Oracle® Communications

PMAC Management and Configuration, Release 6.6

Configuration Guide

E93270-01

August 2018

ORACLE

Oracle Communications PMAC Configuration Guide, Release 6.6

CAUTION: 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 https://www.oracle.com/us/support/contact/index.html.

See more information on MOS in the Appendix G:

Table of Contents

List of Tables

List of Figures

List of Procedures

1. Introduction

This document describes the procedures to configure third-party hardware and platform components that make up Platform 7.6 configurable hardware components include HP ProLiant and Oracle rack mount servers (RMS), 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 and the Platform Management and Configuration (PMAC) application to provision and manage those components when hosting feature applications.

Before 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 need to reference individual procedures in their specific installation and configuration procedures. The application documentation provides the proper sequencing of procedures, application-specific supplemental steps, and passwords to use during the configuration.

1.1 References

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

[1] TPD Initial Product Manufacture Software Installation Procedure

[2] HP Solutions Firmware Upgrade Pack

The latest version is recommended if an upgrade is to be performed; otherwise, version 2.2.12 is the minimum. This pack includes both documentation and firmware media. For HP G6 server models, HP FUP 2.2.10 is the last HP FUP that provides support and is the minimum for G6 servers.

[3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

The latest version is recommended if an upgrade is performed; otherwise, version 2.2.12 is the minimum. For HP G6 server models, HP FUP 2.2.10 is the last HP FUP that provides support and is the minimum for G6 servers.

[4] Oracle Firmware Upgrade Pack Release Notes

The latest version is recommended if an upgrade is performed; otherwise, version 3.1.8 is the minimum.

[5] Oracle Firmware Upgrade Pack Upgrade Guide, version 3.1.8.

[6] PMAC Incremental Upgrade Procedure, Release 6.6.

[7] PMAC Disaster Recovery, Release 6.6.

1.2 Acronyms

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CA	Certificate Authority
CSR	Certificate Signing Request
DNS	Domain Name System

Acronym	Definition
DSCP	Differentiated Services Code Point, a form of QoS
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FMA	File Management Area
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
HP FUP	HP Firmware Upgrade Pack
iLO	Integrated Lights Out remote management port
iLOM	Integrated Lights Out Manager
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 Delivery Cloud
PMAC	Platform Management and 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

Term	Definition
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 PMAC 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 use the same physical network.
PMAC	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 use 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 PMAC	Additional term for PMAC - used in networking procedures to distinguish activities done on a PMAC guest and not the TVOE host running on the Management server.

1.4 How to Use this Document

Although this document is primarily to be used as an initial installation guide, its secondary purpose is as a reference for disaster recovery procedures. When executing this document for either purpose, there are a few points to help ensure the user understands the document's intent. These points are as follows:

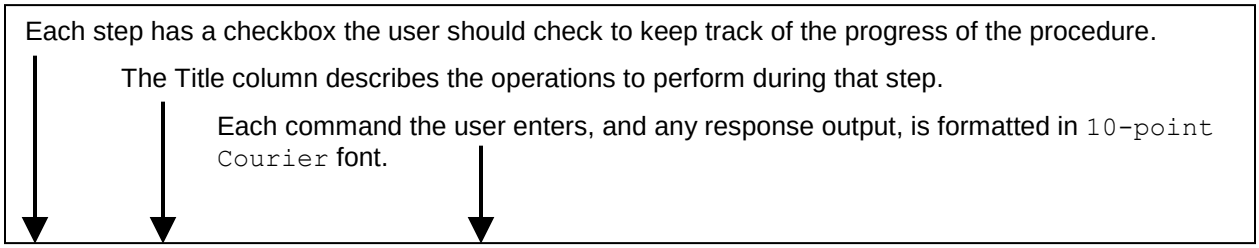
- Before beginning a procedure, completely read the instructional text (it displays immediately after the section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.

If a procedural step fails to execute successfully, stop and contact Oracle's Help Center for assistance before attempting to continue. See Appendix R for information on contacting My Oracle Support (MOS).

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 through 3, and step 3.1.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.

- Where it is necessary to identify the server explicitly on which a particular step is to be taken, the server name is given in the title box for the step (for example, **ServerX** in step 2 Figure 1).



	Title	Directive/Result Step
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	**ServerX**: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. `$ cu -l /dev/ttyS7`
3. ☐	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example of a Procedure Step Used in This Document

2. 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 Blade System 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
  - MSA 2012fc
  - D2200sb (Storage Blade)
  - D2220sb (Storage Blade)

  - D2700
  - P2000
- Cisco 4948/4948E/4948E-F Rack Mount Network Switches
- Cisco 9372TX-E Rack Mount Network Switches

2.1 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 > Platforms > Tekelec**.

For customers who 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 2.2.12.

The minimum firmware release required for PMAC 6.6 is HP Solutions Firmware Upgrade Pack 2.2.12. For HP G6 server models, HP FUP 2.2.10 is the last HP FUP that provides support and is the minimum for G6 servers.

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 2.2.12 releases are:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC Firmware ISO image
- Refer to the [4] Oracle Firmware Upgrade Pack Release Notes

2.2 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 6.6 is 3.1.8. 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.

3. Network Procedures

3.1 Configure netConfig Repository

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

Prerequisites:

- 8.1 IPM Management Server
- If the PMAC is included in the installation:
  - 9.1 Install TVOE on the Management Server

- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC

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

- For switches, use the command:

  ```
  sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
  ```

- For services, use the command:

  ```
  sudo /usr/TKLC/plat/bin/netConfig --repo listServices
  ```

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

IPv4 and IPv6

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

Terminology

The term **netConfig server** refers to the entity where netConfig is executed. This may be a virtualized or physical environment. **Management server** may also accurately describe this location, but has been historically used to describe the physical environment, while **Virtual PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments 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 in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

Variable	Value
<management_server_iLO_IP>	
<management_server_mgmt_IP_address>	
<netConfig_server_mgmt_IP_address>	
<switch_backup_user>	admusr
<switch_backup_user_password> See application documentation	
<serial console type>	U=USB, c=PCIe

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

Variable	Value
<switch_hostname> From NAPD or output from `listDevices` command	

Variable	Value
<device_model>	
<console_name>	
<switch_console_password> See referring application documentation	
<switch_platform_username>	
<switch_platform_password> See referring application documentation	
<switch_enable_password> See referring application documentation	
<switch_mgmt_IP_address> CIDR format	
<switch_mgmt_netmask>	
<mgmt_VLAN_ID>	
<control_VLAN_ID>	
<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> See referring application documentation	
<switch_platform_username>	
<switch_platform_password> See referring application documentation	
<switch_enable_password> See referring application documentation	
<switch_mgmt_IP_address>	
<switch_mgmt_netmask>	
<mgmt_VLAN_ID> Value gathered from NAPD	
<control_VLAN_ID>	
<IOS_filename>	
<IP_version>	

For each enclosure switch (6120XG, 6125G, 6125XLG, or 3020), fill in the appropriate value for this site (make as many copies of this table as needed).

Variable	Value
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password> See referring application documentation	
<io_bay>	
<OA1_enX_IP_address>	X= the enclosure #
<OA_password>	
<FW_image> FW file used in firmware upgrade/switch replacement/or initial install	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 1. Configure netConfig Repository

Step	Procedure	Result
1. ☐	**Management Server iLO**: Login	Log into the management server iLO on the remote using the password provided by the application following Appendix E.1 Access a Server Console Remotely.

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

2. ☐	**Management Server**: Pre-check	If the installation is not designed for a virtual PMAC, skip to the next step.
		If there is a virtual PMAC, log into the console.
		1. Verify virtual PMAC 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`
		2. If this command provides no output, it is likely that a virtual instance of PMAC is not installed.
		• If there is a virtual PMAC, log into the console of the virtual PMAC.
		• If the installation is not designed for a virtual PMAC, skip to the next step.
		3. From the management server, log into the console of the virtual PMAC 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 PMAC is not installed.
		• If this is unexpected, refer to application documentation or My Oracle Support (MOS).

