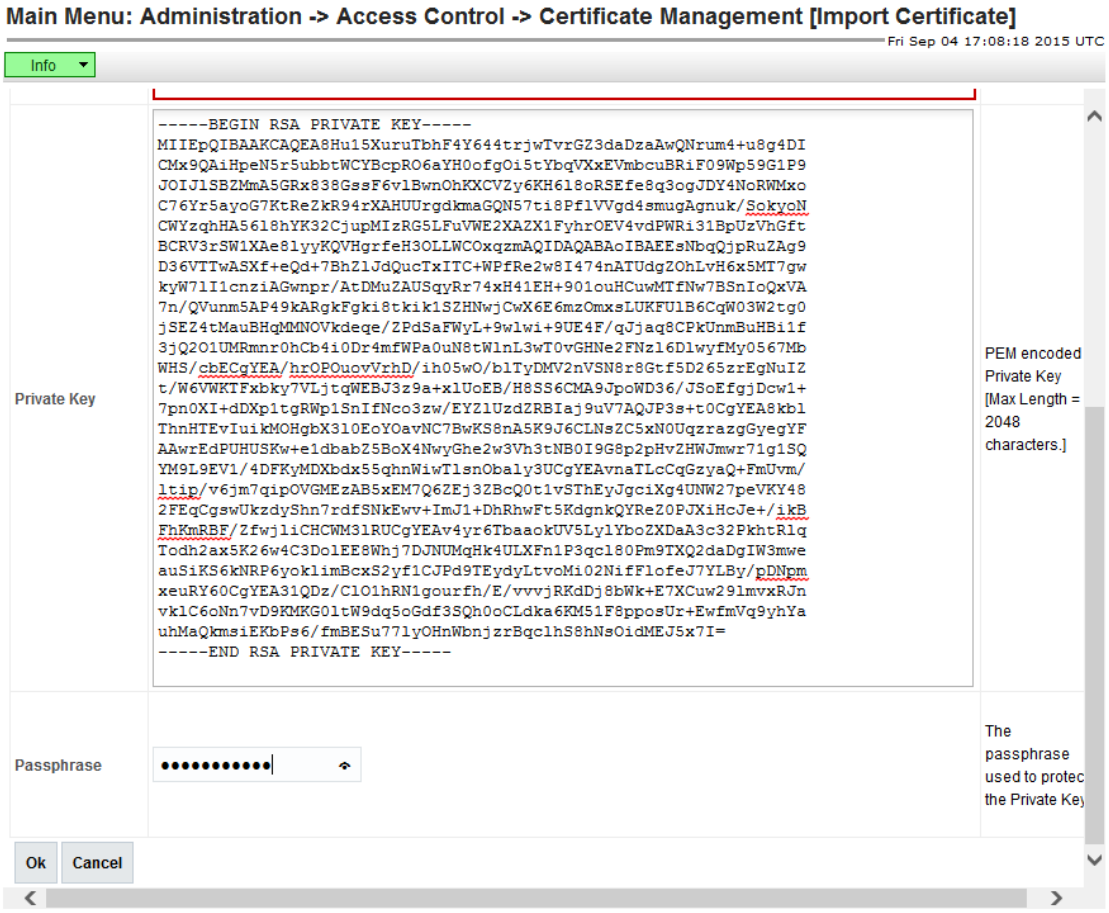
6. Using an ASCII text editor on the PC, open the private key file.
7. Copy the private key from the editor to the "Private Key" field on the PM&C screen.

   Include the BEGIN and END lines and everything between:

```
-----BEGIN RSA PRIVATE KEY-----
<encoded key data>
-----END RSA PRIVATE KEY-----
```



8. If the private key is encrypted, type or paste the passphrase into the "Passphrase" field.



9. Click the Ok button.

   The PM&C web server will be restarted immediately to put the new certificate into effect. If the signing CA is not known to the browser or the PM&C was not accessed by DNS name, the user will have to re-establish the GUI session and accept the new certificate.

   Users will now be able to access the PM&C GUI without having to acknowledge and accept the server's certificate if the following conditions are met:

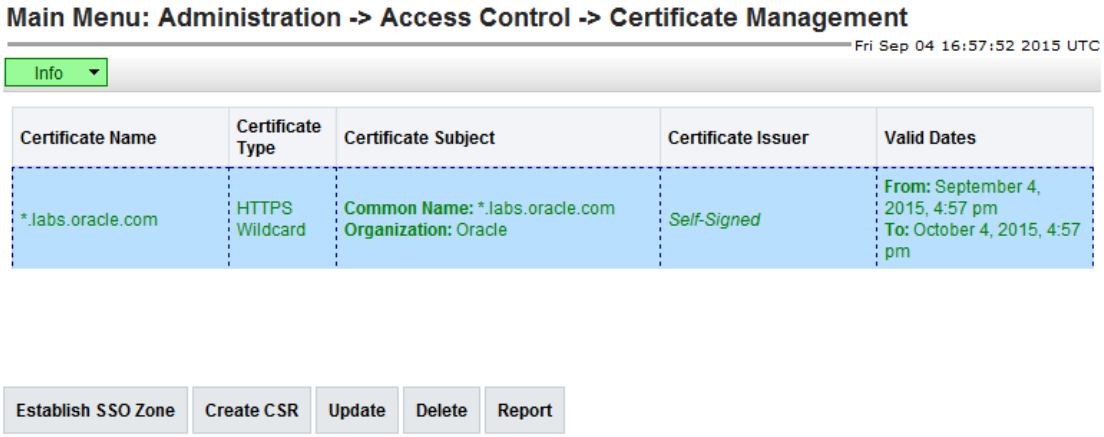
   - The PM&C is accessed by DNS name, not by IP address. This will require either a DNS server provided by the customer or configuration of the PM&C host name in the client PC's hosts file.
   - The browser recognizes the CA's signature on the certificate. This requires that the certificate be signed by a Certificate Authority known to the browser. Browsers are shipped with well-known CAs already installed, but certificates for additional CAs, such as customer-operated CAs, can be installed manually.

3.7.30.5 Delete an HTTPS Certificate

This procedure is used to remove a certificate from PM&C. PM&C will then revert to using the default HTTPS certificate. This will require that the user acknowledge and accept the certificate when accessing the PM&C GUI.

1. Login to the PM&C GUI as the guiadmin user.

2. Navigate to **Main Menu** > **Administration** > **Access Control** > **Certificate Management**.
3. Select the certificate to be deleted.



4. Click the Delete button.

   The PM&C web server will be restarted immediately to put the default certificate into effect.

   Users will now have to acknowledge and accept the certificate when accessing the PM&C GUI.

   For this reason the current session might need to be re-established.

3.7.31 Using the PM&C File Management System

This section details how to use the PM&C GUI interface to manage files on the PM&C server. These files are stored locally in the /var/TKLC/db/filemgmt/csr directory (considered to be the FMA or File Management Area). Any files added to the FMA will be visible from the **Main** > **Status and Management** > **Files** menu on the PM&C GUI interface. Up to 20 files are visible on the page. After that, scrollbars are enabled to view the remaining files.

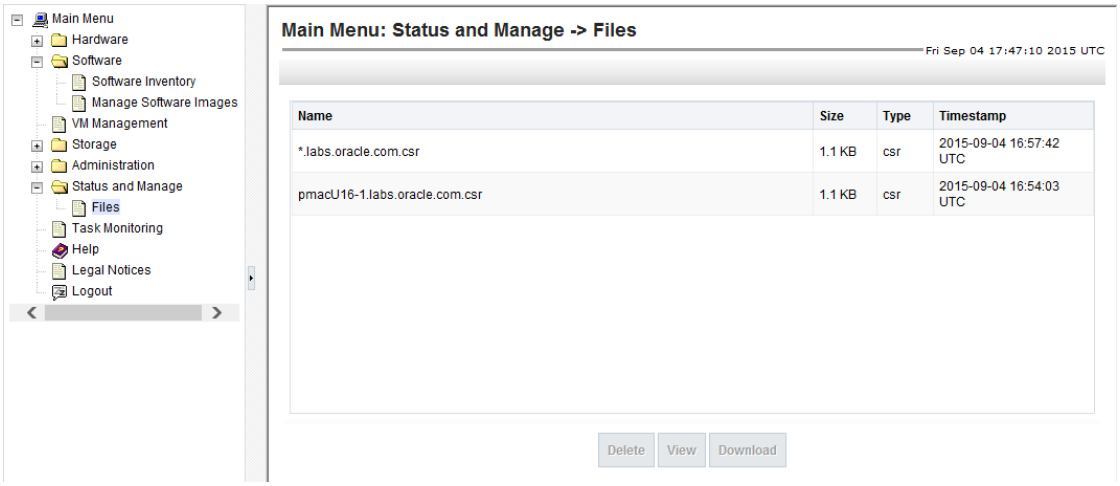
Note: Do not manually copy files to the FMA. Currently only Certificate Signing Request (CSR) files are stored in the FMA when Certificates are created (see *3.7.30 Certificate Management*).

There are three possible actions which can be invoked on a file:

- Delete - Select one or more files to be deleted.
- View - View a single selected file.
- Download - Download to the client browser a single selected file.

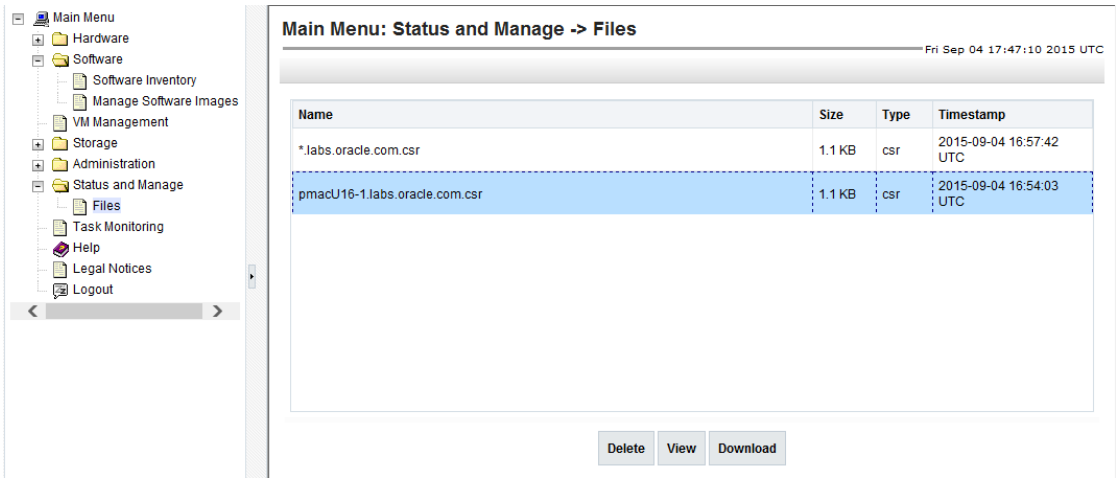
Note: The user must be logged in as the Admin user to access this page.

1. Delete one or more files:
   a) PM&C GUI: Navigate to **Main Menu** > **Status and Management** > **Files**.



b) PM&C GUI: Select one or more files to be deleted.

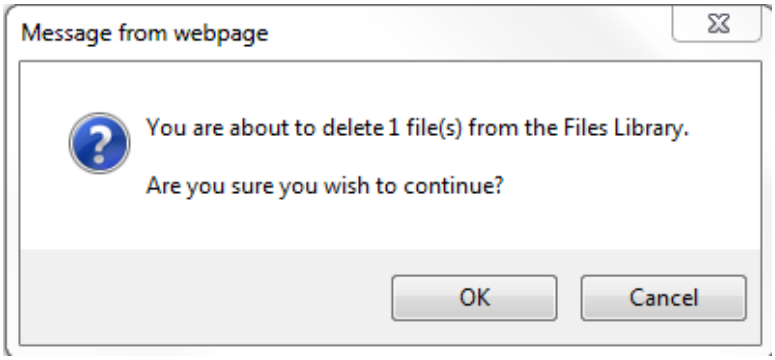
Note: Upon initial display of the Files Management page, all available files located within the FMA will be visible. If no files are located within the FMA, "There are no files present" is displayed. No files will be selected and all buttons will be visible but disabled. If a single file is selected all buttons will be enabled. If more than one file is selected, the View and Download buttons will be disabled.



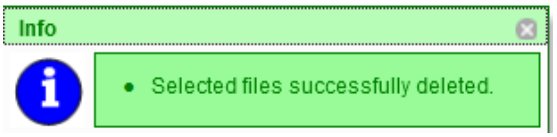
c) PM&C GUI: Select the Delete button.

d) The user is prompted to acknowledge that the selected files are to be deleted.

The user should click on the OK button (or click on the Cancel button if the operation is to be cancelled).

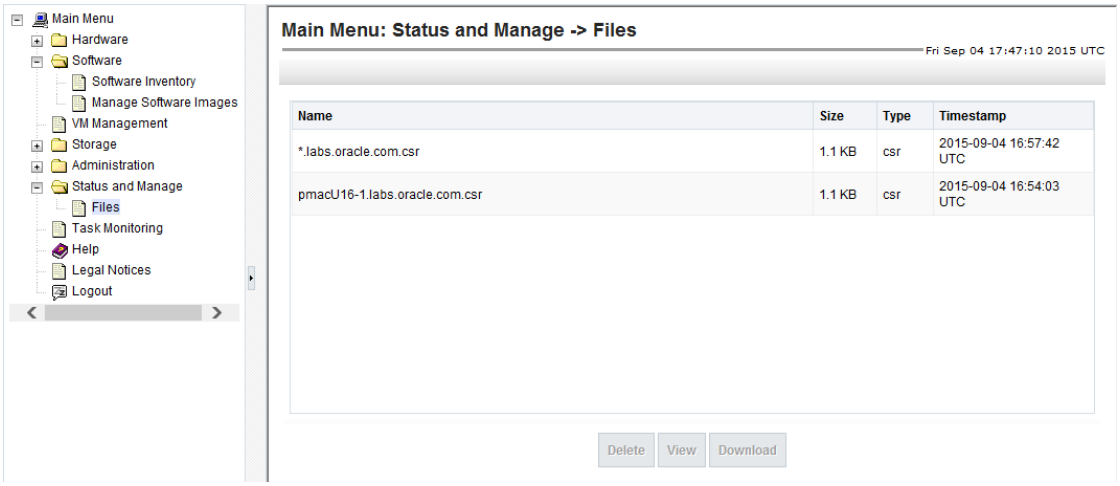


e) PM&C GUI: If the OK button is selected, the user is returned to the Files Management page with the selected file(s) no longer displayed and a status info box (which can be selected) indicating the action was successful.



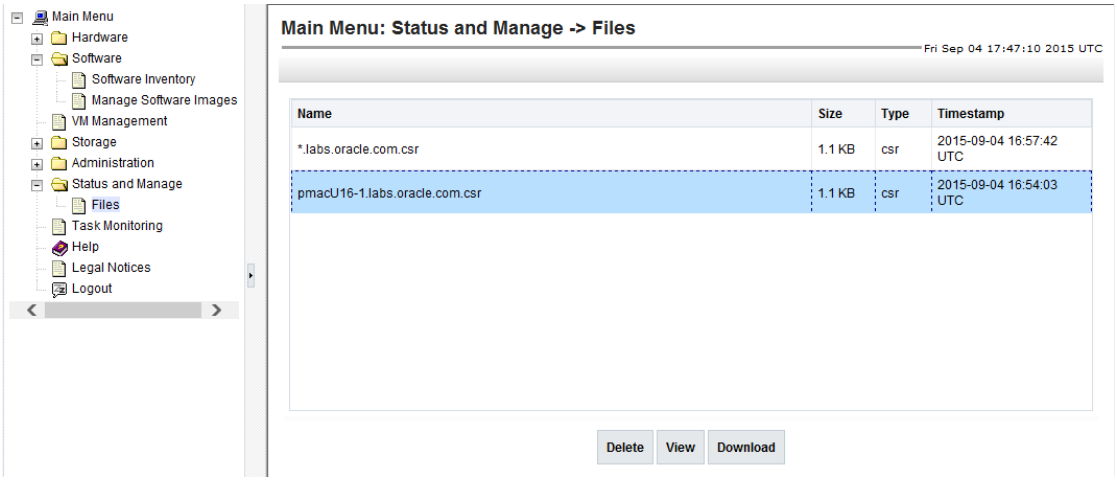
2. View a single file:

a) PM&C GUI: Navigate to **Main Menu** > **Status and Management** > **Files**.

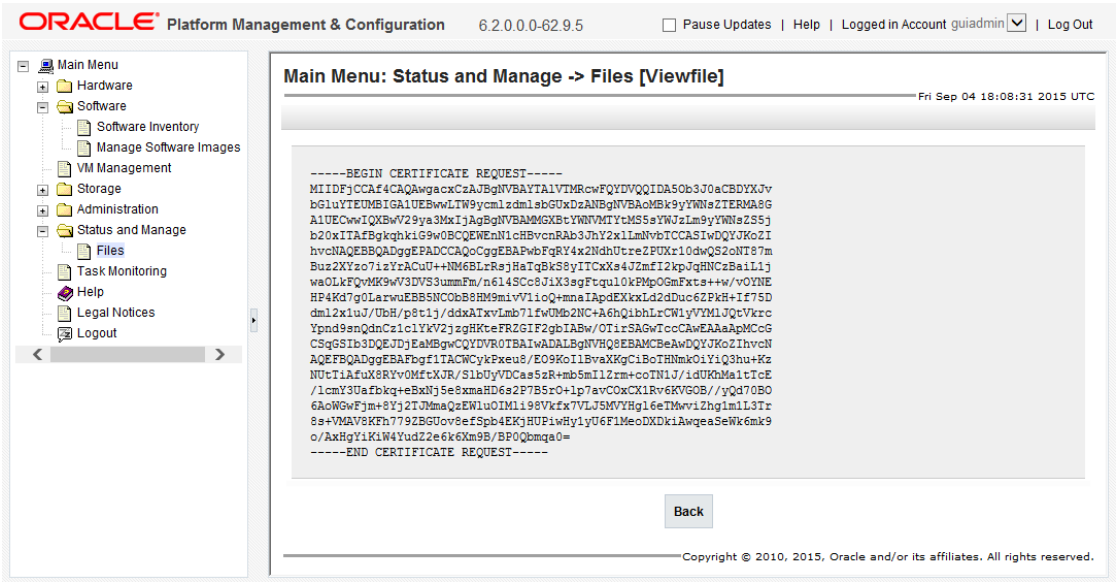


b) PM&C GUI: Select a single file to be viewed.

Note: Only one file may be selected for viewing. If more than one file is selected the View button is disabled.



c) PM&C GUI: The following View File page is displayed which includes the contents of the file.

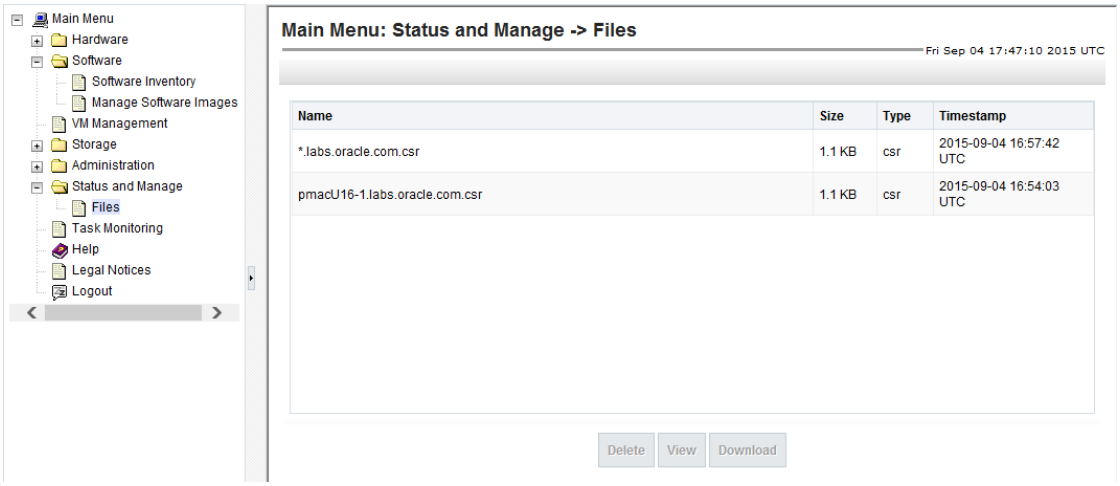


d) PM&C GUI: Once the file has been viewed the user can click on the Back button to return to the original Files Management page (no files will be selected).

3. Download a single file:

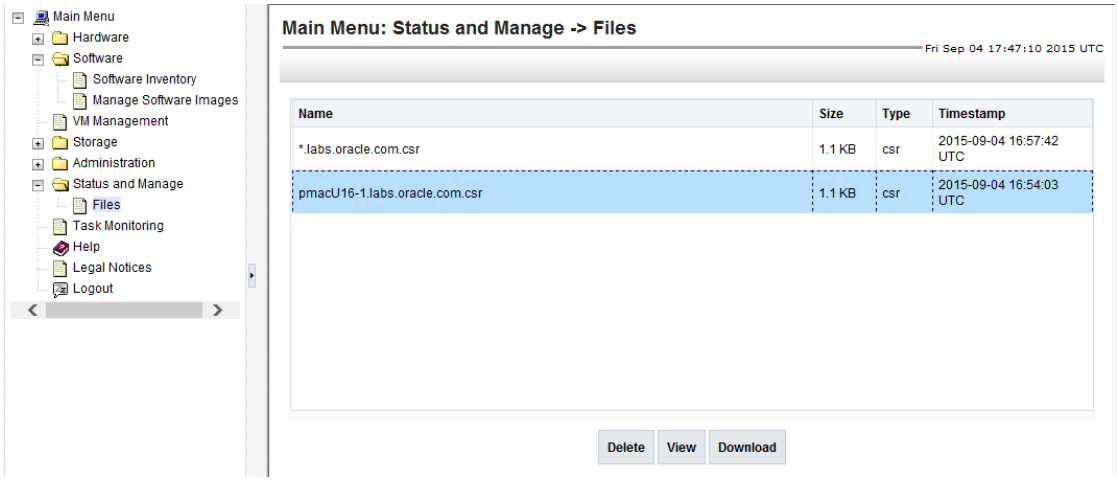
Note: These download steps are browser specific. In this case these instructions apply to Internet Explorer 9 only.

a) PM&C GUI: Navigate to **Main Menu** > **Status and Management** > **Files**.



b) PM&C GUI: Select a single file to be downloaded

Note: Only one file may be selected for downloading. If more than one file is selected the Download button is disabled.



c) PM&C GUI: The Download button should be enabled. Select the Download button.

d) PM&C GUI: Depending on the browser, the user is prompted to save or open the file. The user can choose to open the file or save the file to disk.

Note: The default editor program (usually set to Notepad which does not format files completely) used by Internet Explorer can be changed (as of IE 9) by going to **Tools** > **Internet Options** > **Programs** > **Set Programs** > **Associate a file type or protocol with a program** and choosing the desired default editor for the given file type.

3.7.32 Deleting ISO Images From the PM&C Image Repository

This procedure provides the steps for deleting ISO images from the PM&C repository.

Prerequisite: *3.7.9 Adding ISO Images to the PM&C Image Repository* has been completed.

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

1. PM&C GUI: Login

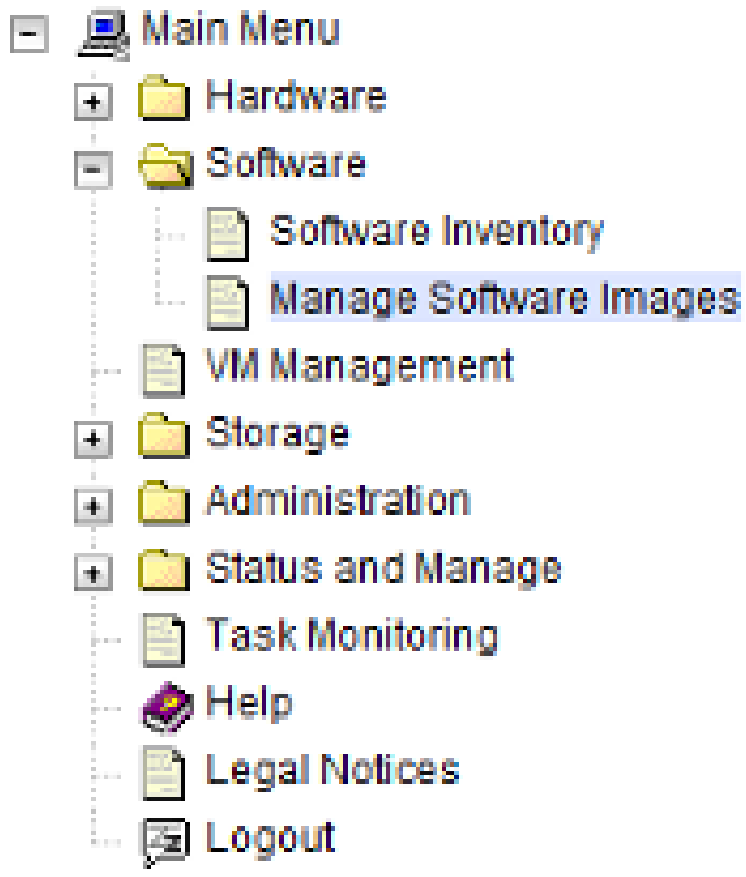
   Open web browser and enter:

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

   Login as guiadmin user.

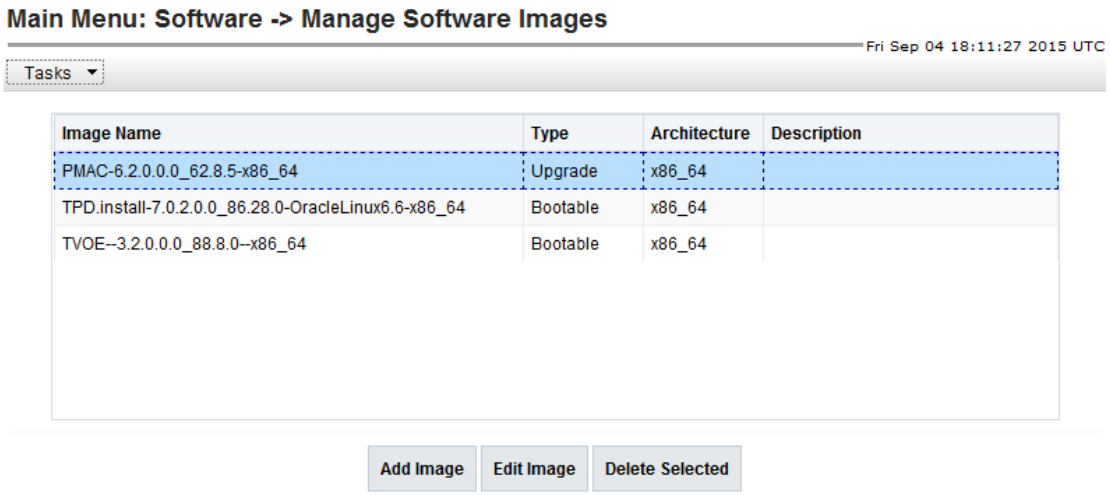
2. PM&C GUI: Navigate to Manage Software Images

   Navigate to **Main Menu** > **Software** > **Manage Software Images**



3. PM&C GUI: Select image to delete.

   Select a software image to delete.

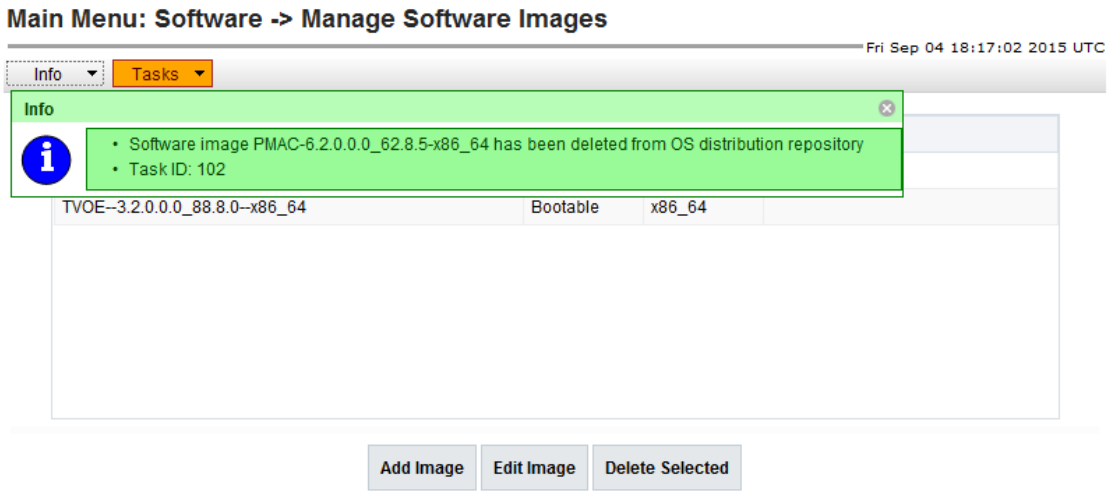


4. PM&C GUI: Delete the image.

   Press the **Delete Image** button. Confirm that you wish to delete the image by pressing OK in the popup dialog.

5. PM&C GUI: Confirm Delete Image finishes successfully.

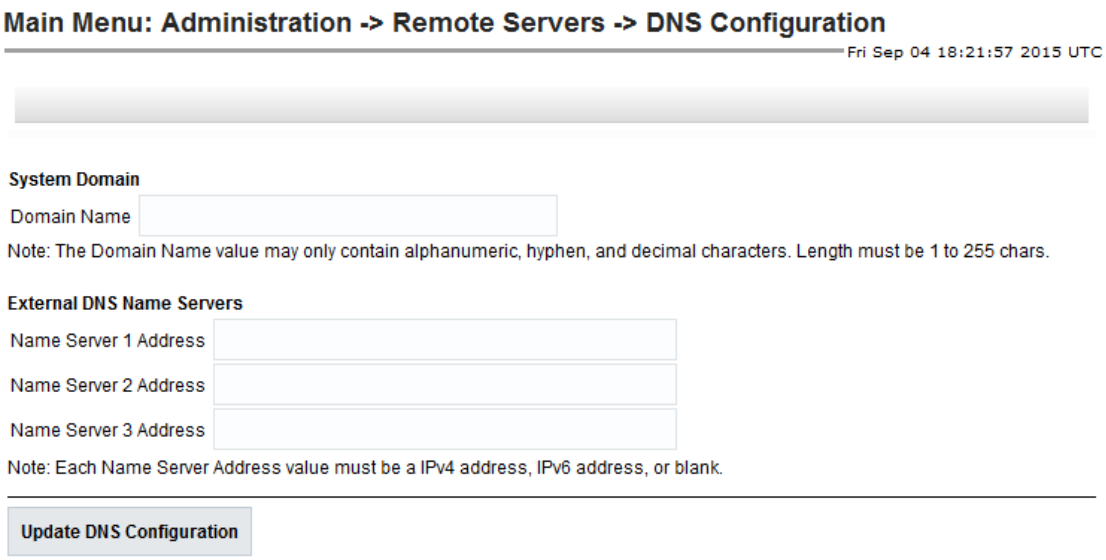
   The Manage Software Images page is then redisplayed with a new Info button displayed in green above the image list. Press **Info** and confirm that the correct image name appears in the info popover.



3.7.33 Configuring PM&C Domain Name System

This procedure provides the steps to configure the PM&C Domain Name System (DNS).

1. Update the Domain Server only
   a) PM&C GUI: Go to **Main Menu** > **Administration** > **Remote Servers** > **DNS Configuration**.

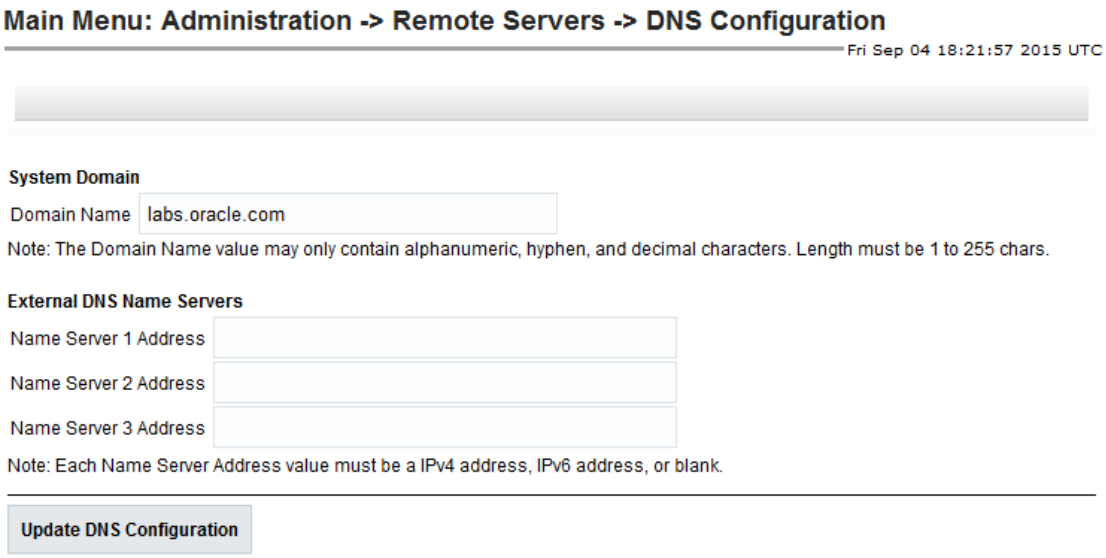


b) PM&C GUI: On initial setup, all fields should be empty. Enter the required Domain Name into the Domain text box. This should be a valid domain name consisting of 1 to 255 alpha numeric characters plus the "." and "-" characters.

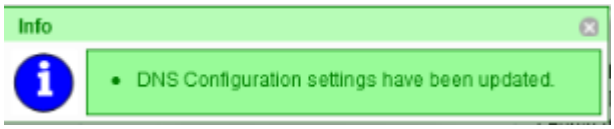
c) PM&C GUI: Leave all Name Server text boxes blank.

d) PM&C GUI: Click on the **Update DNS Configuration** button.

Note: This action will save the Domain Name into the PM&C database. It will not update the DNS **/etc/resolv.conf** file nor enable DNS for the PM&C. After the update, the DNS Configuration page is reloaded and the domain name will be displayed in the Domain text box.



- Upon success, the following Info popup displays:

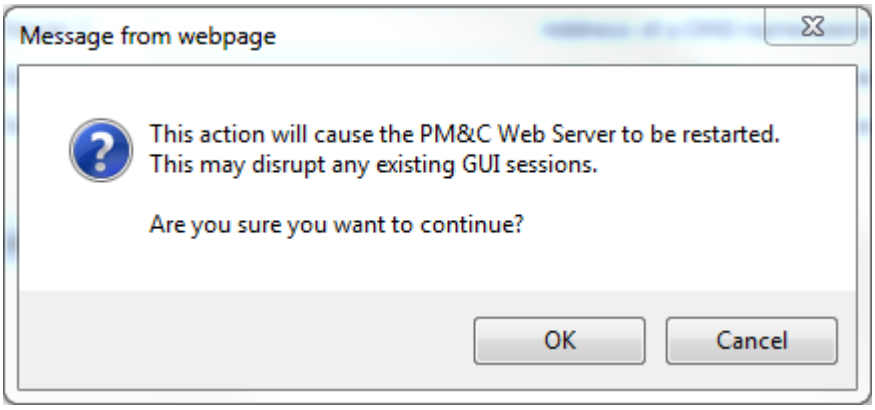


Note: The **/etc/resolv.conf** file will not be updated from the textbox fields in this case. This file will be in the following format (TPD Default):

```
# Generated by NetworkManager


# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so:
#
# DNS1=xxx.xxx.xxx.xxx
# DNS2=xxx.xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
$ cat /etc/resolv.conf
# Generated by NetworkManager
```

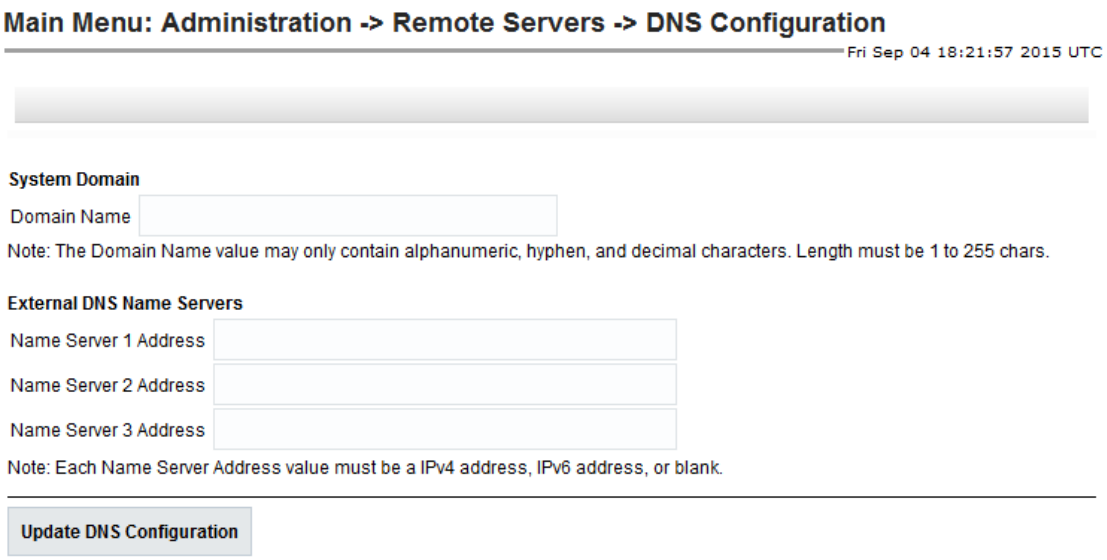
- Upon Domain Name validation failure, the following error popup displays:

e) A user prompt is displayed indicating that this action will cause the PM&C Web Server to be restarted. This action can disrupt any existing GUI sessions in progress. The user must respond with "**OK**" or "**Cancel**". If the user hits "**OK**", the action continues. If the user hits "**Cancel**", the action is stopped and the user is returned back to the DNS Configuration page.



f) When the update is complete, the DNS Configuration page must be refreshed due to the Web Server restart.

2. PM&C GUI: Update the full DNS Configuration.
   a) PM&C GUI: Go to **Main Menu** > **Administration** > **Remote Servers** > **DNS Configuration**.

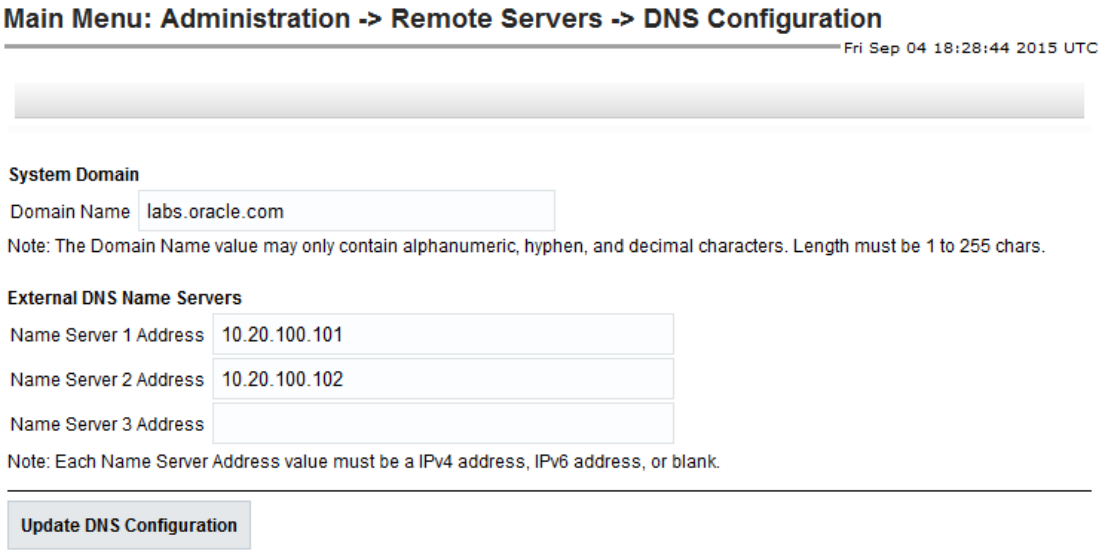


b) PM&C GUI: On initial setup, all fields should be empty. Enter the required Domain Name into the Domain text box. This should be a valid domain name consisting of 1 to 255 alpha numeric characters plus the "." and "-" characters.

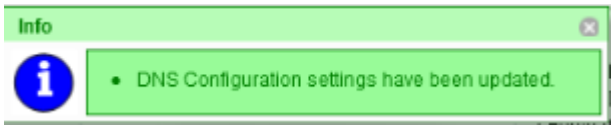
c) PM&C GUI: Enter a valid IPv4 or IPv6 address into each Name Server text box. Note that it is not required to enter an IP into all three Name Server text boxes.

d) PM&C GUI: Click on the **Update DNS Configuration** button.

Note: This action will save the Domain Name into the PM&C database. It will also update the DNS **/etc/resolv.conf** file and enable DNS for the PM&C. After the update, the DNS Configuration page is reloaded and the domain name and all servers entered will be displayed in the appropriate text box.



- Upon success, the following Info popup displays:

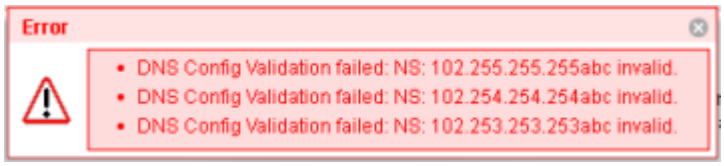


Note: Note: The **/etc/resolv.conf** file will be updated from the textbox fields. This file will be in the following format (TPD Default):

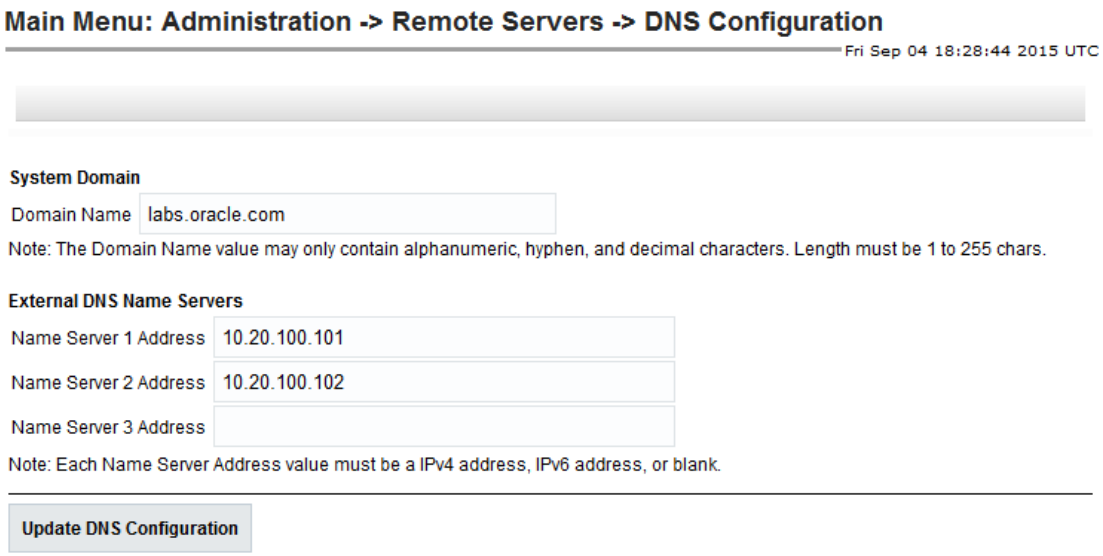
```
# PM&C DNS Configuration File
# ------------------------------------------------------------
# WARNING: Do not make manual changes to this file. This file
#          is auto generated by the PM&C GUI Application at
#          Administration->Remote Servers->DNS Configuration.

domain labs.tekelec.com
nameserver 102.255.255.255
nameserver 102.255.255.254
nameserver 102.255.255.253
```

- Upon Domain Name validation failure, the following error popup displays:

- Upon Server Name validation failure, the error popup may contain a failure message for each Name Server if it was entered incorrectly.



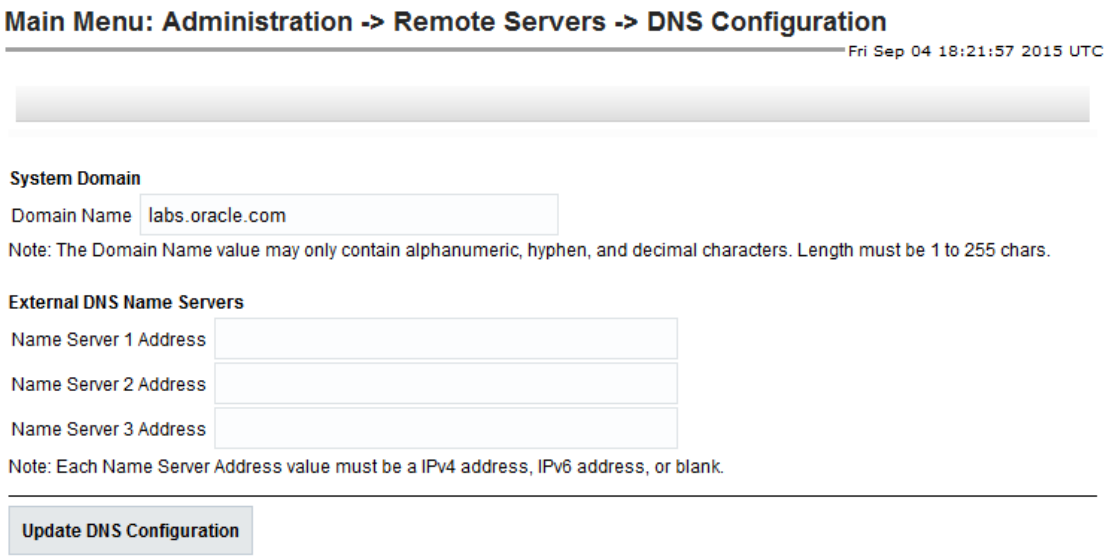
3. **PM&C GUI:** Remove the current DNS Configuration.
   a) PM&C GUI: Go to **Main Menu** > **Administration** > **Remote Servers** > **DNS Configuration**.



b) PM&C GUI: Delete all entries from all Name Server fields. This is assuming that the Domain Name must remain defined for use by the Certificates Management page at **Main Menu** > **Administration** > **Access Control** > **Certificate Management**.

c) PM&C GUI: Click on the **Update DNS Configuration** button.