3. ☐	**netConfig Server**: Check switch templates directory	Make sure the switch templates directory exists.
		`$ /bin/ls -i /usr/TKLC/smac/etc/switch/xml`
		If the command returns an error:
		`ls: cannot access /usr/TKLC/smac/etc/switch/xml/: No such file or directory`
		Create the directory:
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/xml`
		Change directory permissions:
		`$ sudo /bin/chmod go+rx /usr/TKLC/smac/etc/switch/xml`
		Change directory ownership:
		`$ sudo /bin/chown -R pmacd:pmacbackup /usr/TKLC/smac/etc/switch`

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

4. ☐	**netConfig Server**: Set up netConfig repository with ssh information	1. Use netConfig to create a repository entry that uses the ssh service. This command provides the user with several prompts. Modify the prompts with <variables> as the answers, which are site specific. The other prompts, which do not have a <variable> shown as the answer, must be entered EXACTLY as they are shown here.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <netConfig_server_mgmt_IP_address>`
		`Enter an option name <q to cancel>: user`
		`Enter the value for user: <switch_backup_user>`
		`Enter an option name <q to cancel>: password`
		`Enter the value for password: <switch_backup_user_password>`
		`Verify Password: <switch_backup_user_password>`
		`Enter an option name <q to cancel>: q`
		`Add service for ssh_service successful`
		
		`[admusr@minilab-pmac-1~]$ sudo netConfig --repo addService name=ssh_service`
		`Service type? (dhcp, oa, oobm, ssh, tftp, conserver) ssh`
		`Service host? 1.2.3.4`
		`Enter the value for user: admusr`
		`Enter the value for password: <admusr_password>`
		`Verify Password: <admusr_password>`
		`Add service for ssh_service successful`
		2. To ensure you entered the information correctly, use the following command and inspect the output, which is 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`

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

5. ☐	**netConfig Server**: Set up netConfig repository with TFTP information	***Note***: If there are no new Cisco (3020, 4948, 4948E or 4948E-F) switches to be configured, go to the next step.
		
		Use netConfig to create a repository entry that uses the tftp service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		
		• For a PMAC system:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service`
		`Service type? [dhcp, oa, oobm, ssh, tftp, conserver] tftp`
		`Service host? <netConfig_server_mgmt_IP_address>`
		`Directory on host? /var/TKLC/smac/image/`
		`Add service for tftp_service successful`
		
		• For a non-PMAC system:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service`
		`Service type? [tftp, ssh, conserver, oa] tftp`
		`Service host? <netConfig_server_mgmt_IP_address>`
		`Directory on host? /var/lib/tftpboot/`
		`Add service for tftp_service successful`

6. ☐	**netConfig Server**: Set up netConfig repository with OA information	***Note***: If there are no new HP 6125G/6125XLG/6120XG switches to configure, go to the next step.
		
		Use netConfig to create a repository entry that uses the OA service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not 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=oa_service_en<enclosure #>`
		`Service type? [dhcp, oa, oobm, ssh, tftp, conserver]? oa`
		`Primary OA IP? <OA1_enX_ip_address>`
		`Secondary OA IP? <OA2_enX_ip_address>`
		`OA username? root`
		`OA password? password`
		`Verify password:<OA_password>`
		`Add service for oa_service successful`

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

7. ☐	**netConfig Server**: Run conserverSetup command	`$ sudo /usr/TKLC/plat/bin/conserverSetup -<serial console type> -s <management_server_mgmt_IP_address>`
		You are asked for the platcfg credentials.
		Example:
		`[admusr@vm-pmac1A]$ sudo /usr/TKLC/plat/bin/conserverSetup -u -s <management_server_mgmt_IP_address>`
		`Enter your platcfg username, followed by [ENTER]:platcfg`
		`Enter your platcfg password, followed by [ENTER]:<platcfg_password>`
		`Checking Platform Revision for local TPD installation...`
		`The local machine is running:`
		`Product Name: PMAC`
		`Base Distro Release: 7.0.0.0.0_86.1.0`
		`Checking Platform Revision for remote TPD installation...`
		`The remote machine is running:`
		`Product Name: TVOE`
		`Base Distro Release: 7.0.0.0.0_86.2.0`
		`Configuring switch 'switch1A_console' console server...Configured.`
		`Configuring switch 'switchBA_console' console server...Configured.`
		`Configuring iptables for port(s) 782...Configured.`
		`Configuring iptables for port(s) 1024:65535...Configured.`
		`Configuring console repository service...`
		`Repo entry for "console_service" already exists; deleting entry for:`
		`Service Name: console_service`
		`Type: conserver`
		`Host: <management_server_mgmt_IP_address>`
		`...Configured.`
		`Slave interfaces for bond0:`
		`bond0 interface: eth01`
		`bond0 interface: eth02`
		• If this command fails, contact My Oracle Support (MOS).
		• Verify the output of the script.
		• Verify your Product Release is based on Tekelec Platform 7.4.
		• Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

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	***Note***: If there are no Cisco switches, skip to the next step.
		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 PMAC system:
		`<tftp_directory> = /var/TKLC/smac/image/`
		• For a non-PMAC 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`

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

10. ☐	**netConfig Server**: Copy HP switch	***Note***: If there are no HP switches, skip to the next step.
		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 ssh 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`

11. ☐	**netConfig Server**: Unmount ISO	`$ sudo /bin/unmount /mnt/upgrade`

12. ☐	**netConfig Server**: Set up netConfig repository with aggregation switch information	***Note***: If there are no new aggregation switches to configure, go to the next step.
		Use netConfig to create a repository entry for each switch. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the 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 My Oracle Support (MOS).
		• The device name must be 20 characters or less.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? Cisco`
		`Device Model? <device_model>`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>`
		`Is the management interface a port or a vlan? [vlan]: [Enter]`
		`What is the VLAN ID of the management VLAN? [2]: [mgmt_vlanID]`
		`What is the name of the management VLAN? [management]: [Enter]`
		`What switchport connects to the management server? [GE40]: [Enter]`
		`What is the switchport mode (access|trunk) for the management server port? [trunk]: [Enter]`
		`What are the allowed vlans for the management server port?`

Procedure 1. Configure netConfig Repository

Step	Procedure	Result
		[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 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 is similar to the one shown: $ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> Device: <switch_hostname> Vendor: Cisco Model: <device_model> FW Ver: 0 FW Filename: <IOS_image> FW Service: tftp_service

Procedure 1. Configure netConfig Repository

Step	Procedure	Result
		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	***Notes***: • If there are no new 3020s to be configured, go to the next step. • The Cisco 3020 is not compatible with IPv6 management configuration. Use netConfig to create a repository entry for each 3020. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here. • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. $ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? Cisco Device Model? 3020 What is the management address? <enclosure_switch_ip> Enter the name of the firmware file [cbs30x0-ipbasek9-tar.122-58.SE1.tar]: <FW_image> Firmware file to be used in upgrade: <IOS_image> Enter the name of the upgrade file transfer service: <tftp_service> File transfer service to be used in the upgrade: <tftp_service> Should the init network adapter be added (y/n)? y Adding netBootInit protocol for <switch_hostname> using network...

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

		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 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 is similar to the one shown below.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>`
		`Device: <switch_hostname>`
		`Vendor: Cisco`
		`Model: <device_model>`
		`FW Ver: 0`
		`FW Filename: <FW_image>`
		`FW Service: tftp_service`
		`Access: Network: <enclosure_switch_IP>`
		`Init Protocol Configured`
		`Live Protocol Configured`
		Repeat this step for each 3020, using appropriate values for those 3020s.
		Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. or 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	***Note***: If there are no 6120XGs to be configured, stop and continue with the appropriate switch configuration procedure.

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

	repository with HP 6120XG switch information	Use netConfig to create a repository entry for each 6120XG. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		• If you do not know any of the required answers, stop now and contact My Oracle Support (MOS).
		• The device name must be 20 characters or less.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? HP`
		`Device Model? 6120`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>`
		`Enter the name of the firmware file [Z_14_37.swi]: <FW_image>`
		`Firmware file to be used in upgrade: <FW_image>`
		`Enter the name of the upgrade file transfer service: ssh_service`
		`File transfer service to be used in upgrade: ssh_service`
		`Should the init oob adapter be added (y/n)? y`
		`Adding consoleInit protocol for <switch_hostname> using oob...`
		`What is the name of the service used for OOB access? oa_service_en<enclosure #>`
		`What is the name of the console for OOB access? <io_bay>`
		`What is the platform access username? <switch_platform_username>`
		`What is the device console password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`What is the platform user password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`What is the device privileged mode password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`Should the live network adapter be added (y/n)? y`
		`Adding cli protocol for <switch_hostname> using network...`
		`Network device access already set: <switch_mgmt_IP_address>`
		`Should the live oob adapter be added (y/n)? y`
		`Adding cli protocol for <switch_hostname> using oob...`
		`OOB device access already set: oa_service_en<enclosure #>`
		`Device named <switch_hostname> successfully added`
		The image is being unpacked and validated. This takes approximately 4

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

		minutes. Once the unpacking, validation, and rebooting have completed, you are returned to the normal prompt. Proceed with the next step.
		To verify 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 is similar to the one shown:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>`
		`Device: <switch_hostname>`
		`Vendor: HP`
		`Model: 6120`
		`FW Ver: 0`
		`FW Filename: <FW_image>`
		`FW Service: ssh_service`
		`Initialization Management Options`
		`mgmtIP: <enclosure_switch_IP>`
		`Access: Network: <enclosure_switch_IP>`
		`Access: OOB:`
		`Service: oa_service`
		`Console: <console_name>`
		`Init Protocol Configured`
		`Live Protocol Configured`
		Repeat this step for each 6120, using appropriate values for those 6120s.
		Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image:
		WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.

15. ☐	**netConfig Server**: Set up netConfig repository with HP 6125G switch information	***Note***: If there are no 6125Gs to be configured, stop and continue with the appropriate switch configuration procedure.
		Use netConfig to create a repository entry for each 6125G. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		• If you do not know any of the required answers, stop now and contact My Oracle Support (MOS).
		• The device name must be 20 characters or less.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? HP`

Procedure 1. Configure netConfig Repository

Step	Procedure	Result

		Device Model? 6125
		
		What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management? <switch_mgmt_IP_address>
		
		Enter the name of the firmware file [6125-CMW520-R2105.bin]: <FW_image>
		
		Firmware file to be used in upgrade: <FW_image>
		
		Enter the name of the upgrade file transfer service: ssh_service
		
		Should the init oob adapter be added (y/n)? y
		
		Adding consoleInit protocol for <switch_hostname> using oob...
		
		What is the name of the service used for OOB access? oa_service_en<enclosure #>
		
		What is the name of the console for OOB access? <io_bay>
		
		What is the platform access username? <switch_platform_username>
		
		What is the device console password? <switch_platform_password>
		
		Verify password: <switch_platform_password>
		
		What is the platform user password? <switch_platform_password>
		
		Verify password: <switch_platform_password>
		
		What is the device privileged mode password? <switch_platform_password>
		
		Verify password: <switch_platform_password>
		
		Should the live network adapter be added (y/n)? y
		
		Adding cli protocol for <switch_hostname> using network...
		
		Network device access already set: <switch_mgmt_IP_address>
		
		Should the live oob adapter be added (y/n)? y
		
		Adding cli protocol for <switch_hostname> using oob...
		
		OOB device access already set: oa_service_en<enclosure #>
		
		Device named <switch_hostname> successfully added.
		
		Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image:
		
		WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.
		
		To verify 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 is similar to the one shown:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice`

Procedure 1. Configure netConfig Repository

Step	Procedure	Result
		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 provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here. • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. $ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? HP Device Model? 6125XLG What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address> Enter the name of the firmware file [6125XLG-CMW710-R2403.ipe]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service: ssh_service File transfer service to be used in upgrade: ssh_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? oa_service_en<enclosure#> What is the name of the console for OOB access? <io_bay> What is the platform access username? <switch_platform_username>

Procedure 1. Configure netConfig Repository

Step	Procedure	Result
		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 verify 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 is 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

3.2 Aggregation Switch — netConfig Procedures

3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)

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

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC
- Application management network interfaces must be configured on the management servers before executing this procedure.
- Application username and password for creating switch backups must be configured on the management server before 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] HP Solutions Firmware Upgrade Pack.

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> See referring application documentation	
<switch_enable_password> See referring application documentation	
<management_server_mgmt_IP_address>	
<pmac_mgmt_IP_address>	
<switch_mgmtVLAN_ID>	
<switch1A_mgmtVLAN_IP_address>	
<mgmt_Vlan_subnet_ID>	
<netmask>	
<switch1B_mgmtVLAN_IP_address>	
<switch_Internal_VLAN_list>	
<management_server_mgmtInterface>	
<management_server_iLO_IP>	
<customer_supplied_ntp_server_address>	
<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	

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Uplinks must be disconnected from the customer network before executing this procedure. One of the steps in this procedure instructs when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.
- Filenames and sample command line input/output throughout this procedure 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 is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result
1. ☐	**Virtual PMAC**: Verify IOS image is on the system	Determine if the IOS image for the 4948/4948E/4948E-F is on the PMAC. `$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file>` If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

2. ☐	**Virtual PMAC**: Modify P&C feature to allow TFTP	Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=1`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Note: Ignore the sentry restart instructions.
		Note: This may take up to 60 seconds to complete.

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

3. ☐	**Virtual PMAC > Management Server**: Manipulate host server physical interfaces	Exit from the virtual PMAC console, by pressing **Ctrl-]** and you are returned to the server prompt.
		Ensure 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>.
		`$ sudo /usr/bin/virsh console vm-pmac1A`
		Note: On a TVOE host, if you open 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 the virsh console, and run `ps -ef |grep virsh`, then kill the existing process `$ sudo kill -9 <PID>`. Execute the `$ sudo virsh console X` command again. Your console session should now run as expected.

4. ☐	**Management Server**: Determine if switch1A PROM upgrade is required	***Note***: ROM and PROM are intended to have the same meaning for this procedure. Connect to switch1A and 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 My Oracle Support (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

5. ☐	**Virtual PMAC**: Extract configuration files	Extract the configuration files from the ZIP file copied in 9. of Procedure 1.
		`$ cd /usr/TKLC/smac/etc`
		`$ sudo unzip DSR_NetConfig_Templates.zip`
		`$ sudo chown -R admusr.admgrp DSR_NetConfig_Templates`
		This creates a directory called **DSR_NetConfig_Templates**, which contains the configuration files for all the supported deployments. Copy the necessary init file from **init/Aggregation** and the necessary config files from **config/TopoX** (where X refers to the appropriate topology) using the following commands. Make sure to replace **X** with the appropriate Topology number.
		Note: The following workaround is needed:
		Remove the double right brackets for:
		DSR_NetConfig_Templates/Topo1_L2/4948E-F_L2_configure.xml: <option name="type">access</option>>
		DSR_NetConfig_Templates/Topo4/6125XLG_Pair-2_template_configure.xml: <!-- Multiple VLANs can be entered by stringing the VLANs in the setAllowedVlans option, i.e., 1-5 or 1,2,3,4,5 -->>
		DSR_NetConfig_Templates/Topo1_L3/3020_template_configure.xml: <!-- 'mode' is required on Cisco when adding interfaces -->>
		Replace <configure> with <configure apiVersion="1.1"> within: DSR_NetConfig_Templates/utility/addQOS_trafficeTemplate_6120XG.xml
		`# sudo cp DSR_NetConfig_Templates/init/Aggregation/* /usr/TKLC/smac/etc/switch/xml/`
		`# sudo cp DSR_NetConfig_Templates/config/TopoX/* /usr/TKLC/smac/etc/switch/xml/`