Note: This action will save the Domain Name into the PM&C database. It will also update the DNS **/etc/resolv.conf** file to the TDP default value and disable DNS for the PM&C. After the update, the DNS Configuration page is reloaded and the Domain Name will be displayed in the **Domain** text box. The Name Servers will be blank.



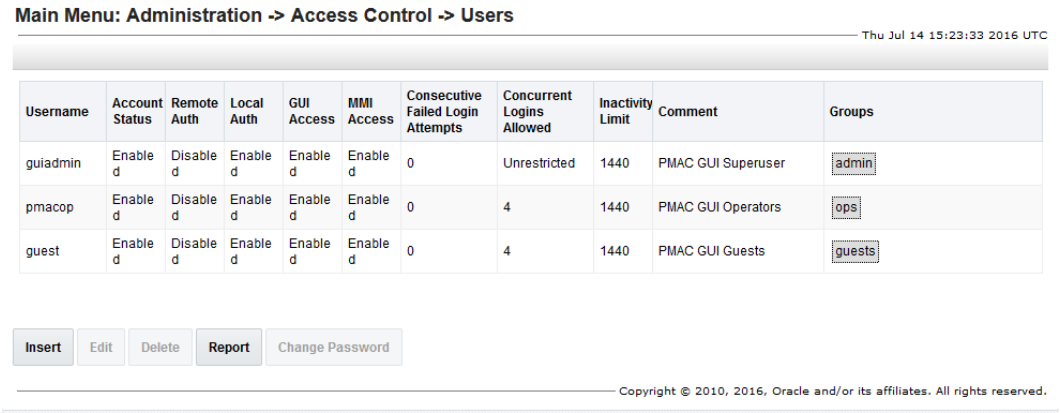
Note: The **/etc/resolv.conf** file will be updated from the text box fields. This file will be in the following format (TPD Default):

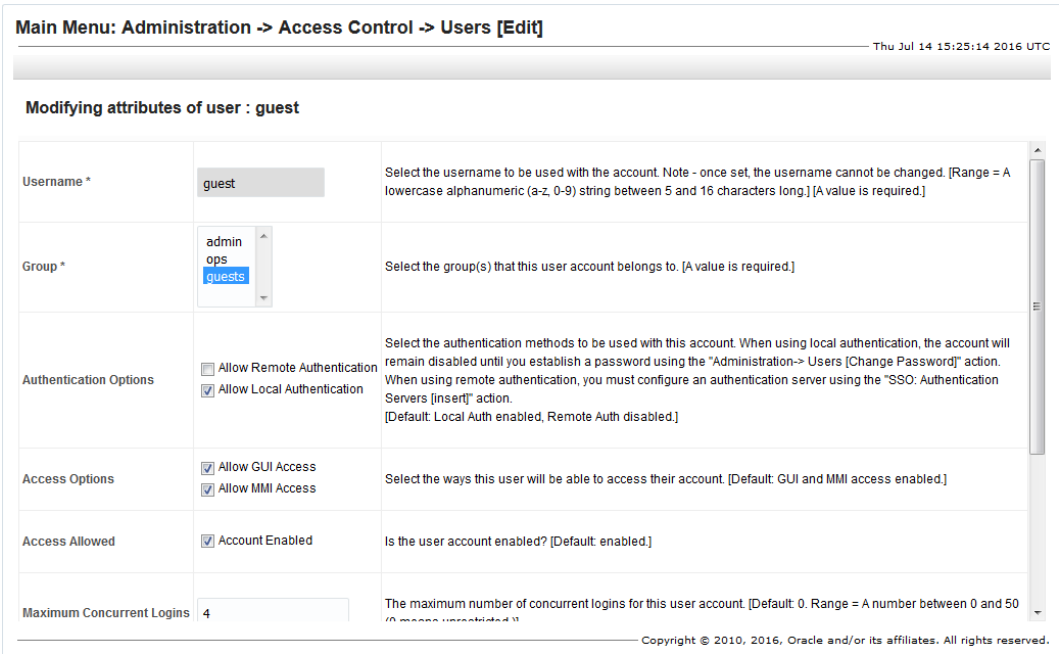
```
# Generated by NetworkManager
```

```
# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so:
#
# DNS1=xxx.xxx.xxx.xxx
# DNS2=xxx.xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
$ cat /etc/resolv.conf
# Generated by NetworkManager
```

3.7.34 Setting User Authentication on the PM&C

This procedure provides information necessary to properly configure the authentication on a new or existing user from the **Main Menu** > **Administration** > **Access Control** > **Users** page using the **Insert** button for new users or selecting an existing user entry and selecting the **Edit** button. Remote Authentication can only be used if an LDAP Server has been properly configured on the PM&C. Please see section *3.7.36 Configuring an LDAP Server on the PM&C* for information regarding LDAP Server configuration.





When creating a new user or updating an existing user, the **Authentication Options - Allow Local Authentication** checkbox is initially checked. The user must apply the following rules when selecting the authentication type:

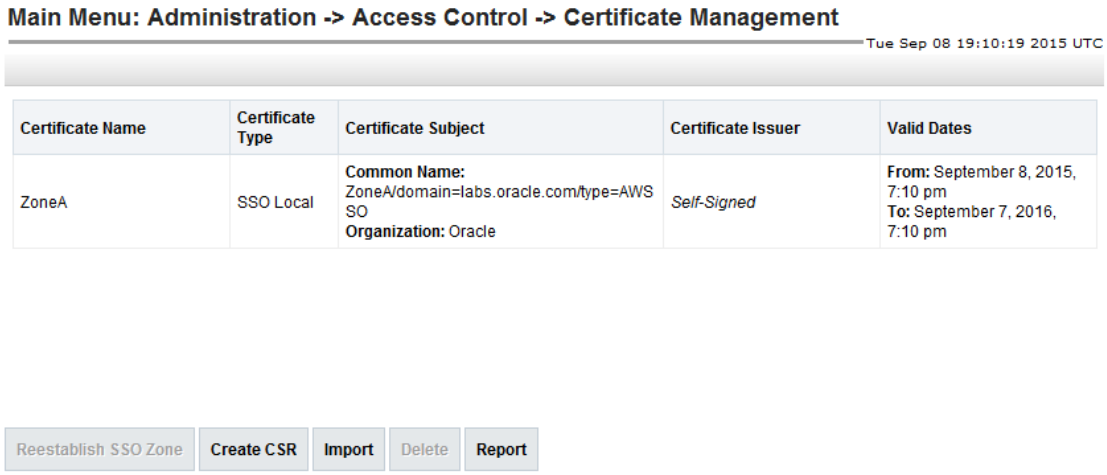
1. The three default users (guiadmin, pmacops, and guest) will have a default setting of **Allow Local Authentication** selected and **Allow Remote Authentication** not selected. On upgrade these settings will be configured according to the setting of the **GUI Site Settings** > **Local Authentication Enabled** (if included in the "from" release).
2. The guiadmin user authentication settings cannot be changed and will be disabled. All other user authentication settings are configurable.
3. The authentication settings for each user (except for the guiadmin user) can be **Allow Local Authentication** or **Allow Remote Authentication** only selected, both **Allow Local Authentication** and **Allow Remote Authentication** selected, or neither selected.
4. If a user is created with neither authentication selected, that user will fail local authentication unless it is an admin group user. It will not attempt remote authentication.
5. If a new user is created with **Allow Remote Authentication** only selected, on first login, the password change request will not be initiated. Once **Allow Local Authentication** is selected on this new user, the user will be prompted for a password change on the next login. After the password change, operation behaves normally.
6. If both **Allow Local Authentication** and **Allow Remote Authentication** are selected, the system will attempt remote authentication first. If communication is established to the LDAP server for authentication and authentication fails, local authentication will not be attempted. The login will be rejected.
7. If both **Allow Local Authentication** and **Allow Remote Authentication** are selected, the system will attempt remote authentication first. If communication is NOT established to the LDAP server for authentication, local authentication will be attempted. The login request will be accepted if the proper local credentials were used.

8. The local password and the remote password do not have to be the same. When logging in, the user must use the appropriate password for the given authentication method. For remote authentication, it is not necessary to enter the password as it is maintained on the LDAP Server.

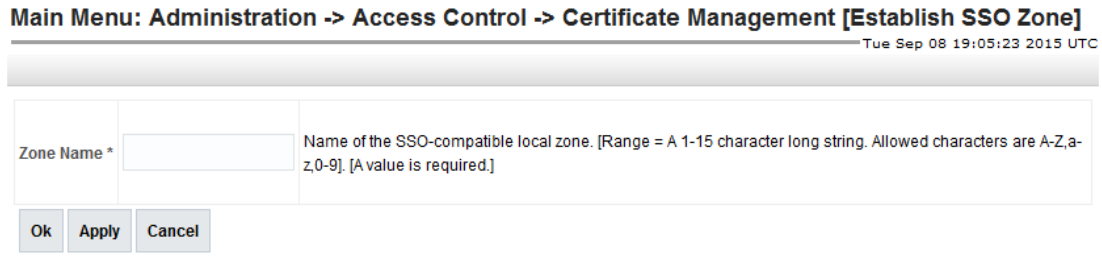
3.7.35 Configuring the PM&C into an existing Single-Sign-On (SSO) Domain

This procedure provides instructions on how to setup and incorporate the PM&C into an existing Single Sign-On Domain. Within a given Domain (SSO can only be configured within a single Domain), the PMAC will be defined within a different Domain Zone than the NO/SO/MP. The SSO certificates of the different zones must be imported manually using the Certificate Management interface of the two Zones (typically from the Appworks GUI and the PM&C GUI). Once each Zone includes the Local SSO certificate and the Remote SSO certificate, the user can log in from one Zone Management GUI which then logs the user into the other Zone Management GUIs.

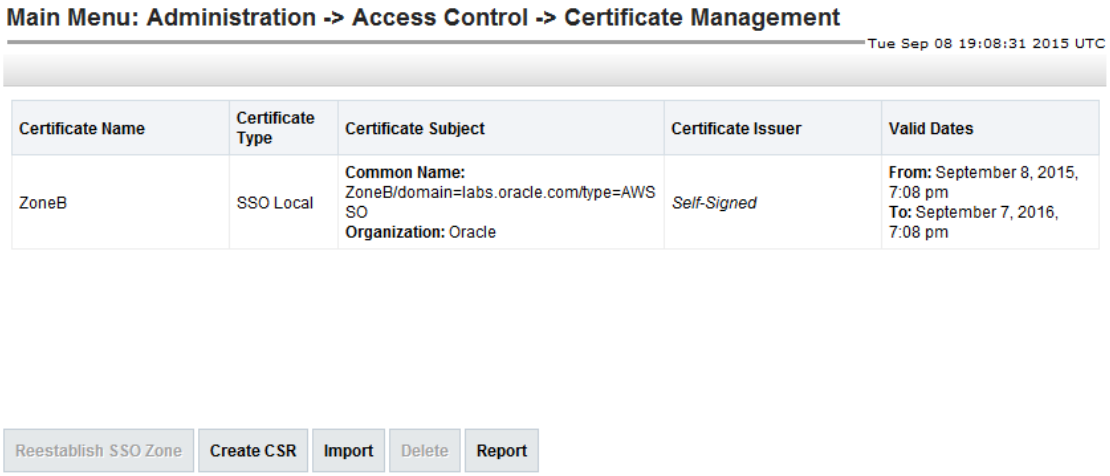
1. There must be a common user defined on both zones with the same group privileges. This user can be configured to use Local or Remote Authentication (see section *3.7.34 Setting User Authentication on the PM&C*).
2. The current zone (ZoneA - consisting of the NO/SO/MP architecture) should already have an existing SSO certificate configured from the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page using the **Establish SSO Zone** button. This would be indicated as the "SSO Local" certificate type.



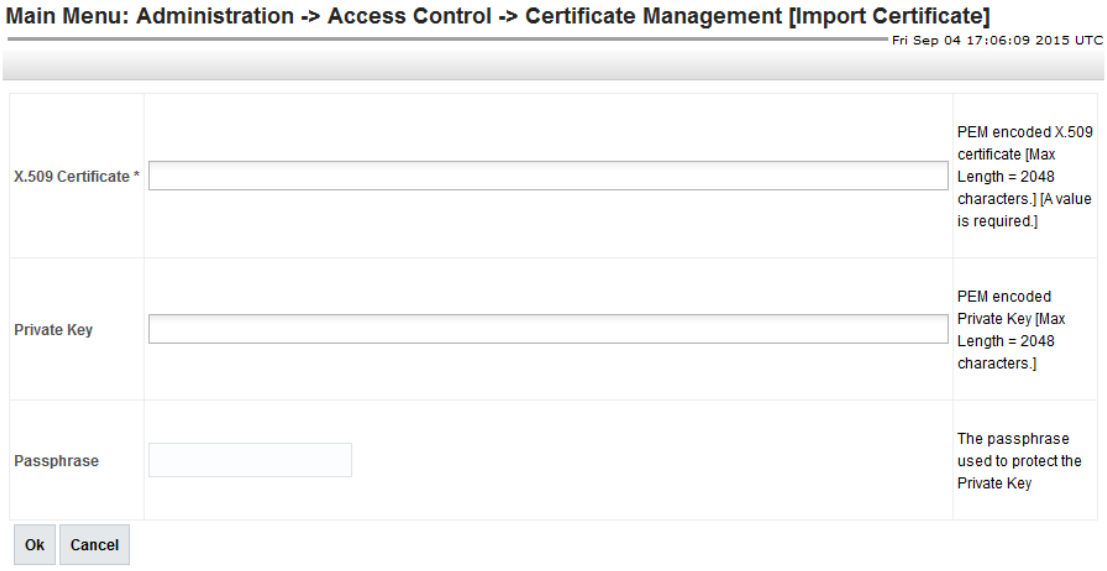
3. From the ZoneB (PM&C) GUI go to **Main Menu** > **Administration** > **Access Control** > **Certificate Management**, select the **Establish SSO Zone** button.



4. Enter a valid name in the **Zone Name** field. Select the **Ok** button. This will create a "SSO Local" certificate type on the PM&C and return the user to the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page.

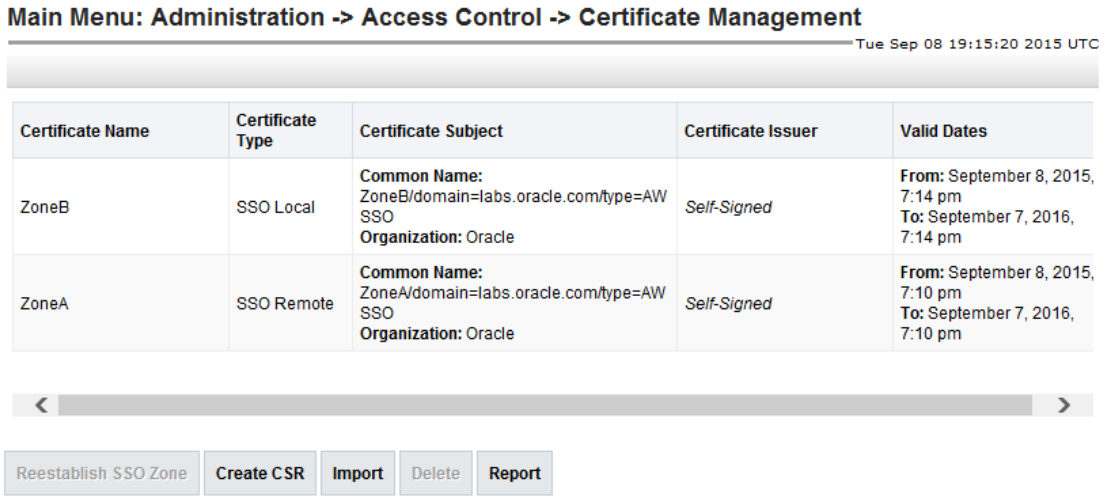


5. From ZoneA (Appworks) GUI go to the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page. Select the ZoneA SSO Local certificate and select the **Report** button. This should display a printable encrypted version of the certificate.
6. Copy the certificate from the "-----BEGIN CERTIFICATE-----" to the end of the "-----END CERTIFICATE-----".
7. Select the **Back** button to return to the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page.
8. Go to the ZoneB (PM&C) GUI **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page.
9. Select the **Import** button.

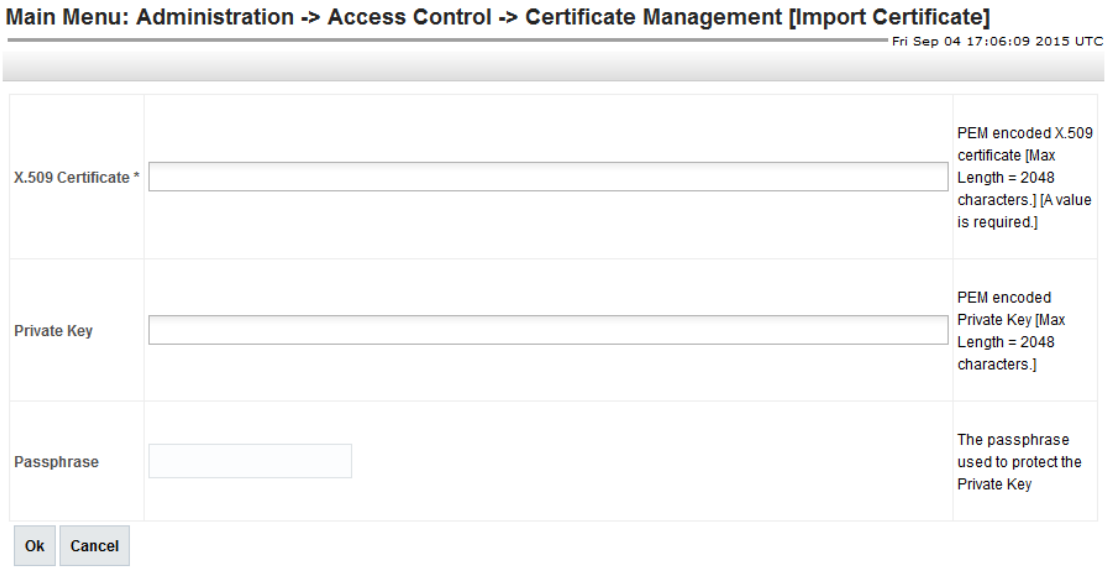


10. Paste the copied certificate from ZoneA into the **X.509 Certificate** field. Leave the other fields blank.

11. Select the **Ok** button. This should create a Remote SSO certificate and return to the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page displaying ZoneB as the SSO Local certificate type and ZoneA as the SSO Remote certificate type.

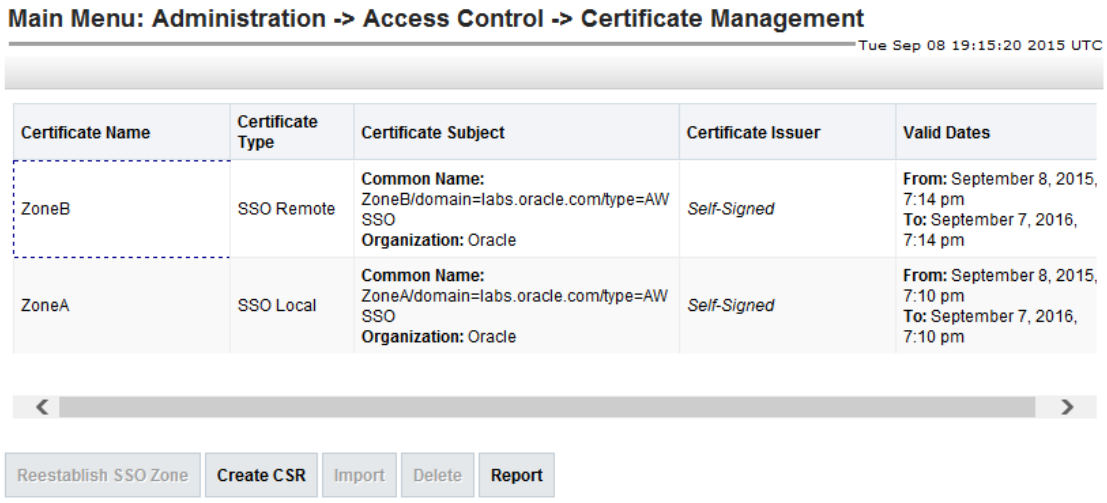


12. From ZoneB (PM&C) GUI go to the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page. Select the ZoneB SSO Local certificate and select the **Report** button. This should display a printable encrypted version of the certificate.
13. Copy the certificate from the "-----BEGIN CERTIFICATE-----" to the end of the "-----END CERTIFICATE-----".
14. Select the **Back** button to return to the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page.
15. Go to the ZoneA (Appworks) GUI **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page.
16. Select the **Import** button.



17. Paste the copied certificate from ZoneB into the **X.509 Certificate** field. Leave the other fields blank.

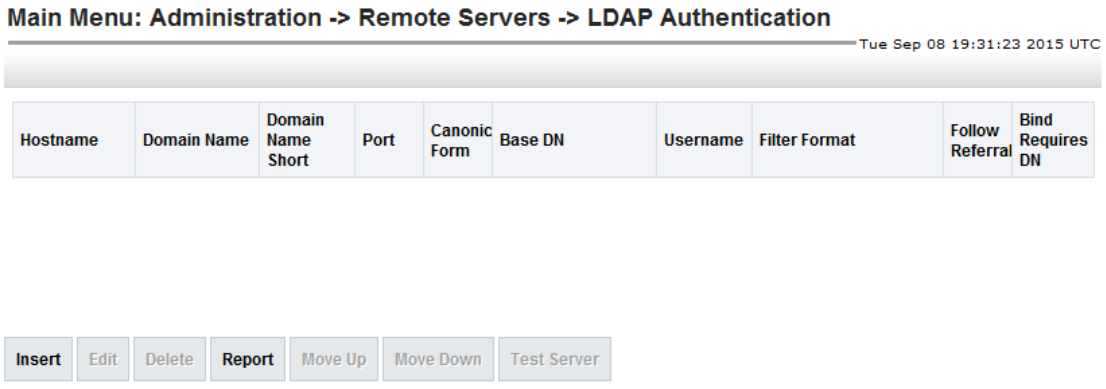
18. Select the **Ok** button. This should create a Remote SSO certificate and return to the **Main Menu** > **Administration** > **Access Control** > **Certificate Management** page displaying ZoneA as the SSO Local certificate type and ZoneB as the SSO Remote certificate type.



19. Once both Zones have their Local and Remote SSO certificates configured, the user should be able to login from ZoneA or ZoneB using the configured user that is defined on both zones. Once logged in from one zone, the other zone GUI should be logged in immediately.
20. If the user logs out from either Zone, both zones will be logged out.
21. If a user logs in from ZoneA, which logs in ZoneB, and later the ZoneB session times out due to a short session timeout settings configured on ZoneB, ZoneA will remain logged in. This works the same in either direction.

3.7.36 Configuring an LDAP Server on the PM&C

This procedure provides instructions on how to configure a LDAP server on the PM&C. The main configuration page is at **Main Menu** > **Administration** > **Remote Servers** > **LDAP Authentication**

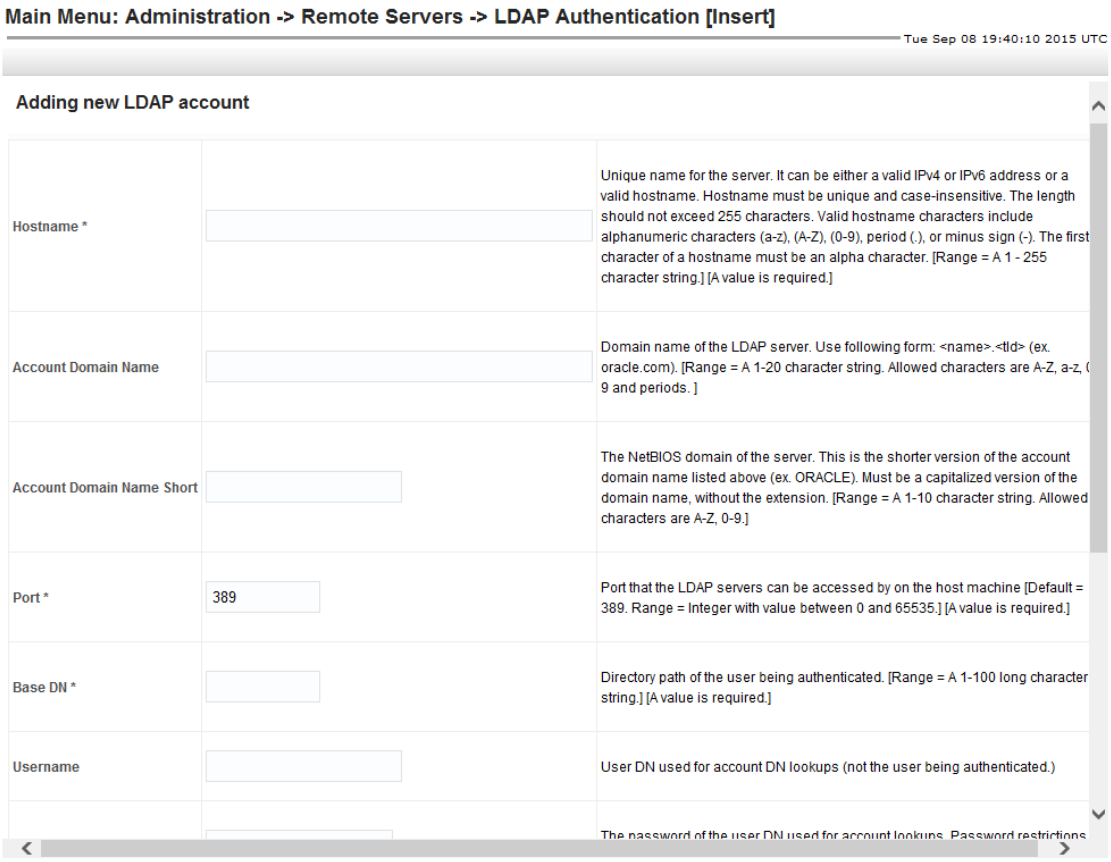


Only the **Insert** and **Report** buttons should be available for selection and no LDAP Servers configured.

1. Select the **Insert** button.

   The following page is displayed:

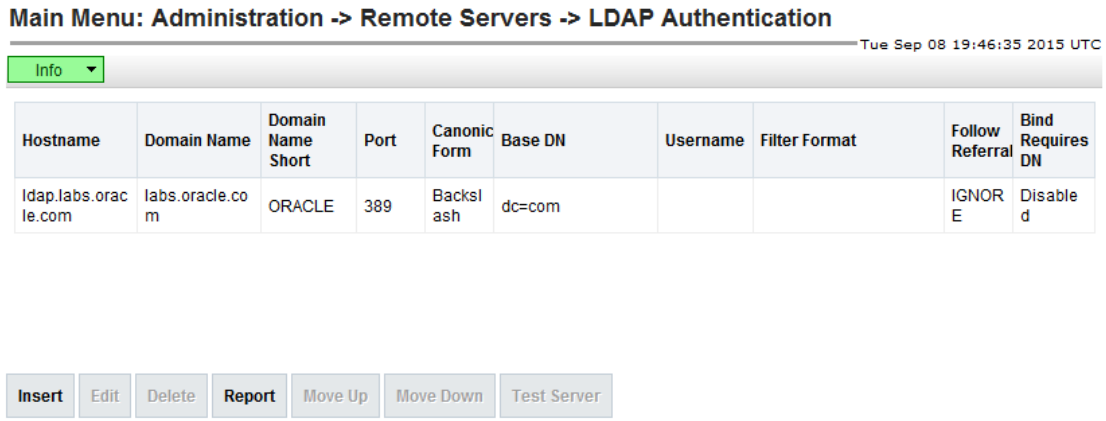
Note: Port 389 has been set as default. This is the standard port number for LDAP communication. (Change it if necessary):



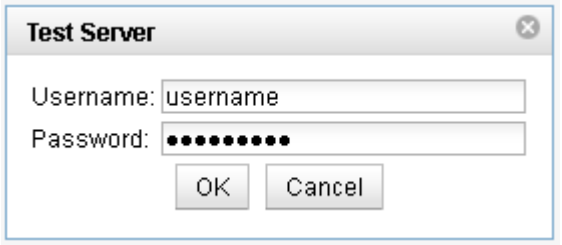
This page contains the necessary fields required to configure a LDAP Server. Please contact your LDAP Server Administrator for the proper values required to complete the fields provided.

2. Select the **OK** button which configures the LDAP Server and returns to the **Main Menu** > **Administration** > **Remote Servers** > **LDAP Authentication** page or select the **Apply** button which remains on the **Insert** page.

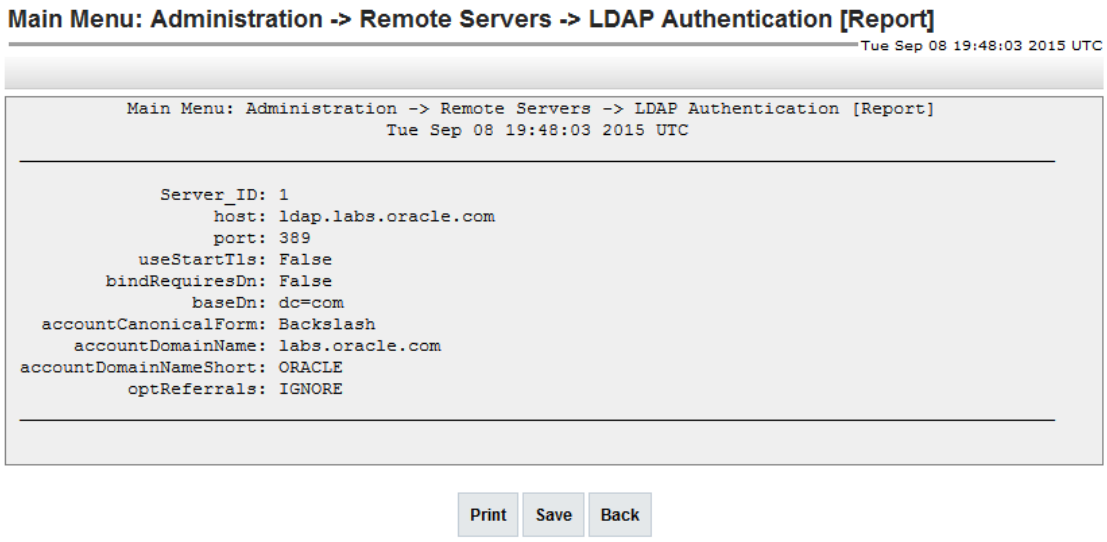
   Once entered the following is displayed at the **Main Menu** > **Administration** > **Remote Servers** > **LDAP Authentication** page (assuming the configuration indicated):



The user can verify the communication to the LDAP server if they know a valid username and password configured on the LDAP Server by selecting the **Test Server** button. This will send a LDAP message to the server to verify the user and verify communication to the LDAP Server.



The user can also select the **Report** button to display the configuration data of the LDAP for printing purposes.



3.7.37 Transfer Image from PM&C Repository to Other Servers

This procedure provides the steps for transferring a software image from the PM&C image repository to servers managed by PM&C.

Prerequisites:

- Enclosures containing blade servers or servers containing a TVOE host targeted for application install/upgrade have been configured using the *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory* procedure.
- Rack mount servers targeted for application install/upgrade have been configured using the *3.7.16 Add Rack Mount Server to the PM&C System Inventory* procedure.
- An image was added to the PM&C image repository using the *3.7.9 Adding ISO Images to the PM&C Image Repository* procedure.

Note: The image transfer is only supported for discovered entities (IP address is known).

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

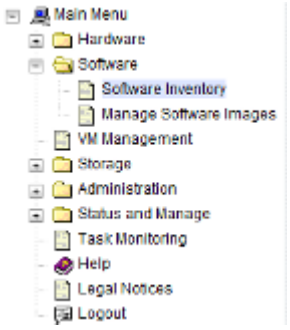
   If needed, open your web browser and enter:

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

   Login as the guiadmin user.

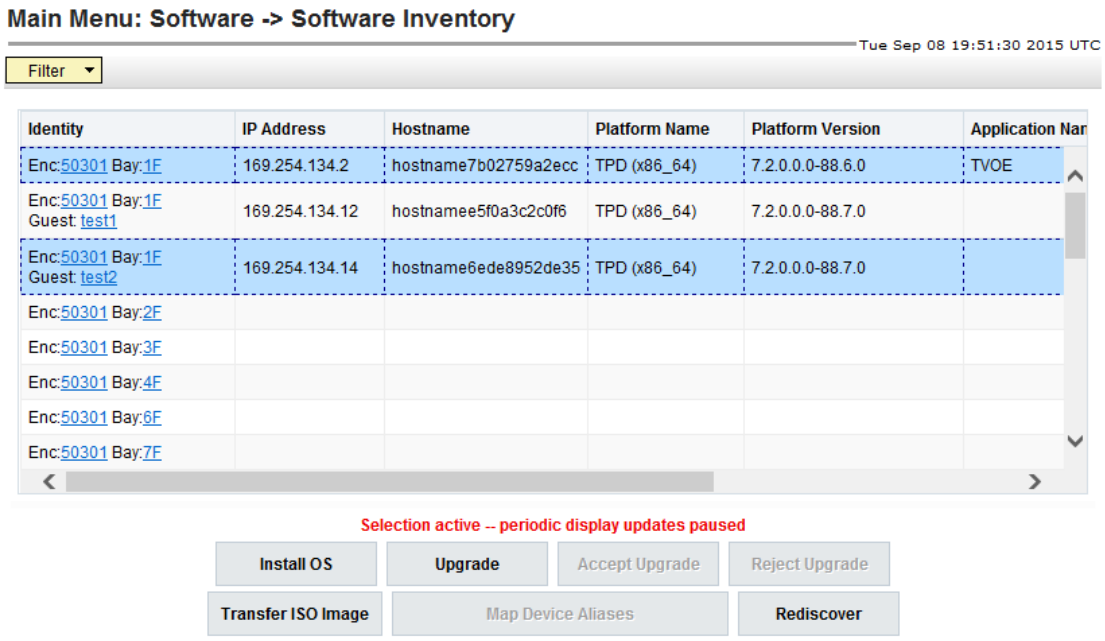
2. PM&C GUI: Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory.**

3. PM&C GUI: Select Servers

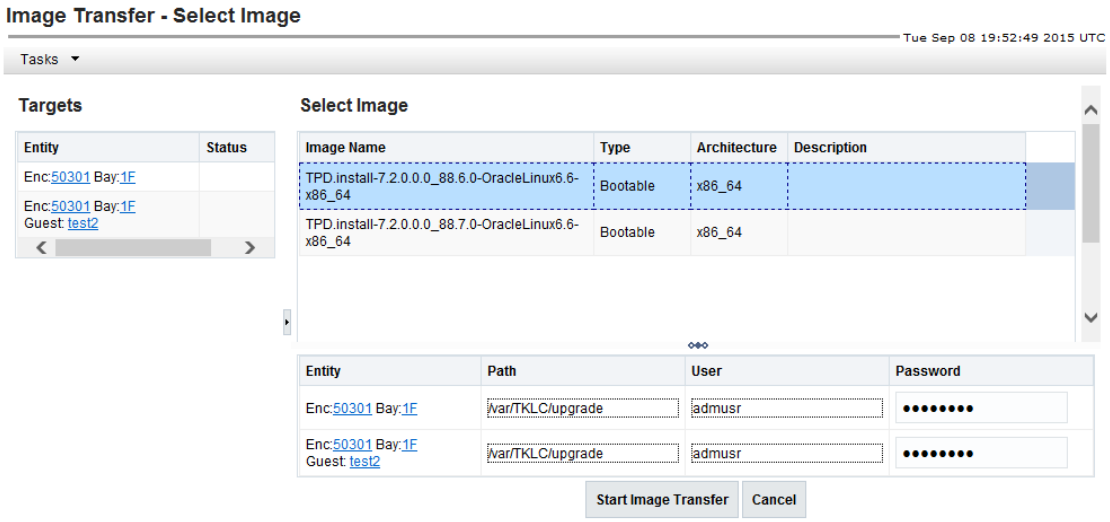
   Select the servers you want to transfer the image to. If you want to perform an upgrade on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted.



Press the **Transfer ISO Image** button.

4. PM&C GUI: Select image

   The left side of the screen displays the servers to be targeted for the transfer. From the list of ISO images on the right side of the screen, select the image to transfer to the previously selected servers.

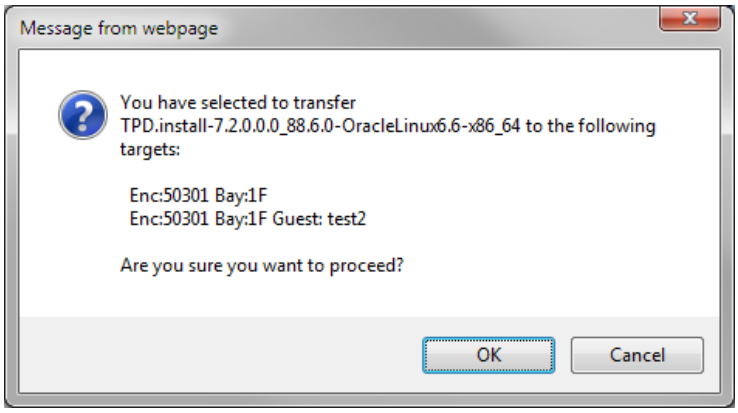


5. PM&C GUI: Supply path, user and password for target entities

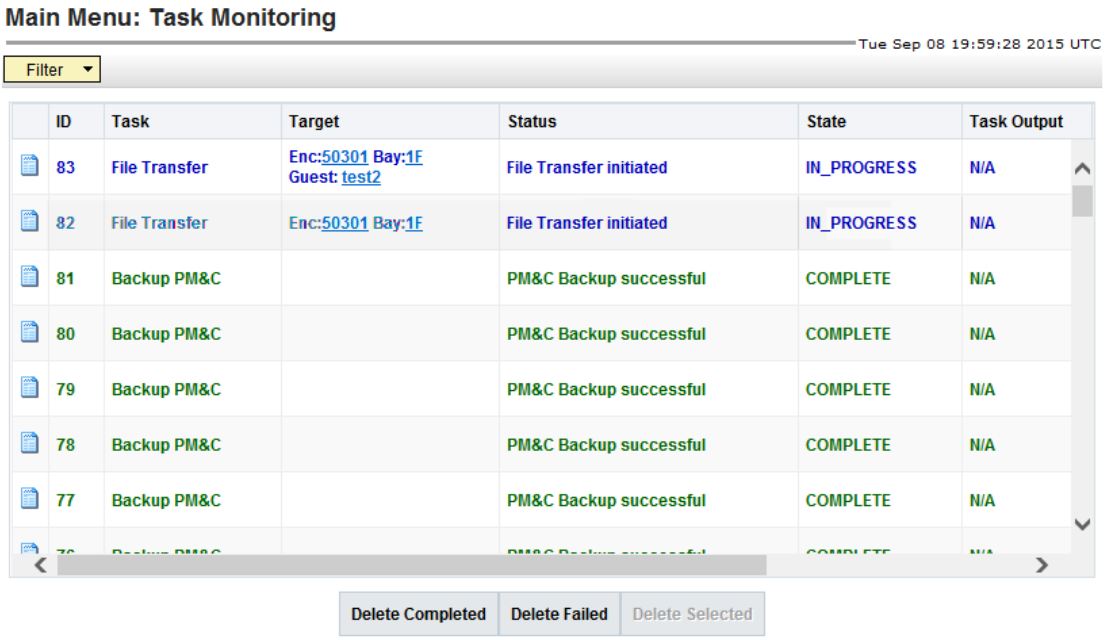
   The arguments to be used for transfer of the image to previously selected servers can be supplied by entering them into the fields displayed below the software images table.

   Note: PM&C does not validate supplied arguments; it only verifies they are all present. The credentials should be consistent with credentials that would be used for SCP. The path should be accessible with the credentials given.

6. PM&C GUI: Start Image Transfer
   Press the **Start Image Transfer** button.
7. PM&C GUI: Confirm the image transfer action
   Press the **OK** button to proceed with the image transfer.



8. PM&C GUI: Monitor the Image Transfer
   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the File Transfer background task. A separate task will appear for each server being updated.



When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

3.8 Configuring SAN

3.8.1 Configure SAN Storage Using PM&C Application

This procedure will configure a SAN storage using the PM&C application. The end user will be able to configure the SAN controller and corresponding host volumes using XML files uploaded by the PM&C application. The XML files will allow the end user to: add virtual disks, delete virtual disks without an associated volume, add global spares, delete global spares and delete volumes on the SAN controller and/or host volume. Refer to the instructions provided by the application to obtain or create XML files used in this procedure.

Prerequisite:

- *3.5.2 Configure Initial OA Settings Using the Configuration Wizard* and
- *3.7.6 Configure PM&C Application* have been completed.
- *3.3.3 Configuring Advanced Settings on MSA2012fc Fibre Channel Disk Controllers* or
- *3.3.4 Configuring Advanced Settings on P2000 Fibre Channel Disk Controllers* have been completed for given SAN storage type.
- *3.2.3 Configure Zones in Brocade Switches* has been completed.

Note: When a disk fails, the system looks for a dedicated spare first. If it does not find a properly sized dedicated spare, it looks for a global spare. A best practice is to designate spares for use if disks fail. Dedicating spares to vdisks is the most secure method, but it is also expensive to reserve spares for each vdisk. Alternatively, you can assign global spares. A properly sized spare is one whose capacity is equal to or greater than the largest disk in the vdisk.

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. Handle failed SAN configuration

   Note: If any attempt to add SAN storage components have failed, a partial configuration may exist. This needs to be cleaned-up before attempting again.

   Note: If an attempt to add SAN storage components fails before any configuration is done, such as an invalid XML file or a wrong disk name, then correct the XML file error and attempt the SAN storage configuration again.

   If a partial configuration exists, follow the instructions provided by application to obtain/create XML files that will delete the partial configuration and clear the SAN controller or host volume. Note that after a host volume is deleted or cleared, PM&C will automatically reboot the server blade. Once the XML file is obtained, continue following *3.8.1 Configure SAN Storage Using PM&C Application* to correctly upload and execute the XML file using the PM&C application. If the end user desires to IPM the blade server to cleanup host volumes, refer to *3.7.10 IPM Servers Using PM&C Application*.

2. PM&C server: Provide SAN configuration xml files

   Log in to the management server as user 'admusr'.

   Copy all SAN configuration xml files into **`/usr/TKLC/smac/etc/storage`** directory.

3. PM&C server: Update SANcontroller password in PM&C

If default password has been changed on SAN controllers, then the stored password in PM&C must be changed to match. Run this script on PM&C and set the SAN controller password for the manage user:

$ **sudo /usr/TKLC/smac/bin/updateCredentials --type=msa**

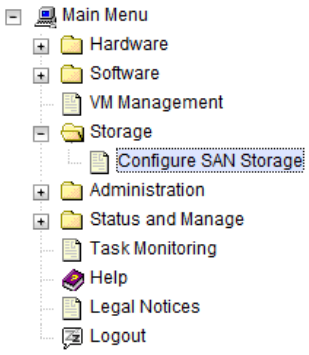
4. PM&C GUI: Login

   If needed, open web browser and enter: **https://<pmac_management_network_ip>**

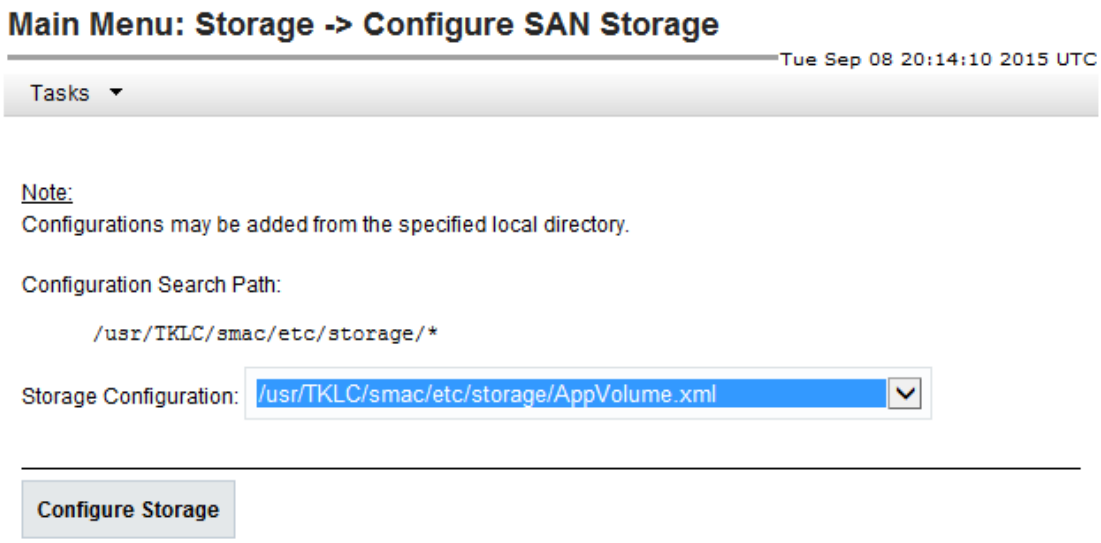
   Login as guiadmin user.

5. PM&C GUI: Configure SAN

   Navigate to **Main Menu** > **Storage** > **Configure SAN Storage** .



From the **Storage Configuration** drop down menu choose SAN configuration file and press **Configure Storage**.

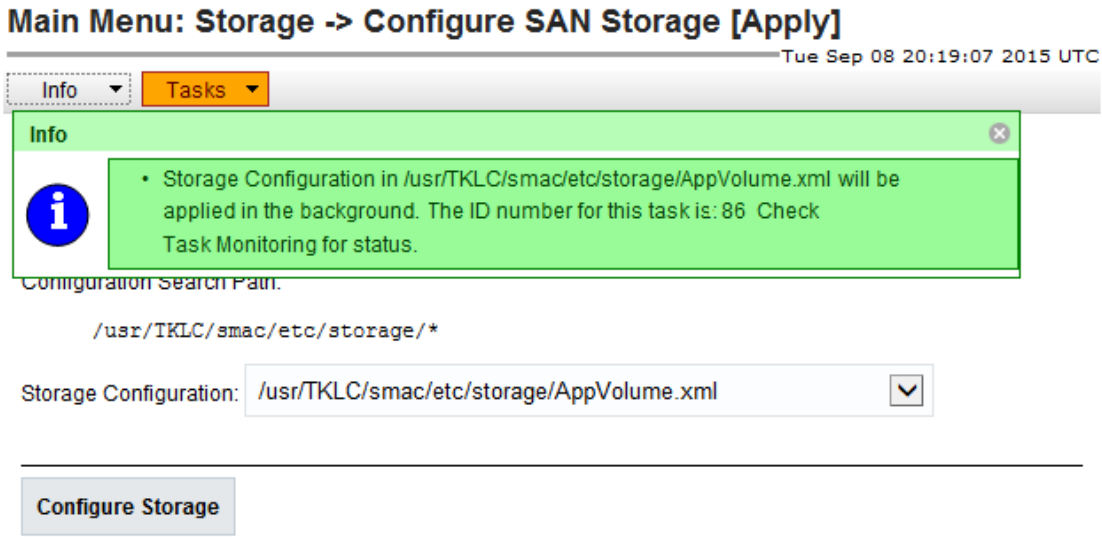


Note: Concurrent execution of SAN configuration files is supported. Do not run configuration files at the same time if the xml files configure either the same blade server or the same MSA storage system, otherwise a failure may occur . Additionally, configuration on a server blade is being cleared, or if a host volume is being deleted, then execution may take longer since PM&C will automatically reboot the server blade after configuration removal.