6. ☐	**Management Server**: Modify switch1A_4948_4948E.xml and switch1B_4948_4948E.xml	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 `$some_variable_name`, that value is modified and the dollar sign must be removed during the modification. When done editing the file, save and exit to return to the command prompt.
7. ☐	**Management Server**: Modify 4948E-F_configure.xml	Modify 4948E-F_configure.xml for information needed to configure the switches. Update the configure.xml file for all values preceded by a dollar sign. For example, if a value has `$some_variable_name`, that value is modified and the dollar sign must be removed during the modification. When done editing the file, save and exit to return to the command prompt. ***Note***: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the Cisco 4948E-F aggregation switches. This function must be configured for IPv4.

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

8. ☐	**Management Server**: 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 My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname`
		`Hostname: switch1A`

9. ☐	**Management Server**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		`$ 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 PMAC > Management Server**: Manipulate host server physical interfaces	Exit from the virtual PMAC console, by pressing **Ctrl-]** and you are returned to the server prompt.
		Ensure 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_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 PMAC by logging into the console of the virtual PMAC instance found in 2. of Procedure 1.
		`$ sudo /usr/bin/virsh console vm-pmac1A`
		Note: On a TVOE host, if you open the virsh console, for example, `$ 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, run `ps -ef |grep virsh`, and then kill the existing process, run `kill -9 <PID>`. Then execute the `virsh console X` command. Your console session should now run as expected.

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result
11. ☐	**Management Server**: Determine if switch1B PROM upgrade is required	***Note***: ROM AND PROM are intended to have the same meaning for this procedure. Connect to switch1A and 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 My Oracle Support (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1B.

12. ☐	**Virtual PMAC**: Initialize	Initialize switch1B 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 My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname`
		`Hostname: switch1B`

13. ☐	**Virtual PMAC**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware`
		`Version: 122-54.XO`
		`License: entservicesk9`
		`Flash: cat4500e-entservicesk9-mz.122-54.XO.bin`

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

14. ☐	**Virtual PMAC**: Disable TFTP	Modify PMAC Feature to disable TFTP.
		Disable the DEVICE.NETWORK.NETBOOT feature.
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=0`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Note: This may take up to 60 seconds to complete.

15. ☐	**Virtual PMAC**: 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 up to 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

16. ☐	**Management Server**: Ensure interface are enabled on the TVOE host	Press **Ctrl-]** to exit the virtual PMAC console. This returns the terminal to the server prompt.
		Ensure the interfaces of the server connected to switch1A and switch1B are up by performing the following commands:
		`$ sudo /sbin/ifup <ethernet_interface_1>`
		`$ sudo /sbin/ifup <ethernet_interface_2>`

17. ☐	**Cabinet**: Connect cables from customer network	Attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. ***Note***: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

18. ☐	**Virtual PMAC**: Verify access to customer network	Verify connectivity to the customer network by issuing the following command:
		`$ /bin/ping <customer_supplied_ntp_server_address>`
		`PING ntpserver1 (10.250.32.51) 56(84) bytes of data.`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms`

19. ☐	**Cabinet**: Connect 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.

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

20. ☐	**Virtual PMAC**: 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 cables from customer network	Re-attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. ***Note***: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.
22. ☐	**Management Server**: Restore the TVOE host back to its original state	Press **Ctrl-]** to exit the virtual PMAC console. This returns the terminal to the server prompt. Restore the server networking back to original state: `$ sudo /sbin/service network restart`
23. ☐	Back up switch and/or enclosure switch	Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) for each switch configured in this procedure.

3.2.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (RMS System, No PMAC Installed) (netConfig)

This procedure configures 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 Platform 7.6 interconnect. If the system being configured follows a different platform interconnect, then follow the appropriate platform procedures.

Prerequisites:

- 3.1 Configure netConfig Repository
- 8.1 IPM Management Server
- Application management network interfaces must be configured on the management servers before executing this procedure.
- Application username and password for creating switch backups must be configured on the management server before 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] HP Solutions Firmware Upgrade Pack.

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>	
<pmac_mgmt_IP_address>	
<switch_mgmtVLAN_ID>	
<switch1A_mgmtVLAN_IP_address>	
<mgmt_Vlan_subnet_ID>	
<netmask>	
<switch1B_mgmtVLAN_IP_address>	
<switch_Internal_VLAN_list>	
<management_server_mgmtInterface>	
<management_server_iLO_IP>	
<customer_supplied_ntp_server_address>	
<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	

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Uplinks must be disconnected from the customer network before executing this procedure. One of the steps in this procedure instructs when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.
- Filenames and sample command line input/output throughout this procedure 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 is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result
1. ☐	**Virtual PMAC**: Verify IOS image is on the system	Determine if the IOS image for the 4948/4948E/4948E-F is on the PMAC. `$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file>` If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

2. ☐	**Management Server**: Enable tftp on the system for tftp transfer of IOS upgrade file	`$ 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 firewall is configured	`$ 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`

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

4. ☐	**Management Server**: Manipulate host server physical interfaces	Ensure 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>
		`$ sudo /usr/bin/virsh console vm-pmac1A`
		Note: On a TVOE host, if you open 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 the virsh console, and run `ps -ef |grep virsh`, then kill the existing process `$ sudo kill -9 <PID>`. Execute the `$ sudo virsh console X` command again. Your console session should now run as expected.

5. ☐	**Management Server**: Determine if switch1A PROM upgrade is required	***Note***: ROM and PROM are intended to have the same meaning for this procedure. Connect to switch1A and 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 My Oracle Support (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

6. ☐	**Management Server**: Verify the initialization template xml files care the correct versions	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 the files from application media.
		1. 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.
		2. 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`

7. ☐	**Virtual PMAC**: Modify switch1A_4948_4948E.xml and switch1B_4948_4948E.xml	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 `$some_variable_name`, that value is modified and the dollar sign must be removed during the modification. When done editing the file, save and exit to return to the command prompt.
8. ☐	**Virtual PMAC**: Modify 4948E-F_configure.xml	Modify 4948E-F_configure.xml for information needed to configure the switches. Update the configure.xml file for all values preceded by a dollar sign. For example, if a value has `$some_variable_name`, that value is modified and the dollar sign must be removed during the modification. When done editing the file, save and exit to return to the command prompt. ***Note***: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the Cisco 4948E-F aggregation switches. This function must be configured for IPv4.

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

9. ☐	**Virtual PMAC**: Initialize	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 My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify 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 My Oracle Support (MOS).

10. ☐	**Management Server**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware`
		`Version: 122-54.XO`
		`License: entservicesk9`
		`Flash: cat4500e-entservicesk9-mz.122-54.XO.bin`

11. ☐	**Management Server**: Manipulate host server physical interfaces	Ensure 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_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>.

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result
12. ☐	**Management Server**: Determine if switch1B PROM upgrade is required	***Note***: ROM AND PROM are intended to have the same meaning for this procedure. Connect to switch1A and 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 My Oracle Support (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1B.