If any errors occur with this procedure, collect logs from the affected blade in **`/var/TKLC/log/tpdProvd/tpdProvd.log`**

6. PM&C GUI: Monitor the configuration status

   The **Configure SAN Storage** page is then redisplayed with a new background task entry in the table at the bottom of the page:



7. Recovery from configuration errors

   If PM&C is able to successfully parse the XML configuration file, the actual configuration process is executed. If any error is encountered, the processing is aborted, and the state is left as it was at the point of failure. For recovery suggestions, refer to step 1: Handle failed SAN Configuration.

3.8.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation

This procedure describes how to remove volumes from the partially installed SAN. This can happen if the SAN configuration fails. Blade servers are IPMed again.

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

1. Management server: Update SAN controller password

   If default password has been changed on SAN controllers, then the stored password in the PM&C must be changed to match. Run this script on PM&C and set the SAN controller password for the manage user:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=msa
```

2. Log into the Fibre Channel Controller GUI as manage

   https://<controller_IP_address>

   a) For MSA2012 Dual Controller Array configuration:

1. Navigate to **Manage > Volume Management > Delete volume** and select the volume to delete.

   Repeat for all volumes.

2. Navigate to **Virtual Disk Config > Delete a vdisk** and select the vdisk to delete.

   Repeat for all vdisks.

3. Navigate to **Virtual Disk Config > global spares menu > delete global spares.**

   Select all of the global spare disks and click **Delete Global Spares** button.

Repeat this step for second controller.

b) For P2000 MSA Dual Controller Array configuration:

1. Navigate to **Provisioning > Delete volumes** and select all volumes to delete.
2. Navigate to **Provisioning > Delete vdisks** and select all vdisks to delete.
3. Navigate to **Provisioning > Manage Global Spares** and unselect all the global spare disks, then click **Modify Spares** button.

Repeat this step for second controller.

3. OA GUI: Login to active OA

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

4. OA GUI: Delete zones from Brocade switches

   Select one of the Brocade switches and click on **Management Console**

   Login as an administrative user.

   Select **Zone Admin** and click on **Clear All**.

   Wait for success message in bottom left of window and `Effective zone Config: Default, All Access` in bottom right of window.

   Click **Save Config**.

   Repeat for the second switch.

5. Run IPM on the blade servers

   Run IPM on blade servers following *3.7.10 IPM Servers Using PM&C Application* application.

   Note: A new IP address will be assigned to bond0 of each blade at the end of the IPM process, so the .xml files will need to be updated accordingly.

3.9 Virtualization Procedures

3.9.1 Create guest server using PM&C application

This procedure provides the steps for creating a virtualized guest server on a TVOE host, using the PM&C web GUI.

Prerequisites:

- Enclosure containing the TVOE host blade server to host the guest has been configured using *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory*.
- The TVOE host has been installed using *3.7.10 IPM Servers Using PM&C Application*.

Note: PM&C will not prevent over-subscription of memory or CPU resources.

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

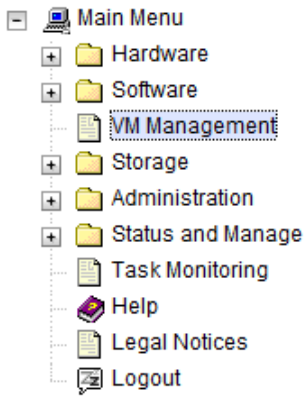
   If needed, open web browser and enter:

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

   Login as **guiadmin** user.

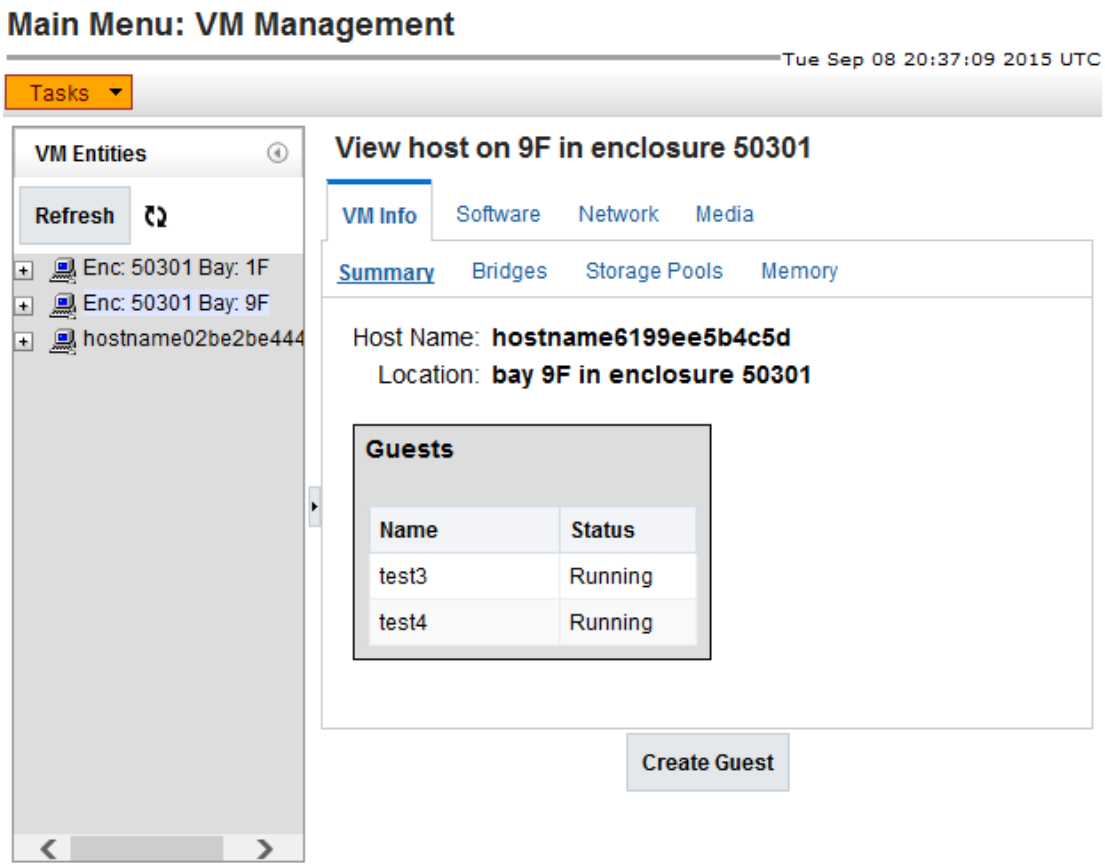
2. PM&C GUI: Navigate to VM Management

   Navigate to **Main Menu** > **VM Management**.

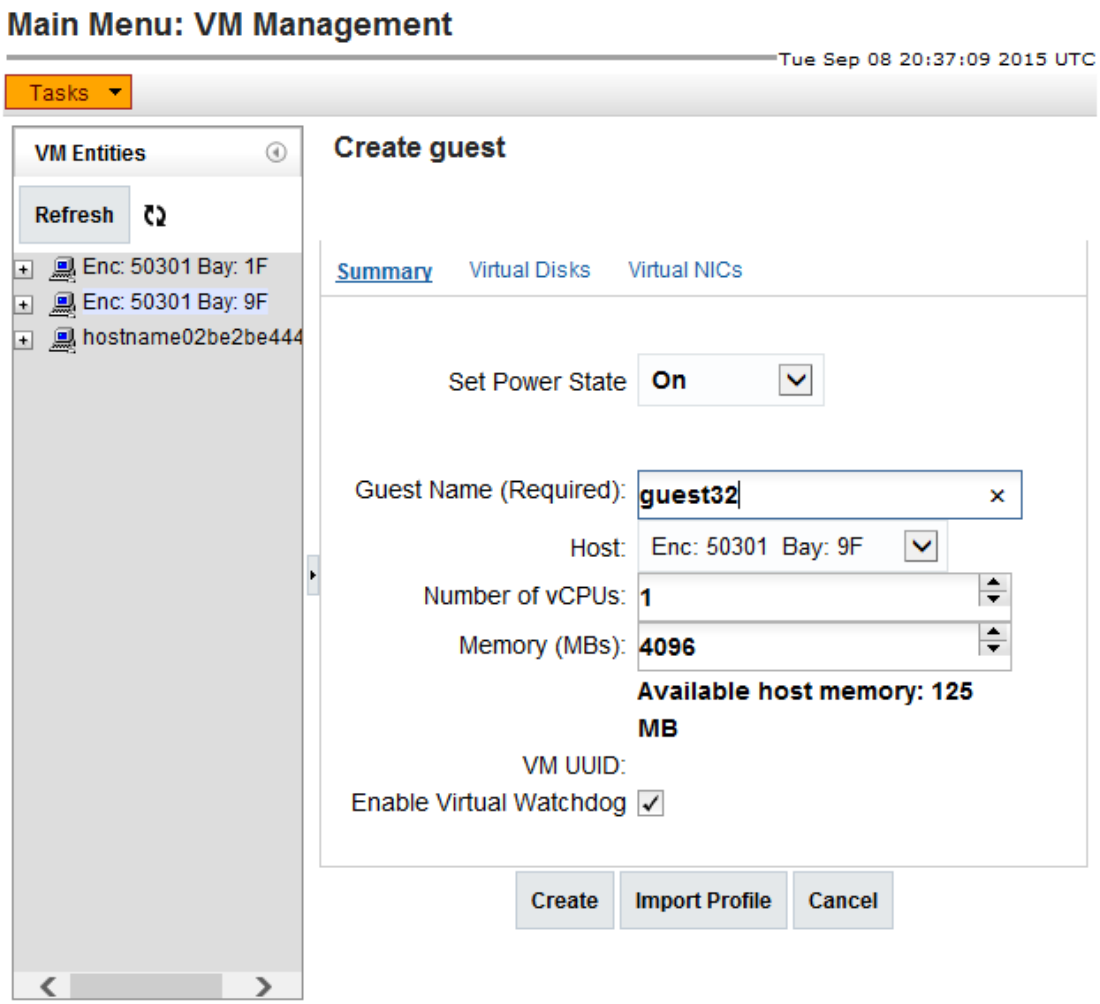
3. PM&C GUI: Click the "**Create Guest**" button.

   On the Virtual Machine Management page, click the **Create Guest** button

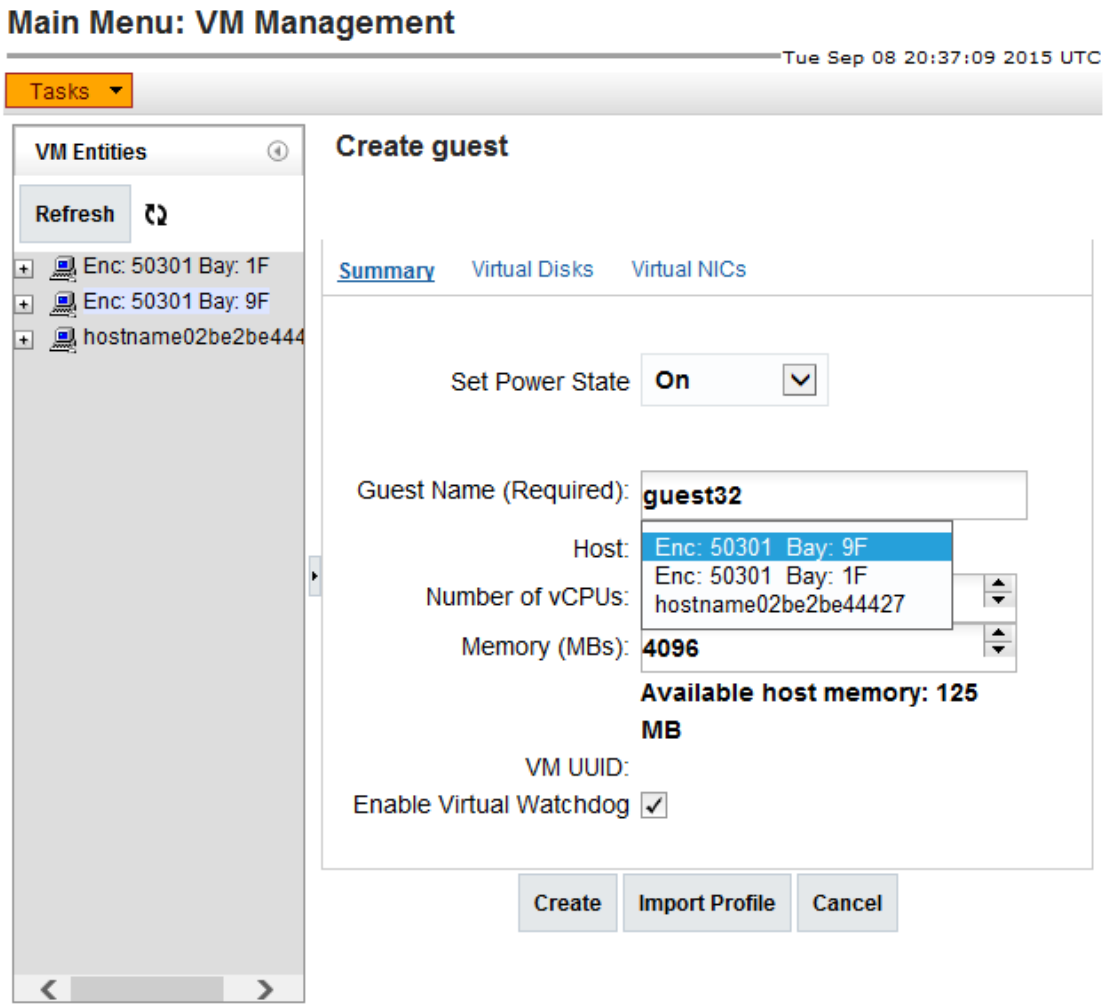


4. PM&C GUI: Enter guest name

   Fill in the **Name** field with something unique to the TVOE host. The name can be identical to a guest on a different host.

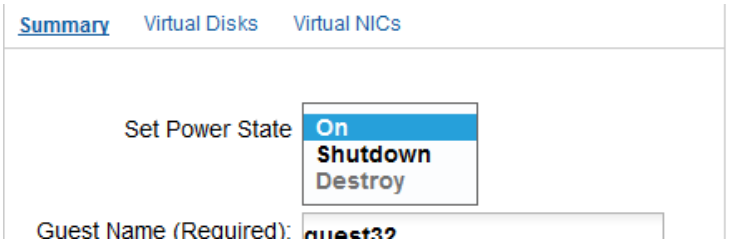


5. PM&C GUI: Select the TVOE Host for the new guest.
   Using the dropdown Host field, select the TVOE host on which to create the guest.



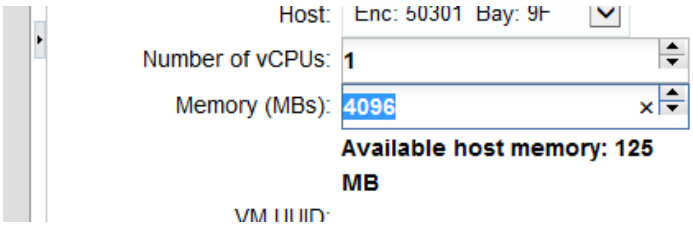
6. PM&C GUI: Select the desired initial power state

   Using the dropdown field to the right, select the initial power state for the guest. In this context, **Shutdown** and **Destroy** both behave the same, the guest will not be powered on upon creation.



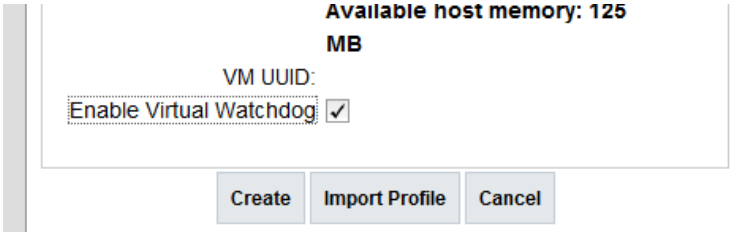
7. PM&C GUI: Edit the vCPU count and Memory size.

   Using the arrows to the right of the fields, adjust the number of virtual CPUs and the amount of memory (in MBs) to use for the guest. These fields are also manually editable test fields. PM&C will not prevent over-subscription of these resources.



8. PM&C GUI: Edit the Watchdog setting (if available)

   If this Guest is being created on a version of TVOE having support for virtual guest watchdogs, the Enable Virtual Watchdog item will be present. Set this checkbox according to whether or not watchdog support is desired for this Guest.



9. PM&C GUI: Edit the primary virtual disk

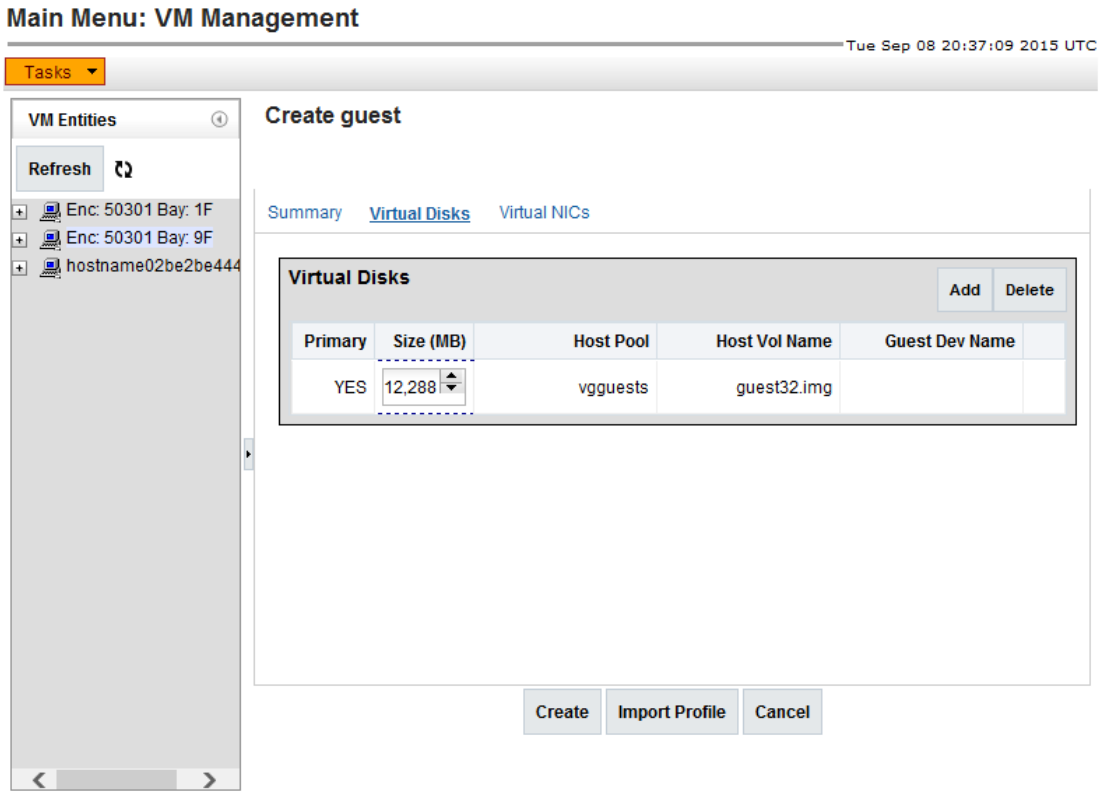
   A primary disk is specified by default. The Virtual Disks list can be edited to change the details of the primary disk and to add virtual disks. The primary disk will be used to install the OS. See the application requirements for the desired settings.

   Size (MB): By default, a primary disk is specified with the minimum size supported by TPD, click on the number to adjust the size via arrow or the keyboard.

   Host Pool: The default vgguests storage pool is selected. Using the dropdown box, other pools that have been configured on the TVOE can be selected.

   Host Vol Name: For the primary disk, this will be filled in automatically based on the guest name provided above. It can be modified manually if needed.

   Guest Dev Name: For the primary disk, this value is not set.



10. PM&C GUI: Add extra virtual disks

    If the application requires extra virtual disks to be specified, repeat this step for each extra disk.

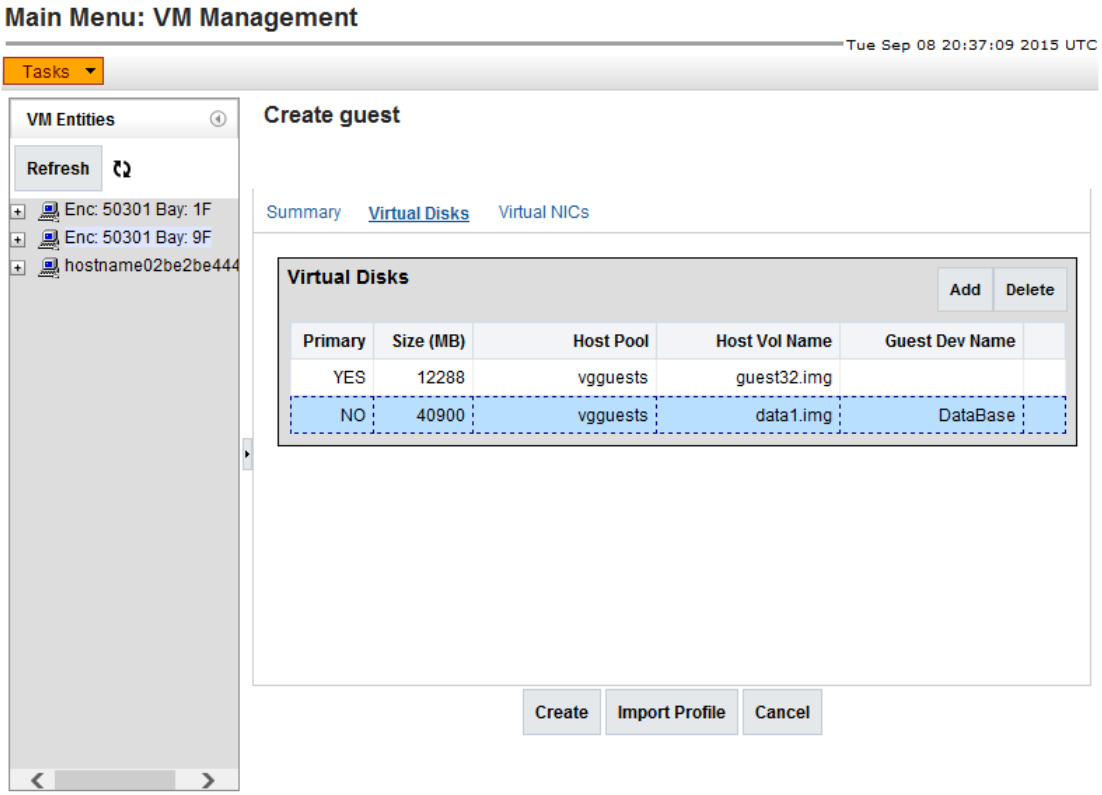
    Click on the **Add** button at the top-right corner of the Virtual Disks pane

    Size (MB): Click on the number to adjust the size via arrow or the keyboard.

    Host Pool: The default vgguests storage pool is selected. Using the dropdown box, other pools that have been configured on the TVOE can be selected.

    Host Vol Name: Fill in this value. It must be unique among all disks on all guest hosted on the TVOE.

    Guest Dev Name: This is the alias that will be used inside of the TPD instance running on the guest. It will help the application identify the disk.



Repeat, as needed, for all extra disks.

11. PM&C GUI: Add virtual NICs.

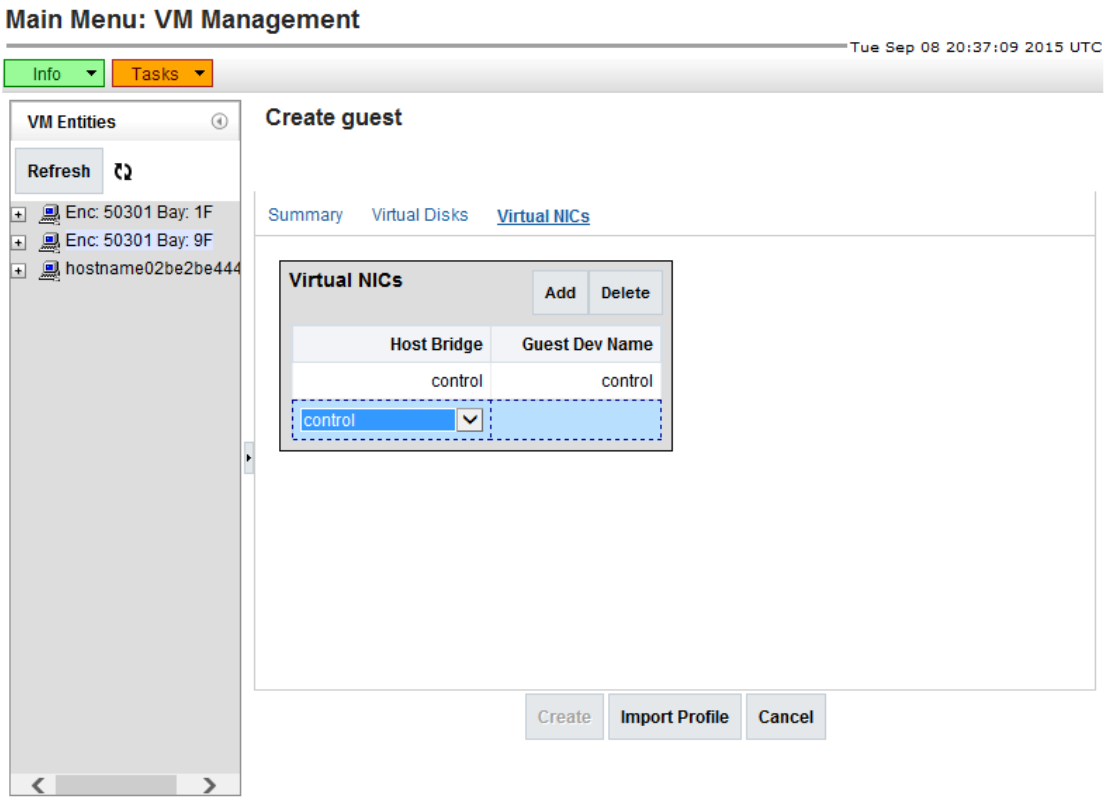
    By default, the control network is configured, and is required for PM&C to install and upgrade the guest. If this is removed, one will be added during the guest creation.

    To add additional NICs, repeat this step using the instructions below for each virtual NIC.

    Click on the **Add** button at the top-right corner of the Virtual NICs pane

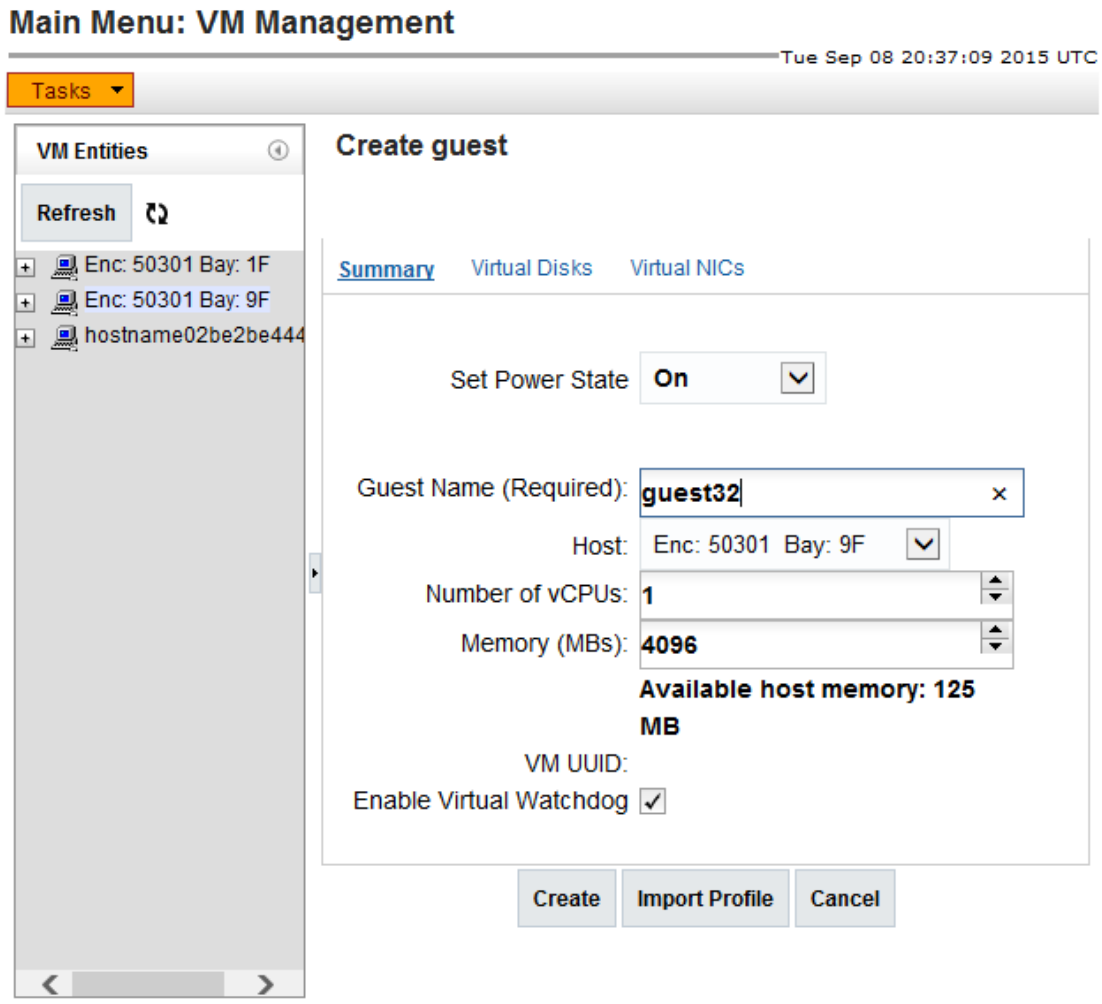
    Host Bridge: Using the dropdown box, select the desired bridge that has been previously configured on the TVOE.

    Guest Dev Name: This is the alias that will be used inside of the TPD instance running on the guest. It will help the application identify the network.



Repeat, as needed, for all vNICs.

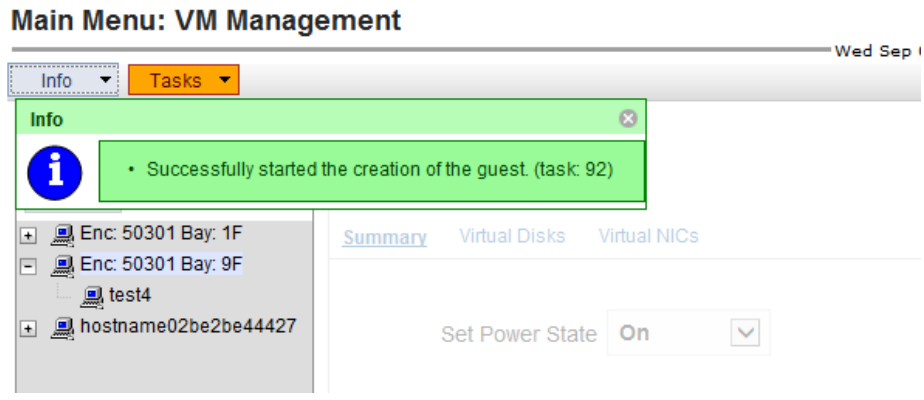
12. PM&C GUI: Create the guest.
    Verify the guest configuration.



Click on the **Create** button.

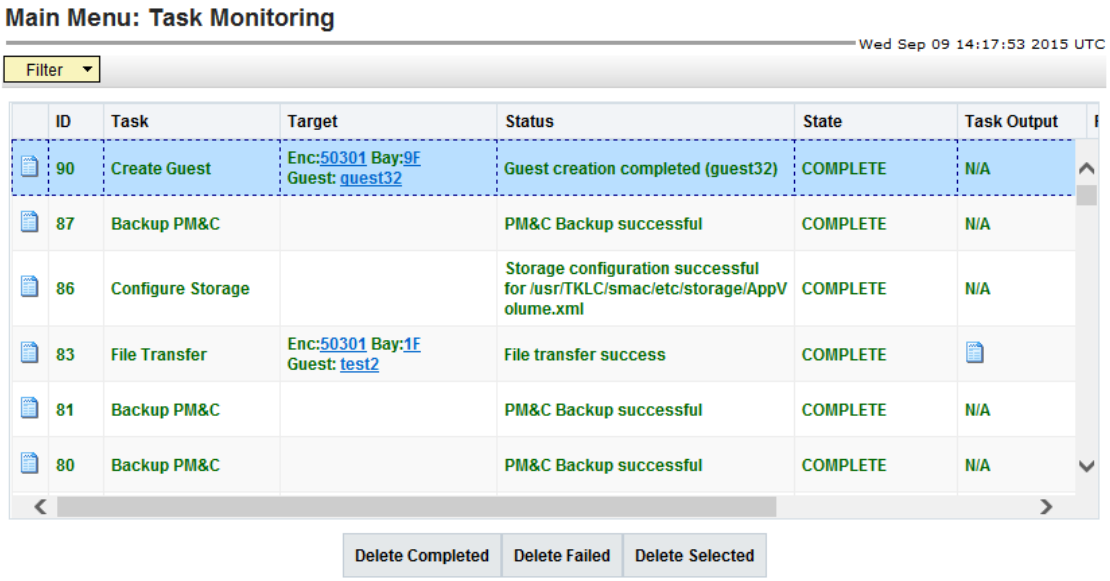
13. PM&C GUI: Verify guest creation started.

    If there was an immediate problem, an alert box will report the error, and the values can be corrected and retried. Otherwise, the Info box will confirm the creation of a Background Task.



14. PM&C GUI: Monitor guest create

    Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the "VirtAction: Create" background task.



    When the task is complete, the text will change to green and the Progress column will indicate "100%".

3.9.2 Delete guest server using PM&C application

This procedure provides the steps for deleting a virtualized guest server on a TVOE host, using the PM&C web GUI.

Prerequisites:

- Enclosure containing the host blade server hosting the guest has been configured using *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory*.

Note: All data belonging to this guest server will be lost in the execution of this procedure.

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

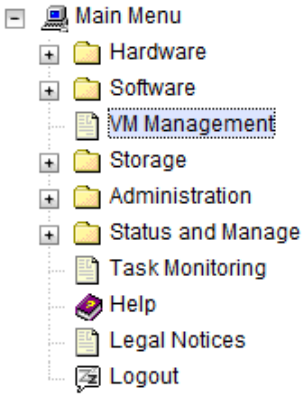
   If needed, open web browser and enter:

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

   Login as **guiadmin** user.

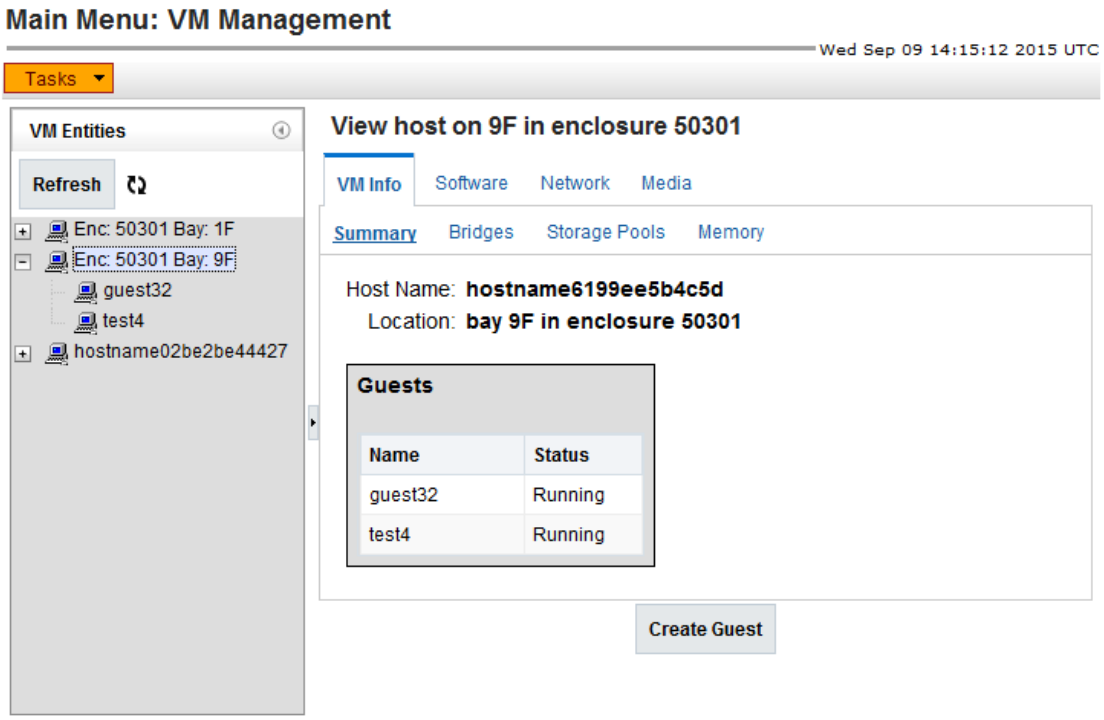
2. PM&C GUI: Navigate to VM Management

   Navigate to **Main Menu** > **VM Management**.



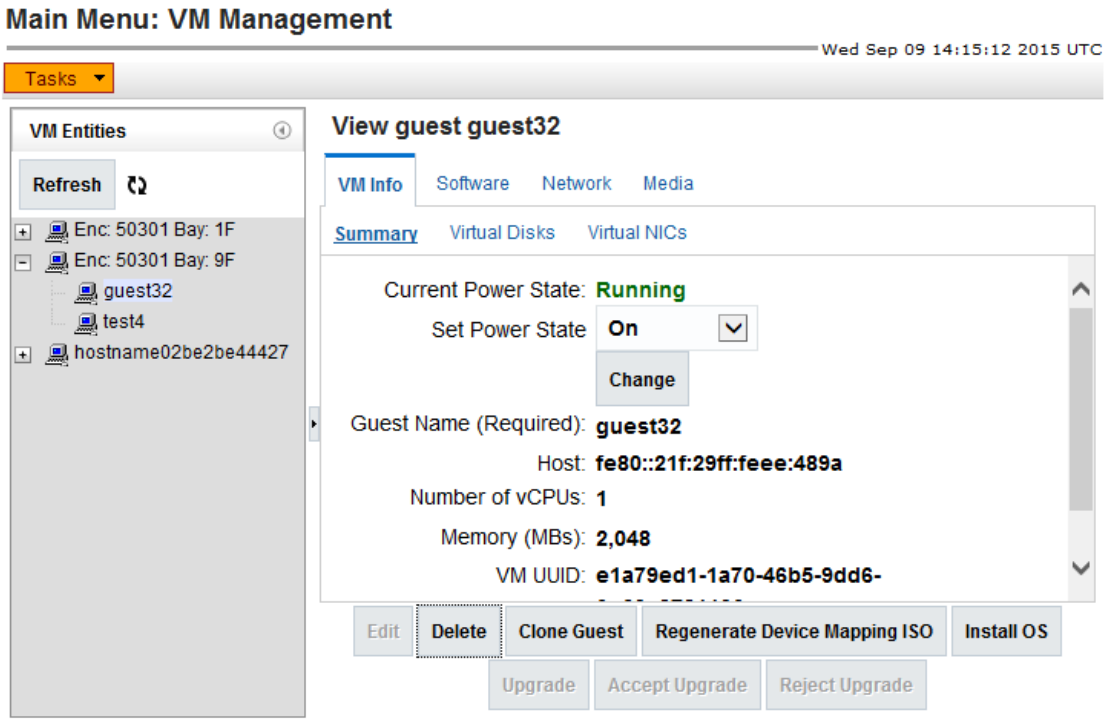
3. PM&C GUI: Select TVOE hosting the guest

   Click on the ⊞ to the left of the TVOE host that contains the guest server to delete. This will expand the tree to make the guests hosted on the selected TVOE visible.



4. PM&C GUI: Select the guest and delete

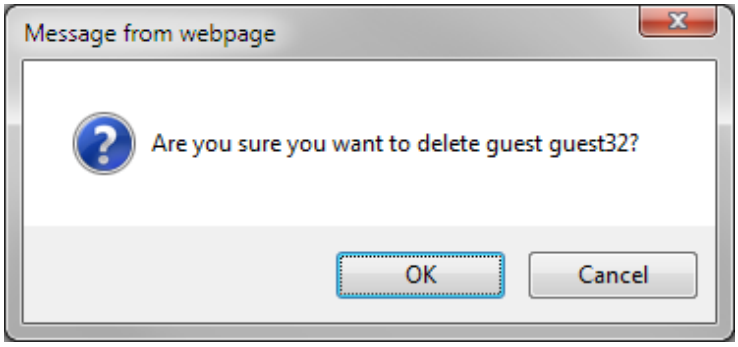
   The left side of this screen shows the guest servers on the TVOE host. Select the desired guest and the guest details will be displayed on the right.



Then press the **Delete** button.

5. PM&C GUI: Confirm delete

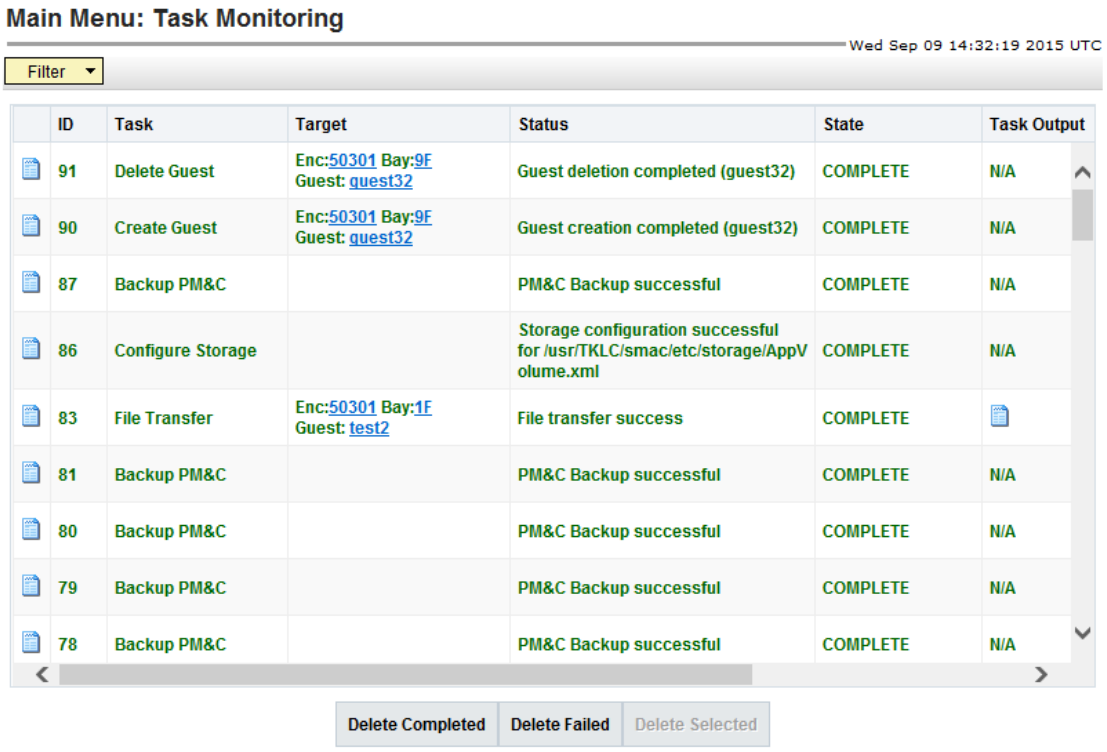
   Take a moment to double-check that the guest name is correct. There will be no further confirmation and the delete will be final.



   Click on the **OK** button to confirm the delete.

6. PM&C GUI: Monitor guest delete

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the "VirtAction: Delete" background task.



When the task is complete, the text will change to green and the Progress column will indicate "100%".

3.9.3 Create guest server from guest archive using PM&C application

This procedure provides the steps for creating a virtualized guest server from a guest archive image on a TVOE host, using the PM&C web GUI.

Prerequisites:

- Enclosure containing the TVOE host blade server to host the guest has been configured using *3.7.7 Add Cabinet and Enclosure to the PM&C System Inventory*.
- The TVOE host has been installed using *3.7.10 IPM Servers Using PM&C Application*.
- The ISO image providing the guest archive image and profile has been provisioned using *3.7.9 Adding ISO Images to the PM&C Image Repository*.

Note: PM&C will not prevent over-subscription of memory or CPU resources.

Note: The guest archive profiles might not contain values for all required fields.

Note: The values provided by the guest archive profile can be overridden before the guest is created.

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

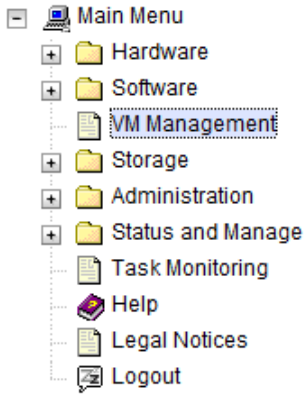
1. PM&C GUI: Login

If needed, open web browser and enter:

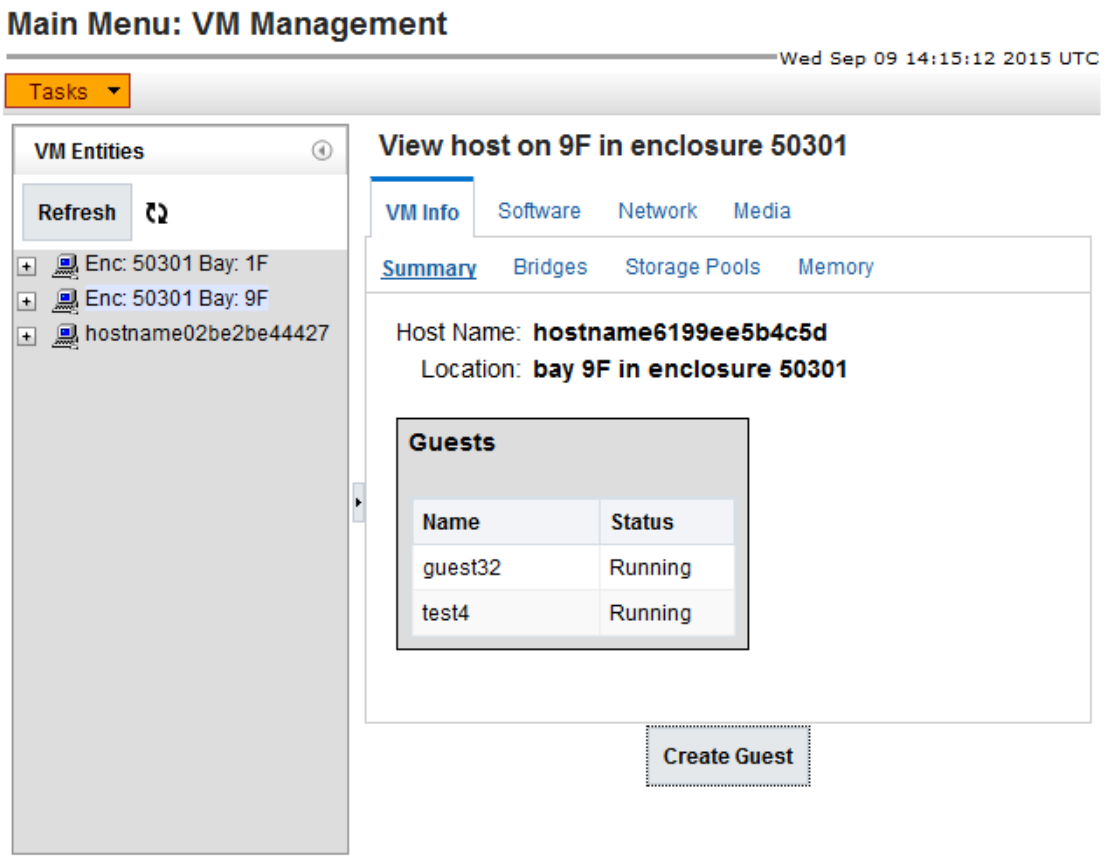
```
https://<pmac_management_network_ip>
```

Login as **guiadmin** user.

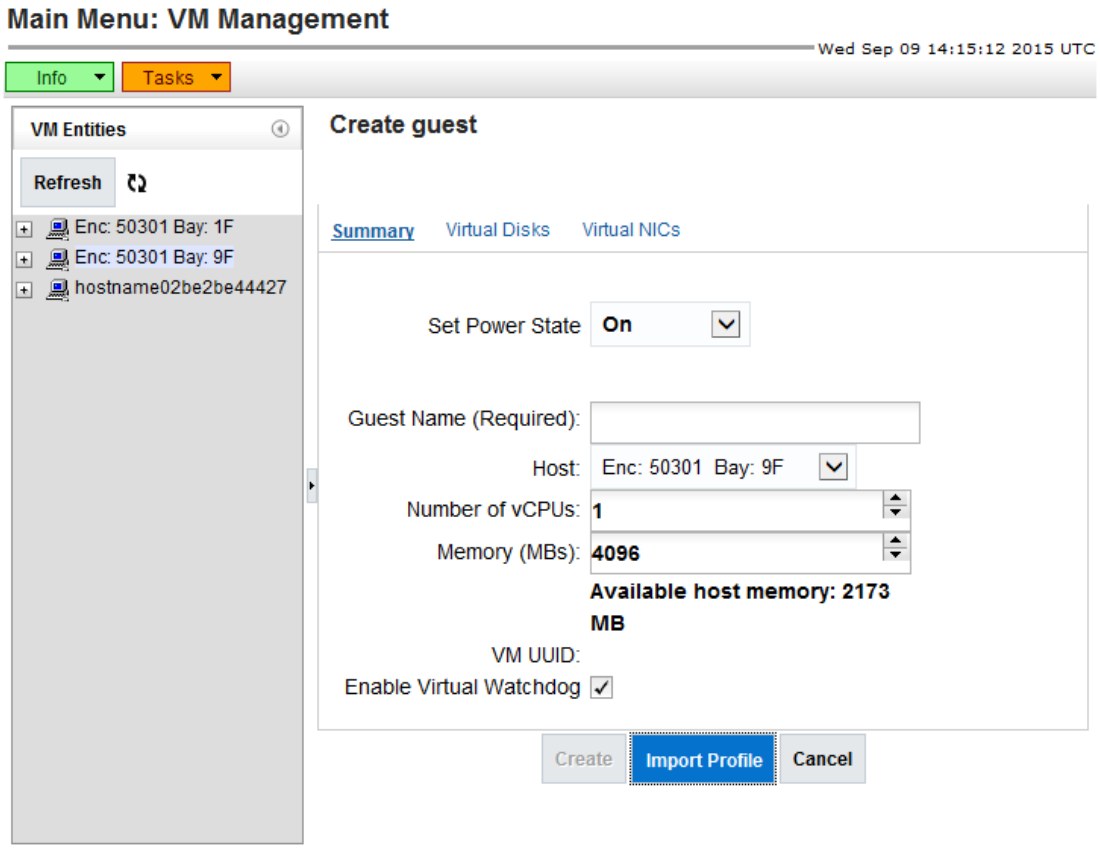
2. PM&C GUI: Navigate to VM Management
   Navigate to **Main Menu** > **VM Management**.



3. PM&C GUI: Click the **Create Guest** button.
   On the Virtual Machine Management page, click the **Create Guest** button.

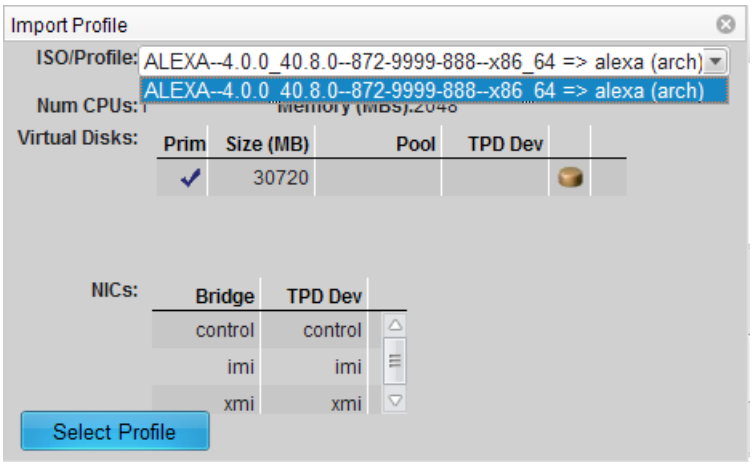


4. PM&C GUI: Click the **Import Profile** button
   Select the **Import Profile** button to bring up the pop-in dialog box



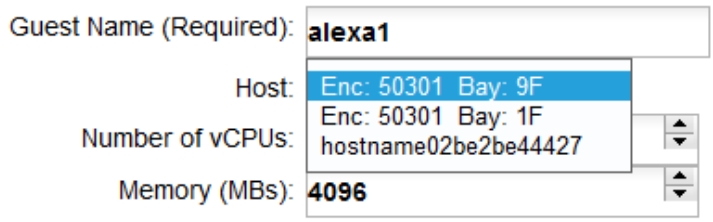
5. PM&C GUI: Select the desired profile, and click the **Select Profile** button

   Using the drop-down menu, select the desired ISO/Profile (It is possible there will be multiple profiles on an ISO). Verify the details, then select the **Select Profile** button.



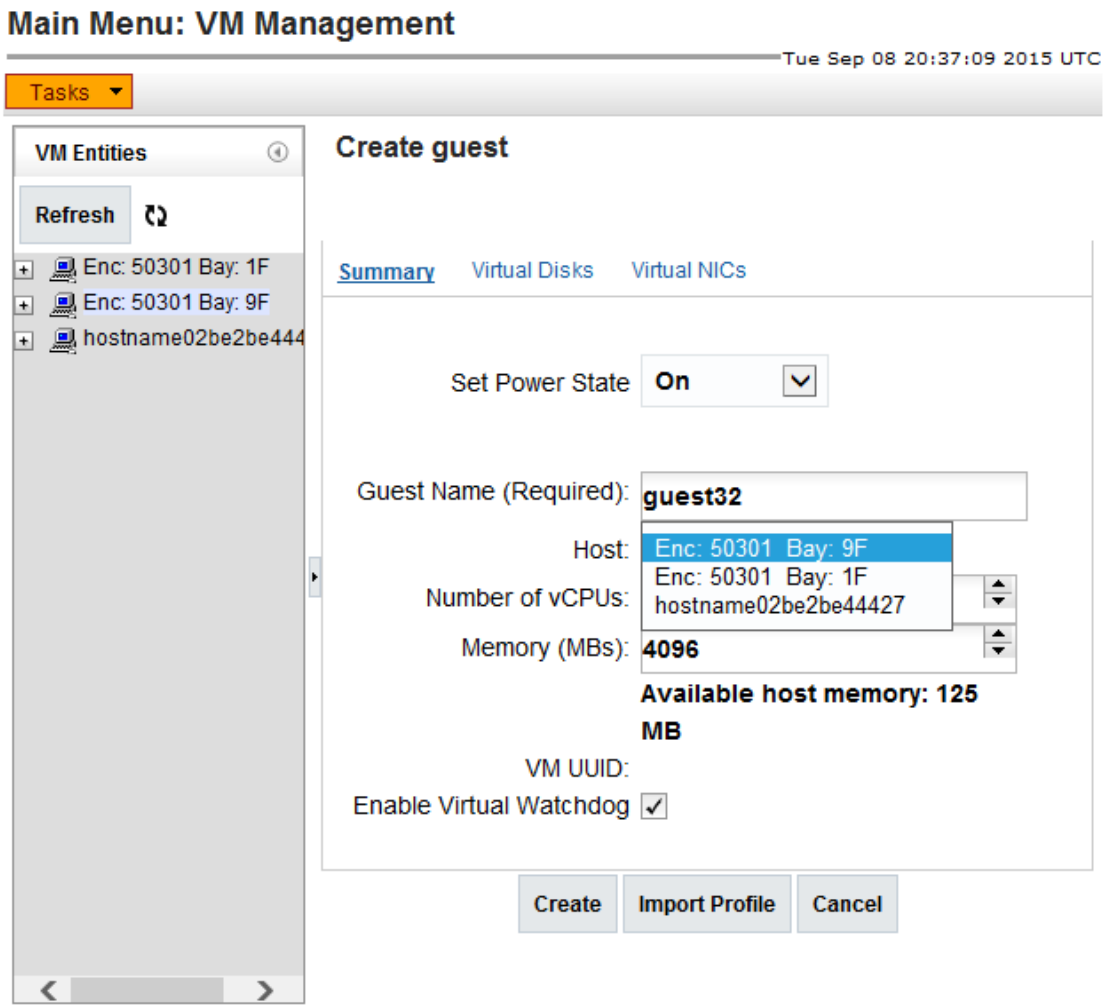
6. PM&C GUI: Enter guest name

   The profile fills in the default name. If a different name is desired, fill in the "**Name**" field with something unique to the TVOE host. The name can be identical to a guest on a different host.



7. PM&C GUI: Select the TVOE Host for the new guest

   Using the dropdown "**Host**" field, select the TVOE host on which to create the guest.

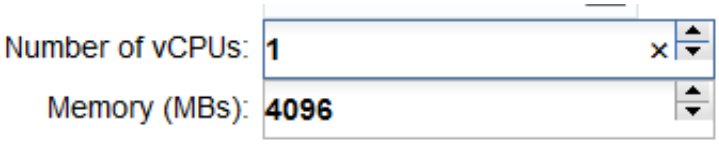


8. PM&C GUI: Select the desired initial power state.

   Using the dropdown field to the right, select the initial power state for the guest. In this context, Shutdown and Destroy both behave the same, the guest will not be powered on upon creation.

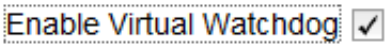
9. PM&C GUI: Edit the vCPU count and Memory size

   The profile inserted the profile's vCPUs and Memory settings. These can be adjusted using the arrows to the right of the fields, adjust the number of virtual CPUs and the amount of memory (in MBs) to use for the guest. These fields are also manually editable test fields. PM&C will not prevent over-subscription of these resources.



10. PM&C GUI: Edit the Watchdog setting (if available)

    If this Guest is being created on a version of TVOE having support for virtual guest watchdogs, the Enable Virtual Watchdog item will be present. Set this checkbox according to whether or not watchdog support is desired for this Guest.

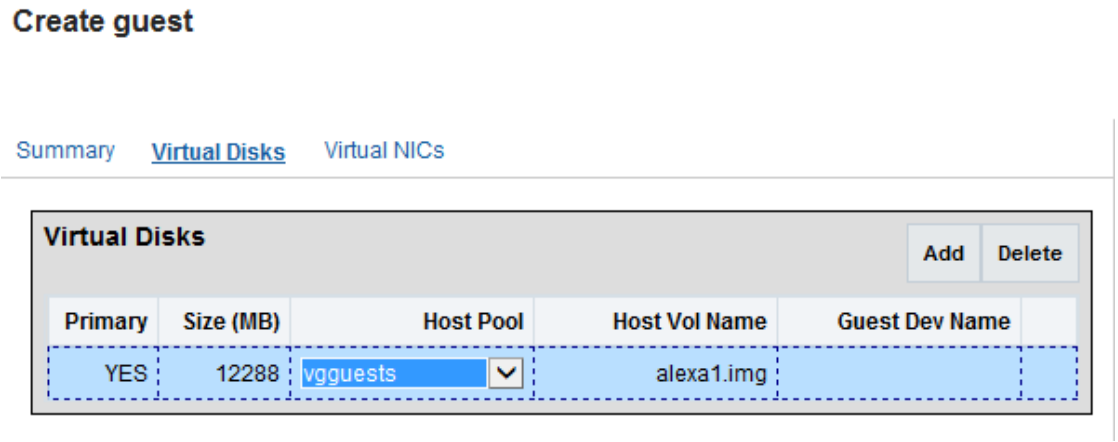


11. PM&C GUI Edit the primary virtual disk

    The primary disk is specified by the profile. The disk image at the left shows how the disk will be populated with the archive's image. The only fields that should be modified are the Host Pool, and Host Vol Name columns.

    Host Pool: The desired storage pool can be selected here. It is possible that the profile did not specify a value for the storage pool. The GUI will not allow you to continue until one is selected.

    Host Vol Name: For the primary disk, this will be filled in automatically based on the guest name provided above. It can be modified manually if needed.



12. PM&C GUI: Modify extra virtual disks

If the profile provides extra virtual disks to be specified they will show up below the primary disk. If needed, extra virtual disks may be added at this time, as well.

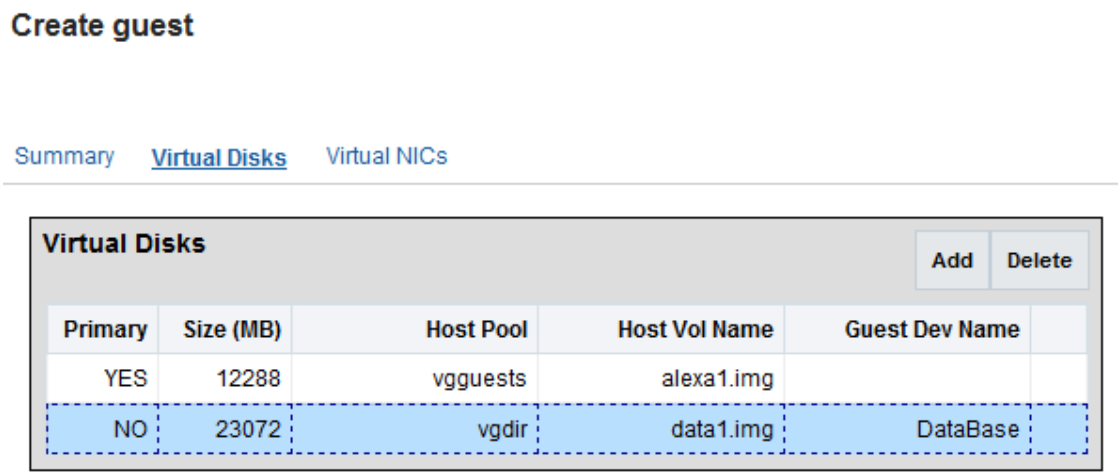
Click on the **Add** button at the top-right corner of the Virtual Disks pane

Size (MB) : Click on the number to adjust the size via arrow or the keyboard.

Host Pool: The default vgguests storage pool is selected, but using the dropdown box, other pools that have been configured on the TVOE can be selected.

Host Vol Name: Fill in this value. It must be unique among all disks on all guests hosted on the TVOE.

Guest Dev Name: This is the alias that will be used inside of the TPD instance running on the guest. It will help the application identify the disk.



Repeat, as needed, for all extra disks.

13. PM&C GUI: Edit virtual NICs

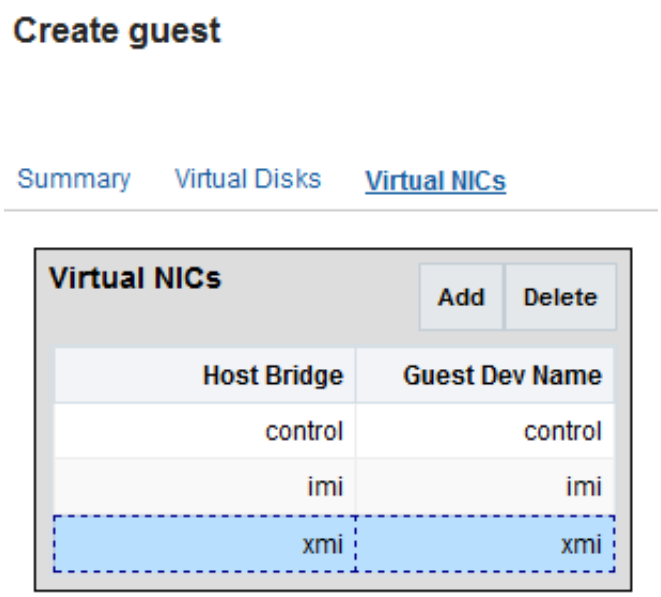
    The required networks should be defined by default, the control network is configured, and is required for PM&C to install and upgrade the guest. If this is removed, one will be added during the create.

    If additional NICs are required, repeat this step for each virtual NIC.

    Click on the **Add** button at the top-right corner of the Virtual NICs pane

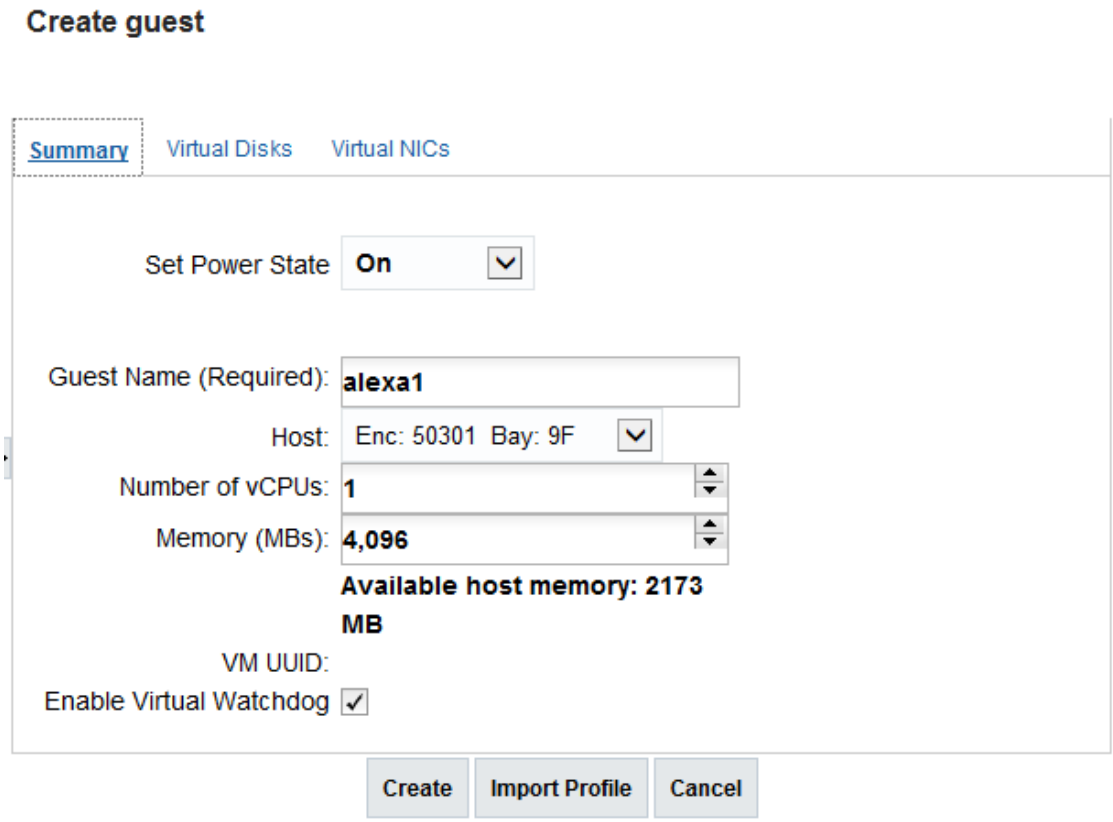
    Host Bridge: Using the dropdown box, select the desired bridge that has been previously configured on the TVOE.

    Guest Dev Name: This is the alias that will be used inside of the TPD instance running on the guest. It will help the application identify the network.



Repeat, as needed, for all vNICs

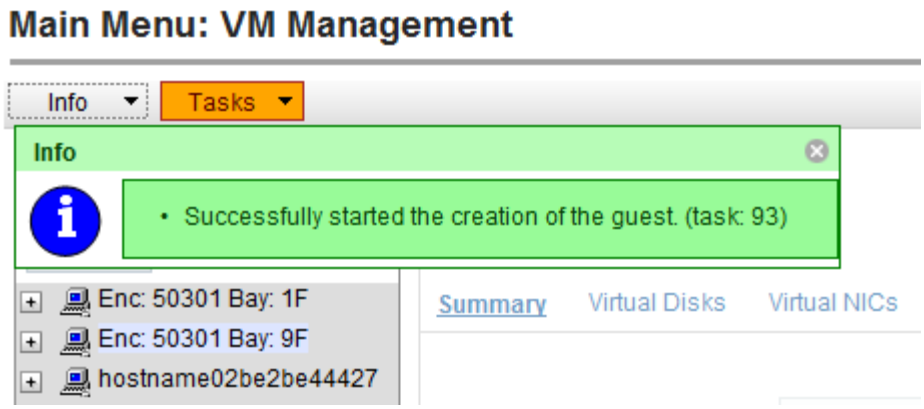
14. PM&C GUI: Create the guest
    Verify the guest configuration.



Click on the **Create** button.

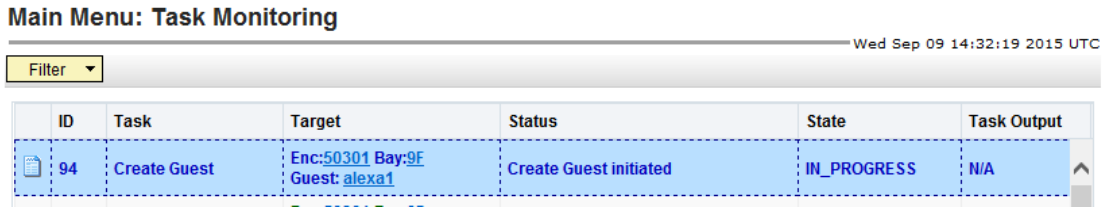
15. PM&C GUI: Verify guest creation started

    If there was an immediate problem, an alert box will report the error, and the values can be corrected and retried. Otherwise, the alert box will confirm the creation of a Background Task.



16. PM&C GUI: Monitor guest create

    Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the "VirtAction: Create" background task.



    When the task is complete, the text will change to green and the Progress column will indicate "100%".

3.10 General TPD Based Application Procedures

3.10.1 Backup Procedure for TVOE

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

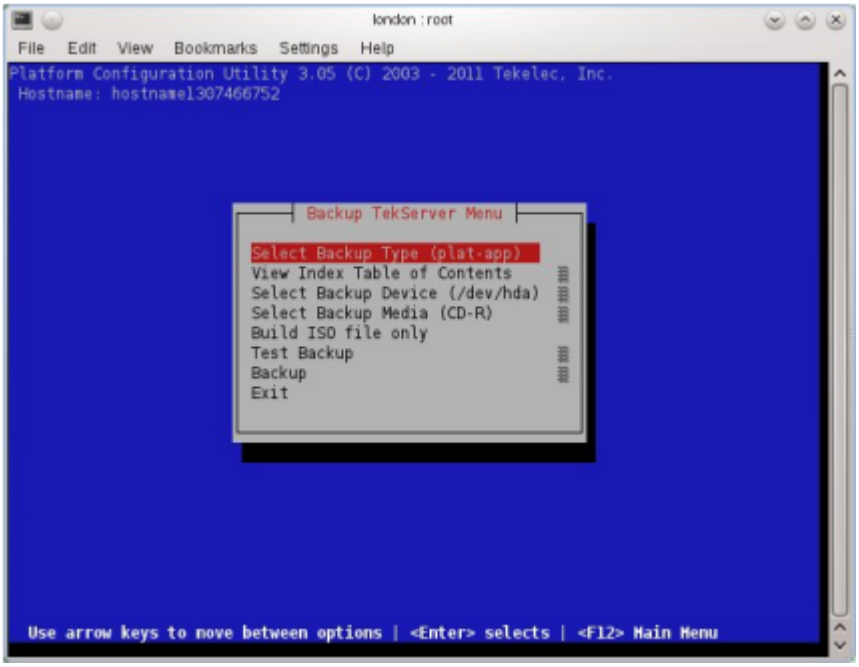
Note: The backup image is to be stored on a customer provided medium.

1. TVOE Host: Login as platcfg user.

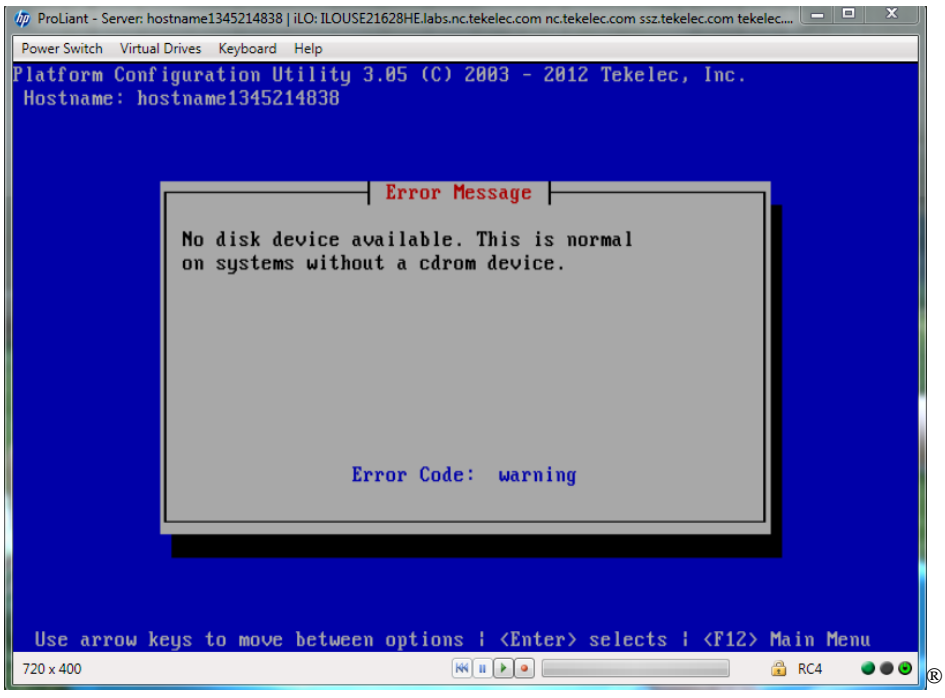
   Login as platcfg user on the server. The platcfg main menu will be shown.

2. TVOE Host: Navigate to the Backup TekServer Menu page

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



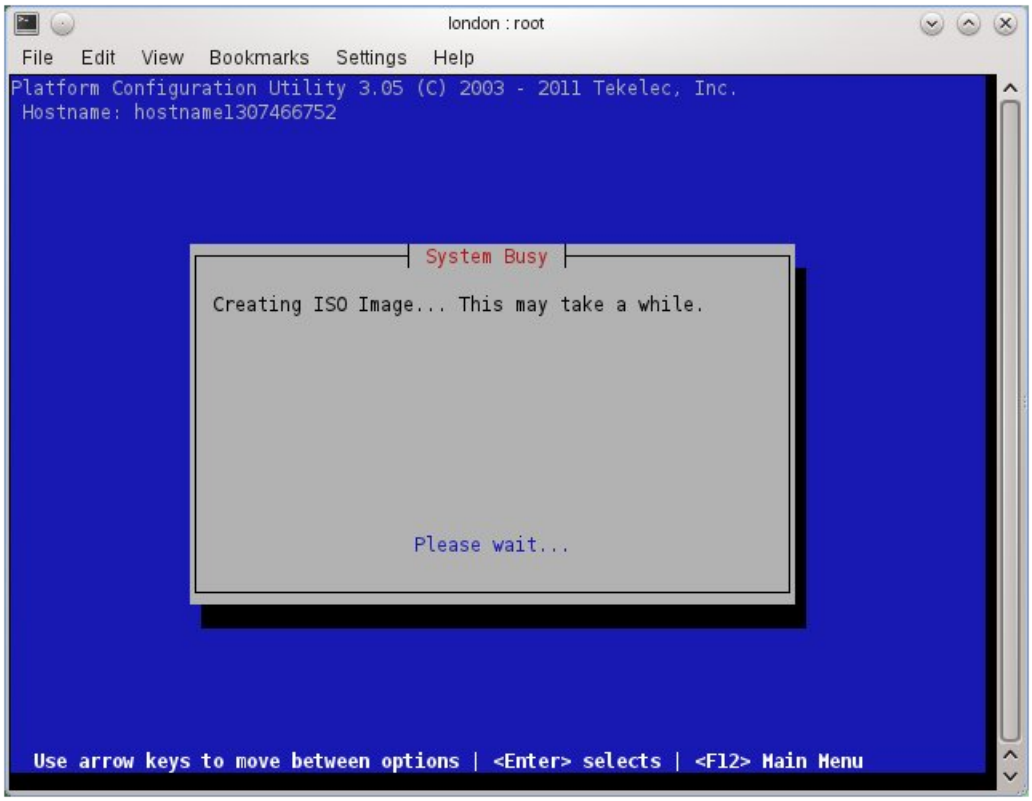
Note: If this operation is attempted on a system without media, the following message will appear:



3. 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"

4. TVOE Host: Exit platcfg

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

5. 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 *A.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.

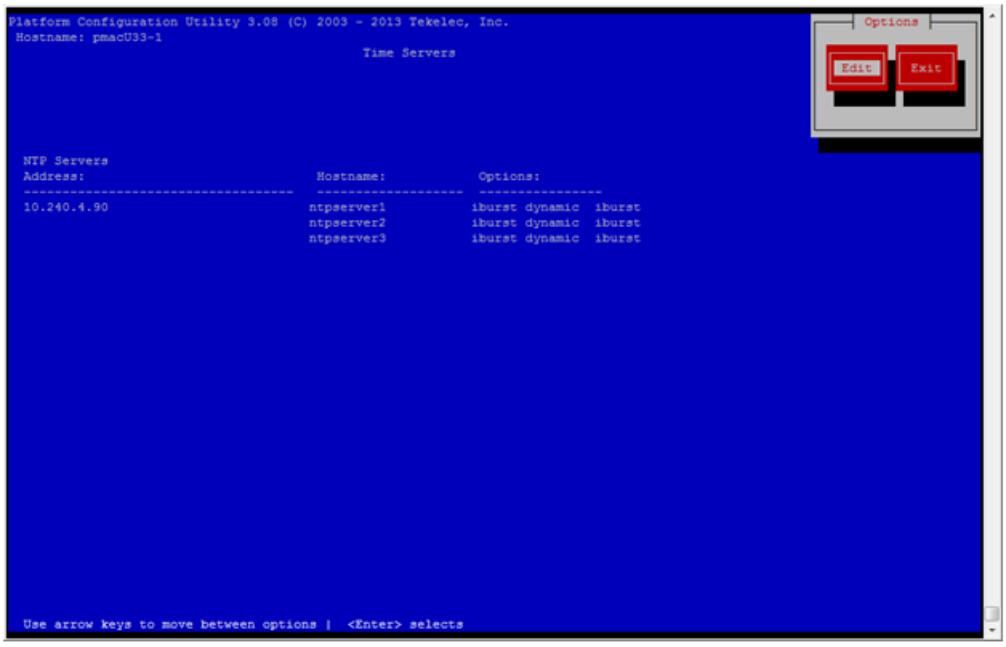
3.10.2 Configure NTP on TPD based Application

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

1. Server: Login as platcfg user

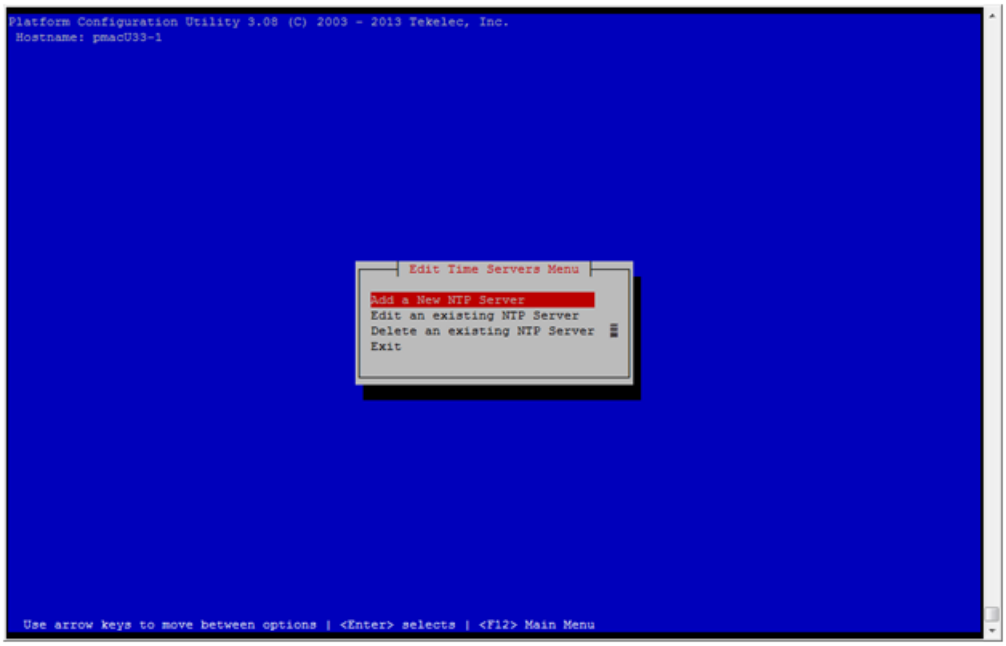
   Login as platcfg user on the server. The platcfg main menu will be shown.

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.



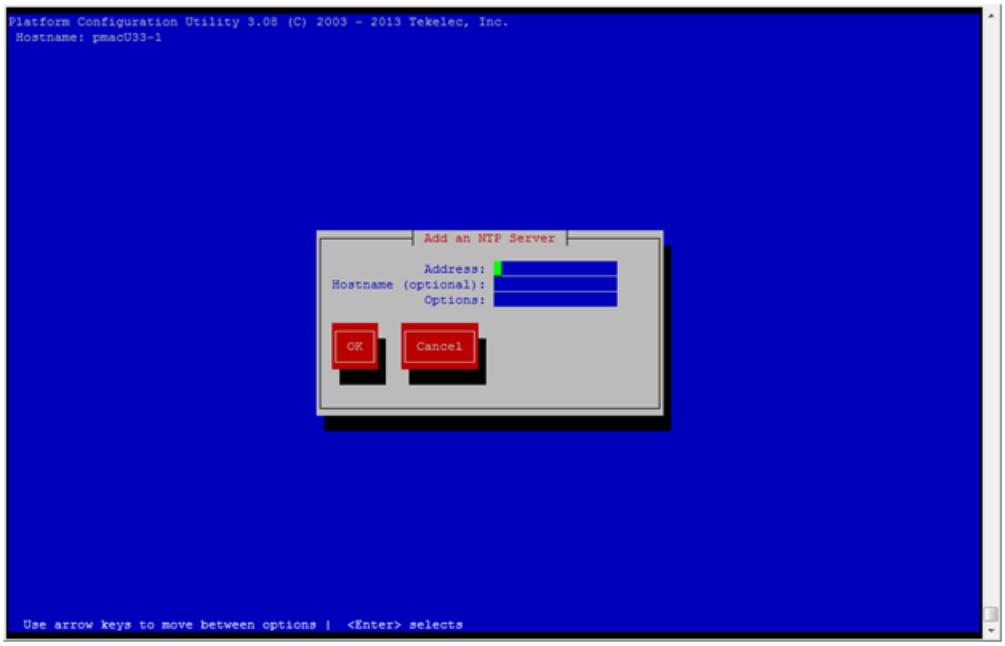
4. Server: Edit NTP Information

   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

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

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



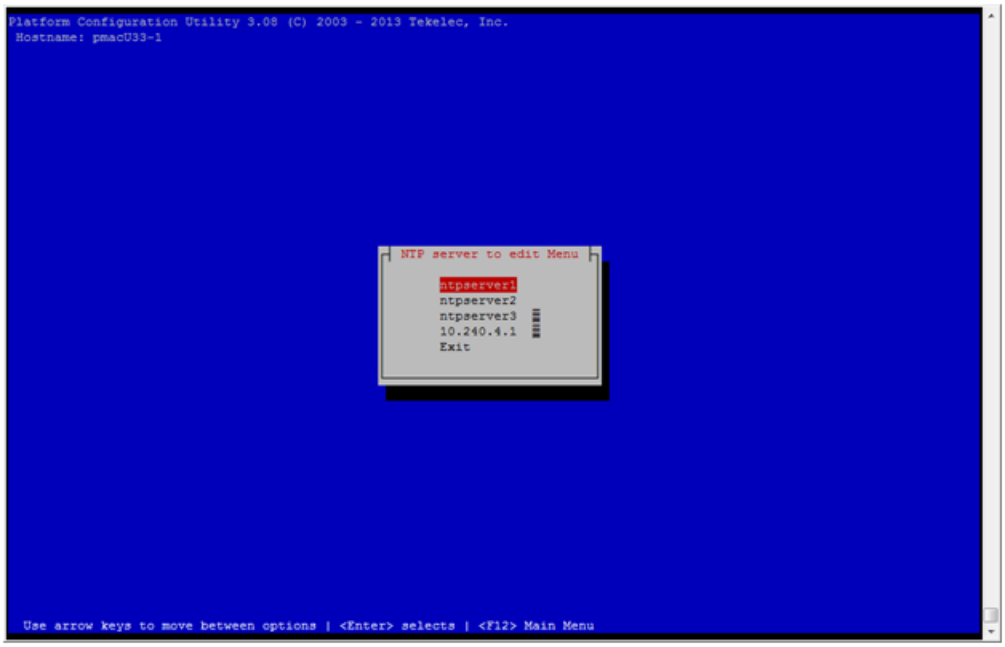
      b. Server: Enter Appropriate data, and select **OK**

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

b. Editing an NTP Server

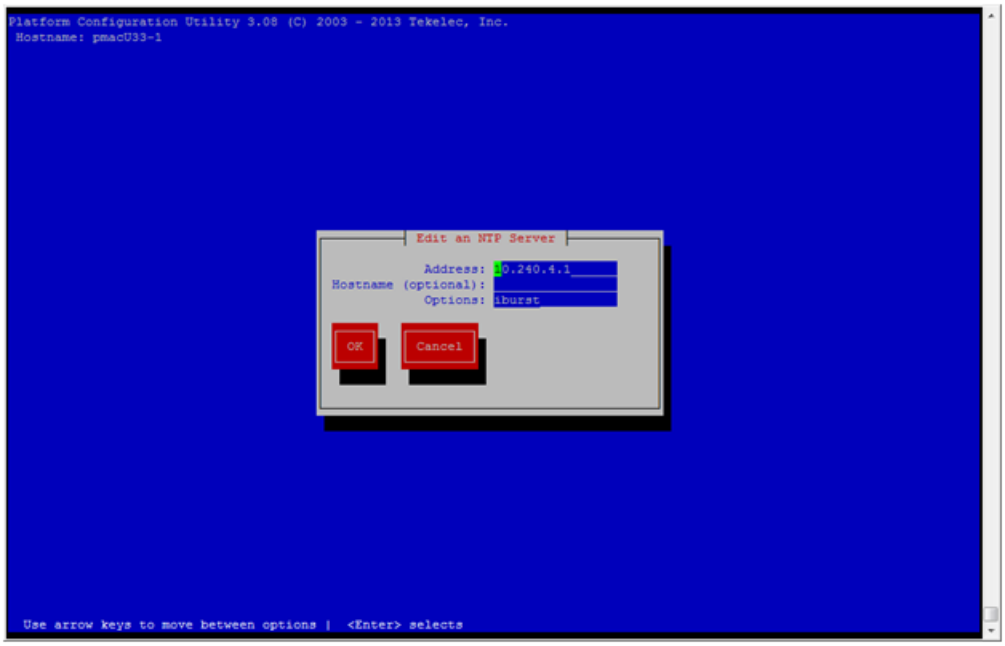
a. Server: If editing an existing NTP server select **Edit an existing NTP Server**.

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



b. Server: Select appropriate NTP server.

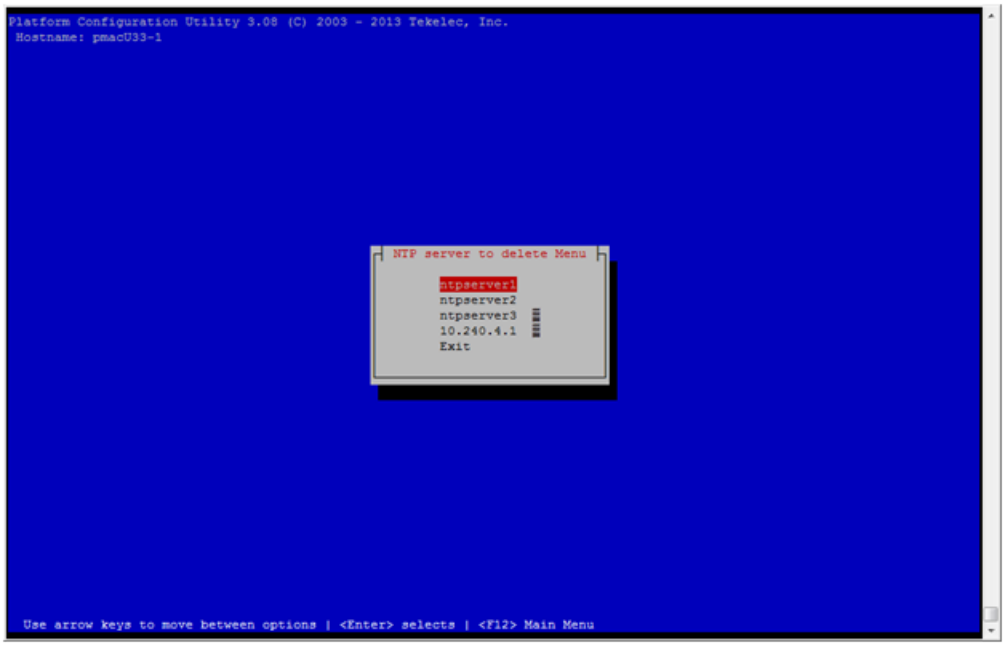
The **Edit an NTP Server** window is displayed.



c. 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.

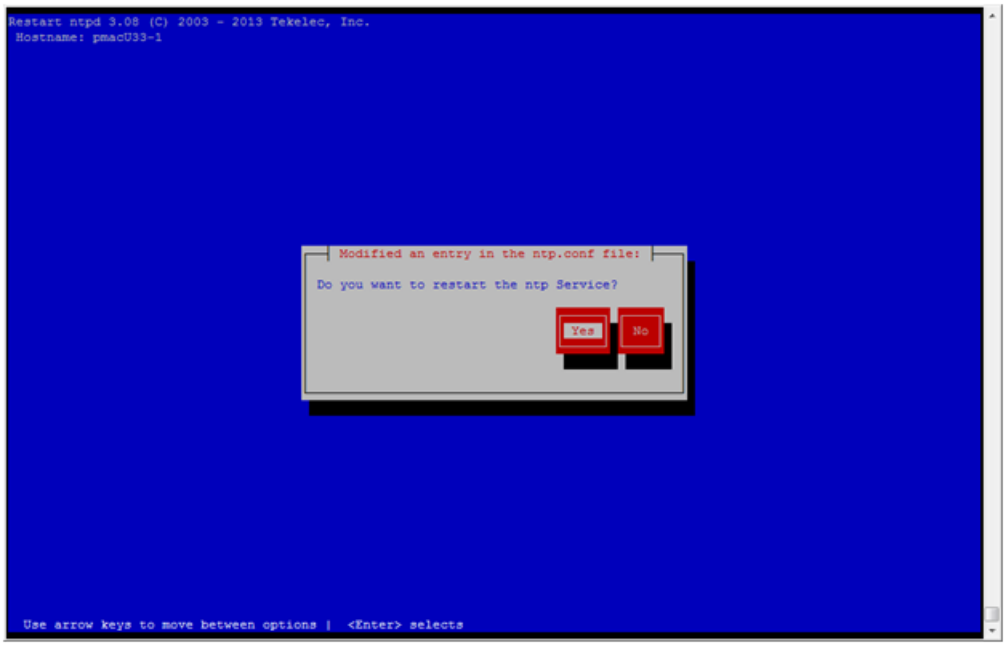


b. Server: Select appropriate NTP server.

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

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.



a. Server: Restart the NTP service by selecting **Yes**. The **Network Configuration Menu** is displayed.

6. Server: Exit platcfg.

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

3.10.3 Add SNMP trap destination on TPD based Application

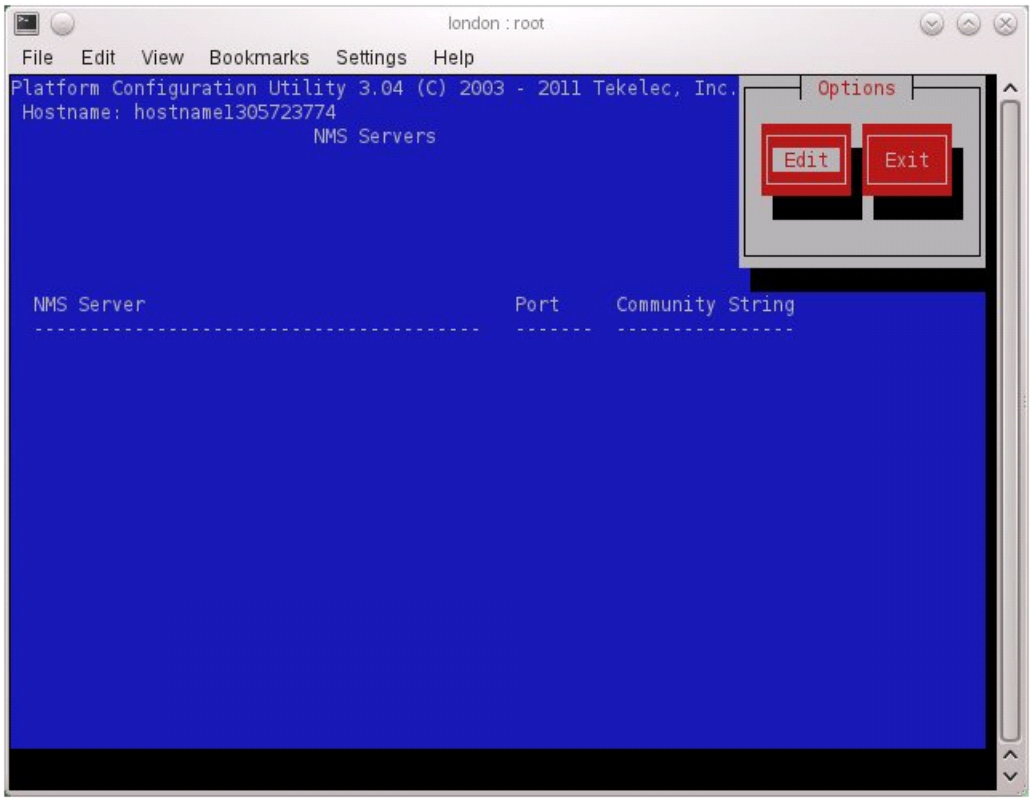
This procedure will add an SNMP trap destination to a server based on TPD. All alarm information will then be sent to the NMS located at the destination.

1. Server: Log in as platcfg user

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

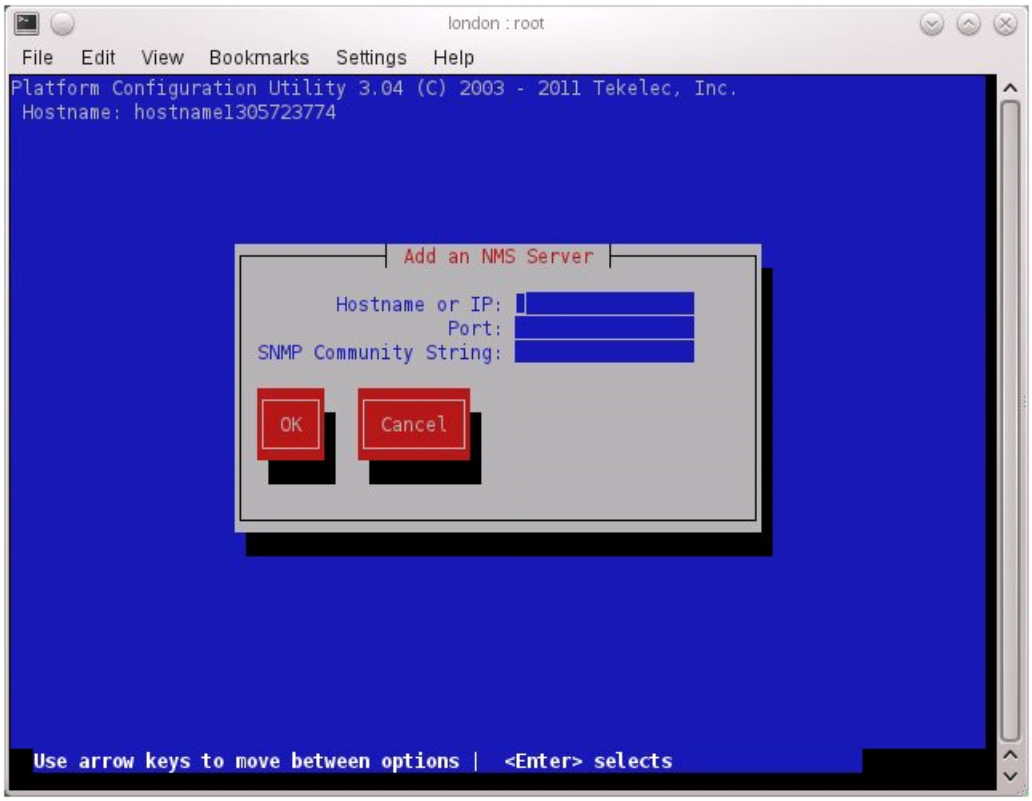
2. Server: Navigate to NMS server configuration page

   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.



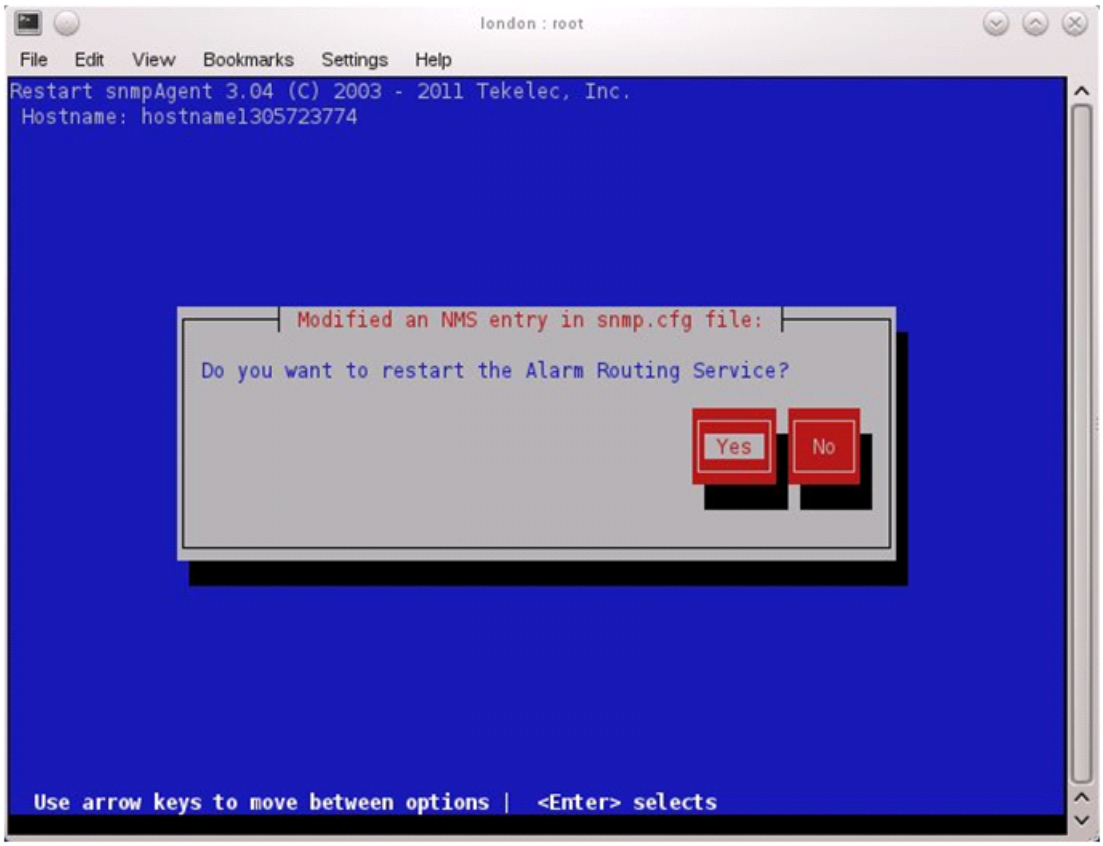
3. Server: Add the SNMP trap destination.

   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. 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.

3.10.4 Delete SNMP trap destination on TPD based Application

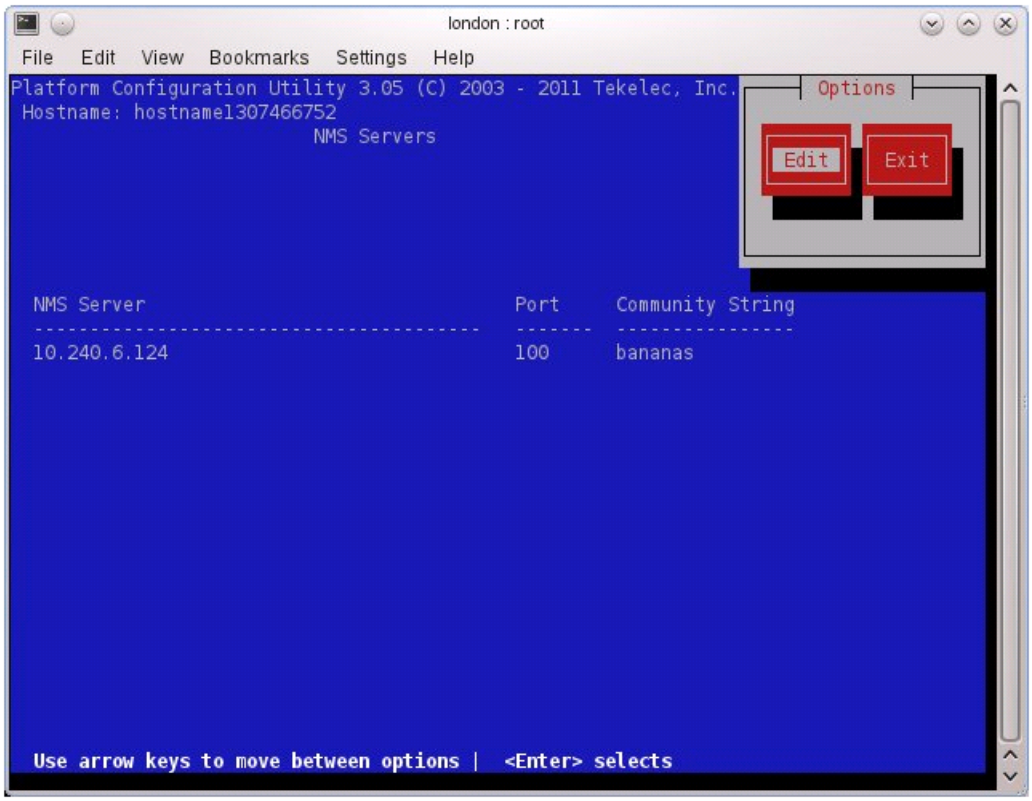
This procedure will remove an SNMP trap destination on a server.

1. Server: Login as platcfg user

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

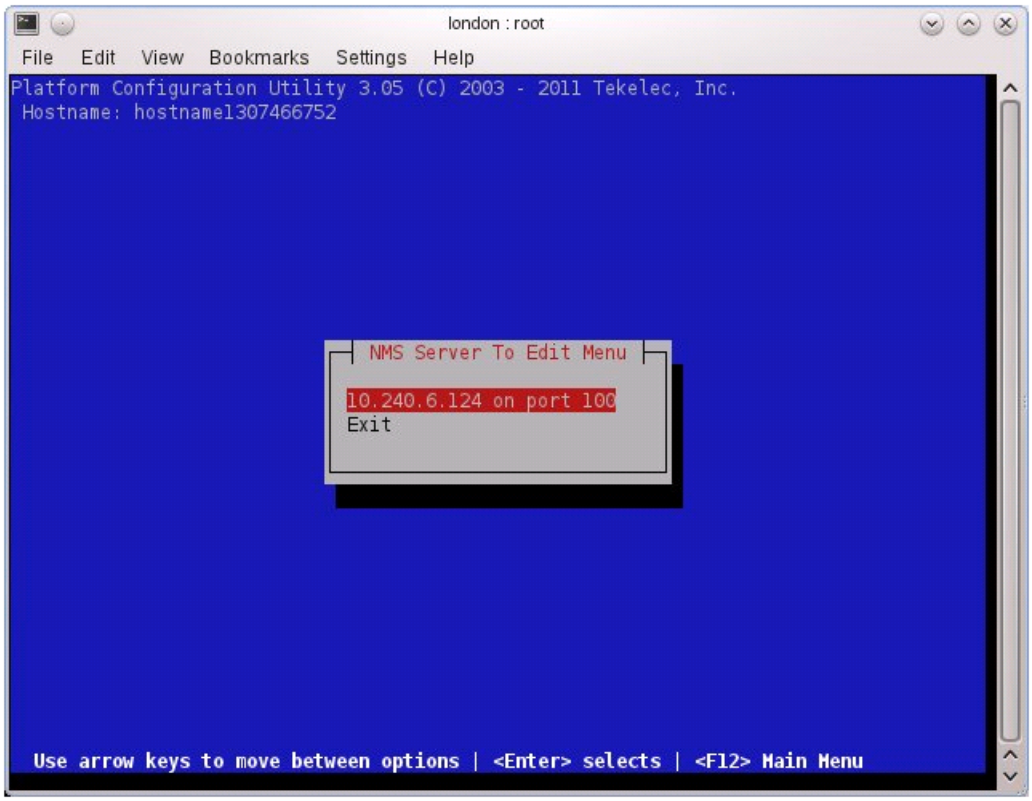
2. Server: Navigate to NMS server configuration page.

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



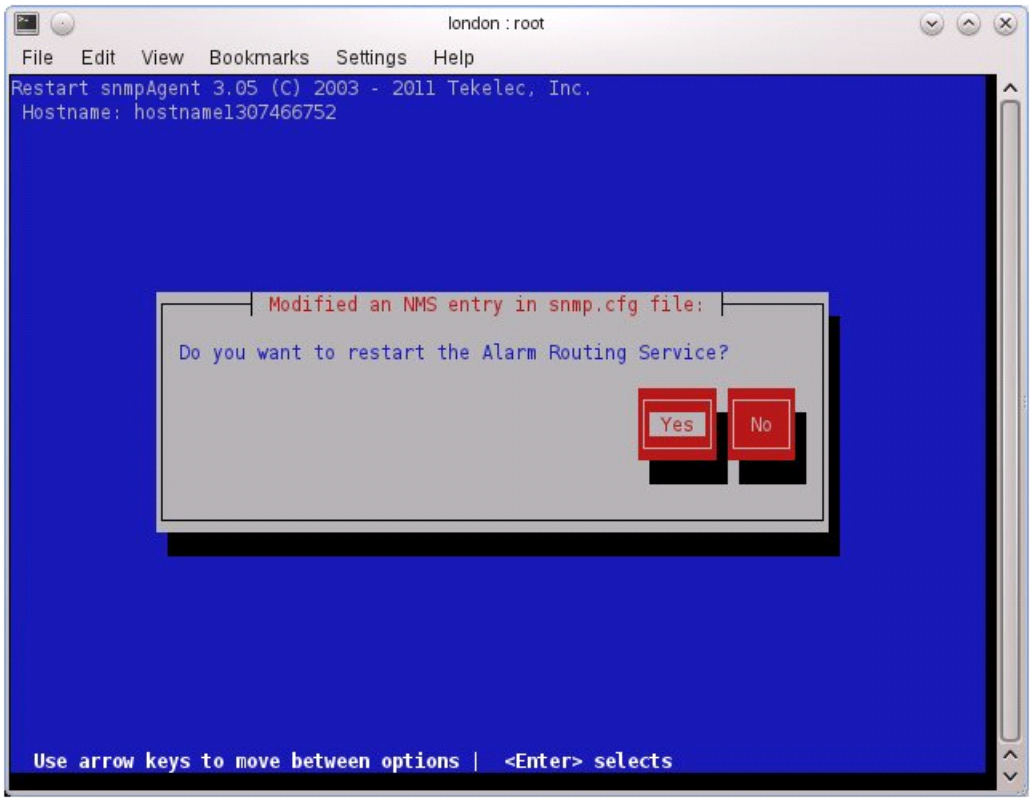
3. Server: Remove the SNMP trap destination

   Select **Edit** and then choose **Delete an Existing NMS Server**. The 'NMS Server to Edit' page will be displayed as shown below.



Select the server to remove from the configuration and press **ENTER**. A confirmation dialog will appear. Select **Yes** to confirm the removal of the NMS server.

The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialog will 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.

3.10.5 Application NetBackup Client Install 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: PM&C 6.3 supports NetBackup 7.1, 7.5, and 7.6 clients. Any other Netbackup client installation should first be vetted by Oracle Customer support before it can be installed. *3.10.13 Create NetBackup Client Config File* can be used once the contents of the config are known.

Note: PM&C 6.4 supports NetBackup 7.1, 7.5, 7.6 and 7.7 clients. Any other Netbackup client installation should first be vetted by Oracle Customer support before it can be installed. *3.10.13 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 an Oracle software upgrade.

Prerequisites:

- Application server platform installation has been completed.
- NAPD has been completed to determine the network requirements for the application server, and interfaces have been configured.
- NetBackup server is available to copy, sftp, the appropriate Netbackup client software to the application server.
- Filesystem for Netbackup client software has been created *3.10.11 Create LV and Filesystem for NetBackup Client Software*.

  Note: For PM&C Application deployed with NetBackup Volume option "--netbackupVol" the guest virtual disk will be created by deploy. If Netbackup version 7.7 or greater is being used, the "--netbackupVolSize=5" option should be included on the command line.

- Config file has been created if the version of NetBackup Client is not supported *3.10.13 Create NetBackup Client Config File*.

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 *3.10.9 Netbackup Client Install with nbAutoInstall*. This is not common and if the answer to the previous question is not known then do not use *3.10.9 Netbackup Client Install with nbAutoInstall*.
   - If you don't use *3.10.9 Netbackup Client Install with nbAutoInstall*, use *3.10.10 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:

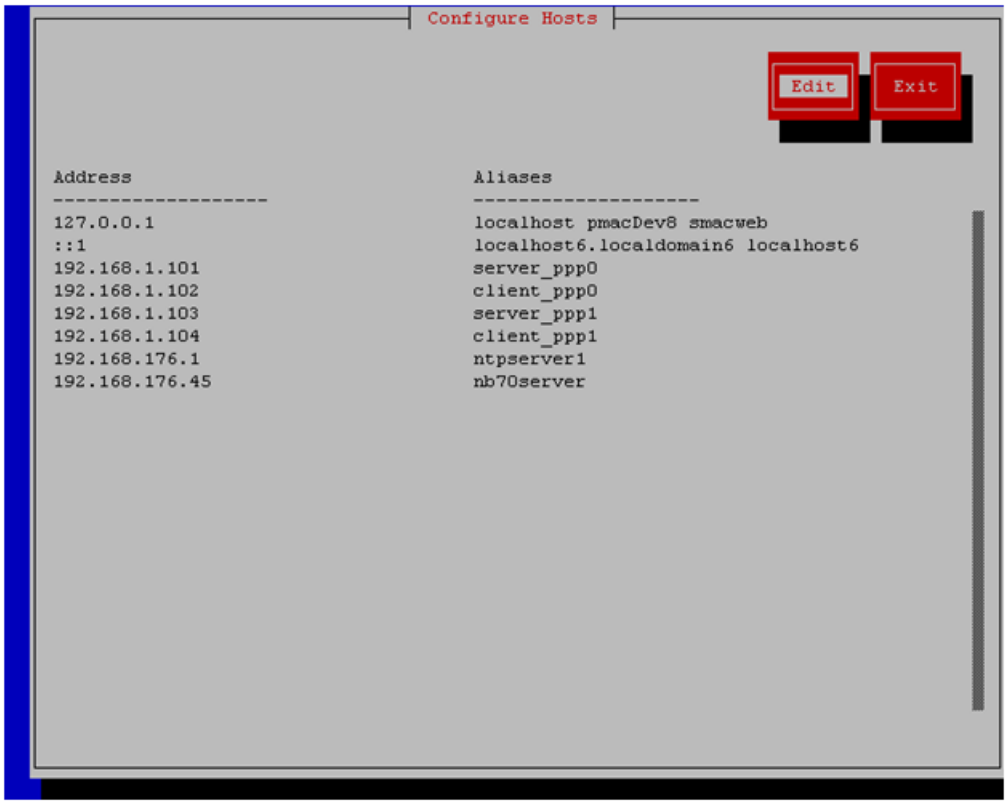
```
$ sudo cat /usr/openv/netbackup/bp.conf
SERVER = NB76Server
CLIENT_NAME = 10.240.117.134
CONNECT_OPTIONS = localhost 1 0 2
```

   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.

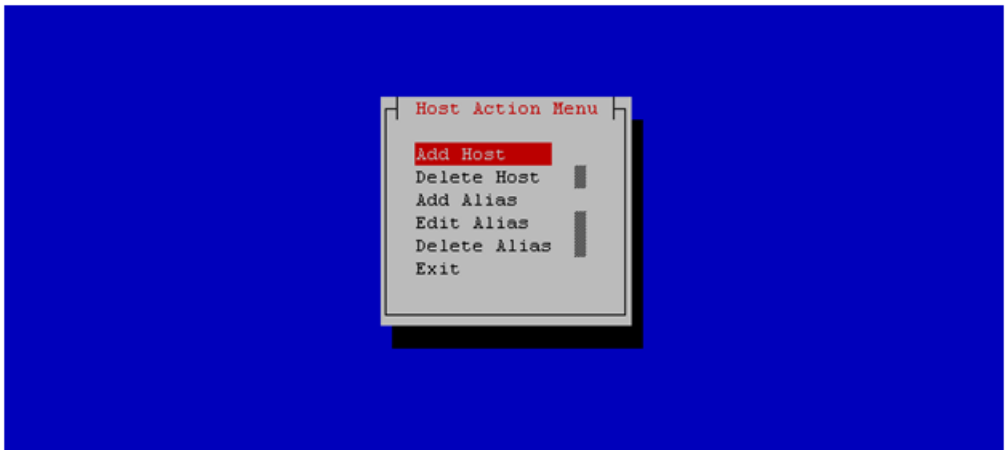
   Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
$ sudo su - platcfg
```