13. ☐	**Virtual PMAC**: Initialize	Initialize switch1B 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 My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname`
		`Hostname: switch1B`

14. ☐	**Virtual PMAC**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware`
		`Version: 122-54.XO`
		`License: entservicesk9`
		`Flash: cat4500e-entservicesk9-mz.122-54.XO.bin`

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result
15. ☐	**Virtual PMAC**: Validate XML file	This script validates the XML file to a limited extent. It verifies: • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values To validate the XML file: `$ 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 above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.

16. ☐	**Virtual PMAC**: Configure the 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 up to 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

17. ☐	**Management Server**: Ensure interface are enabled on the TVOE host	Press **Ctrl-]** to exit the virtual PMAC console. This returns the terminal to the server prompt.
		Ensure 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 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 PMAC**: 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`

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result
20. ☐	**Cabinet**: Connect 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 PMAC**: 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 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	Press **Ctrl-]** to exit the virtual PMAC console. This returns the terminal to the server prompt. Restore the server networking back to original state: `$ sudo /sbin/service network restart`

24. ☐	**Management Server**: Disable TFTP	`$ 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 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.

25. ☐	**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"`

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

Step	Procedure	Result

26. ☐	**Management Server**: Verify the firewall is configured properly	`$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter`
		
		`Persist Domain Table Chain Match`

27. ☐	Back up switch and/or enclosure switch	Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) for each switch configured in this procedure.

3.2.3 Configure Cisco 9372TX-E Aggregation Switches (PMAC Installed) (netConfig)

This procedure configures Cisco 9372TX-E switches to be used in a 10GE-RMS deployment. This procedure also includes how to configure the netConfig repository for all required services and switch information.

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC

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 in section 3.1, IPv4 or IPv6 may be used. Commands such as ping or ssh may also be used in these procedures, where for IPv6 cases may need to be `ping6` or `ssh -6` as needed.

Terminology

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

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
<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> /usr/TKLC/smac/etc/switch/backup	
<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 frames to be added: Valid frame 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_VLAN_ID>	
<control_VLAN_ID>	
<oobm_VLAN_ID> For switch Frame 1 ID A and Frame 1 ID B the oobm_vlanID should be 1	

Variable	Value
<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> The firmware version must match the operational redundant switch. This is checked in a procedural step.	
<ssh_service> ssh_service to be used for firmware transfer	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

Step	Procedure	Result
1. ☐	**Management Server iLO**: Login	Log into the management server iLO on the remote console using application provided passwords via Appendix E. ***Note***: If executing this procedure to add switches/frames after the initial deployment (that is, a second pass to add hardware to an existing deployment), the virtual PMAC can be accessed directly via SSH instead of iLO and steps 1 and 2 may be skipped.

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

Step	Procedure	Result

2. ☐	**Management Server**: Pre-check	1. Verify virtual PMAC 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`
		Note: If this command provides no output, it is likely that a virtual instance of PMAC is not installed. If there is a virtual PMAC, log into the console of the virtual PMAC.
		2. From the management server, log into the console of the virtual PMAC 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`
		Note: On a TVOE host, if you open 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 the virsh console, and run `ps -ef |grep virsh`, then kill the existing process `$ sudo kill -9 <PID>`. Execute the `$ sudo virsh console X` command again. Your console session should now run as expected.
		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`

3. ☐	**netConfig Repository**: Configure the netConfig repository	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, 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) (for example, 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?`

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

Step	Procedure	Result
		<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 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.

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

Step	Procedure	Result

4. ☐	**netConfig Server**: Verify FW file is in correct location with 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 PMAC.
		`$ 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 PMAC.
		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 JSON file exists and modify with site information	1. 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 PMAC from the application media using application provided procedures. 2. Modify the JSON file(s) with necessary site information

6. ☐	**netConfig Server**: Initialize and configure the switches	The configureSwitch utility allows initialization/configuration of one or many switches with a single execution. If desired, 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 (for example, 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>`

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

Step	Procedure	Result

7. ☐	**Virtual PMAC**: Verify firmware update	Verify if a final reboot is needed by making sure 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 is 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.

8. ☐	**Virtual PMAC**: Verify proper configuration of switches	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 it is configured as per site requirements.
		It is important to note that the output of **showConfiguration** provides data 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. ☐	Back up HP for each switch	Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure.

3.2.4 Replace a Failed 4948/4948E/4948E-F Switch (PMAC Installed) (netConfig)

This procedure replaces a failed 4948/4948E/4948E-F switch.

This procedures assumes a PMAC 6.6 interconnect. If the system being configured follows a different platform interconnect, then the appropriate platform procedures should be followed.

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC
- 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] HP Solutions Firmware Upgrade Pack.

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

Ethernet Interface	DL 360	DL 380	X3-2	X5-2 and X6-2	X7-2
<ethernet_interface_1>	eth01	eth01	eth01	eth01	eth02
<ethernet_interface_2>	eth02	eth02	eth02	eth03	eth03

Variable	Platform 7.6
<management_server_switchport>	gi1/40

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Filenames and sample command line input/output throughout this procedure 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 is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result
1. ☐	**Cabinet**: Power off 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	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 before removal.
3. ☐	**Cabinet**: Replace switch	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 cable 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.

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

6. ☐	**Virtual PMAC**: Verify IOS image is on system	If the appropriate image does not exist, copy the image to the PMAC.
		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=switch1A getFirmware`
		If replacing switch1B:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B 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 PMAC.
		`$ 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 PMAC**: Modify PMAC 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`
		This may take up to 60 seconds to complete.

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

8. ☐	**Management Server**: Manipulate host server physical interfaces	Exit from the virtual PMAC console, by pressing **Ctrl-]** and you are returned to the server prompt.
		Ensure 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>.
		`$ sudo /usr/bin/virsh console vm-pmac1A`
		Note: On a TVOE host, if you open 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 the virsh console, and run `ps -ef |grep virsh`, then kill the existing process `$ sudo kill -9 <PID>`. Execute the `$ sudo virsh console X` command again. Your console session should now run as expected.

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result
9. ☐	**Management Server**: Get PROM information	***Note***: ROM and PROM are intended to have the same meaning for this procedure. Connect to switch and 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 (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.

10. ☐	**Virtual PMAC**: Reset switch to factory defaults	Connect serially to the switch and reload the switch by issuing the following commands:
		`Switch# write erase`
		`Switch reload`
		Wait until the switch reloads, then exit from console; press **<Ctrl-e><c><.>** and you are 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**.

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

11. ☐	**Virtual PMAC**: Initialize switch	Older platform init files may not work on Platform 7.6 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`
		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/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 My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify 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`

12. ☐	**Virtual PMAC**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		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`

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

13. ☐	**Virtual PMAC**: 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`

14. ☐	**Virtual PMAC**: Restore	`$ 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`
		Note: If the command failed with error message same as or similar to **Error saving to service**, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to **Error! Reference source not found.**.

15. ☐	**Virtual PMAC**: Make sure both interfaces are enabled on the TVOE host	Connect to the TVOE host and ensure 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>`

16. ☐	**Virtual PMAC**: 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>`

17. ☐	**Virtual PMAC**: Verify switch is using proper IOS image per platform version	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`

18. ☐	**Cabinet**: Connect cables from customer network	Attach 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.

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

19. ☐	**Virtual PMAC**: 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. ☐	**Virtual PMAC**: Clean up 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>`

3.2.5 Replace a Failed 4948/4948E/4948E-F Switch (RMS System, No PMAC Installed) (netConfig)

This procedure replaces a failed 4948/4948E/4948E-F switch.

This procedure assumes a Platform 7.6 interconnect. If the system being configured follows a different platform interconnect, then the appropriate platform procedures should be followed.

Prerequisites:

- Complete 8.1 IPM Management Server before this procedure is attempted.
- A fully configured and operational redundant switch must be in operation. 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 before 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] HP Solutions Firmware Upgrade Pack.

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>	

Variable	Value
<switch1A_mgmtVLAN_IP_address>	
<switch1B_mgmtVLAN_IP_address>	
<switch_mgmtVLAN_ID>	
<management_server_iLO_IP>	
<switch_backup_user>	admusr
<switch_backup_user_password> Check application documentation	

Ethernet Interface	DL 360	DL 380	X3-2	X5-2 and X6-2	X7-2
<ethernet_interface_1>	eth01	eth01	eth01	eth01	eth02
<ethernet_interface_2>	eth02	eth02	eth02	eth03	eth03

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Filenames and sample command line input/output throughout this procedure 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 is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result
1. ☐	**Cabinet**: Power off 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	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 before removal.
3. ☐	**Cabinet**: Replace switch	Remove failed switch and replace with new switch of same model.

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result
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 cable 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 IOS image is on 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/TFTP directory.
		To check the FW on the mate switch, use the following command:
		If replacing switch1A:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware`
		If replacing switch1B:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B 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 management server 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/`

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

7. ☐	**Management Server**: Enable tftp on the system for tftp transfer of IOS upgrade file	`$ 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 firewall is configured	`$ 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**: Manipulate host server physical interfaces	Ensure the interface of the server connected to the switch 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>

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result
10. ☐	**Management Server**: Get PROM information	***Note***: ROM and PROM are intended to have the same meaning for this procedure. Connect to switch and 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 (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.

11. ☐	**Management Server**: Reset switch to factory defaults	Connect serially to the switch and reload the switch by issuing the following commands:
		`Switch# write erase`
		`Switch reload`
		Wait until the switch reloads, then exit from console; press **<Ctrl-e><c><.>** and you are 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**.

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

12. ☐	**Management Server**: Initialize switch	Older platform init files may not work on Platform 7.6 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`
		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/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 My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify 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`

13. ☐	**Management Server**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		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`

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

14. ☐	**Management Server**: Initialize switch	Older platform init files may not work on Platform 7.6 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`
		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/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 My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify 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`

15. ☐	**Management Server**: Verify switch is using proper IOS image per platform version	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		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`

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

16. ☐	**Management Server**: Disable TFTP	`$ 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 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.

17. ☐	**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"`
18. ☐	**Management Server**: Verify the firewall is configured properly	`$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter` `Persist Domain Table Chain Match`

19. ☐	**Management Server**: 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`
		`switch1A-backup.vlan`

20. ☐	**Management Server**: Restore	`$ 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`
		Note: If the command failed with error message same as or similar to **Error saving to service**, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to **Error! Reference source not found.**.

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

Step	Procedure	Result

21. ☐	**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>`

22. ☐	**Management Server**: Verify switch is using proper IOS image per platform version	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`

23. ☐	**Cabinet**: Connect cables from customer network	Attach 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**: 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`

25. ☐	**Management Server**: Clean up 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>`

3.2.6 Replace a Failed 9372TX-E Switch (PMAC Installed) (netConfig)

This procedure replaces a failed 9372TX-E switch.

This procedure assumes a healthy PMAC with the original netConfig repository intact. If this is not the case and a PMAC disaster recovery needs to be performed, see [7] PMAC Disaster Recovery, Release 6.6.. If a PMAC does not exist and a DR is not possible, disregard this procedure and perform 3.2.3 Configure Cisco 9372TX-E Aggregation Switches (PMAC 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 PMAC, 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. 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 PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments allow for future simplification of network configuration procedures.

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
<switch_backup_user_password> Check application documentation	
<fw_filename> The firmware version must match the operational redundant switch. This is checked in a procedural step.	
<switch_backup_user_home_directory> /usr/TKLC/smac/etc/switch/backup	
<management_server_mgmtInterface>	
<management_server_mgmt_IP_address>	

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

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

Needed Material: Cisco FW file acquired through My Oracle Support (MOS).

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 7. Replace a Failed 9372TX-E Switch

Step	Procedure	Result
1. ☐	**Cabinet**: Power off 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	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 before removal.
3. ☐	**Cabinet**: Replace switch	Remove failed switch and replace with new switch of same model.

Procedure 7. Replace a Failed 9372TX-E Switch

Step	Procedure	Result
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 cable 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 PMAC**: Verify IOS image is on system	If the appropriate image does not exist, copy the image to the PMAC.
		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:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=<mate_switchname> getFirmware`
		`Version: 7-0.I4.2`
		`Flash: nxos.7.0.3.I4.bin`
		Determine if the IOS image for the 9372TX-E is on the virtual PMAC.
		`$ sudo /bin/ls -l <switch_backup_directory>/<fw_filename>`
		or
		`$ sudo /bin/ls -l /var/TKLC/upgrade/<fw_filename>`
		If the FW file exists, verify a symbolic link exists to the firmware file in the backup user directory by using the following command:
		If the file is in the backup directory copy it to the TFTP directory:
		`$ 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 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>`

Procedure 7. Replace a Failed 9372TX-E Switch

Step	Procedure	Result

		`$ 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 PMAC, 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	This step only pertains to failed switches in the first frame with a switchID of A or B. In other words, the switches that host the management server interface. 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 the next step.
		Connect to the management server and perform 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>.
		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>.

Procedure 7. Replace a Failed 9372TX-E Switch

Step	Procedure	Result

8. ☐	**Virtual PMAC**: Initialize 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 PMAC**: Copy switch backup file	Copy the switch backup files to the home directory of the <switch_backup_user> 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 PMAC**: Restore	`$ 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`
		Note: If the command failed with error message same as or similar to **Error saving to service**, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to **Error! Reference source not found.**.

11. ☐	**Management Server**: Make sure both interfaces are enabled host server	Connect to the management server perform the following commands:
		`$ sudo /sbin/ifup <ethernet_interface_1>`
		`$ sudo /sbin/ifup <ethernet_interface_2>`

12. ☐	**Cabinet**: Connect cables from customer network	Attach customer uplink cables. Refer to application documentation for which ports are uplink ports.

13. ☐	**Virtual PMAC**: Verify proper configuration of switches	Verify network reachability and configuration.
		`$ /bin/ping -w3 <switch_IP>`
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> showConfiguration`
		Inspect the **showConfiguration** output to ensure it is configured per site requirements.
		Note the **showConfiguration** output provides output in vendor-specific syntax/language. Look for the existence of expected VLANs and IP addresses to verify the configuration is correct.

Procedure 7. Replace a Failed 9372TX-E Switch

Step	Procedure	Result

14. ☐	**Management Server**: Clean up 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>`

3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)

This procedure backs up the Cisco aggregation and enclosure switches.

***Prerequisites* for RMS system aggregation switch**:

- 8.1 IPM Management Server
- Step 2 of 9.1 Install TVOE on the Management Server to install the IPM DL380 server.
- 9.2 Configure TVOE Network
- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.

***Prerequisites* for c-Class system aggregation switch (Oracle-provided)**:

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)

***Prerequisites* for Cisco 3020 enclosure switch**:

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 3.3.1 Configure Cisco 3020 Switch (netConfig)

Variable	Value
<switch_backup_user> (also needed in switch configuration procedure)	admusr
<switch_backup_user_password> (also needed in switch configuration procedure) Check application documentation	
<switch_name> Hostname of the switch	

Variable	Value
<switch_backup_directory> Non-PMAC System: /usr/TKLC/plat/etc/switch/backup PMAC System: /usr/TKLC/smac/etc/switch/backup	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 8. Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch

Step	Result

1. ☐	Verify switch is initialized correctly and connectivity to the switch by verifying the 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 the **netConfig --repo showService name=ssh_service** command 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:** is the value for the variable <switch_backup_user>.