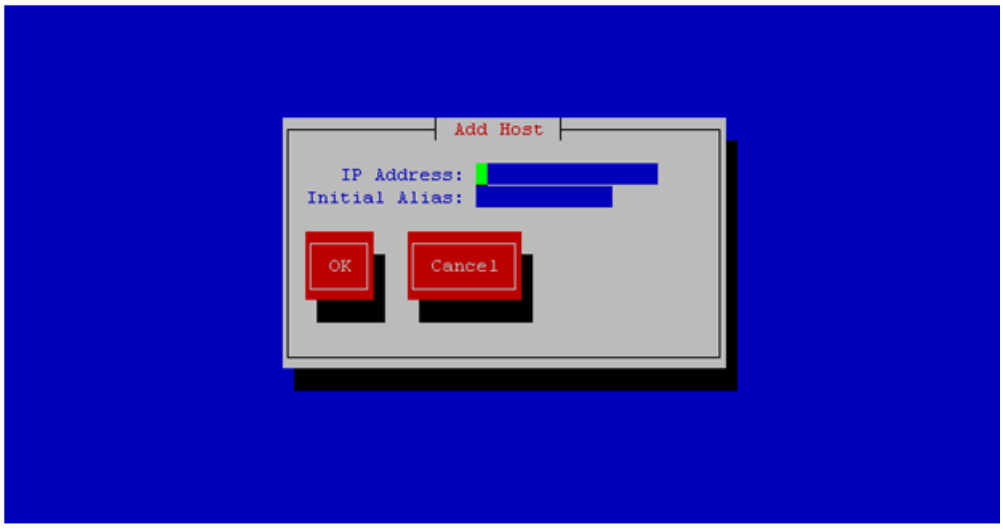
   Navigate to **Network Configuration** > **Modify Hosts File**



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
```

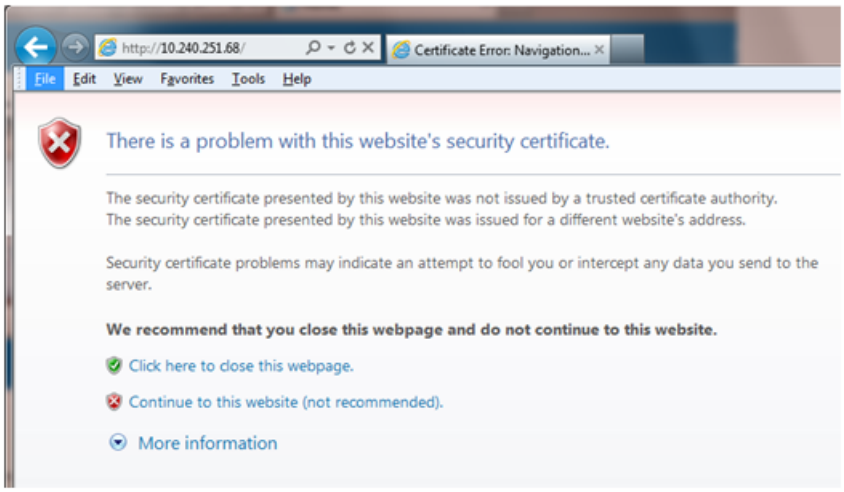
5. Application Console: Netbackup client software installation complete; if applicable return to calling procedure.

3.10.6 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.

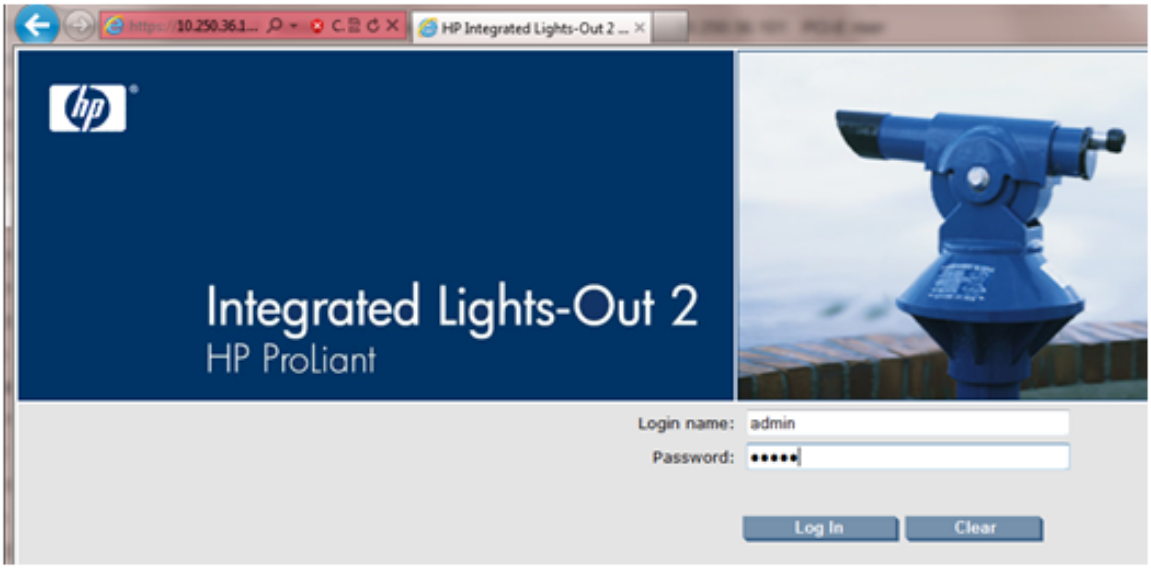
1. From Workstation: Launch Internet Explorer 7.x or higher and connect to the iLO2 device using "https://"



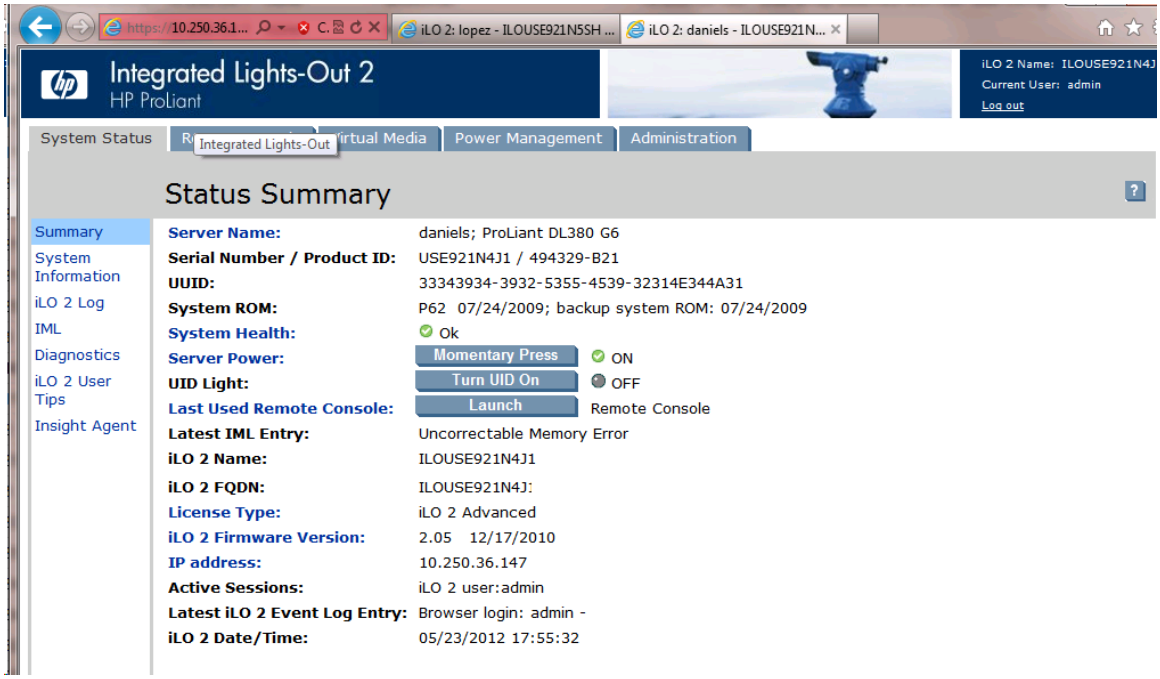
2. **iLO2 Web UI:**

   The user should be presented the login screen shown below.

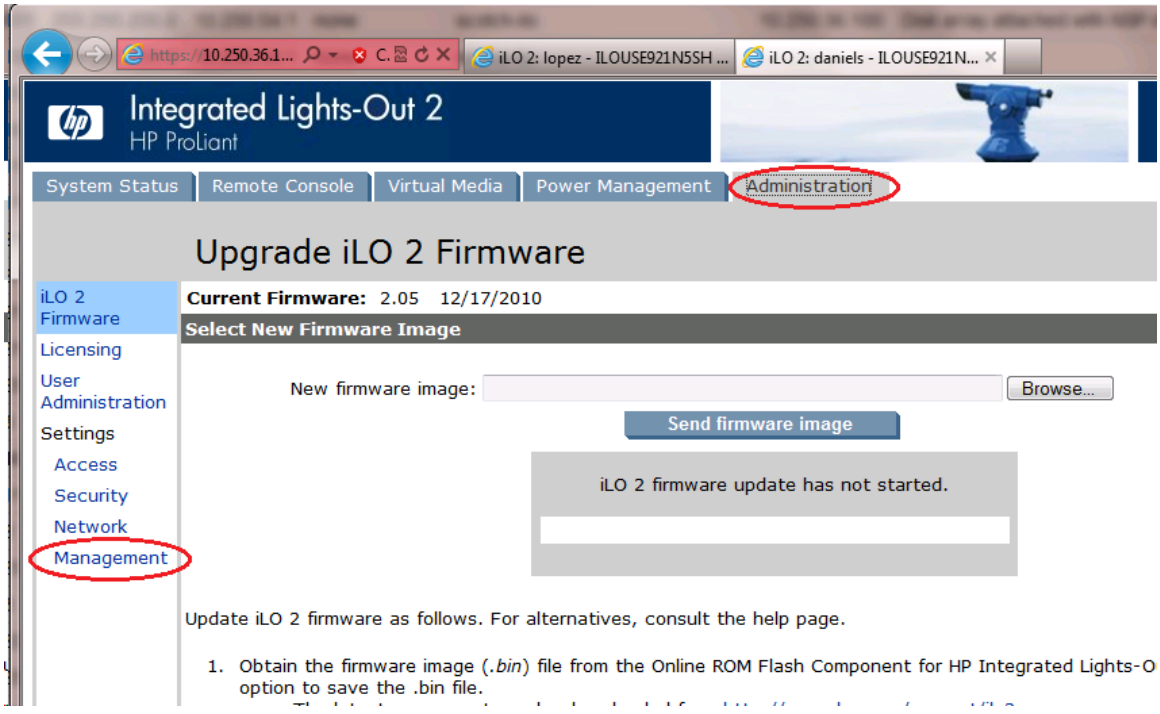
   Login to the GUI using an Administrator account name and password.



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.

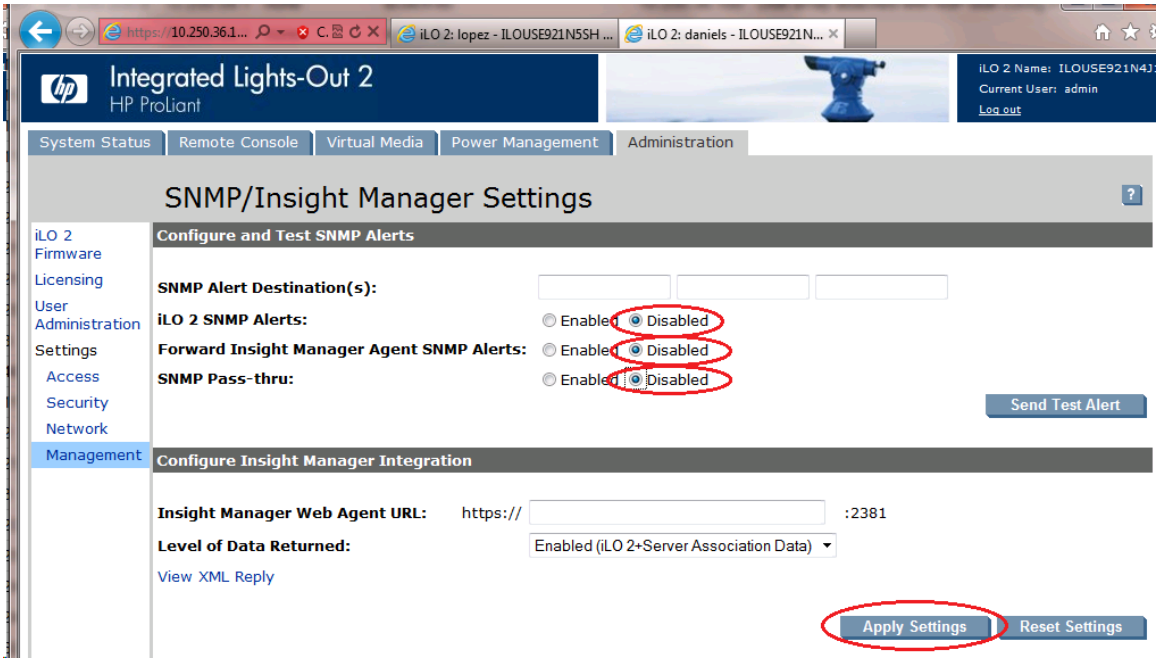


5. iLO2 Web UI:

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.

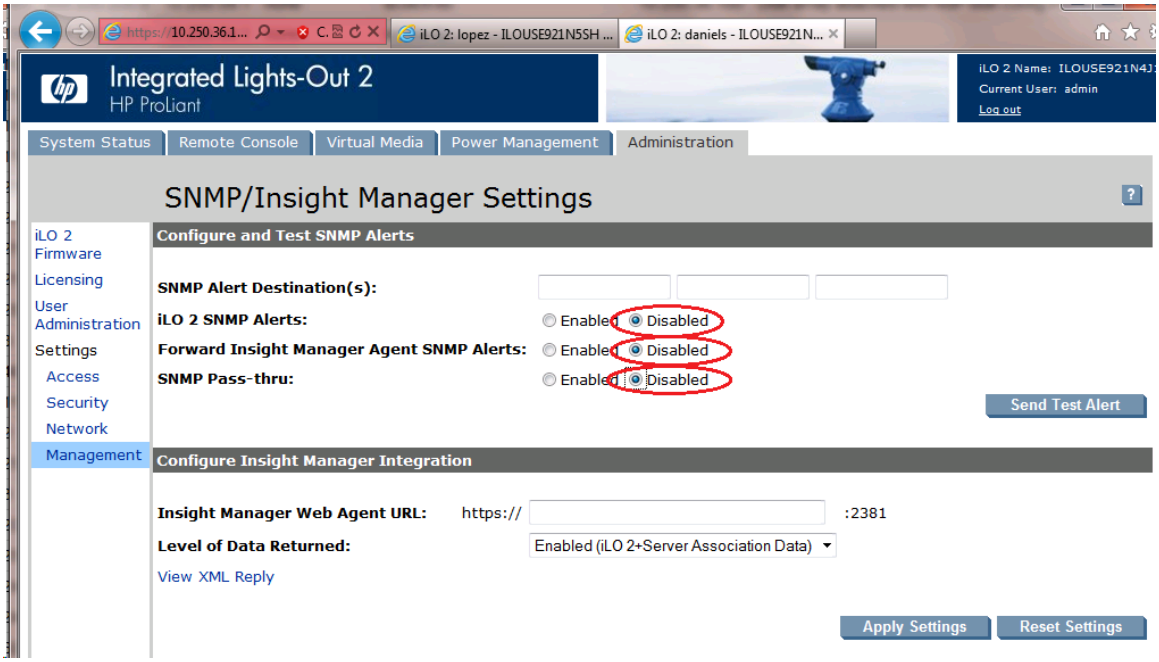
The web page will refresh but no specific indication will be given that settings have been saved.



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

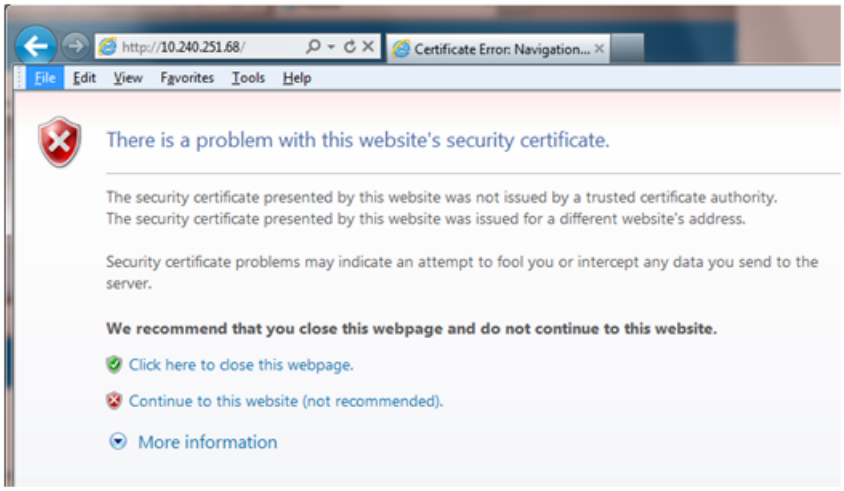
   Repeat this procedure all remaining iLO 2 devices on network.

3.10.7 Changing SNMP Configuration Settings for iLO 3 and iLO4

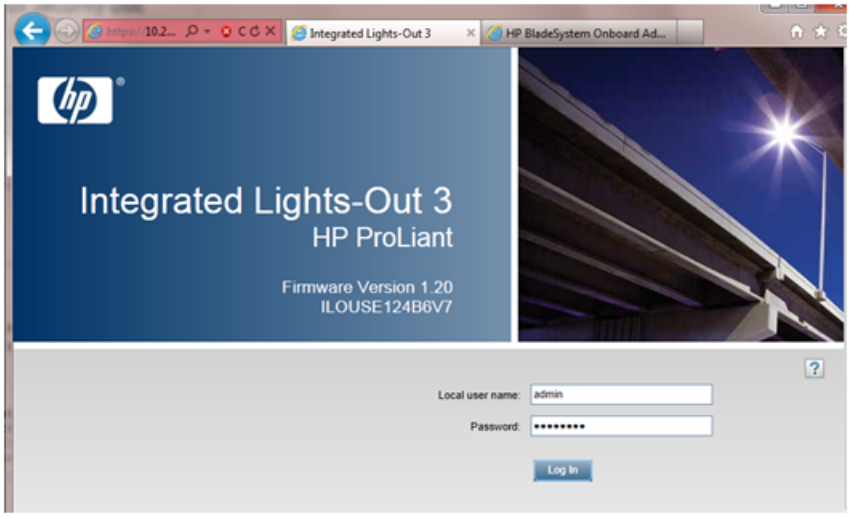
This procedure provides instructions to change the default SNMP settings for the HP ProLiant iLO 3 devices.

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://"

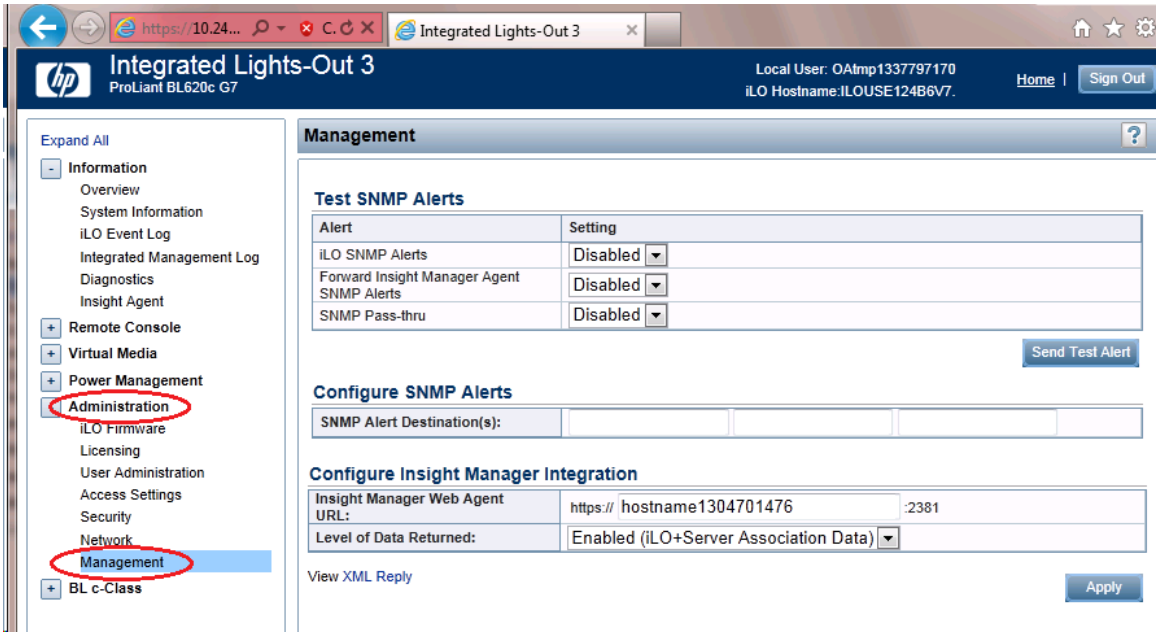


2. iLO 3/iLO 4 Web UI:
   The user should be presented the login screen shown below.
   Login to the GUI using an Administrator account name and password.



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.



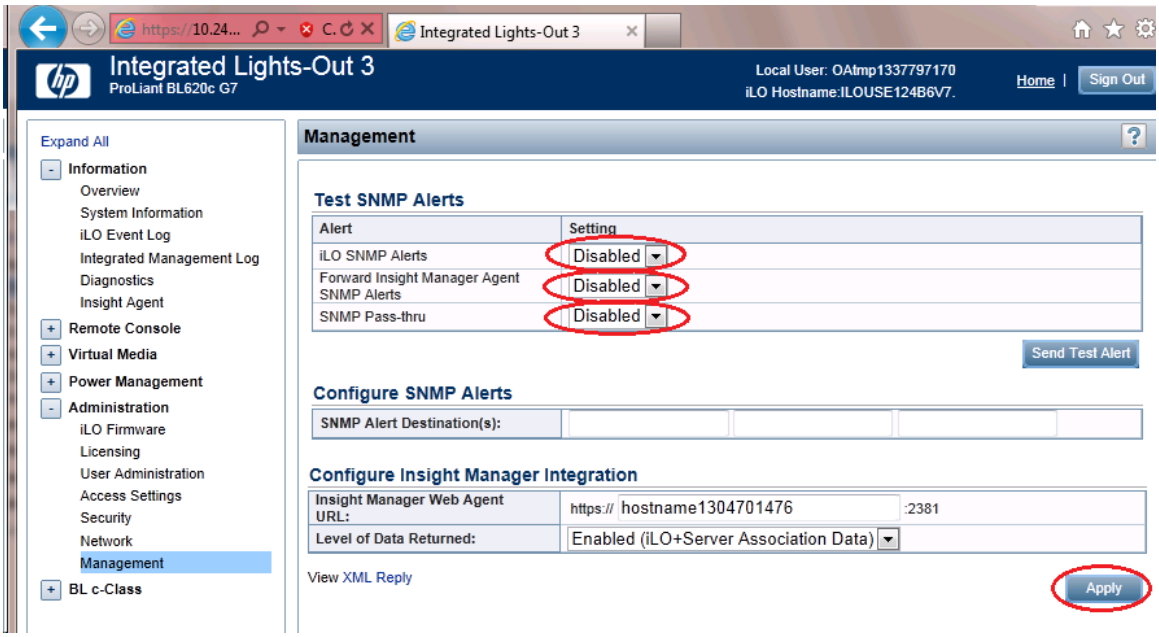
5. iLO 3/iLO 4 Web UI:

   The user should be presented the Management configuration page as shown on the right.

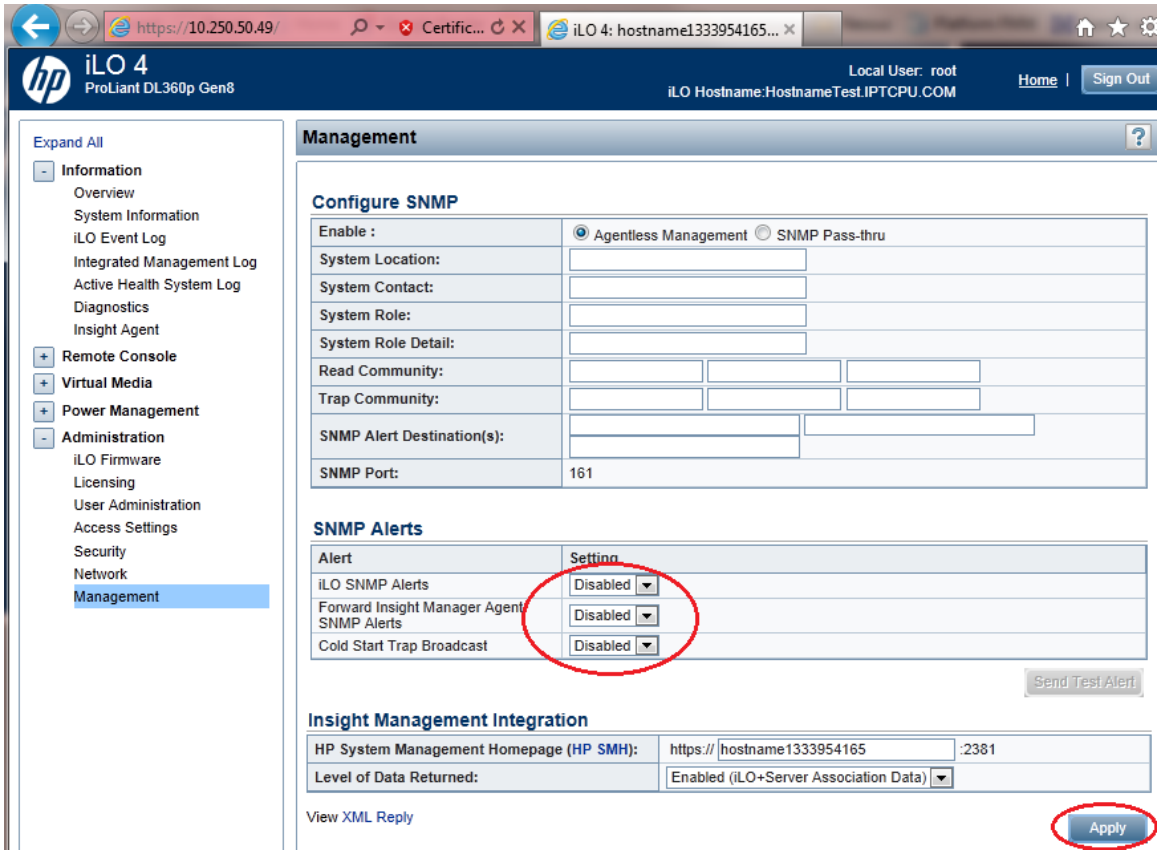
   1. Select setting [Disabled] for each of the 3 SNMP Alerts options as shown to the right.
   2. Click [Apply] to save the change.

   On the iLO 3 the web page will refresh but no specific indication will be given that settings have been saved.

   iLO3 Web UI:



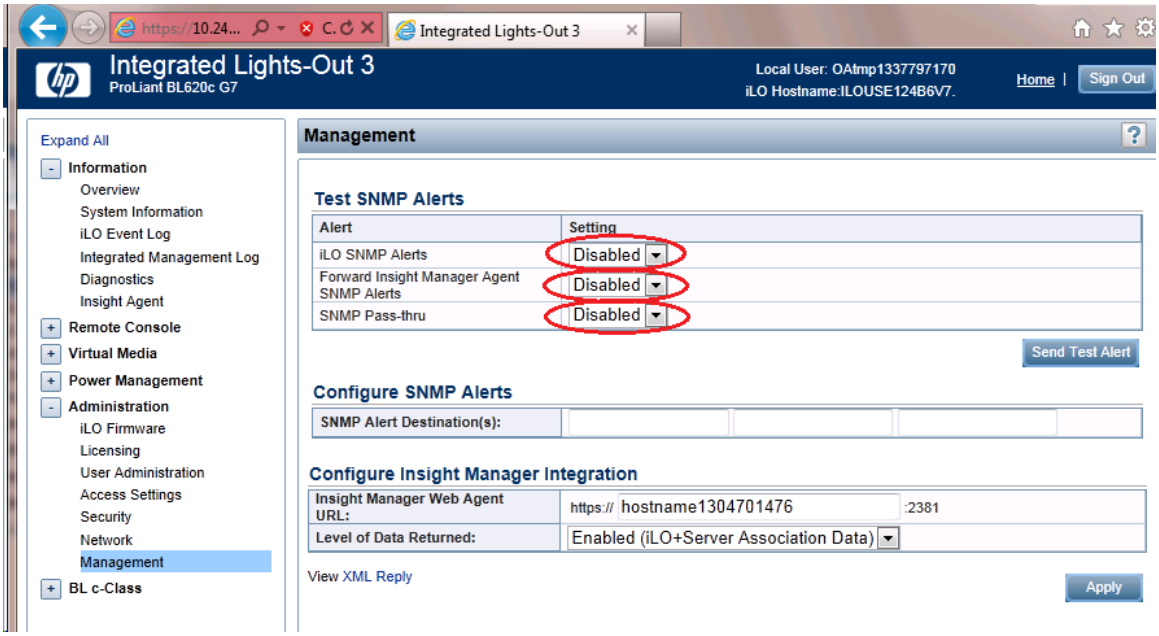
   iLO4 Web UI:



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.

3.10.8 Change SNMP Configuration Settings for ILOM

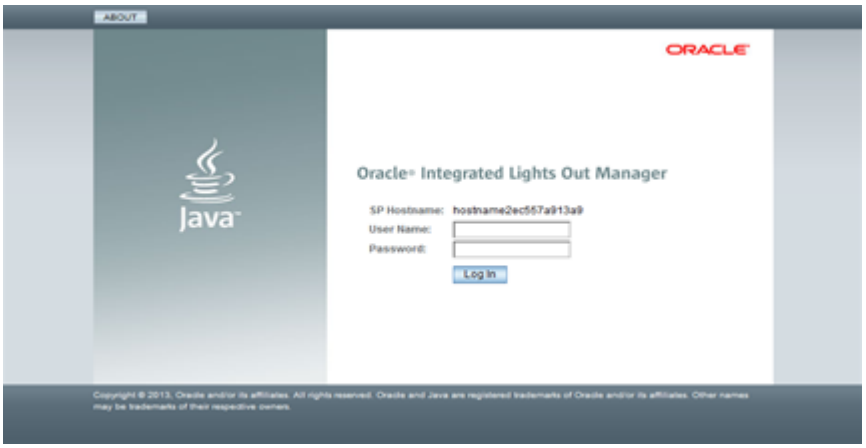
This procedure provides instructions on how to change the default SNMP settings for ILOM devices. Perform this procedure for every ILOM device on the network.

1. From Workstation:

   Launch a web browser and connect to the ILOM device.

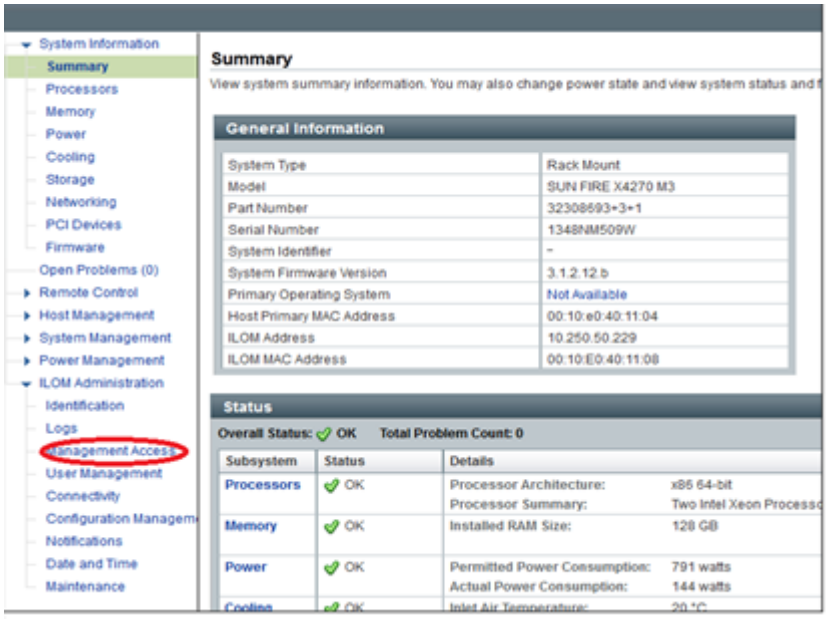
2. ILOM Web UI:

   The user will be presented within a login screen as shown below. Login using an account that has the admin level of privileges.



3. ILOM Web UI:

   The user will be presented with the **System Information > Summary page**. From the menu on the left select the ILOM Administration option. From the drop-down list, click on the **Management Access** option.



4. ILOM Web UI:

   At the top of the Management Access page click on the SNMP tab. In the Settings sections click on the State Enabled checkbox in order to uncheck it. Click the Save button.

3.10.9 Netbackup Client Install 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 *3.10.10 NetBackup Client Install/Upgrade with platcfg*.

Note: It is required that this procedure is executed before the customer does the Netbackup Client install.

Prerequisites:

- Application server platform installation has been completed.
- NAPD has been completed to determine the network requirements for the application server, and interfaces have been configured.
- NetBackup server is available to copy, sftp, the appropriate Netbackup client software to the application server.
- Filesystem for Netbackup client software has been created using *3.10.11 Create LV and Filesystem for NetBackup Client Software*.

- Contact *1.4 My Oracle Support (MOS)* to determine if the version of Netbackup Client being installed requires workarounds.

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.

3.10.10 NetBackup Client Install/Upgrade with platcfg

Executing this procedure will push and install NetBackup Client using platcfg menus.

Prerequisites:

- Application server platform installation has been completed.
- NAPD has been completed to determine the network requirements for the application server, and interfaces have been configured.
- NetBackup server is available to copy, sftp, the appropriate Netbackup client software to the application server.
- Filesystem for Netbackup client software has been created. Execute *3.10.11 Create LV and Filesystem for NetBackup Client Software* if the application installed on the server does not provide an alternative to creating the NetBackup logical volume.
- Config file has been created if the version of NetBackup Client is greater than 7.5.0.0.

Note: If a procedural STEP fails to execute successfully, STOP and contact *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.

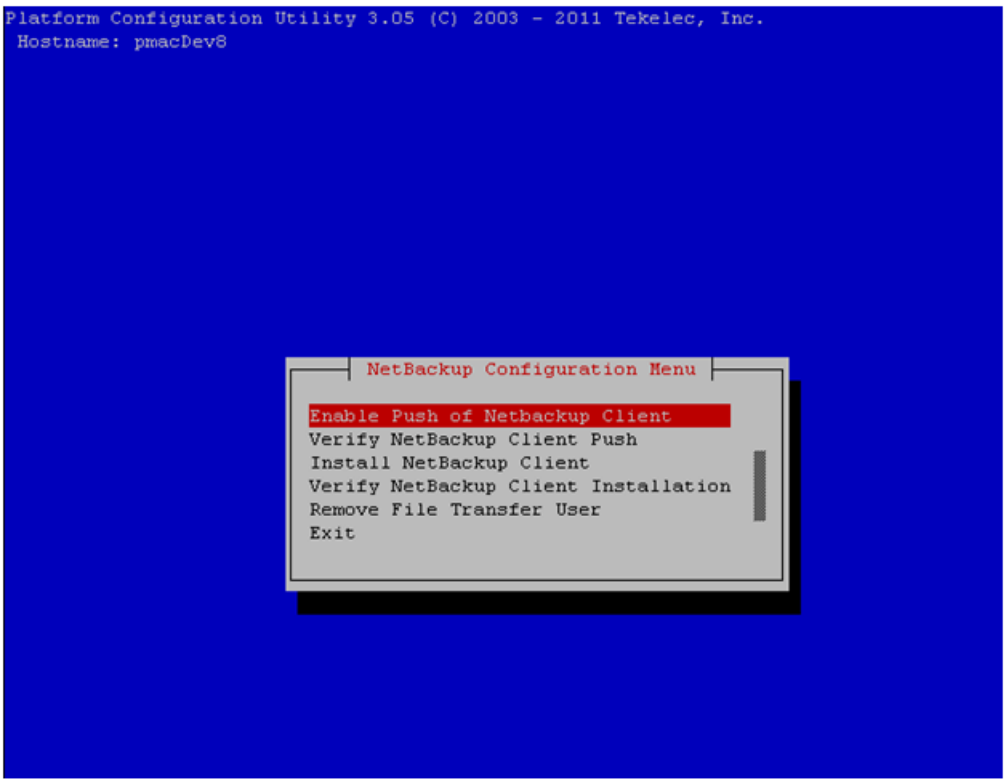
Login to application console using virsh, and wait until you see the login prompt:

```
$ 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:
```

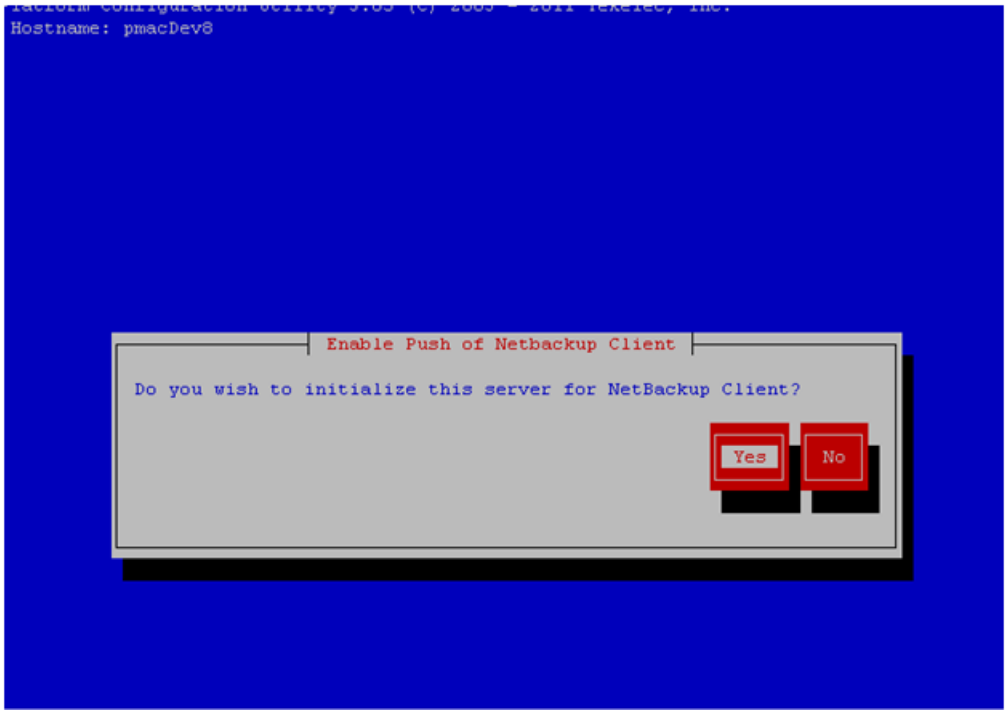
3. Application Console: Configure NetBackup Client on application server

```
$ sudo su - platcfg
```

Navigate to **NetBackup Configuration**

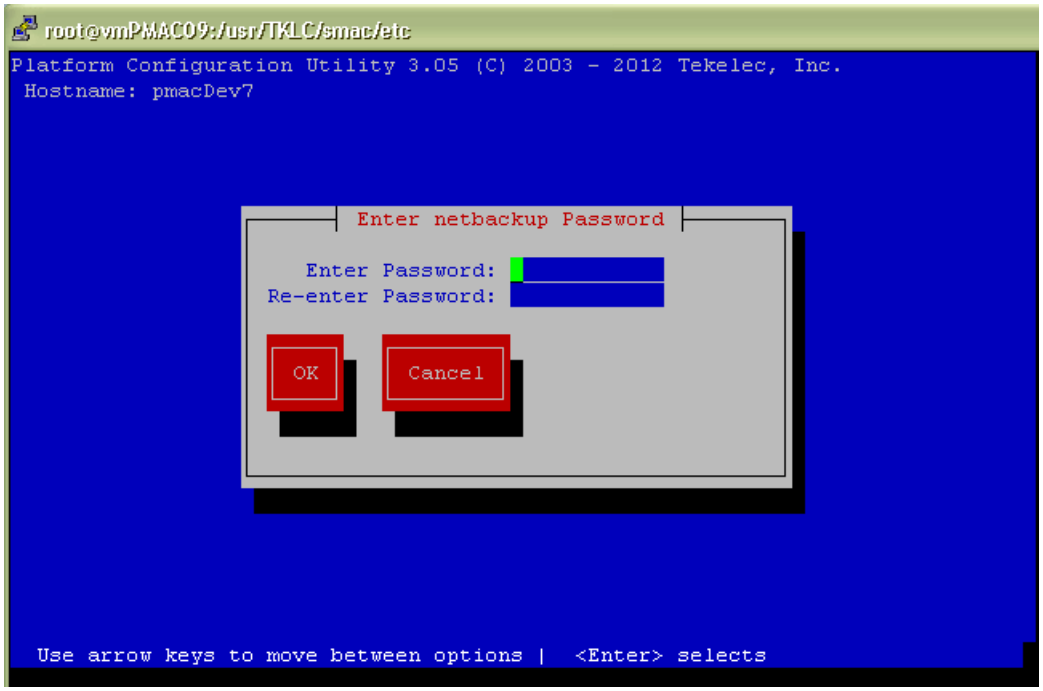


4. Application Console: Enable Push of NetBackup Client
   Navigate to **NetBackup Configuration** > **Enable Push of NetBackup Client**



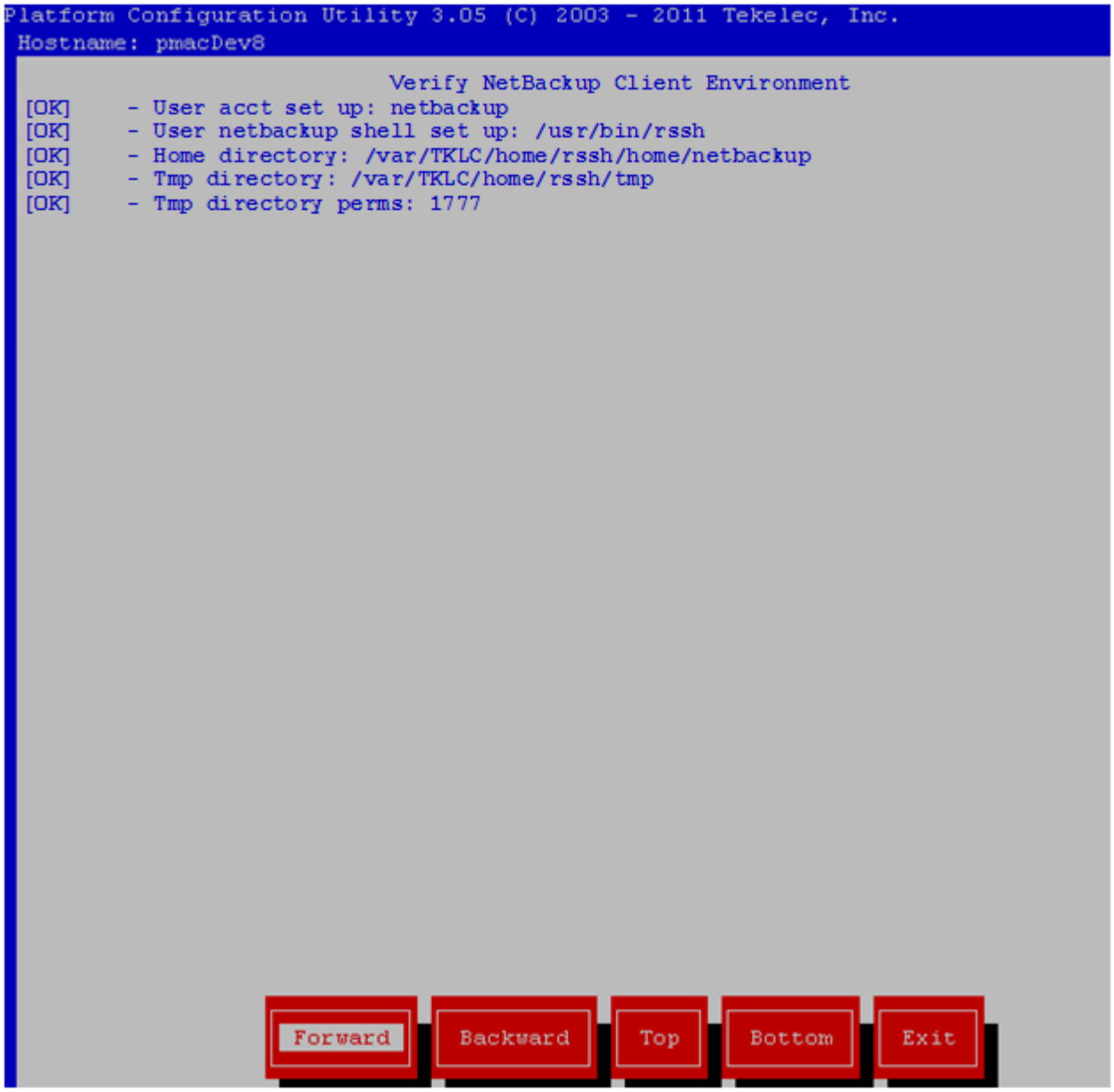
Select **Yes** to initialize the server and enable the Netbackup client software push.

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.

Note: The NetBackup user on the client will be a new user which will require the operator to change the password immediately. The operator should login to client to change the initial password.

Log in to the NetBackup server using password provided by customer:

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.
```

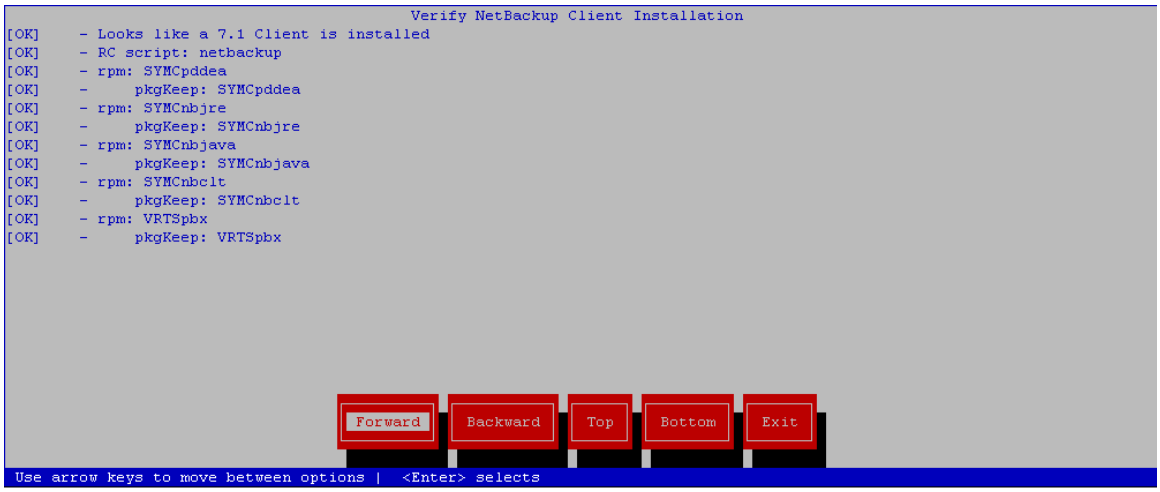
9. Application Console: Install Netbackup client software on application server.

   Navigate to **NetBackup Configuration** > **Install NetBackup Client**

   Select **Yes** to install the Netbackup client software.

   Select "**Exit**" to return to NetBackup Configuration menu.

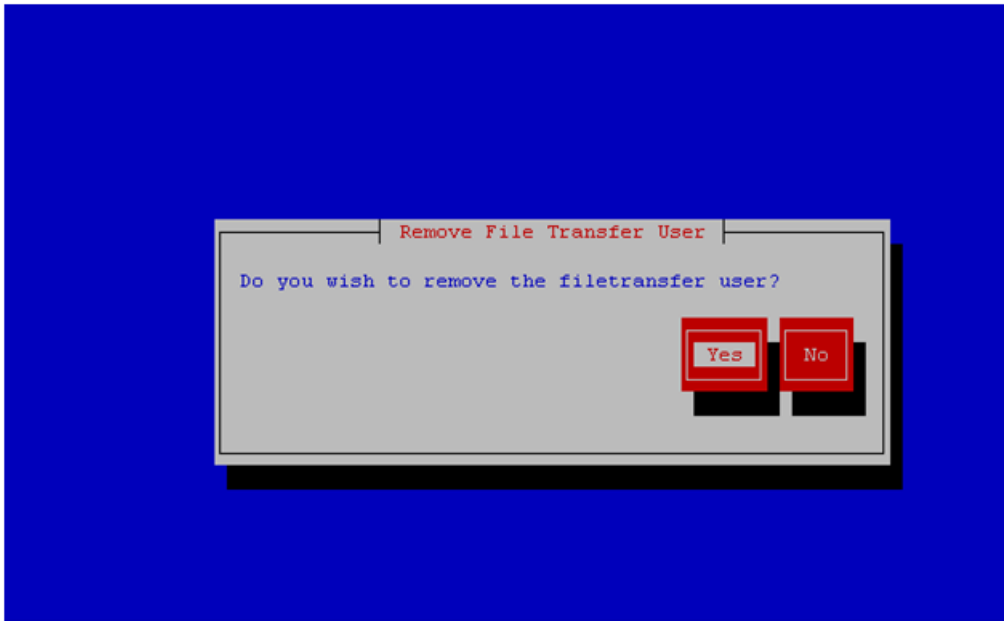
10. Application Console: Verify Netbackup client software installation on the application server.
    Navigate to **NetBackup Configuration** > **Verify NetBackup Client Installation**.



    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
SERVER = NB76Server
CLIENT_NAME = 10.240.117.134
CONNECT_OPTIONS = localhost 1 0 2
```

13. Application server iLO: Exit platform configuration utility (platcfg)
14. Return to calling procedure if applicable.

3.10.11 Create LV and Filesystem for NetBackup Client Software

This procedure will carve out storage for the NetBackup Client to reside on. This is necessary so that the NetBackup Client does not lead to disk shortage in the /usr/ filesystem.

Prerequisites:

- The volume group that the NetBackup logical volume will reside in has been previously determined. You can determine what space is available in each volume group by running the 'vgs' command and looking at the 'VFree' column. Ultimately applications should decide what volume group that the NetBackup LV should reside in.

1. Server: Login as admusr user.
2. Server: Create a storageMgr configuration file that defines the LV to be created.

```
$ sudo echo "lv --mountpoint=/usr/openv --size=5G --name=netbackup_lv --vg=$VG"
  > /tmp/nb.lvm
```

   The above example uses the $VG as the volume group. Replace $VG with the desired volume group as specified by the application group.

3. 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 is shown below:

```
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!

3.10.12 Migrate NetBackup Client to New Filesystem

This procedure will migrate the installed files for NetBackup Client from the /usr/ filesystem into a filesystem dedicated to NetBackup Client.

1. Server: Login as admusr user.
2. Server: Stop the NetBackup services using the following two commands:

```
$ sudo service netbackup stop
$ sudo service vxpbx_exchanged stop
```

3. Server: Bind mount /usr/openv to a temporary mount point

```
$ sudo mkdir /tmp/openv
$ sudo mount --bind /usr/openv /tmp/openv
```

4. Server: Follow *3.10.11 Create LV and Filesystem for NetBackup Client Software* to create the LV and filesystem.
5. Server: Move all contents of /tmp/openv to /usr/openv

```
$ sudo mv /tmp/openv/* /usr/openv
```

6. Server: Unmount bind mount and remove mount point

```
$ sudo umount /tmp/openv
$ sudo rmdir /tmp/openv
```

7. Server: Start the NetBackup services.

```
$ sudo service vxpbx_exchanged start
$ sudo service netbackup start
```

Note: If Netbackup version 7.7 or greater is being installed or upgraded to, follow procedure *P.1 Increase the PM&C Netbackup Filesystem Size* to increase the PM&C Netbackup filesystem Size. The Netbackup client requires additional space than the standard 2G volume used by previous versions.

3.10.13 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.

Prerequisites:

- The TPD-NetBackup RPM has been installed on the server.
- The contents of the NetBackup Client config file are known.

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
```

3.11 TVOE Host Procedures

3.11.1 Enable Virtual Guest Watchdogs as appropriate for the application

This procedure provides instructions for using the PM&C application on the management server to enable the Virtual Guest Watchdog on VM Guests after upgrading a TVOE VM Host to a version that adds watchdog support (TVOE version 2.0.0_80.11.0 or later).

Prerequisites:

- One or more installations of TVOE have been upgraded to TVOE version 2.0.0_80.11.0 or higher.

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

1. On the PM&C managing each newly upgraded TVOE server, navigate to the **Main Menu** > **VM Management** page of the PM&C GUI.
2. In the "VM Entities" list, locate the Host that was just upgraded and click its '+' icon to expand its list of VM Guests.
3. Using the VM Entities list, for each VM Guest on the TVOE Host that was upgraded, select the VM Guest and do the following:

   If virtual watchdog support is not desired for the current VM Guest, no further action is needed for this guest. Proceed to the next VM Guest on this TVOE Host.

   To enable virtual watchdog support for the current Guest:

a) Shut down the VM Guest by setting its power state to "**Shutdown**" and clicking the adjacent "**Change to...**" button. Wait for the shutdown to complete, as indicated by the Current Power State field of the GUI.
b) Click the **Edit** button to enter edit mode for this VM Guest. Click the "**Enable Virtual Watchdog**" checkbox to enable the watchdog, and then click **Save**. Wait for the Edit operation to finish.
c) Start the VM Guest by setting the Current Power State back to On and clicking the "**Change to...**" button.
d) When the VM Guest's power state indication shows "**Running**", proceed to the next VM Guest on this Host.

3.11.2 TVOE NetBackup Client Configuration

This procedure will setup and install NetBackup Client on a TVOE host.

Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to backup the following file from the TVOE host:

- `/var/TKLC/bkp/*.iso`

1. TVOE Server: Log in as 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 ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt
/usr/TKLC/plat/etc/ip6tables/
$ 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. TVOE Server: Create LV and filesystem for Netbackup client software.

   Using the **vgguests** volume group, use *3.10.11 Create LV and Filesystem for NetBackup Client Software* to create an LV and filesystem for the Netbackup client software.

5. TVOE Server: Install the Netbackup client software.

   Install the Netbackup client software by executing *3.10.5 Application NetBackup Client Install Procedures*.

   Note: Skip any steps relating to copying NetBackup "notify" scripts to /usr/openv/netbackup/bin. The TVOE NetBackup notify scripts are taken care of in the next step.

6. TVOE Server: Create softlinks for TVOE specific NetBackup notify scripts.

```
$ 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
```

Appendix A

Using WinSCP

Topics:

- *Using WinSCP.....399*

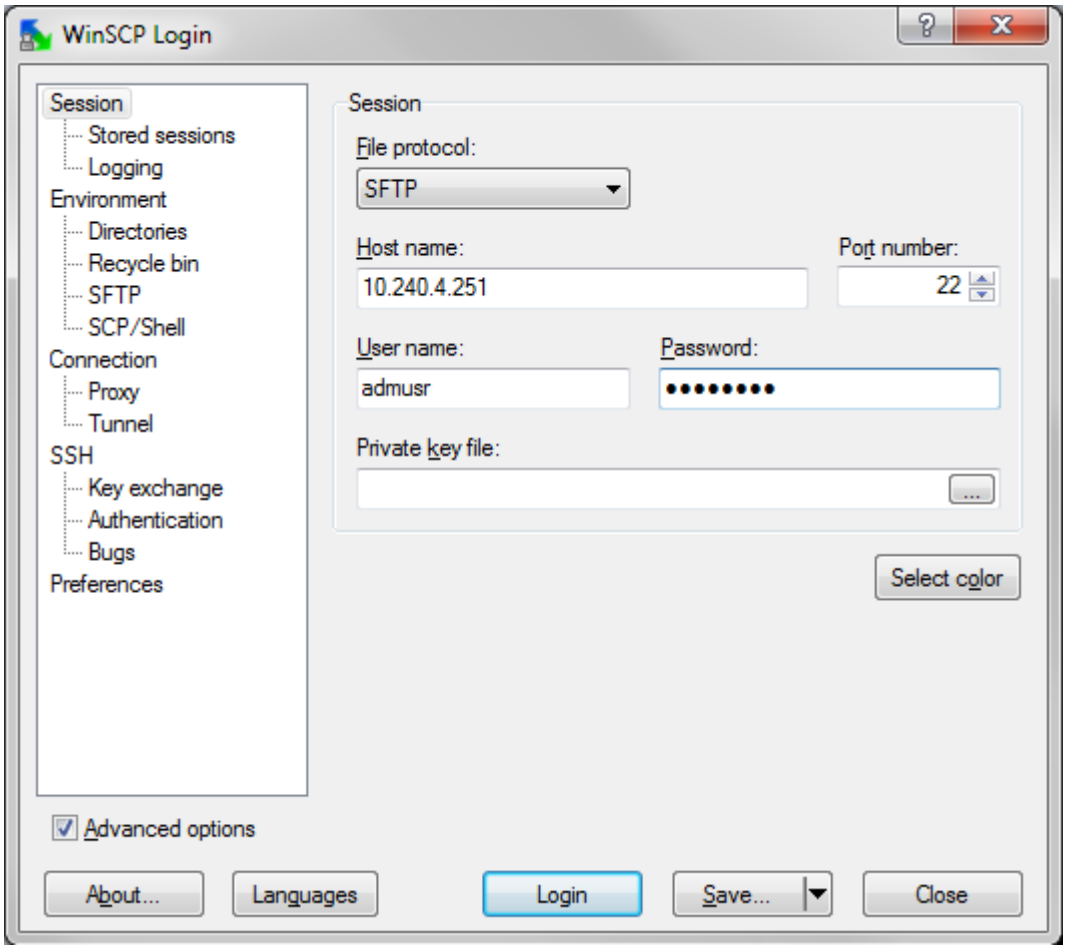
A.1 Using WinSCP

The following is an example of how to copy a file from the management server to your PC desktop

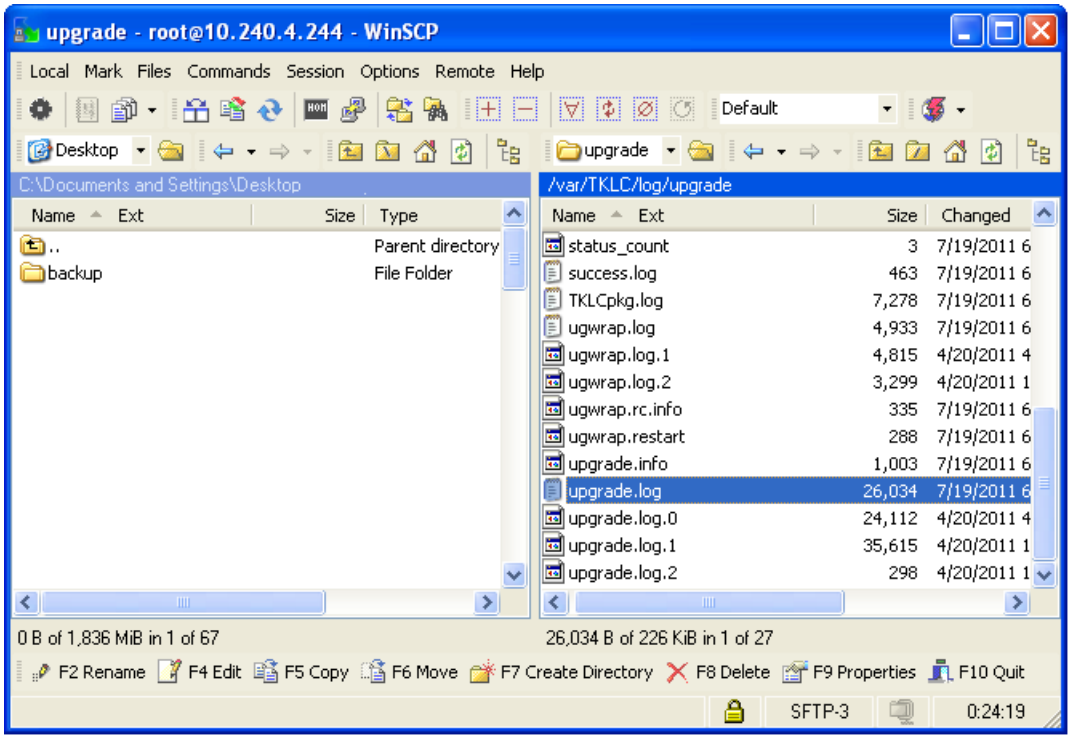
1. Download the WinSCP Application
   Download the WinSCP application:

```
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, **admusr** into the `User name` field, and **<admusr_password>** into the `Password` field. Click **Login**.



3. Copy the target file from the management server
   On the left side 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 and 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 B

P2000 MSA USB Driver Installation

Topics:

- *P2000 MSA USB Driver Installation.....402*

B.1 P2000 MSA USB Driver Installation

The P2000 USB Driver allows Microsoft Windows to recognize the USB Port on HP StorageWorks P2000 G3 MSA Controllers. This appendix describes how to install the driver on your laptop.

Prerequisite: *3.7.9 Adding ISO Images to the PM&C Image Repository* has been completed using the HP MISC firmware ISO image.

Note: If you are unable to detect the P2000 array after installing the USB driver, power cycle the P2000 array once.

Needed material:

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

1. Management Server: Obtain the USB driver executable

   Copy the following file form the management server to your PC using an scp client:

   ```
   /usr/TKLC/smac/html/TPD/HPFW--872-2488-XXX--HPFW/files/<USB_Driver>.exe
   ```

   Windows users:

   Refer to *A.1 Using WinSCP* to copy the zip file to your PC.

   Note: Refer to the Release Notes of the HP Solutions Firmware Upgrade Pack [2] to select the correct file to copy.

2. Microsoft Windows Laptop: Initiate the setup wizard.

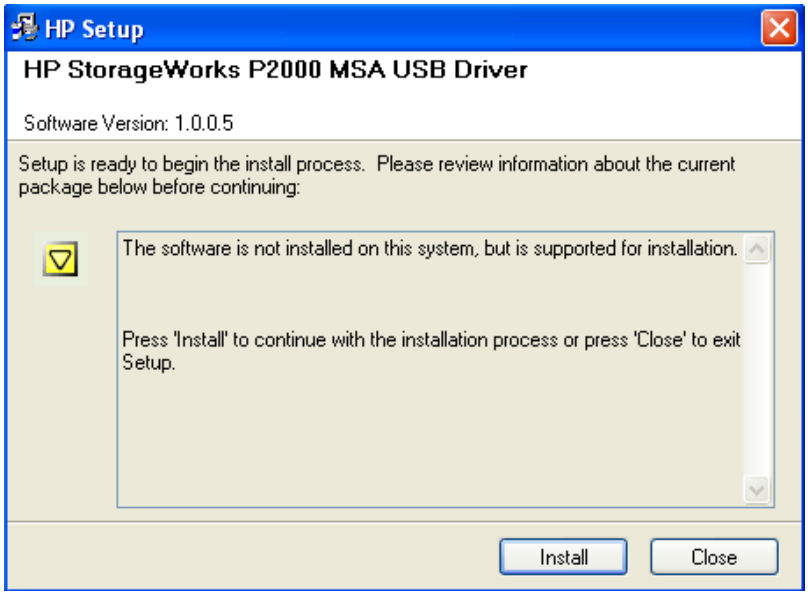
   Click the USB Driver executable on your laptop. If a security window pops up asking whether to run the executable, click **Run**.

   The following window should appear:

   Click **Install**

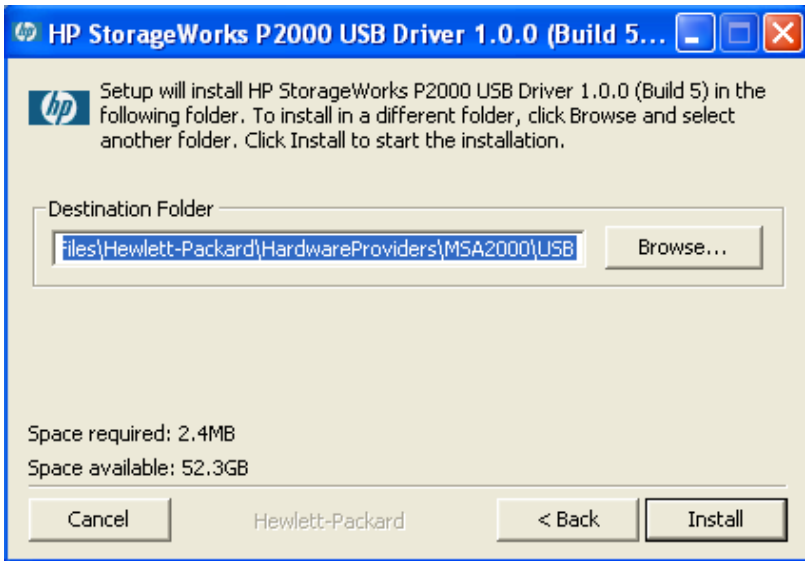
3. Microsoft Windows Laptop: Agree to install

   After brief content extraction, the following window will present itself:



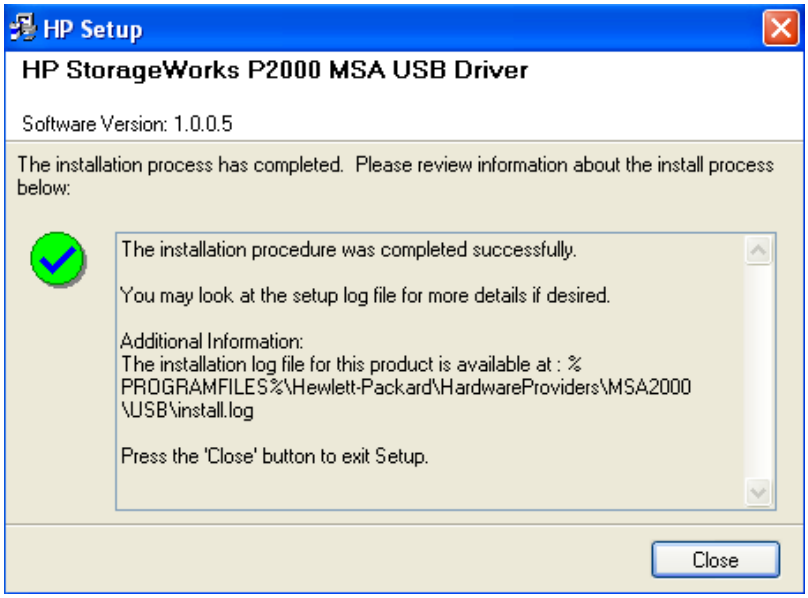
Click **Install**. In the next window, click **I agree** to proceed with the installation

4. Microsoft Windows Laptop: Select installation directory
   Then use the **Browse** button to select the folder where to install



Click **Install**

5. Microsoft Windows Laptop: Verify the installation
   The success confirmation window concludes the installation. Click the **Close** button


HP Setup
HP StorageWorks P2000 MSA USB Driver
Software Version: 1.0.0.5
The installation process has completed. Please review information about the install process below:
The installation procedure was completed successfully.
You may look at the setup log file for more details if desired.
Additional Information:
The installation log file for this product is available at : %PROGRAMFILES%\Hewlett-Packard\HardwareProviders\MSA2000\USB\install.log
Press the 'Close' button to exit Setup.
Close

Appendix C

Determining which Onboard Administrator is Active

Topics:

- *Determining Which Onboard Administrator Is Active.....406*

C.1 Determining Which Onboard Administrator Is Active

This appendix describes how to determine which Onboard Administrator is active in an enclosure with two OAs.

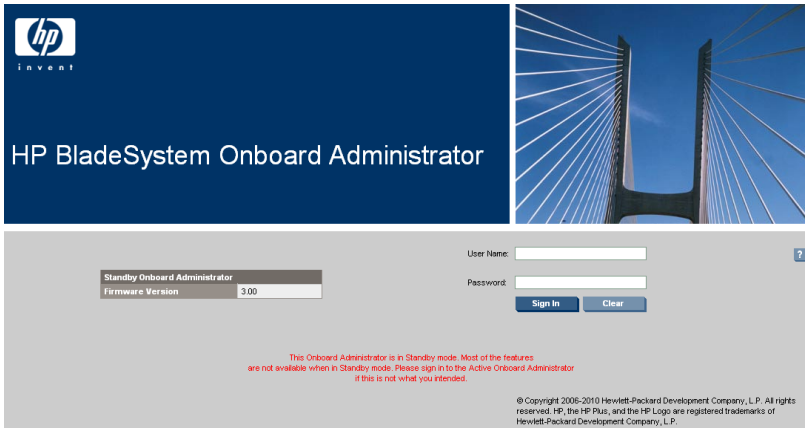
Prerequisite: *3.5.2 Configure Initial OA Settings Using the Configuration Wizard* has been completed.