3. ☐	Verify existence of the backup directory.
	`$ sudo /bin/ls -i <switch_backup_directory>`
	If the output contains:
	`ls: cannot access <switch_backup_directory>: No such file or directory`
	Create the directory with:
	`$ sudo /bin/mkdir -p <switch_backup_directory>`
	Change directory permissions:
	`$ sudo /bin/chmod go+x <switch_backup_directory>`
	If this is a PMAC 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` ***Note***: If the command failed with error message same as or similar to **Error saving to service**, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to **Error! Reference source not found.**.

Procedure 8. Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch

Step	Result

5. ☐	Verify switch configuration was backed up by **cat <switch_name>** and inspect its contents to ensure it reflects the latest known good switch configurations. Copy the files to the backup directory.
	`$ sudo /bin/ls -i ~<switch_backup_user>/<switch_name>-backup*`
	`$ sudo /bin/cat ~<switch_backup_user>/<switch_name>-backup*`
	`$ sudo /bin/chmod 644 <switch_name>-backup*`
	`$ sudo /bin/mv -i ~admusr/<switch name>-backup* <switch_backup_directory>/`
	Note: The cat command may leave garbled text on the next terminal prompt. Disregard this text.
	Example:
	`[admusr@pmac ~]$`
	`PuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPu`

6. ☐	Back up the PMAC application.
	`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
	`PMAC backup has 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 PMAC GUI Task Monitor screen, or issue the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
	Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.

7. ☐	Verify PMAC backup was successful.
	Note: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
	The output of pmaccli getBgTasks should look similar to the example below:
	`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
	`2: Backup PMAC COMPLETE - PMAC 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:`
	`::`

Procedure 8. Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch

Step	Result
8. ☐	Save the PMAC backup. The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.

9. ☐	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 PMAC system:
	`$ sudo /bin/mv -i /var/TKLC/smac/image/<fw_image> <switch_backup_directory>/`
	If on a non-PMAC 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.

10. ☐	Repeat steps 1. and 4. through 6. for each switch to be backed up.

3.2.8 Replace a Failed Telco T5C-24GT

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

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 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
<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_24_firmware_image_file>	

Variable	Value
<Remote_customer_target_IP>	

Notes:

- See the T1200 Solutions Firmware Upgrade Pack (Tekelec part# 909-1618-001) for appropriate T5CL3_24G firmware image.
- The <Remote_customer_target_IP> is identified later in this procedure.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 9. Replace a Failed Telco T5C-24GT

Step	Procedure	Result
1. ☐	**Telco T5CL3_24G**: Power off failed switch	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**: Replace 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** is the value for the variable <switch_backup_user>.
3. ☐	**Management Server RMM**: Login	Log into the Remote Management module (RMM) using Internet Explorer with the <T1200_server_RMM_user> and <T1200_server_RMM_user_password>. http://<T1200_server_RMM_IP>
4. ☐	**Management Server RMM**: Log into the Telco T1200 remote console	Click the Console icon in the upper left corner to launch the Remote Console on the server. Click **Don't Block** if the Security Warning window displays. ***Note***: Different versions of Internet Explorer may present additional security prompts. If not already done, login as **admusr** using the <T1200_server_password> password.

5. ☐	**Management Server**: Verify console connection	Determine whether needed minicom files are already available by issuing the following command:
		`$ /bin/ls -l /etc/minirc.*`
		If the **minirc.<Telco_switch_name>** file is not listed, 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`

Procedure 9. Replace a Failed Telco T5C-24GT

Step	Procedure	Result

6. ☐	**Management Server**: Connect serially to the switch	`$ 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 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, restore the factory default configuration by typing:
		`T5C-24GT# write erase`
		`wait …`
		`T5C-24GT# reload no-save`
		`Proceed with reload? [y/n] : y`
		`Rebooting…`
		`[Additional output omitted]`
		The switch reboots to the factory default configuration. The following displays:
		`User Access Verification`
		`Password:`

7. ☐	**Management Server**: Exit the switch console and minicom session	Type **exit** and press **Enter** to exit the console session. Exit the minicom session: 1. Press **Ctrl-A**. 2. Press **X**. 3. Press **Enter**.

8. ☐	**Management Server**: Verify the switch configuration file 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 My Oracle Support (MOS).

9. ☐	**Management Server**: Verify the switch firmware binary exists	`$ /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 (MOS).

Procedure 9. Replace a Failed Telco T5C-24GT

Step	Procedure	Result

10. ☐	**Management Server**: Verify TFTP service is enabled	`$ /sbin/chkconfig --list tftp`
		`tftp off`
		If the tftp service is set to **off**, turn on tftp by issuing the following command:
		`$ sudo /sbin/chkconfig tftp on`
		Verify that it is now enabled:
		`$ /sbin/chkconfig --list tftp`
		`tftp on`

11. ☐	**Management Server**: Verify 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 ]`

12. ☐	**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`

13. ☐	**Management Server**: Verify firewall is configured properly	`$ 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`

Procedure 9. Replace a Failed Telco T5C-24GT

Step	Procedure	Result

14. ☐	**Management Server**: Configure the switch	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 takes approximately 20 minutes to complete.

15. ☐	**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:`

16. ☐	**Management Server**: Disable TFTP services	Disable the tftp service by running the following command: `$ sudo /sbin/chkconfig tftp off`
17. ☐	**Telco T5CL3_24G**: Connect uplink cables	Connect the uplink cables from the new Telco switch to the customer network.

18. ☐	**Management Server**: Test 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:
		1. 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`
		2. On the mated Management server connected to the mated Telco switch, force it to use eth02 by running the following command:

Procedure 9. Replace a Failed Telco T5C-24GT

Step	Procedure	Result
		`$ 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 (MOS). 3. On the new/replacement Telco switch, unplug the customer uplink cables. 4. Verify 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 (MOS). • If the pings continue, this verifies 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. 5. Replace the uplink cables to the customer network on the replacement Telco switch. 6. On the mated Telco switch, unplug the customer uplink cables. 7. Verify 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 (MOS). • If the pings continue, this verifies traffic is flowing over the replacement Telco switch to the customer network and over the ISL and that both switches are functioning as expected. 8. Replace the uplink cables to the customer network on the replacement Telco switch.

Procedure 9. Replace a Failed Telco T5C-24GT

Step	Procedure	Result

19. ☐	**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 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.

20. ☐	**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"`
21. ☐	**Management Server**: Verify the firewall is configured properly	`$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter` `Persist  Domain  Table  Chain  Match`

3.3 C-Class Enclosure Switch — netConfig Procedures

3.3.1 Configure Cisco 3020 Switch (netConfig)

This procedure configures 3020 switches from the PMAC server using templates included with an application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- If the aggregation switches are supported by Oracle, the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the 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 (MOS) for assistance.

- No IPM switches activity can occur during the execution of this procedure.