OA GUI: Determine which OA is Active

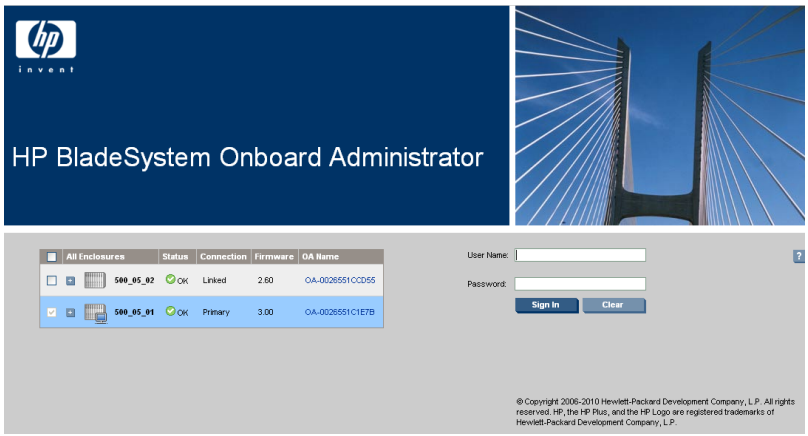
Open your web browser and navigate to the IP address of one of the Administrators:

```
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 D

Worksheet: netConfig Repository

Topics:

- *Worksheet: netConfig Repository.....408*

D.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 #
<OA2_enX_ip_address>	X= the enclosure #
<OA_password>	
<FW_image>	

Appendix E

PM&C Features Configuration

Topics:

- *PM&C Feature Configuration.....410*

E.1 PM&C Feature Configuration

Overview

PM&C configuration allows users to manage identified software features. Features implemented by PM&C may be defined as "editable" in profiles that are used during PM&C Initialization. This is typically decided and specified in profiles by developers. When a feature is defined as "editable," it may be managed by authorized users via the PM&C GUI or CLI. Features may be enabled or disabled, and their associated role may be changed (used for features that expose or configure services on an network interface basis).

Enabling Features

Enabling features may impact available APIs (that is, fail the requests), configure services (for example, configure TFTP), or configure the host firewall. From the CLI, you may "administratively" disable a feature to temporarily block actions. This is useful for NetBackup to prevent actions affecting the backup images, or netConfig to prevent conflicts with TFTP services. Administratively disabled services are either enabled manually or enabled when PM&C is restarted.

Editing Roles

Feature roles are used to associate a feature with a particular set of interfaces. This is used to manage the host firewall or configure services. New roles may be defined and applied to dedicated interfaces. For instance, NetBackup is often provided a unique role.

You should understand the network and product before changing roles. The "control", "management" and "NetBackup" roles are currently used by products. PM&C was designed to be flexible, so you are able to create roles and map them to interfaces as desired (e.g., expanding a system may need to add new non-contiguous networks for control or management).

Features

Features are declared as user editable by profiles. The current PMAC 6.3 TVOE profile exposes the following features:

- "DEVICE.NETWORK.NETBOOT" is used to allow netConfig to initialize Cisco 3020 switches that use TFTP. It is typically enabled on the "management" role.
- "DEVICE.NTP" allows devices to use PM&C as an NTP server. By default, the port is blocked by the firewall.
- "PMAC.MANAGED" allows remote systems to access the SNMP service on PM&C
- "PMAC.REMOTE.BACKUP" is another optional feature.
- "PMAC.NETBACKUP" is an optional feature that should be enabled if NetBackup is used.
- "PMAC.IPV6.NOAUTOCONFIG" is an optional feature that disables auto-configuration of IPv6 on PM&C interfaces.

To add features as editable, they must be declared in the profile during PM&C Initialization. If PM&C is in service, you must use the CLI to reset and re-initialize PM&C. To prevent profile changes from being lost during upgrade, you should avoid modifying profiles delivered with PM&C. Best practice is to copy the profile and edit this version.

GUI Usage

From the PM&C GUI, navigate with: **Main Menu** > **Administration** > **PM&C Configuration** > **Feature Configuration**.

The platform will be reconfigured when the **Apply** button is pressed.

CLI Usage

The `pmacadm` CLI allows features to be modified also. This is the only interface to administratively disable a feature. The options on the `pmacadm` command map to integers for the enable/disable states (see `man pmacadm`).

For example, to 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
```

Appendix F

How to Access a Server Console Remotely

Topics:

- *How to Access a Server Console Remotely.....413*

F.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
<ilom_admin_user>	Privileged username for Oracle RMS ILOM 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. 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 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 G

How to Attach an ISO Image to a Server Using the iLO or ILOM

Topics:

- *How to Attach an ISO Image to an HP Server Using the iLO.....416*
- *How to Attach an ISO Image to an Oracle Rack Mount Server Using the ILOM.....422*

G.1 How to Attach an ISO Image to an HP Server Using the iLO

1. 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>/
   ```

2. iLO Web GUI: Log in to iLO as an "administrator" user.

   Username = <ilo_admin_user>

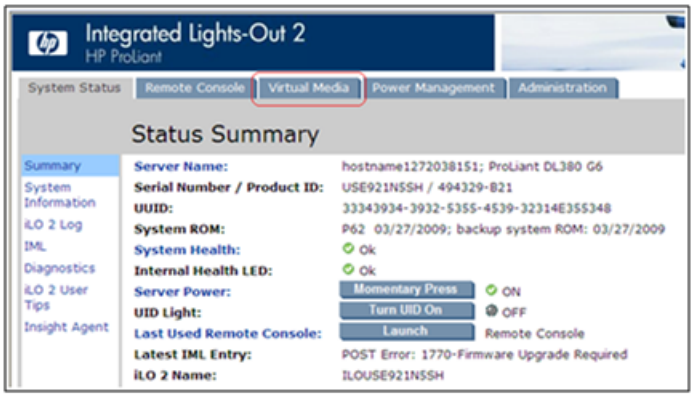
   Password = <ilo_admin_password>

3. Determine which steps to take based on the iLO version

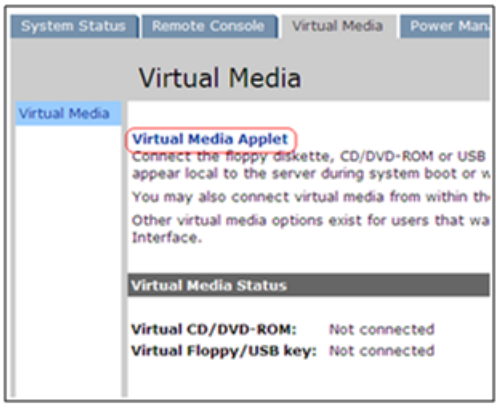
   If the iLO GUI indicates "Integrated Lights-Out 2", continue at the next step.

   If the iLO GUI indicates "Integrated Lights-Out 3" or "Integrated Lights-Out 4", continue at step 12.

4. iLO 2 Web GUI:
   a) Select the **Virtual Media** page.
   b) Click the **Virtual Media** tab on the **System Summary** page.

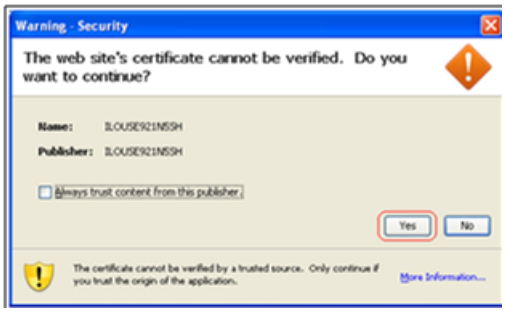


5. iLO 2 Web GUI:
   a) Click on the **Virtual Media Applet** link to launch the Virtual Media application. The iLO GUI should open to the Virtual Media page.



6. iLO 2 Web GUI - Java Security Prompt: Acknowledge Security Warning

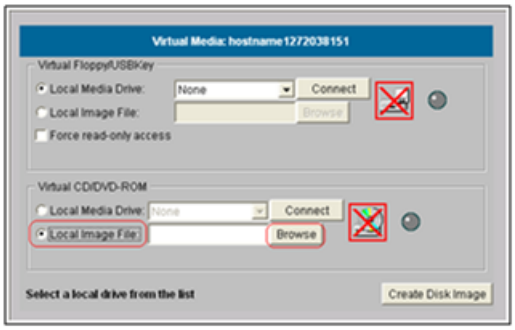
   If a security dialog is presented, click **Yes** to acknowledge the issue and proceed.



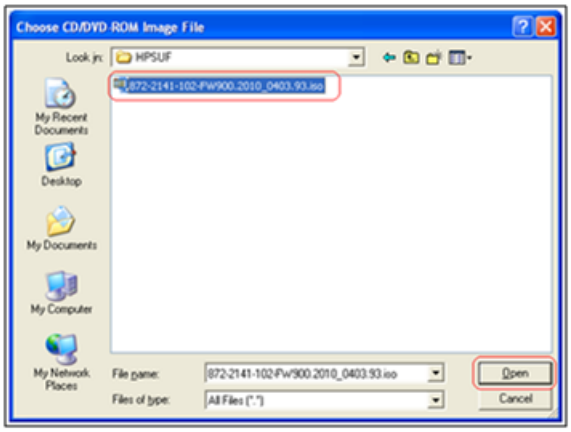
   If other warning dialogs are presented, acknowledge them as well to proceed to the Virtual Media applet.

7. iLO 2 VM Applet: Select the specified ISO file.

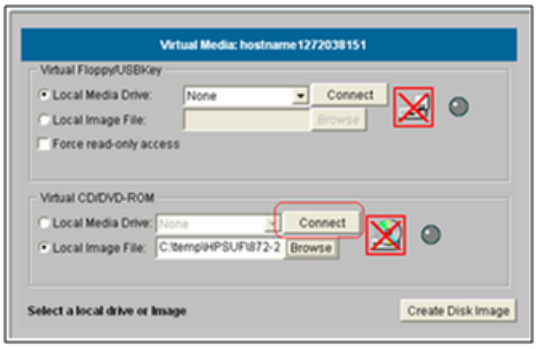
   In the Virtual CD/DVD-ROM Panel, select the **Local Image File** option and click the **Browse** button. Navigate to the ISO image file specified by the procedure which referenced this appendix.



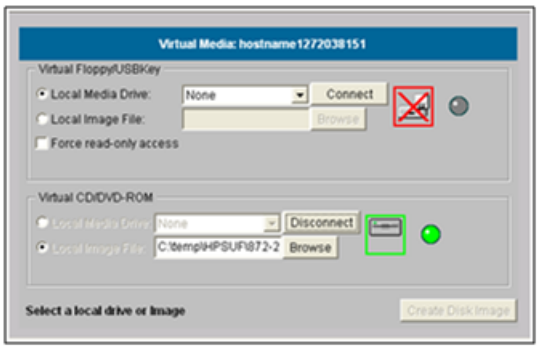
Select the ISO image file and click **Open**.



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



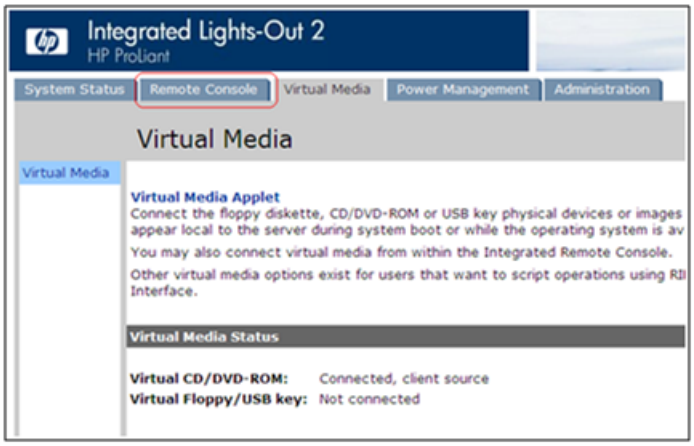
When create the LED Light icon should be green.



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

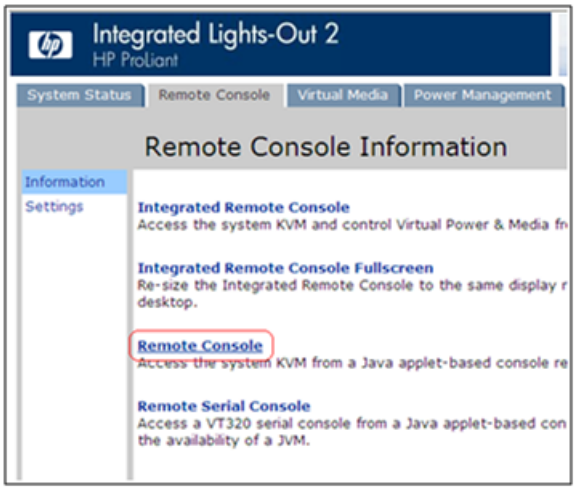
9. iLO 2 Web GUI: Access the Remote Console Page.

   At the iLO 2 Web GUI, click on the **Remote Console** tab.



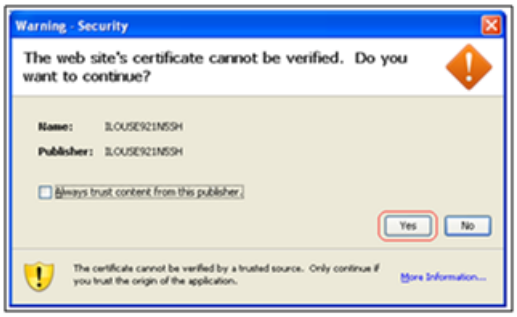
10. iLO 2 Web GUI: Launch the Remote Console Applet.

    On the Remote Console page, click on the **Remote Console** link to launch the console applet.



11. iLO 2 Web GUI - Java Security Prompt: Acknowledge Security Warning.

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

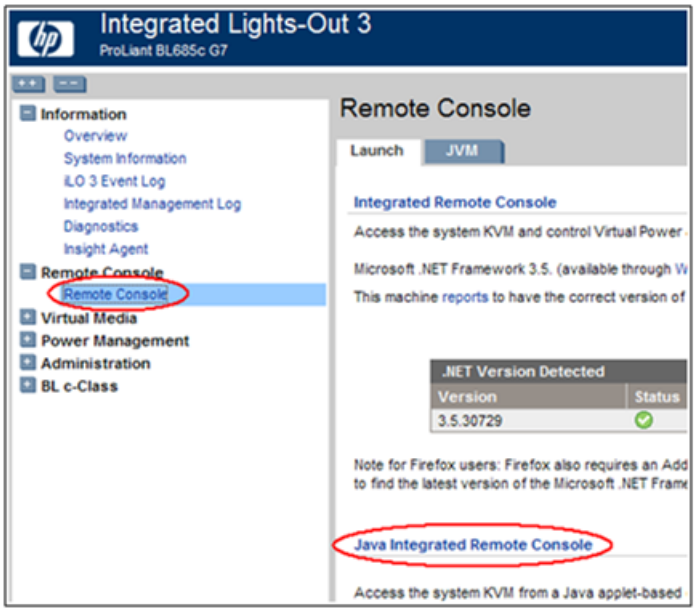


If other warning dialogs are presented you may also acknowledge them as well to proceed to the Java Integrated Remote Console applet.

Skip to step 16

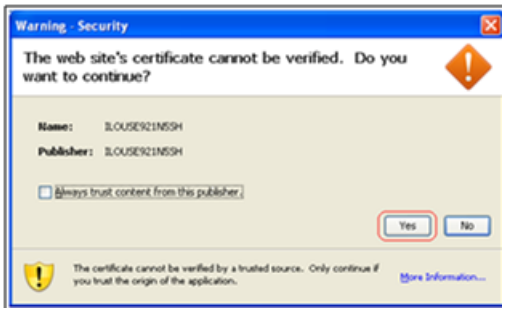
12. iLO 3 / iLO 4 Web GUI: Launch the Java Integrated Remote Console applet.

On the menu to the left navigate to the Remote Console page. Click on the **Java Integrated Remote Console** to open it.



13. iLO 3 / iLO 4 - Java Security Prompt: Acknowledge Security Warning.

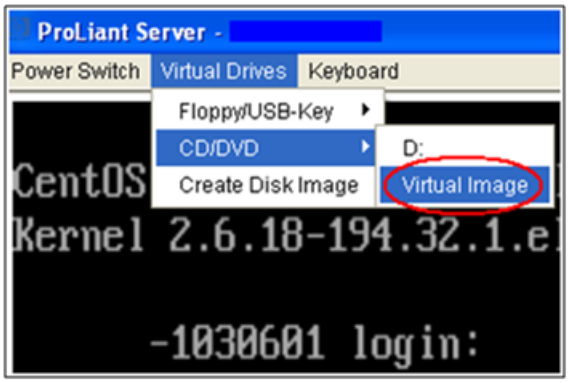
If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed.



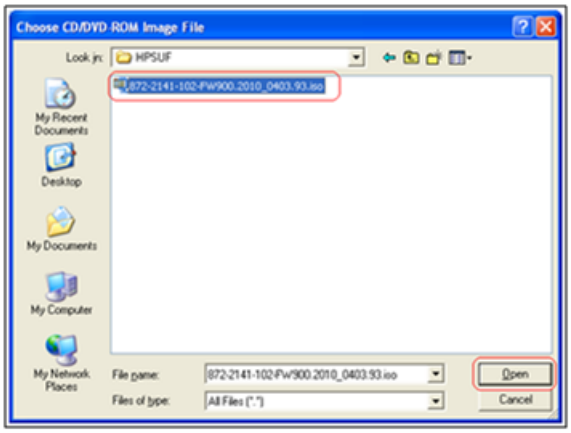
On the menu to the left navigate to the Remote Console page. Click on the **Java Integrated Remote Console** to open it.

14. iLO 3 / iLO 4 - Remote Console: Create Virtual Drive Connection

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



Navigate to the location of the ISO image file specified by the procedure which referenced this appendix.



Select the desired file and click **Open**.

15. iLO 3 / iLO 4 - Remote Console: Verify Virtual Image Connection.

At the bottom of the remote console window, there should now be a green highlighted drive icon and "Virtual M" written next to it.

16. Return to the referencing procedure
    Return to the procedure which referenced this appendix.

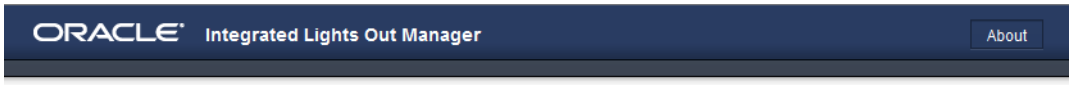
G.2 How to Attach an ISO Image to an Oracle Rack Mount Server Using the ILOM

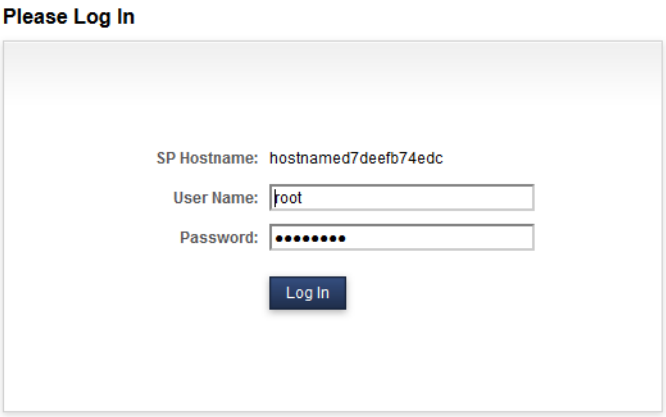
1. **Local Workstation:** Access the ILOM Web GUI

   Use the following URL:

   ```
   https://<ilom_IP>/
   ```

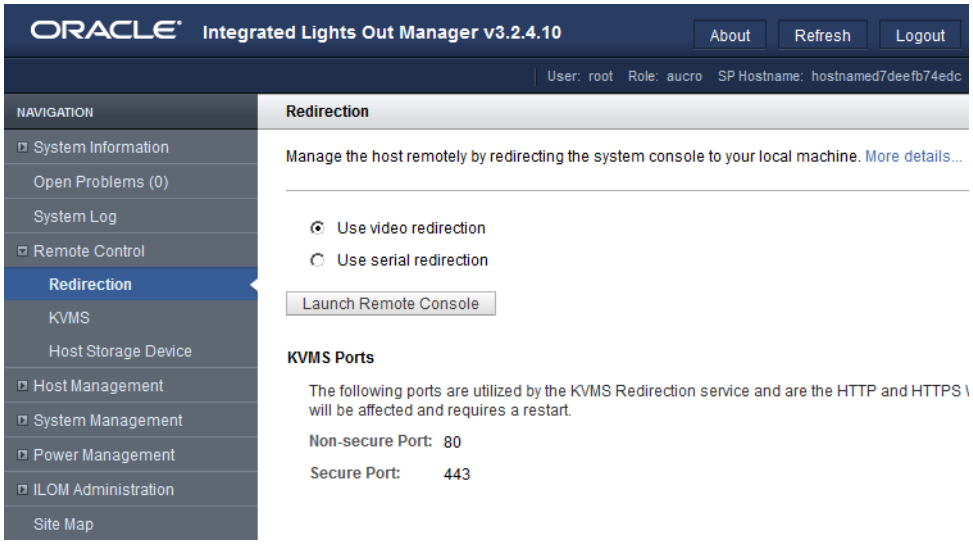
2. ILOM Web GUI: Log in to the ILOM as a "root" user.





3. ILOM Web GUI:

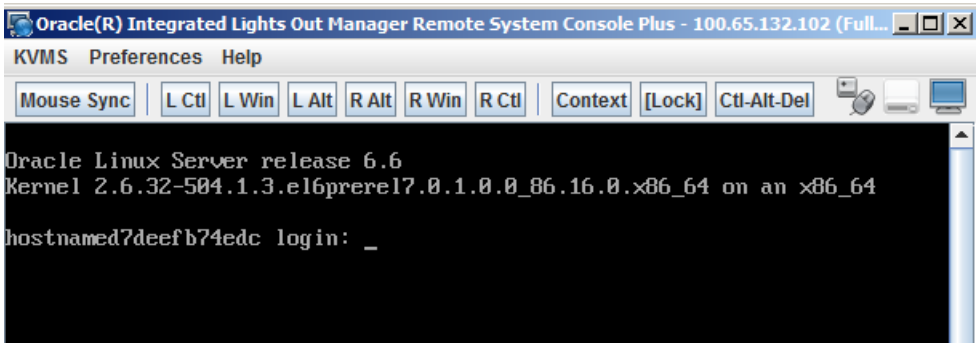
   From the **Redirection** screen, press **Launch Remote Console**.



From the pop-up, click **OK** and then **Accept** the security warning to launch the Remote System Console.

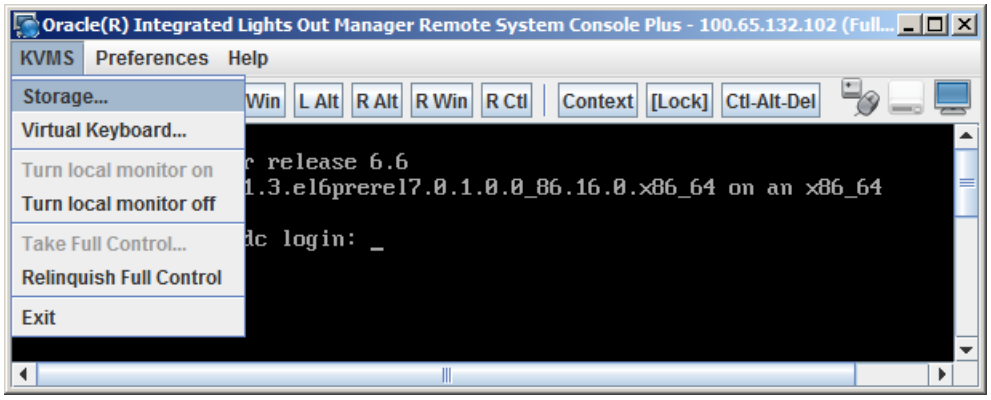
4. ILOM Remote System Console:

   The **Remote Console** will launch.



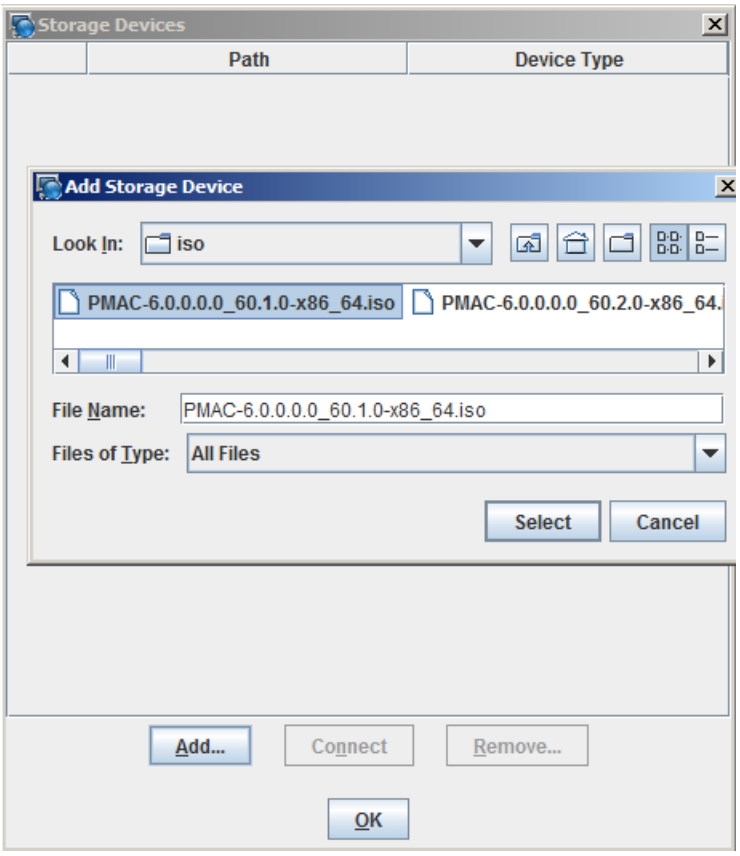
5. ILOM Remote System Console:

   From the **Remote Console** title bar, select **KVMS** and then **Storage**.



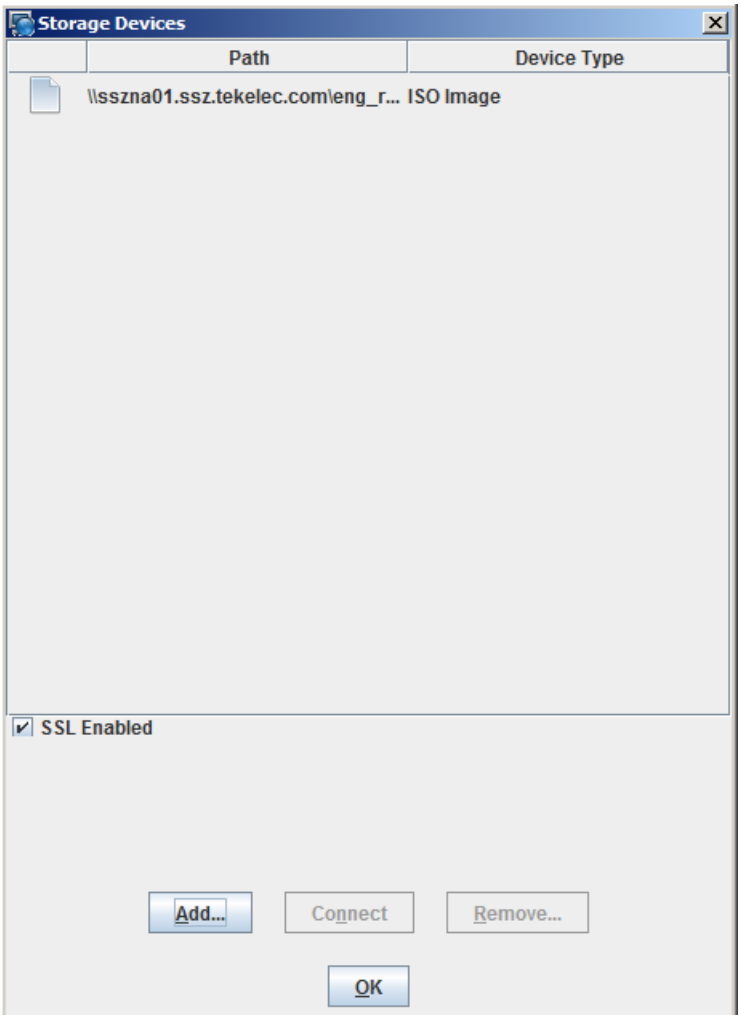
6. ILOM Remote System Console:

   From the **Storage Devices** pop-up window, click **Add**, then navigate to the local directory and select an image. Then press **Select**.



7. ILOM Remote System Console:

   From the **Storage Devices** window, press **OK**. The **Storage Devices** window will close.



8. ILOM Remote System Console:
   Click on the image you just added, then click on **Connect**.

9. ILOM Remote System Console:
   Leave the **Remote Console** active and return to the referencing procedure.

Appendix H

How to Exit a Guest Console Session on an iLO

Topics:

- *How to Exit a Guest Console Session on an iLO.....428*

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 *F.1 How to Access a Server Console Remotely*.

2. Return to the procedure which referenced this appendix.

Appendix I

Upgrade Cisco 4948 PROM

Topics:

- *Upgrade Cisco 4948 PROM.....430*

I.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 *I.1 Step 8*, 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 J

Operational Dependencies on Platform Account Passwords

Topics:

- *PM&C Credentials for Communication with Other System Components.....434*
- *PM&C GUI Accounts Credentials.....435*
- *PM&C Linux User Accounts Credentials.....436*
- *NetConfig Manager Password.....436*

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 *3.7.6 Step 6* through *3.7.6 Step 8* (inclusive) in procedure *3.7.6 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 6.2*, E67647.

J.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 *3.7.16 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 *3.7.17 Edit Rack Mount Server in the PM&C System Inventory*.

J.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.

J.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
```

J.4 NetConfig Manager Password

The netConfig repository stores access credentials for network devices and platform services. To secure these credentials, they are stored as encrypted strings.

Platform 7.0 implemented new cryptographic support. The pass phrase used to encrypt this data can be changed by the user through the netConfig API:

```
$ sudo netConfig --repo setPassword
```

The preceding command prompts for a new pass phrase. It re-encrypts the credentials and stores the pass phrase to a file for use by netConfig.

Appendix K

Disabling SNMP on the OA

Topics:

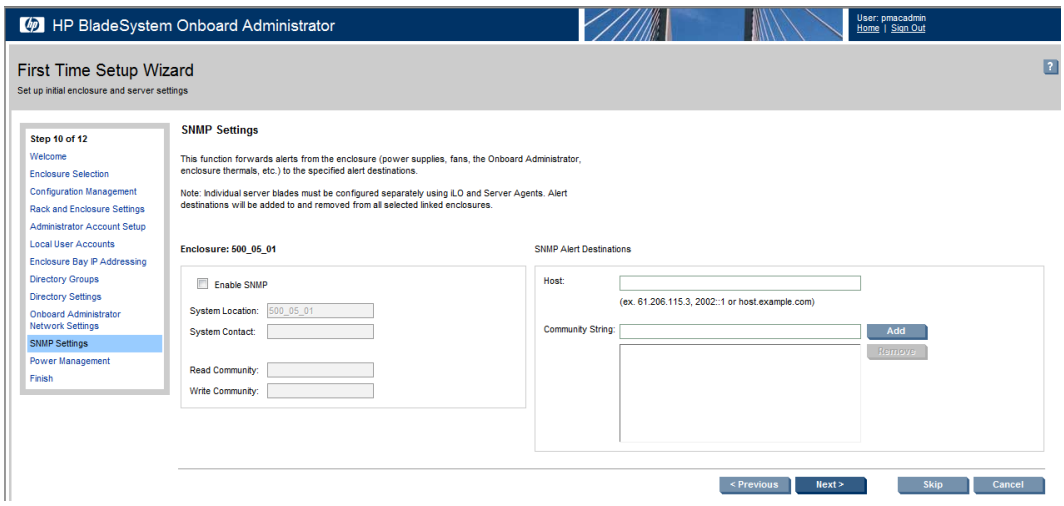
- *Disabling SNMP on the OA.....438*

K.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.



Appendix L

How to Downgrade Firmware on a 6125G Switch

Topics:

- *Downgrade 6125G Switch Firmware.....440*

This appendix describes the procedure to downgrade firmware on the HP 6125G enclosure switch.

L.1 Downgrade 6125G Switch Firmware

Use this procedure to downgrade the 6125G enclosure switches when they are found to contain firmware newer than the qualified baseline. See [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) for the target firmware version.

Prerequisite: This procedure assumes the netConfig repository data fill is complete which includes copying the target firmware to the netConfig Server (PM&C).

Note: Do not use this procedure for 6125XLG switches. See *M.1 Downgrade 6125XLG Switch Firmware* for the correct procedure for that switch.

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. Verify the existing firmware version by executing steps 2-4.
2. Active OA: SSH into the active OA as the administrative user:

```
login as: <oa_user> [Enter]
<oa_user>@<oa_ip>'s password: <oa_password> [Enter]
```

3. Active OA: Gain serial console access to the switch by executing the following command:

   Note: Multiple **Enter** keystrokes are required to gain the switch console prompt.

```
> connect interconnect <io_bay> [Enter] [Enter] [Enter]
Username: <switch_user> [Enter]
Password: <switch_password> [Enter] [Enter]
```

4. Switch: Execute the **display version** command to determine if a downgrade of the firmware needs to be performed.

```
> display version
HP Comware Platform Software
Comware Software, Version 5.20.99, Release 2105
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
HP 6125G Blade Switch uptime is 0 week, 2 days, 23 hours, 49 minutes


Slot 1 (M):
Uptime is 0 weeks,2 days,23 hours,49 minutes
HP 6125G Blade Switch with 1 Processor
1024M   bytes SDRAM
256M    bytes Nand Flash Memory
Hardware Version is Ver.B
CPLD Version is 003
BootWare Version is 1.07
[SubSlot 0] Back Panel
[SubSlot 1] Front Panel
```

5. If the firmware is found to be newer than the target firmware proceed with the rest of this procedure; otherwise, skip to step 21 and gracefully exit the switch and PM&C.

6. Virtual PM&C: SSH into the PM&C and authenticate as admusr:

```
login as: admusr [Enter]
Password: <admusr_password> [Enter]
Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61
[admusr@<pmac> ~]$
```

7. Virtual PM&C: Copy the firmware file to the switch:

```
$ sudo /usr/bin/scp 6125-cmw520-r2105.bin
<switch_user>@<switch_ip>:/6125-cmw520-r2105.bin [Enter]
<switch_user>@<switch_ip>'s password: <switch_platform_password> [Enter]
100% 16MB 766.3KB/s 00:21
```

8. Virtual PM&C: Gracefully exit from the PM&C SSH session:

```
$ logout [Enter]
```

9. Active OA: If not already connected, SSH into the active OA as the administrative user:

```
login as: <oa_user> [Enter]
<oa_user>@<oa_ip>'s password: <oa_password> [Enter]
```

10. Active OA: If not already connected, gain serial console access to the switch by executing the following command:

    Note: Multiple **Enter** keystrokes are required to gain the switch console prompt.

```
> connect interconnect <io_bay> [Enter] [Enter] [Enter]
Username: <switch_user> [Enter]
Password: <switch_password> [Enter] [Enter]
```

11. Switch: Reboot the switch and enter into the extended boot menu by pressing **Ctrl+B** when prompted:

    Note: During this process you may be prompted for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.

```
> reboot [Enter]
Start to check configuration with next startup configuration file, please
wait.........DONE!N
This command will reboot the device. Current configuration will be lost,
save current configuration? [Y/N]: N [Enter]
This command will reboot the device. Continue? [Y/N]: Y [Enter]
#May 15 15:03:44:478 2015 HP6125G_IOBAY5 DEVM/1/REBOOT:
 Reboot device by command.

%May 15 15:03:44:570 2015 HP6125G_IOBAY5 DEVM/5/SYSTEM_REBOOT: System is rebooting
 now.
System is starting...
Press Ctrl+D to access BASIC BOOT MENU
Press Ctrl+T to start memory test
Booting Normal Extend BootWare
The Extend BootWare is
self-decompressing.....................................Done!

[ OUTPUT REMOVED ]
```

```
BootWare Validating...
Backup Extend BootWare is newer than Normal Extend BootWare,Update? [Y/N]
Press Ctrl+B to enter extended boot menu...
BootWare password: Not required. Please press Enter to continue.

[ OUTPUT REMOVED ]
```

12. Switch: Enter file control by selecting **<4>** from the extend-bootware menu:

```
==========================<EXTEND-BOOTWARE MENU>==========================
|<1> Boot System                                                        |
|<2> Enter Serial SubMenu                                               |
|<3> Enter Ethernet SubMenu                                             |
|<4> File Control                                                       |
|<5> Restore to Factory Default Configuration                           |
|<6> Skip Current System Configuration                                  |
|<7> BootWare Operation Menu                                            |
|<8> Clear Super Password                                               |
|<9> Storage Device Operation                                           |
|<0> Reboot                                                             |
================================================================================
Ctrl+Z: Access EXTEND-ASSISTANT MENU
Ctrl+C: Display Copyright
Ctrl+F: Format File System
Enter your choice(0-9): 4 [Enter]
```

13. Switch: Display all files by selecting **<1>** from the file control menu and identify the target firmware from the list:

```
==============================<File CONTROL>==============================
|Note:the operating device is flash                                     |
|<1> Display All File(s)                                                |
|<2> Set Application File type                                          |
|<3> Delete File                                                        |
|<0> Exit To Main Menu                                                  |
================================================================================
Enter your choice(0-3): 1 [Enter]

Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
================================================================================
|NO. Size(B)   Time                 Type   Name                           |
|1   1584      Aug/27/2015 18:41:08 N/A    private-data.txt               |
|2   151       Aug/27/2015 18:41:08 N/A    system.xml                     |
|3   3626      Aug/27/2015 18:41:09 M      config.cfg                     |
|4   16493888  Aug/20/2015 11:14:44 M+B    6125-cmw520-r2106.bin          |
|5   4         Apr/26/2000 07:00:52 N/A    snmpboots                      |
|6   16913408  Aug/20/2015 10:56:42 N/A    6125-cmw520-r2112.bin          |
|7   735       Apr/26/2000 12:04:14 N/A    hostkey_v3                     |
|8   591       Apr/26/2000 12:04:15 N/A    serverkey_v3                   |
|9   16166     Sep/05/2013 10:17:21 N/A    test                           |
|10  16053376  Jun/05/2012 10:14:37 N/A    ~/6125-cmw520-r2103.bin        |
|11  16479296  Apr/26/2000 10:31:54 N/A    ~/6125-cmw520-r2105.bin        |
|12  16493888  Apr/26/2000 10:59:10 N/A    ~/6125-cmw520-r2106.bin        |
|13  16479296  Nov/05/2013 23:24:06 N/A    ~/2105.bin                     |
|14  5361      Jun/25/2013 14:22:05 N/A    ~/config.cfg                   |
|15  16493888  Nov/05/2013 23:20:13 N/A    ~/2106.bin                     |
|16  1048519   Aug/27/2015 23:30:55 N/A    logfile/logfile.log            |
|17  735       Apr/26/2000 12:05:10 N/A    hostkey                        |
|18  591       Apr/26/2000 12:05:11 N/A    serverkey                      |
```

```
================================================================================
[ OUTPUT REMOVED ]
```

14. Switch: Set application file type by entering **<2>** from the file control menu:

```
==============================<File CONTROL>==================================
|Note:the operating device is flash                                           |
|<1> Display All File(s)                                                      |
|<2> Set Application File type                                                |
|<3> Delete File                                                              |
|<0> Exit To Main Menu                                                        |
================================================================================
Enter your choice(0-3): 2 [Enter]
```

15. Switch: Choose the firmware file identified in step 13 and enter the corresponding line number:

```
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
================================================================================
|NO. Size(B)   Time                 Type   Name                               |
|1   16493888  Aug/20/2015 11:14:44 M+B    6125-cmw520-r2106.bin              |
|2   16913408  Aug/20/2015 10:56:42 N/A    6125-cmw520-r2112.bin              |
|3   16053376  Jun/05/2012 10:14:37 N/A    ~/6125-cmw520-r2103.bin            |
|4   16479296  Apr/26/2000 10:31:54 N/A    ~/6125-cmw520-r2105.bin            |
|5   16493888  Apr/26/2000 10:59:10 N/A    ~/6125-cmw520-r2106.bin            |
|6   16479296  Nov/05/2013 23:24:06 N/A    ~/2105.bin                         |
|7   16493888  Nov/05/2013 23:20:13 N/A    ~/2106.bin                         |
|0   Exit                                                                     |
================================================================================
Enter file No: <4> [Enter]
```

16. Switch: Modify the file attribute to **+Main** by selecting **<1>** from the file attributes menu:

```
Modify the file attribute:
================================================================================
|<1> +Main                                                                    |
|<2> -Main                                                                    |
|<3> +Backup                                                                  |
|<4> -Backup                                                                  |
|<0> Exit                                                                     |
================================================================================
Enter your choice(0-4): 1 [Enter]
This operation may take several minutes. Please wait....
Set the file attribute success!
```

17. Switch: Verify the file attribute modification by listing the files and inspecting the **type** attribute for the target firmware. The type attribute on this line should display **M**:

```
==============================<File CONTROL>==================================
|Note:the operating device is flash                                           |
|<1> Display All File(s)                                                      |
|<2> Set Application File type                                                |
|<3> Delete File                                                              |
|<0> Exit To Main Menu                                                        |
================================================================================
Enter your choice(0-3): 1 [Enter]

Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
================================================================================
```

```
|NO. Size(B)   Time                 Type   Name                              |
|1   1584      Aug/27/2015 18:41:08 N/A    private-data.txt                  |
|2   151       Aug/27/2015 18:41:08 N/A    system.xml                        |
|3   3626      Aug/27/2015 18:41:09 M      config.cfg                        |
|4   16493888  Aug/20/2015 11:14:44 B      6125-cmw520-r2106.bin             |
|5   4         Apr/26/2000 07:00:52 N/A    snmpboots                         |
|6   16913408  Aug/20/2015 10:56:42 N/A    6125-cmw520-r2112.bin             |
|7   735       Apr/26/2000 12:04:14 N/A    hostkey_v3                        |
|8   591       Apr/26/2000 12:04:15 N/A    serverkey_v3                      |
|9   16166     Sep/05/2013 10:17:21 N/A    test                              |
|10  16053376  Jun/05/2012 10:14:37 N/A    ~/6125-cmw520-r2103.bin           |
|11  16479296  Apr/26/2000 10:31:54 M      ~/6125-cmw520-r2105.bin           |
|12  16493888  Apr/26/2000 10:59:10 N/A    ~/6125-cmw520-r2106.bin           |
|13  16479296  Nov/05/2013 23:24:06 N/A    ~/2105.bin                        |
|14  5361      Jun/25/2013 14:22:05 N/A    ~/config.cfg                      |
|15  16493888  Nov/05/2013 23:20:13 N/A    ~/2106.bin                        |
|16  1048519   Aug/27/2015 23:30:55 N/A    logfile/logfile.log               |
|17  735       Apr/26/2000 12:05:10 N/A    hostkey                           |
|18  591       Apr/26/2000 12:05:11 N/A    serverkey                         |
================================================================================
```

18. Switch: Exit to main menu by selecting **<0>** from the file control menu:

```
================================<File CONTROL>================================
|Note:the operating device is flash                                           |
|<1> Display All File(s)                                                      |
|<2> Set Application File type                                                |
|<3> Delete File                                                              |
|<0> Exit To Main Menu                                                        |
================================================================================
Enter your choice(0-3): 0 [Enter]
```

19. Switch: Boot the system by selecting **<1>** from the extend-bootware menu:

Note: Do NOT select reboot by choosing **<0>**!

Note: During this process you may be prompted for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.

```
============================<EXTEND-BOOTWARE MENU>============================
|<1> Boot System                                                              |
|<2> Enter Serial SubMenu                                                     |
|<3> Enter Ethernet SubMenu                                                   |
|<4> File Control                                                             |
|<5> Restore to Factory Default Configuration                                 |
|<6> Skip Current System Configuration                                        |
|<7> BootWare Operation Menu                                                  |
|<8> Clear Super Password                                                     |
|<9> Storage Device Operation                                                 |
|<0> Reboot                                                                   |
================================================================================
Ctrl+Z: Access EXTEND-ASSISTANT MENU
Ctrl+C: Display Copyright
Ctrl+F: Format File System
Enter your choice(0-9): 1 [Enter]
Starting to get the main application file--flash:/~/6125-cmw520-r2105.bin!..
................................................................................
.........................................
The main application file is self-decompressing.....................

[ OUTPUT REMOVED ]
```

```
.....................Done!
System application is starting...
User interface aux0 is available.

Press ENTER to get started.

Login authentication

Username:
```

20. Switch: Log back into the switch and verify the firmware version by executing the **display version** command:

    Note: You may have to press **Enter** multiple times after authenticating to land on the switch prompt.

```
Username: username [Enter]
Password: password [Enter] [Enter]
#Aug 28 09:29:09:694 2015 HP6125g_sanity SHELL/4/LOGIN:
 Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:plat login from Console
%Aug 28 09:29:09:819 2015 HP6125g_sanity SHELL/5/SHELL_LOGIN: plat logged in
from aux0.

> display version [Enter]

HP Comware Platform Software
Comware Software, Version 5.20.99, Release 2105
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
HP 6125G Blade Switch uptime is 0 week, 0 day, 0 hour, 9 minutes

[ OUTPUT REMOVED ]
```

21. **Switch:** Gracefully disconnect from the switch serial console session by executing the escape character '<Ctrl>_' (Control + Shift + Underscore).

```
> '<Ctrl>_' (Control + Shift + Underscore)
------------------------------------------------------------------------------
Command: D)isconnect, C)hange settings, send B)reak, E)xit command mode X)modem
 send > D
------------------------------------------------------------------------------
D [Enter]
```

22. Active OA: Logout of the OA.

```
> logout [Enter]
```

You have completed this procedure.

Appendix M

How to Downgrade Firmware on a 6125XLG Switch

Topics:

- *Downgrade 6125XLG Switch Firmware.....447*

This appendix describes the procedure to downgrade firmware on the HP 6125XLG enclosure switch.

M.1 Downgrade 6125XLG Switch Firmware

Use this procedure to downgrade the 6125XLG enclosure switches when they are found to contain firmware newer than the qualified baseline. See [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) for the target firmware version.

Prerequisite: This procedure assumes the netConfig repository data fill is complete which includes copying the target firmware to the netConfig Server (PM&C).

Note: Do not use this procedure for 6125G switches. See *L.1 Downgrade 6125G Switch Firmware* for the correct procedure for that switch.

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. First verify the existing firmware version by executing steps 2-4.
2. Active OA: SSH into the active OA as the administrative user:

```
login as: <oa_user> [Enter]
<oa_user>@<oa_ip>'s password: <oa_password> [Enter]
```

3. Active OA: Gain serial console access to the switch by executing the following command:

   Note: Multiple **Enter** keystrokes are required to gain the switch console prompt.

```
> connect interconnect <io_bay> [Enter] [Enter] [Enter]
Username: <switch_user> [Enter]
Password: <switch_password> [Enter]
```

4. Switch: Execute the **display version** command to determine if a downgrade of the firmware needs to be performed.

   Note: You will need to verify both the boot image version and the system image version.

```
> display version
HP Comware Software, Version 7.1.045, Release 2403
Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.
HP 6125XLG Blade Switch uptime is 0 weeks, 0 days, 0 hours, 1 minute
Last reboot reason : Power on

Boot image: flash:/6125xlg-cmw710-boot-r2403.bin
Boot image version: 7.1.045P08, Release 2403
  Compiled Mar 06 2014 13:13:45
System image: flash:/6125xlg-cmw710-system-r2403.bin
System image version: 7.1.045, Release 2403
  Compiled Mar 06 2014 13:13:57
```

5. If the firmware is found to be newer than the target firmware proceed with the rest of this procedure; otherwise, skip to step 21 and gracefully exit the switch and PM&C.
6. Virtual PM&C: SSH into the PM&C and authenticate as admusr:

```
login as: admusr [Enter]
Password: <admusr_password> [Enter]
```

```
Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61
[admusr@<pmac> ~]$
```

7. Virtual PM&C: Copy the firmware file to the switch:

```
$ sudo /usr/bin/scp 6125XLG-CMW710-R2403.ipe
<switch_user>@<switch_ip>:/6125XLG-CMW710-R2403.ipe [Enter]
<switch_user>@<switch_ip>'s password: <switch_platform_password> [Enter]
100% 16MB 766.3KB/s 00:21
```

8. Virtual PM&C: Gracefully exit from the PM&C SSH session:

```
$ logout [Enter]
```

9. Active OA: If not already connected, SSH into the active OA as the administrative user:

```
login as: <oa_user> [Enter]
<oa_user>@<oa_ip>'s password: <oa_password> [Enter]
```

10. Active OA: If not already connected, gain serial console access to the switch by executing the following command:

    Note: Multiple **Enter** keystrokes are required to gain the switch console prompt.

```
> connect interconnect <io_bay> [Enter] [Enter] [Enter]
Username: <switch_user> [Enter]
Password: <switch_password> [Enter]
```

11. Switch: Reboot the switch and enter into the extended boot menu by pressing **Ctrl+B** when prompted:

    Note: During this process you may be prompted for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.

```
> reboot [Enter]
Start to check configuration with next startup configuration file, please
wait.........DONE!N
This command will reboot the device. Current configuration will be lost,
save current configuration? [Y/N]: N [Enter]
This command will reboot the device. Continue? [Y/N]: Y [Enter]
Now rebooting, please wait...

System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start heavy memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing.....................Done.

[ OUTPUT REMOVED ]

BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
[ OUTPUT REMOVED ]
```

12. Switch: Enter file control by selecting **<4>** from the extend-bootware menu:

```
==========================<EXTEND-BOOTWARE MENU>==========================
|<1> Boot System                                                         |
|<2> Enter Serial SubMenu                                                |
|<3> Enter Ethernet SubMenu                                              |
|<4> File Control                                                        |
|<5> Restore to Factory Default Configuration                            |
|<6> Skip Current System Configuration                                   |
|<7> BootWare Operation Menu                                             |
|<8> Clear Super Password                                                |
|<9> Storage Device Operation                                            |
|<0> Reboot                                                              |
==========================================================================
Ctrl+Z: Access EXTEND-ASSISTANT MENU
Ctrl+C: Display Copyright
Ctrl+F: Format File System
Enter your choice(0-9): 4 [Enter]
```

13. Switch: Display all files by selecting **<1>** from the file control menu and identify the target firmware from the list:

Note: Two files should be identified. One is a system file and the other is a boot file.

```
================================<File CONTROL>================================
|Note:the operating device is flash                                        |
|<1> Display All File(s)                                                   |
|<2> Set Application File type                                             |
|<3> Delete File                                                           |
|<0> Exit To Main Menu                                                     |
==========================================================================
Enter your choice(0-3): 1 [Enter]

Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
==========================================================================
|NO. Size(B)   Time                 Type   Name                          |
|1   110167    Aug/28/2015 18:05:46 N/A    flash:/startup.mdb            |
|2   7388      Aug/28/2015 18:05:46 M      flash:/startup.cfg            |
|3   1039      Aug/28/2015 18:05:46 N/A    flash:/ifindex.dat            |
|4   252       Jan/27/2011 02:29:27 N/A    flash:/.trash/.trashinfo      |
|5   62561280  Aug/19/2015 16:55:55 N/A    flash:/6125XLG-CMW710-R2406P03.i|
|pe                                                                        |
|6   0         Jan/03/2011 20:20:38 N/A    flash:/lauth.dat              |
|7   62660608  Aug/19/2015 17:10:28 N/A    flash:/6125XLG-CMW710-R2403.ipe |
|8   591       Jun/02/2011 17:26:58 N/A    flash:/serverkey              |
|9   735       Jun/02/2011 17:26:58 N/A    flash:/hostkey                |
|10  536       Jan/27/2011 02:39:29 N/A    flash:/versionInfo/version1.dat |
|11  536       Jan/27/2011 02:36:40 N/A    flash:/versionInfo/version0.dat |
|12  8         Jan/01/2011 00:00:21 N/A    flash:/versionInfo/versionCtl.da|
|t                                                                         |
|13  536       Aug/19/2015 17:13:37 N/A    flash:/versionInfo/version7.dat |
|14  536       Mar/29/2011 18:38:24 N/A    flash:/versionInfo/version5.dat |
|15  536       Mar/29/2011 18:35:41 N/A    flash:/versionInfo/version4.dat |
|16  536       Aug/19/2015 16:59:08 N/A    flash:/versionInfo/version6.dat |
|17  536       Mar/29/2011 18:24:06 N/A    flash:/versionInfo/version2.dat |
|18  536       Mar/29/2011 18:31:37 N/A    flash:/versionInfo/version3.dat |
|19  536       Jan/27/2011 02:32:46 N/A    flash:/versionInfo/version9.dat |
|20  536       Jan/27/2011 02:25:15 N/A    flash:/versionInfo/version8.dat |
|21  20        Aug/28/2015 18:48:29 N/A    flash:/.snmpboots             |
|22  53308416  Aug/19/2015 17:11:52 M      flash:/6125xlg-cmw710-system-r24|
|03.bin                                                                    |
```

```
|23  10433677  Jan/01/2011 00:06:50 N/A    flash:/logfile/logfile.log      |
|24  18        Jan/01/2011 00:00:14 N/A    flash:/.pathfile                |
|25  796       Jan/01/2011 00:07:25 N/A    flash:/license/DeviceID.did     |
|26  796       Jan/01/2011 00:07:25 N/A    flash:/license/history/DeviceID_|
|20110101000725.did                                                        |
|27  796       Jan/01/2011 00:00:14 N/A    flash:/license/history/DeviceID_|
|20110101000014.did                                                        |
|28  805       Jan/01/2011 00:00:18 N/A    flash:/license/history/DeviceID_|
|20110101000018.did                                                        |
|29  54222848  Aug/19/2015 16:57:16 N/A    flash:/6125xlg-cmw710-system-r24|
|06p03.bin                                                                 |
|30  8331264   Aug/19/2015 16:57:06 N/A    flash:/6125xlg-cmw710-boot-r2406|
|p03.bin                                                                   |
|31  9345024   Aug/19/2015 17:11:38 M      flash:/6125xlg-cmw710-boot-r2403|
|.bin                                                                      |
============================================================================

[ OUTPUT REMOVED ]
```

14. Switch: Set bin file type by entering **<2>** from the file control menu:

```
==============================<File CONTROL>==============================
|Note:the operating device is flash                                      |
|<1> Display All File(s)                                                 |
|<2> Set Bin File type                                          |        
|<3> Delete File                                                         |
|<0> Exit To Main Menu                                                   |
============================================================================
Enter your choice(0-3): 2 [Enter]
```

15. Switch: Choose the firmware files identified in step 13 and enter the corresponding line numbers:

```
 'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                           |
|1   53308416  Aug/19/2015 17:11:52 M      flash:/6125xlg-cmw710-system-r24|
|03.bin                                                                  |
|2   54222848  Aug/19/2015 16:57:16 N/A    flash:/6125xlg-cmw710-system-r24|
|06p03.bin                                                               |
|3   8331264   Aug/19/2015 16:57:06 N/A    flash:/6125xlg-cmw710-boot-r2406|
|p03.bin                                                                 |
|4   9345024   Aug/19/2015 17:11:38 M      flash:/6125xlg-cmw710-boot-r2403|
|.bin                                                                    |
|0   Exit                                                                |
============================================================================
Note:Select .bin files. One but only one boot image and system image must
be included.
Enter file No.(Allows multiple selection): 1 [Enter]
Enter another file No.(0-Finish choice): 4 [Enter]
Enter another file No.(0-Finish choice):0 [Enter]
You have selected:
flash:/6125xlg-cmw710-system-r2403.bin
flash:/6125xlg-cmw710-boot-r2403.bin
```

16. Switch: Modify the file attribute to **+Main** by selecting **<1>** from the file attributes menu:

```
Modify the file attribute:
============================================================================
|<1>+Main                                                                |
|<2>+Backup                                                              |
|<0> Exit                                                                |
```

```
==============================================================================
Enter your choice(0-2): 1 [Enter]
This operation may take several minutes. Please wait....
Set the file attribute success!
```

17. Switch: Verify the file attribute modification by selecting **<1>** to list the files and inspecting the **type** attribute for the target firmware files. The type attribute on the applicable lines should display **M**:

```
================================<File CONTROL>================================
|Note:the operating device is flash                                           |
|<1> Display All File(s)                                                      |
|<2> Set Bin File type                                                        |
|<3> Delete File                                                              |
|<0> Exit To Main Menu                                                        |
==============================================================================
Enter your choice(0-3): 1 [Enter]

Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
==============================================================================
|NO. Size(B)   Time                 Type   Name                             |
|1   110167    Aug/28/2015 18:05:46 N/A    flash:/startup.mdb               |
|2   7388      Aug/28/2015 18:05:46 M      flash:/startup.cfg               |
|3   1039      Aug/28/2015 18:05:46 N/A    flash:/ifindex.dat               |
|4   252       Jan/27/2011 02:29:27 N/A    flash:/.trash/.trashinfo         |
|5   62561280  Aug/19/2015 16:55:55 N/A    flash:/6125XLG-CMW710-R2406P03.i|
|pe                                                                           |
|6   0         Jan/03/2011 20:20:38 N/A    flash:/lauth.dat                 |
|7   62660608  Aug/19/2015 17:10:28 N/A    flash:/6125XLG-CMW710-R2403.ipe  |
|8   591       Jun/02/2011 17:26:58 N/A    flash:/serverkey                 |
|9   735       Jun/02/2011 17:26:58 N/A    flash:/hostkey                   |
|10  536       Jan/27/2011 02:39:29 N/A    flash:/versionInfo/version1.dat  |
|11  536       Jan/27/2011 02:36:40 N/A    flash:/versionInfo/version0.dat  |
|12  8         Jan/01/2011 00:00:21 N/A    flash:/versionInfo/versionCtl.da|
|t                                                                            |
|13  536       Aug/19/2015 17:13:37 N/A    flash:/versionInfo/version7.dat  |
|14  536       Mar/29/2011 18:38:24 N/A    flash:/versionInfo/version5.dat  |
|15  536       Mar/29/2011 18:35:41 N/A    flash:/versionInfo/version4.dat  |
|16  536       Aug/19/2015 16:59:08 N/A    flash:/versionInfo/version6.dat  |
|17  536       Mar/29/2011 18:24:06 N/A    flash:/versionInfo/version2.dat  |
|18  536       Mar/29/2011 18:31:37 N/A    flash:/versionInfo/version3.dat  |
|19  536       Jan/27/2011 02:32:46 N/A    flash:/versionInfo/version9.dat  |
|20  536       Jan/27/2011 02:25:15 N/A    flash:/versionInfo/version8.dat  |
|21  20        Aug/28/2015 18:48:29 N/A    flash:/.snmpboots                |
|22  53308416  Aug/19/2015 17:11:52 M      flash:/6125xlg-cmw710-system-r24|
|03.bin                                                                       |
|23  10433677  Jan/01/2011 00:06:50 N/A    flash:/logfile/logfile.log       |
|24  18        Jan/01/2011 00:00:14 N/A    flash:/.pathfile                 |
|25  796       Jan/01/2011 00:07:25 N/A    flash:/license/DeviceID.did      |
|26  796       Jan/01/2011 00:07:25 N/A    flash:/license/history/DeviceID_|
|20110101000725.did                                                           |
|27  796       Jan/01/2011 00:00:14 N/A    flash:/license/history/DeviceID_|
|20110101000014.did                                                           |
|28  805       Jan/01/2011 00:00:18 N/A    flash:/license/history/DeviceID_|
|20110101000018.did                                                           |
|29  54222848  Aug/19/2015 16:57:16 N/A    flash:/6125xlg-cmw710-system-r24|
|06p03.bin                                                                    |
|30  8331264   Aug/19/2015 16:57:06 N/A    flash:/6125xlg-cmw710-boot-r2406|
|p03.bin                                                                      |
|31  9345024   Aug/19/2015 17:11:38 M      flash:/6125xlg-cmw710-boot-r2403|
```

```
|.bin                                                                          |
================================================================================
```

18. Switch: Exit to main menu by selecting **<0>** from the file control menu:

```
==============================<File CONTROL>==================================
|Note:the operating device is flash                                          |
|<1> Display All File(s)                                                     |
|<2> Set Application File type                                               |
|<3> Delete File                                                             |
|<0> Exit To Main Menu                                                       |
================================================================================
Enter your choice(0-3): 0 [Enter]
```

19. Switch: Boot the system by selecting **<1>** from the extended-bootware menu:

Note: Do NOT select reboot by choosing **<0>**!

Note: During this process you may be prompted for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.

```
==========================<EXTENDED-BOOTWARE MENU>==========================
|<1> Boot System                                                             |
|<2> Enter Serial SubMenu                                                    |
|<3> Enter Ethernet SubMenu                                                  |
|<4> File Control                                                            |
|<5> Restore to Factory Default Configuration                                |
|<6> Skip Current System Configuration                                       |
|<7> BootWare Operation Menu                                                 |
|<8> Skip Authentication for Console Login                                   |
|<9> Storage Device Operation                                                |
|<0> Reboot                                                                  |
================================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 1
Loading the main image files...
Loading file flash:/6125xlg-cmw710-system-r2403.bin.......................
.............................Done.
Loading file flash:/6125xlg-cmw710-boot-r2403.bin............Done.

Image file flash:/6125xlg-cmw710-boot-r2403.bin is self-decompressing.......

[ OUTPUT REMOVED ]

.......................Done!
System application is starting...
User interface aux0 is available.

Press ENTER to get started.

Login authentication

Username:
```

20. Switch: Log back into the switch and verify the firmware version by executing the **display version** command:

Note: You may have to press **Enter** multiple times after authenticating to land on the switch prompt.

```
login: <switch_user> [Enter]
Password: <switch_password> [Enter]
> display version
HP Comware Software, Version 7.1.045, Release 2403
Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.
HP 6125XLG Blade Switch uptime is 0 weeks, 0 days, 0 hours, 1 minute
Last reboot reason : Power on

Boot image: flash:/6125xlg-cmw710-boot-r2403.bin
Boot image version: 7.1.045P08, Release 2403
  Compiled Mar 06 2014 13:13:45
System image: flash:/6125xlg-cmw710-system-r2403.bin
System image version: 7.1.045, Release 2403
  Compiled Mar 06 2014 13:13:57

[ OUTPUT REMOVED ]
```

21. **Switch:** Gracefully disconnect from the switch serial console session by executing the escape character '<Ctrl>_' (Control + Shift + Underscore).

```
> '<Ctrl>_' (Control + Shift + Underscore)
------------------------------------------------------------------------------
Command: D)isconnect, C)hange settings, send B)reak, E)xit command mode X)modem
 send > D
------------------------------------------------------------------------------
D [Enter]
```

22. Active OA: Logout of the OA.

```
> logout [Enter]
```

You have completed this procedure.

Appendix N

How to Change Switch Passwords (netConfig)

Topics:

- *How to Change Switch Passwords (netConfig).....455*

This appendix describes the procedure to change switch passwords using netConfig. This will update the passwords in both the repository and on the devices.

N.1 How to Change Switch Passwords (netConfig)

Use this procedure to change the switch password on both the device and in the netConfig repository simultaneously.

Prerequisite: This procedure assumes the netConfig repository data fill is complete and the devices have been previously added. If netConfig was not used to configure the switch originally, do not use this procedure.

Caution: Executing these commands as stated will not cause a service interruption. The switches are not rebooted or initialized. However, as with all in-service operations, caution should be taken. This operation should be scheduled with the customer.

At any time, you can view the contents of the netConfig repository by executing the following command on the netConfig Server:

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

Users can run the above command to confirm that the target devices have already been configured. Duplicate entries cannot be added; if changes to a device repository entry are required, use the **editDevice** command.

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. '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. In this procedure, 'netConfig server' and 'Virtual PM&C' are synonymous while management server indicates the TVOE host or bare metal server.

Steps within 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.

Variable	Value
<netConfig_server_mgmt_ip_address>	
<switch_hostname>	Gathered from NAPD or output from `listDevices` command

For each switch fill in the target password in cleartext:

Variable	Value
<cleartext password>	

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. netConfig Server: SSH into the netConfig server:

   SSH into the netConfig server and authenticate as admusr:

```
login as: admusr [Enter]
Password: <admusr_password> [Enter]
```

```
Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61
[admusr@<pmac> ~]$
```

2. netConfig Server: Confirm device.

   Confirm the device is listed in the repository by executing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices [Enter]
```

   Take note of the target device name. This will be referred to as the variable <switch_hostname> in subsequent steps.

3. netConfig Server: Change password.

   Execute the following command for device types of **4948**, **4948E**, **4948E-F**, or **3020**:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> setPassword
type=<console|login|privileged> password=<cleartext_password>; history -d
$(history 1) [Enter]
```

   Perform this step for each password type, i.e. console, login, or privileged.

   Note: The appended part of the command, **`; history -d $(history 1)`**, deletes the history so that the password is not observable in cleartext. If this is not desirable you may omit this part of the command and resolve the risk manually.

4. netConfig Server: Change password.

   Execute the following command for device types of **6120**, **6125G**, or **6125XLG**:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> setPassword
password=<cleartext_password>; history -d $(history 1) [Enter]
```

   Note: The appended part of the command, **`; history -d $(history 1)`**, deletes the history so that the password is not observable in cleartext. If this is not desirable you may omit this part of the command and resolve the risk manually.

5. netConfig Server: Gracefully exit from the netConfig server SSH session:

```
$ logout [Enter]
```

You have completed this procedure.

Appendix O

How to Uninstall Symantec NetBackup Client

Topics:

- *Uninstall Symantec NetBackup Client.....458*

This appendix describes the procedure to uninstall a successfully installed Symantec NetBackup client.

O.1 Uninstall Symantec NetBackup Client

Use this procedure to uninstall the Symantec NetBackup client from a server with an OS based on TPD or TVOE.

Note: If you are attempting to uninstall a failed Symantec NetBackup client installation or upgrade, do not use this procedure. This procedure should only be used when the initial Symantec NetBackup client installation, or subsequent upgrade, was successful.

Prerequisites:

- The TPD NetBackup RPM has been installed on the server.
- The contents of the NetBackup client configuration file are known if one exists. Depending on the version of NetBackup, a configuration file may not exist.
- The firewall rules implementation is known. Depending on the application, the implementation of firewall rules vary. Do not proceed without understanding the appropriate steps to remove the rules for your application. Reference the documentation for your specific application. The steps presented in this procedure are for a TVOE server and likely don't apply to a TPD application server.
- The server health checks return no issues.

In this procedure, target server refers to the TPD or TVOE server where the NetBackup client is installed. In the case of TPD, this is the application server. In the case of TVOE, this is the base server hosting the application virtual machines.

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. Per your application documentation, perform the application backup procedure. Take care not to use NetBackup since the NetBackup client is being removed from the server.
2. If you are performing this procedure on a TVOE server, execute procedure *3.10.1 Backup Procedure for TVOE*.
3. Target Server: SSH into the server and authenticate as admusr:

```
login as: admusr [Enter]
Password: <admusr_password> [Enter]
Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61
[admusr@<target_server> ~]$
```

4. Target Server: Determine the NetBackup client version.

   Execute the following command to determine the NetBackup client version by inspecting the version file.

```
[admusr@<target_server> ~]$ sudo /bin/cat /usr/openv/netbackup/bin/version [Enter]
NetBackup-RedHat2.6.18 7.6.0.1
[admusr@<target_server> ~]$
```

   In this case, the version is 7.6.0.1.

5. Target Server: Determine the packages installed and services configured.

   Execute the following command to determine the NetBackup client packages installed, and services configured, on the server by inspecting the client profile configuration file. For some versions of

NetBackup, a configuration file is not used and does not exist. In those cases, reference the table at the bottom of this step.

Note: The client profile configuration file includes the client version in the name. For example, `NB7601.conf` where `7601` represents the client version number with the periods removed. In this example, version 7.6.0.1 is used.

```
[admusr@<target_server> ~]$ sudo /bin/cat
/usr/TKLC/plat/etc/netbackup/profiles/NB7601.conf [Enter]
VERSION=7.6.0.1
RPMS="SYMCpddea,SYMCnbjre,SYMCnbjava,SYMCnbclt,VRTSpbx"
RC_SERVICES="netbackup,vxpbx_exchanged"
[admusr@<target_server> ~]$
```

If your installation does not use a client profile file, refer to this table for your specific release.

NetBackup Client Version	Packages (RPMs)	Services
NB 7.0	VRTSpbx	RC: netbackup
NB 7.1	SYMCpddea SYMCnbjre SYMCnbjava SYMCnbclt VRTSpbx	RC: netbackup
NB 7.5	SYMCpddea SYMCnbclt SYMCnbjava SYMCnbjre VRTSpbx	RC: netbackup RC: vxpbx_exchanged

6. Target Server: Stop all NetBackup processes.

   Execute the following commands to stop the Symantec NetBackup client services identified in step *O.1 Step 5*. The following example will stop the services for NB version 7.6.0.1:

```
[admusr@<target_server> ~]$ sudo service netbackup stop [Enter]
stopping the NetBackup Deduplication Multi-Threaded Agent
stopping the NetBackup Discovery Framework
stopping the NetBackup client daemon
stopping the NetBackup network daemon

[admusr@<target_server> ~]$ sudo service vxpbx_exchanged stop [Enter]
Stopped Symantec Private Branch Exchange
[admusr@<target_server> ~]$
```

7. Target Server: Verify that the NetBackup processes are stopped.

   Execute the following command to verify all processes are stopped. No output expected:

```
[admusr@<target_server> ~]$ sudo /usr/openv/netbackup/bin/bpps [Enter]
[admusr@<target_server> ~]$
```

8. Target Server: Navigate to home directory.

   Execute this step to ensure that the directory to which the netbackup LV is mounted is not used. This is a precautionary step:

```
[admusr@<target_server> ~]$ cd ~ [Enter]
[admusr@<target_server> ~]$
```

9. Target Server: Delete the services.

   Execute the following command to delete the NetBackup services identified in the client profile from *O.1 Step 5*. In this example the Netbackup client services are: `netbackup` and `vxpbx_exchanged`.

```
[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf del netbackup
[Enter]
[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf del
vxpbx_exchanged [Enter]
[admusr@<target_server> ~]$
```

10. Target Server: Reconfigure the services.

    Execute the following command to reconfigure the server services after the deletion.

```
[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf reconfig [Enter]
[admusr@<target_server> ~]$
```

11. Target Server: Uninstall the packages.

    Execute the following command to uninstall the NetBackup client packages identified in the client profile from *O.1 Step 5*. In this example the NetBackup client packages are: `SYMCnbclt`, `SYMCnbjava`, `SYMCnbjre`, `SYMCpddea`, and `VRTSpbx`.

    Note: Warnings can be ignored.

```
[admusr@<target_server> ~]$ sudo rpm -ev SYMCnbclt SYMCnbjava SYMCnbjre SYMCpddea
 VRTSpbx [Enter]
warning:    erase unlink of /opt/VRTSpbx/lib/libvxicui18n.so.6 failed: No such
file or directory
warning:    erase unlink of /opt/VRTSpbx/bin/vxpbxcfg failed: No such file or
directory

Starting SYMCpddea postremove script.

Removing link /opt/pdag
Removing link /opt/pdshared
Removing /opt/pdde directory.
Removing link /usr/openv/lib/ost-plugins/libstspipd.so
Removing link /usr/openv/lib/ost-plugins/libstspipdMT.so
Removing PDDE installation directory.

SYMCpddea postremove script done!
[admusr@<target_server> ~]$
```

12. Target Server: Verify the removal of the client RPMs.

Execute the following command to verify the removal of the NetBackup client rpms. In this example the NetBackup client RPMs are: `SYMCnbclt`, `SYMCnbjava`, `SYMCnbjre`, `SYMCpddea`, and `VRTSpbx`. No output is expected.

```
[admusr@<target_server> ~]$ sudo rpm -qa | egrep
"SYMCnbclt|SYMCnbjava|SYMCnbjre|SYMCpddea|VRTSpbx" [Enter]
[admusr@<target_server> ~]$
```

13. Target Server: Cleanup the `/etc/rc.d/init.d` directory.

Execute the following command to list any NetBackup client service files that may not have been removed by the uninstall of the client rpms. In this example the client services are: `netbackup` and `vxpbx_exchanged`.

```
[admusr@<target_server> ~]$ sudo ls -l /etc/rc.d/init.d/netbackup
/etc/rc.d/init.d/vxpbx_exchanged [Enter]
ls: cannot access /etc/rc.d/init.d/vxpbx_exchanged: No such file or directory
-r-x------ 1 root root 22776 Sep  6 16:04 /etc/rc.d/init.d/netbackup
[admusr@<target_server> ~]$
```

From the output we see that we need to remove the `netbackup` service file. Execute the following command to delete this service file:

```
[admusr@<target_server> ~]$ sudo rm -f /etc/rc.d/init.d/netbackup [Enter]
[admusr@<target_server> ~]$
```

14. Target Server: Identify the NetBackup logical volume (LV) and volume group (VG).

Execute the following command to identify the LV and VG used by NetBackup. This will be used in subsequent commands.

```
[admusr@<target_server> ~]$ sudo lvs [Enter]
LV           VG     Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync
 Convert
  netbackup_lv  vgroot -wi-ao---- 5.00g
  plat_root     vgroot -wi-ao---- 1.00g
  plat_tmp      vgroot -wi-ao---- 1.00g
  plat_usr      vgroot -wi-ao---- 4.00g
  plat_var      vgroot -wi-ao---- 1.00g
  plat_var_tklc vgroot -wi-ao---- 4.00g

[admusr@<target_server> ~]$
```

From the output we see that the NetBackup LV is named `netbackup_lv` and the volume group is `vgroot`.

15. Target Server: Identify processes using this Logical Volume (LV).

Execute the following command to verify no processes are using the LV identified in the previous step. Use the VG and LV values identified in the previous step. No output is expected.

```
[admusr@<target_server> ~]$ sudo /sbin/fuser -m /dev/vgroot/netbackup_lv [Enter]
[admusr@<target_server> ~]$
```

16. Target Server: Unmount device `/usr/openv`.

Execute the following command to unmount device `/usr/openv` from the NetBackup LV.

```
[admusr@<target_server> ~]$ sudo /bin/umount -l /usr/openv [Enter]
[admusr@<target_server> ~]$
```

17. Target Server: Remove the NetBackup LV entry from `/etc/fstab`.

    Execute the following command to remove the NetBackup LV entry from `/etc/fstab`.

```
[admusr@<target_server> ~]$ sudo /bin/sed -i.bak '/netbackup_lv/d' /etc/fstab
[Enter]
[admusr@<target_server> ~]$
```

18. Target Server: Check in the `/etc/fstab` file.

    Execute the following command to RCS check in the `/etc/fstab` file.

```
[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/rcscheck /etc/fstab [Enter]
[admusr@<target_server> ~]$
```

19. Target Server: Verify the removal of the entry from the `/etc/fstab` file.

    Execute the following command to compare the `/etc/fstab` file to the backup, `/etc/fstab.bak`.

```
[admusr@<target_server> ~]$ sudo /usr/bin/diff /etc/fstab.bak /etc/fstab [Enter]
19d18
< /dev/vgroot/netbackup_lv /usr/openv              ext4    defaults        1 2
[admusr@<target_server> ~]$
```

    The output should reflect a difference similar to the example.

20. Target Server: Remove the `/etc/fstab.bak` file.

    Execute the following command to remove the `/etc/fstab.bak`.

```
[admusr@<target_server> ~]$ sudo rm -f /etc/fstab.bak [Enter]
[admusr@<target_server> ~]$
```

21. Target Server: Remove the Netbackup Logical Volume (LV).

    Execute the following command to remove the Netbackup LV identified in *O.1 Step 14*. Take care to use the correct volume group.

```
[admusr@<target_server> ~]$ sudo /sbin/lvremove -f /dev/vgroot/netbackup_lv
[Enter]
[admusr@<target_server> ~]$
```

22. Target Server: Remove the NetBackup client package entries.

    Execute the following command to remove the NetBackup client package entries from the `pkgKeep.conf` file. The NetBackup client packages were identified in *O.1 Step 5*. If the `pkgKeep.conf` only contains these packages the `pkgKeep.conf` file can be removed. In this example the NetBackup client packages are: `SYMCnbclt`, `SYMCnbjava`, `SYMCnbjre`, `SYMCpddea`, and `VRTSpbx`.

```
[admusr@<target_server> ~]$ sudo /bin/sed -i.bak
'/SYMCnbclt\|SYMCnbjava\|SYMCnbjre\|SYMCpddea\|VRTSpbx/d'
/usr/TKLC/plat/etc/upgrade/pkgKeep.conf [Enter]
[admusr@<target_server> ~]$
```

23. Target Server: Verify the removal of the NetBackup client package entries.

Execute the following command to verify the removal of the NetBackup client package entries from the `pkgKeep.conf` file by comparing the `pkgKeep.conf` to the backup file, `pkgKeep.conf.bak`.

```
[admusr@<target_server> ~]$ sudo /usr/bin/diff
/usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak
/usr/TKLC/plat/etc/upgrade/pkgKeep.conf [Enter]
1,5d0
< SYMCnbclt
< SYMCnbjava
< SYMCnbjre
< SYMCpddea
< VRTSpbx
[admusr@<target_server> ~]$
```

The output should reflect a difference similar to the example.

24. Target Server: Remove the `pkgKeep.conf.bak` file.

Execute the following command to remove the `pkgKeep.conf.bak` file.

```
[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak
 [Enter]
[admusr@<target_server> ~]$
```

25. Target Server: Remove the client profile configuration file.

Execute the following command to remove the client profile configuration file if one exists. The existence of this file was determined in *O.1 Step 5*.

Note: The client profile configuration file includes the client version in the name. For example, `NB7601.conf` where `7601` represents the client version number with the periods removed. In this example, version 7.6.0.1 is used.

```
[admusr@<target_server> ~]$ sudo rm -f
/usr/TKLC/plat/etc/netbackup/profiles/NB7601.conf [Enter]
[admusr@<target_server> ~]$
```

26. Target Server: Remove the client script file.

Execute the following command to remove the NetBackup client script file. For some versions of NetBackup, a script file is not used and does not exist. Proceed to the next step if this is the case.

Note: The client script file includes the client version in the name. For example, `NB7601` where `7601` represents the client version number with the periods removed. In this example, version 7.6.0.1 is used.

```
[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/netbackup/scripts/NB7601
 [Enter]
[admusr@<target_server> ~]$
```

27. Target Server: Remove the firewall rules related to NetBackup.

Note: This step varies depending on how the application implemented the firewall rules. This example reflects the correct steps for a TVOE server. If you are uninstalling NetBackup on a TPD application server refer to the documentation for your specific application.

Execute the following commands to remove the `iptables` and `ip6tables` firewall rules related to NetBackup on a TVOE server.

```
[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/iptablesAdm delete
--type=domain --domain=60netbackup --protocol=ipv4 [Enter]
[admusr@<target_server> ~]$ sudo /sbin/service iptables restart [Enter]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/iptablesAdm delete
--type=domain --domain=60netbackup --protocol=ipv6 [Enter]
[admusr@<target_server> ~]$ sudo /sbin/service ip6tables restart [Enter]
ip6tables: Setting chains to policy ACCEPT: filter         [  OK  ]
ip6tables: Flushing firewall rules:                        [  OK  ]
ip6tables: Applying firewall rules:                        [  OK  ]
[admusr@<target_server> ~]$
```

28. Target Server: Remove firewall configuration files related to NetBackup.

Note: This step varies depending on how the application implemented the firewall rules. This example reflects the correct steps for a TVOE server. If you are uninstalling NetBackup on a TPD application server refer to the documentation for your specific application.

Execute the following commands to remove firewall configuration files related to Netbackup on a TVOE server.

```
[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/iptables/60netbackup.ipt
[admusr@<target_server> ~]$ sudo rm -f
/usr/TKLC/plat/etc/ip6tables/60netbackup.ipt
[admusr@<target_server> ~]$
```

29. Target Server: Update the `/etc/hosts` file to remove the NetBackup server host.

Execute the following steps to update the `/etc/hosts` file using the platcfg utility:

Note: If the NetBackup entry in the `/etc/hosts` is an alias and you do not wish to delete the host, simply choose `Delete Alias` instead of `Delete Host`. The rest of the steps are similar.

1. As admusr, execute the command **`sudo su - platcfg`** to launch the platcfg utility.
2. Select `Network Configuration`.
3. Select `Modify Hosts File`.
4. Select `Edit`.
5. Select `Delete Host`.
6. Select the host entry for NetBackup.
7. Select `Yes` to confirm delete.
8. Exit out of the platcfg utility.

30. Target Server: Verify server health.

Execute the following command to verify the server health. No unexpected alarms should be presented and no missing package files should exist.

```
[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/alarmMgr -alarmStatus [Enter]
[admusr@<target_server> ~]$ sudo rpm -Va
[admusr@<target_server> ~]$
```

You have completed this procedure.

Appendix P

How to Increase the PM&C Netbackup Filesystem Size

Topics:

- *Increase the PM&C Netbackup Filesystem Size.....466*

This appendix describes how to increase the PM&C Netbackup filesystem to accommodate upgrading to Netbackup 7.7 or greater.

P.1 Increase the PM&C Netbackup Filesystem Size

This procedure describes how to increase the PM&C Netbackup filesystem to accommodate upgrading to Netbackup 7.7 or greater. Currently the recommended filesystem size for Netbackup 7.7 is 5G. This filesystem is mounted to a logical volume maintained on the TVOE host.

Prerequisites:

- There is a volume defined on the TVOE host called '**<pmac guest name>_netback.img**' set to 2G.
- There is a filesystem on the PM&C guest at '**/dev/<device_name>**' mounted to '**/usr/openv**' and sized to 2G.
- The Netbackup filesystem on the PM&C must be type ext2/3/4.
- This procedure assumes there is an entry in the /etc/fstab file for the mounted /usr/openv filesystem.

Notes:

- The device_name used could be different from '/dev/vdd'. This can be determined by issuing the 'df -h' command on the PM&C prior to starting this procedure and searching for the '/usr/openv' Netbackup filesystem. Once Netbackup has been enabled and configured on a PM&C, there should be a softlink defined, called '/dev/netbackup', which points to the actual device. Usually this points to '/dev/vdd'. If that is available then all references to '/dev/vdd' can be replaced with '/dev/netbackup' and the user does not have to know what actual device is used for the filesystem. The procedure below assumes this to be true.
- The commands listed below require root access to execute them. SUDO is used to elevate the user permissions to be able to execute the commands. Any command that is not prefixed with SUDO does not require elevation to execute.
- All commands are executed from a PM&C shell or from a TVOE shell.
- The procedure is written to increase the size of the Netbackup filesystem to 5G. This procedure can be used to increase the Netbackup volume to any size as can be accommodated by the TVOE host. 5G is the required size for Netbackup 7.7.
- Each step in this procedure will start by identifying the target server on which the command is to be executed. In this procedure, commands are executed on either the TVOE host or the PM&C.

Execute the following steps to increase the size of the Netbackup filesystem.

1. Connect to the management server's TVOE host shell and the PM&C shell via ssh using the admusr credentials.
2. TVOE Host: Verify the existing TVOE Netbackup volume is set to 2G.
   a) Display the logical volume sizes.

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvs [Enter]
  LV                    VG       Attr       LSize
  <pmac_guest>.img           vgguests -wi-ao----  50.00g
  <pmac_guest>_images.img    vgguests -wi-ao----  20.00g
  <pmac_guest>_logs.img      vgguests -wi-ao----  10.00g
  <pmac_guest>_netbackup.img vgguests -wi-ao----   2.00g
  plat_root             vgroot   -wi-ao---- 768.00m
  plat_swap             vgroot   -wi-ao----   2.00g
  plat_tmp              vgroot   -wi-ao----   1.00g
  plat_usr              vgroot   -wi-ao----   3.00g
  plat_var              vgroot   -wi-ao----   1.00g
```

```
[admusr@<tvoe_host> ~]$
```

b) Display the logical volume details.

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvdisplay
/dev/vgguests/<pmac_guest>_netbackup.img [Enter]
  --- Logical volume ---
  LV Path                /dev/vgguests/<pmac_guest>_netbackup.img
  LV Name                <pmac_guest>_netbackup.img
  VG Name                vgguests
  LV UUID                CWe1Nl-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp
  LV Write Access        read/write
  LV Creation host, time <tvoe_host>, 2016-11-14 10:00:54 -0500
  LV Status              available
  # open                 1
  LV Size                2.00 GiB
  Current LE             64
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     4096
  Block device           253:19

[admusr@<tvoe_host> ~]$
```

3. PM&C: Verify the Netbackup filesystem is set to 2G.

```
[admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv [Enter]
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdd        2.0G   69M  2.3G   1% /usr/openv

[admusr@<pmac_guest> ~]$
```

4. TVOE Host: Resize the Netbackup volume from 2G to 5G.

```
[admusr@<tvoe_host> ~]$ usr/bin/sudo /sbin/lvextend --size 5G
/dev/vgguests/<pmac_guest>_netbackup.img [Enter]
Size of logical volume vgguests/<pmac_guest>_netbackup.img changed from 2.00 GiB
 (64 extents) to 5.00 GiB (160 extents).
Logical volume <pmac_guest>_netbackup.img successfully resized

[admusr@<tvoe_host> ~]$
```

5. TVOE Host: Verify the size of the volume has increased to 5G.

a) Display the logical volume sizes.

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvs [Enter]
LV                     VG       Attr       LSize
  <pmac_guest>.img           vgguests -wi-ao----  50.00g
  <pmac_guest>_images.img    vgguests -wi-ao----  20.00g
  <pmac_guest>_logs.img      vgguests -wi-ao----  10.00g
  <pmac_guest>_netbackup.img vgguests -wi-ao----   5.00g
  plat_root              vgroot   -wi-ao---- 768.00m
  plat_swap              vgroot   -wi-ao----   2.00g
  plat_tmp               vgroot   -wi-ao----   1.00g
  plat_usr               vgroot   -wi-ao----   3.00g

[admusr@<tvoe_host> ~]$
```

b) Display the logical volume details.

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvdisplay
/dev/vgguests/<pmac_guest>_netbackup.img [Enter]
  --- Logical volume ---
  LV Path                /dev/vgguests/<pmac_guest>_netbackup.img
  LV Name                <pmac_guest>_netbackup.img
  VG Name                vgguests
  LV UUID                CWe1Nl-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp
  LV Write Access        read/write
  LV Creation host, time <tvoe_host>, 2016-11-14 10:00:54 -0500
  LV Status              available
  # open                 1
  LV Size                5.00 GiB
  Current LE             64
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     4096
  Block device           253:19

[admusr@<tvoe_host> ~]$
```

6. PM&C: Verify the space on the PM&C Netbackup filesystem has not changed.

```
[admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv [Enter]
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdd        2.0G   69M  1.3G   1% /usr/openv

[admusr@<pmac_guest> ~]$
```

7. TVOE Host: Ensure the PM&C is made aware of the volume size increase.

a) TVOE Host: Identify the PM&C guest using a virsh command.

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh list --all [Enter]
Id    Name                           State
----------------------------------------------------
86    <pmac_guest>                   running

[admusr@<tvoe_host> ~]$
```

b) TVOE Host: Shutdown the PM&C guest.

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh shutdown <pmac_guest> [Enter]
Domain <pmac_guest> is being shutdown

[admusr@<tvoe_host> ~]$
```

c) TVOE Host: Wait for the PM&C to shut down (if the State is "running", repeat the command until it indicates the State is "shut off').

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh list --all [Enter]
Id    Name                           State
----------------------------------------------------
86    <pmac_guest>                       shut off
```

d) TVOE Host: Once shutdown is complete, restart the PM&C.

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh start <pmac_guest> [Enter]
Domain <pmac_guest> started

[admusr@<tvoe_host> ~]$
```

e) TVOE Host: Verify the PM&C has completed the restart. This can be checked by executing the command 'sudo virsh console <pmac_guest>' and checking for the PM&C guest login prompt (once the escape character is displayed, hit <cr> once more to get the login prompt - afterwards hit 'ctrl]' to drop out of the PM&C login prompt and back to the TVOE host prompt).

```
[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh console <pmac_guest> [Enter]
Connected to domain <tvoe_host>
Escape character is ^]

Oracle Linux Server release 6.8
Kernel 2.6.32-642.6.1.el6prerel7.3.0.0.0_88.30.0.x86_64 on an x86_64

<pmac_guest> login:
```

8. PM&C: Verify the volume size increase is 5G as seen from the PM&C.

```
[admusr@<pmac_guest> ~]$ /usr/bin/sudo admusr /sbin/fdisk -l /dev/netbackup
[Enter]

Disk /dev/netbackup: 5368 MB, 5368709120 bytes
16 heads, 63 sectors/track, 10402 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

[admusr@<pmac_guest> ~]$
```

9. PM&C: Resize the PM&C Netbackup filesystem to 5G.

a) PM&C: Verify the filesystem is still mounted by issuing the 'mount' command and looking for '/dev/vdd' mounted on '/usr/openv'.

```
[admusr@<pmac_guest> ~]$ /bin/mount [Enter]
/dev/mapper/vgroot-plat_root on / type ext4 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/vda1 on /boot type ext4 (rw)
/dev/mapper/vgroot-plat_tmp on /tmp type ext4 (rw)
/dev/mapper/vgroot-plat_usr on /usr type ext4 (rw)
/dev/mapper/vgroot-plat_var on /var type ext4 (rw)
/dev/mapper/vgroot-plat_var_tklc on /var/TKLC type ext4 (rw)
/dev/mapper/vgroot-smac_root on /usr/TKLC/smac type ext4 (rw)
/dev/mapper/vgroot-smac_var on /var/TKLC/smac type ext4 (rw)
/dev/mapper/vgroot-smac_backup on /var/TKLC/smac/backup type ext4 (rw)
/dev/mapper/vgroot-smac_isoimages on /var/TKLC/smac/image/isoimages type ext4
(rw)
/var/TKLC/smac/image/core on /var/TKLC/core type none (rw,bind)
/dev/vdb on /var/TKLC/smac/logs type ext3 (rw)
/dev/vdc on /var/TKLC/smac/image/repository type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
```

```
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
nfsd on /proc/fs/nfsd type nfsd (rw)
/dev/vdd on /usr/openv type ext3 (rw)

[admusr@<pmac_guest> ~]$
```

b) PM&C: Un-mount the Netbackup filesystem. The 'umount' command can be verified by issuing the 'mount' command again. The '/usr/openv' filesystem should not be displayed as in the previous command. Note: There is no output generated from the 'umount' command on success.

```
[admusr@<pmac_guest> ~]$ /usr/bin/sudo /bin/umount /usr/openv [Enter]
[admusr@<pmac_guest> ~]$
```

c) PM&C: Execute the 'e2fsck' command to make sure the Netbackup filesystem is clean.

```
[admusr@<pmac_guest> ~]$ /usr/bin/sudo /sbin/e2fsck /dev/netbackup [Enter]
e2fsck 1.43-WIP (20-Jun-2013)
/dev/netbackup: clean, 11/327680 files, 37999/1310720 blocks

[admusr@<pmac_guest> ~]$
```

d) PM&C: Execute the 'resize2fs' command to resize the filesystem and map it to the 5G size of the disk volume on the TVOE host. If the 'size' attribute is not included in the command, the Netbackup filesystem will be resized to the total free space on the TVOE host volume. This should be 5G as there should not be any other filesystems mounted to this volume. If the 'resize2fs' command returns an indication that the 'e2fsck' command must be executed on the Netbackup filesystem, then re-execute that command.

```
[admusr@<pmac_guest> ~]$ /usr/bin/sudo /usr/bin/resize2fs /dev/netbackup [Enter]
resize2fs 1.43-WIP (20-Jun-2013)
Resizing the filesystem on /dev/netbackup to 1310720 (4k) blocks.
The filesystem on /dev/netbackup is now 1310720 blocks long.

[admusr@<pmac_guest> ~]$
```

e) PM&C: Re-mount the '/usr/openv' Netbackup filesystem with the 'mount -a' command.

```
[admusr@<pmac_guest> ~]$ mount -a [Enter]
[admusr@<pmac_guest> ~]$
```

Note: This command can only be used if the existing entry to mount the filesystem is contained in the '/etc/fstab' file (which is expected).

f) PM&C: Verify the new size of the Netbackup filesystem. Issue the 'mount' command to verify the filesystem is correctly mounted. Issue the '/bin/df -h /usr/openv' command to show the Netbackup filesystem using 5G instead of 2G.

```
[admusr@<pmac_guest> ~]$ /bin/mount [Enter]
/dev/mapper/vgroot-plat_root on / type ext4 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/vda1 on /boot type ext4 (rw)
/dev/mapper/vgroot-plat_tmp on /tmp type ext4 (rw)
/dev/mapper/vgroot-plat_usr on /usr type ext4 (rw)
/dev/mapper/vgroot-plat_var on /var type ext4 (rw)
```

```
/dev/mapper/vgroot-plat_var_tklc on /var/TKLC type ext4 (rw)
/dev/mapper/vgroot-smac_root on /usr/TKLC/smac type ext4 (rw)
/dev/mapper/vgroot-smac_var on /var/TKLC/smac type ext4 (rw)
/dev/mapper/vgroot-smac_backup on /var/TKLC/smac/backup type ext4 (rw)
/dev/mapper/vgroot-smac_isoimages on /var/TKLC/smac/image/isoimages type ext4
(rw)
/var/TKLC/smac/image/core on /var/TKLC/core type none (rw,bind)
/dev/vdb on /var/TKLC/smac/logs type ext3 (rw)
/dev/vdc on /var/TKLC/smac/image/repository type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
nfsd on /proc/fs/nfsd type nfsd (rw)
/dev/vdd on /usr/openv type ext3 (rw)

[admusr@<pmac_guest> ~]$
```

The second command in this sub-step shows the Netbackup filesystem using 5G instead of 2G.

```
[admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv [Enter]
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdd        5.0G   69M  4.3G   1% /usr/openv

[admusr@<pmac_guest> ~]$
```

g) PM&C: Change directory to the '/usr/openv' directory and verify any files contained on the original 2G Netbackup filesystem are still available on the new 5G Netbackup filesystem.

```
[admusr@<pmac_guest> ~]$ /bin/ls -l /usr/openv  [Enter]
java lost+found pack regid.1992-12.com.symantec_netbackup-7.6.0.1_1.swidtag share
 var
lib msg pack.7.6.0.1 regid.1992-12.com.symantec_netbackup-7.7.1.0_1.swidtag
swidtag.xml
logs netbackup pdde resources tmp

[admusr@<pmac_guest> ~]$
```

You have completed this procedure.