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

Needed Material

- HP MISC Firmware ISO image
- Refer to the [4] Oracle Firmware Upgrade Pack Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 10. Configure Cisco 3020 Switch (netConfig)

Step	Procedure	Result
1. ☐	**Virtual PMAC**: Prepare for switch configuration	Login as **admusr** to the PMAC, then run: `$ /bin/ping -w3 <mgmtVLAN_gateway_address>`
2. ☐	**Virtual PMAC**: Verify network connectivity	For each 3020 switch, verify network reachability. `$ /bin/ping -w3 <enclosure_switch_IP>`

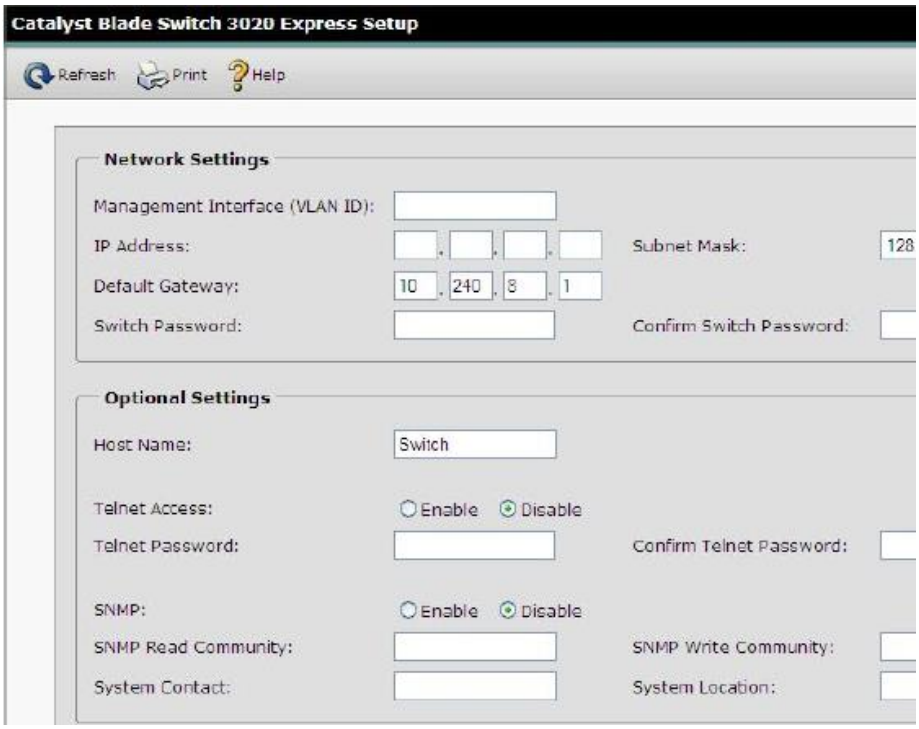
3. ☐	**Virtual PMAC**: Modify PMAC feature to allow TFTP	Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=1`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Note: This may take up to 60 seconds to complete.

4. ☐	**Virtual PMAC**: Verify template xml files exist	Verify the **initialization xml** and **configuration xml** template files 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 alternatives.
		`$ /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.
		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 continue to step 6.
		If 3020_configure.xml file exists, page through the contents to verify it is the appropriate file for this site and edited for this site. All network information is necessary for this activity. If the template file is appropriate, then continue to step 6.

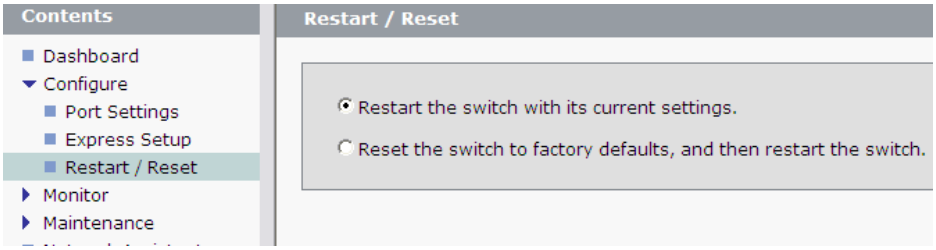
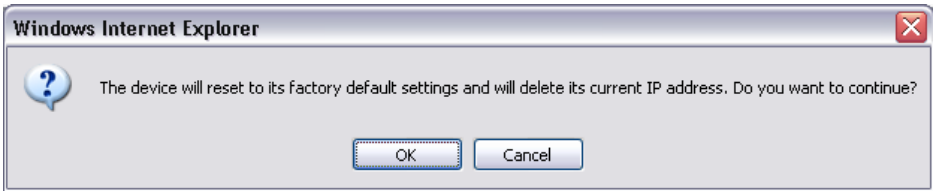
Procedure 10. Configure Cisco 3020 Switch (netConfig)

Step	Procedure	Result

5. ☐	**Virtual PMAC**: Modify 3020 xml files for information needed to configure the switch	Update 3020_init.xml file:
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_init.xml`
		Update 3020_configure.xml file:
		`sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_config.xml`
		Note: Modify values notated with a preceding dollar sign. So a value with `$some_variable_name` needs to be modified. Remove the dollar sign and the less than, greater than sign.
		When editing is complete, save the file and quit.

6. ☐	**Virtual PMAC/OA GUI**: Reset switch to factory defaults	1. 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 command fails, use Internet Explorer to navigate to <enclosure_switch_ip_address>. 2. If you are asked for a username and password, leave the username blank and use the appropriate password provided by the application documentation. 3. Click **OK**. 4. If you are prompted with the Express Setup screen, click **Refresh**.  5. If you are prompted with **Do you want a secured session with the switch?**, click **No**. A new Catalyst Blade Switch 3020 Device Manager displays.

Procedure 10. Configure Cisco 3020 Switch (netConfig)

Step	Procedure	Result
		6. Navigate to **Configure -> Restart/Reset**.  7. Select the **Reset the switch to factory defaults, and then restart the switch** option. 8. Click **Submit**. 9. Click **OK** to continue with the reset.  ***Note***: Do not wait for the switch to finish reloading before proceeding to the next step.

7. ☐	**Virtual PMAC**: 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 returns 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 (MOS).

Procedure 10. Configure Cisco 3020 Switch (netConfig)

Step	Procedure	Result

8. ☐	**Virtual PMAC**: 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 PMAC**: Validate XML file	This script validates the XML file to a limited extent. It verifies:
		• The file is valid
		• All required options for commands are present
		• All provided options for commands are valid
		• SOME, but not all, option values
		To validate the XML file:
		`$ 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 above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.

10. ☐	**Virtual PMAC**: 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 may take up to 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

Procedure 10. Configure Cisco 3020 Switch (netConfig)

Step	Procedure	Result

11. ☐	**Virtual PMAC**: 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 PMAC**: Modify PMAC 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. ☐	**Virtual PMAC**: Repeat	Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) for each switch configured in this procedure.
14. ☐	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f /var/TKLC/smac/image/<FW_image>`

3.3.2 Replace a Failed 3020 Switch (netConfig)

This procedure configures a replacement 3020 switch.

Prerequisite: User has determined which switch has failed.

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] HP Solutions Firmware Upgrade Pack.

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

Needed Material: HP MISC firmware ISO image

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 11. Replace a Failed 3020 Switch

Step	Procedure	Result
1. ☐	**Cabinet**: Replace switch	Remove failed switch and replace with new switch of same model.
2. ☐	**Cabinet**: Attach cable to new switch	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.

3. ☐	**Virtual PMAC**: 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 PMAC System:
		`$ sudo /bin/mv -i <switch_backup_directory/<FW_image> /var/TKLC/smac/image/`
		For a non-PMAC 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. ☐	**Virtual PMAC**: Apply configuration	Perform 3.3.1 Configure Cisco 3020 Switch (netConfig), steps 3. through 9. and 12. , replacing the values for the switch being replaced.

5. ☐	**Virtual PMAC**: 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 PMAC**: Copy switch backup file	Copy the switch backup files to the home directory of the <switch_backup_user> by performing the following command:
		`$ 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`

Procedure 11. Replace a Failed 3020 Switch

Step	Procedure	Result

7. ☐	**Virtual PMAC**: Verify switch is initialized	Verify switch is initialized correctly and connectivity to the switch by verifying the 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.

8. ☐	**Virtual PMAC**: Restore	`$ 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`
		Note: If the command failed with error message same as or similar to **Error saving to service**, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to **Error! Reference source not found.**.

9. ☐	**Virtual PMAC**: Verify connectivity	Perform 3.3.1 Configure Cisco 3020 Switch (netConfig), step 10.

10. ☐	**Virtual PMAC**: Clean up 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>`

3.3.3 Configure HP 6120XG Switch (netConfig)

This procedure configures the HP 6120XG switches from the PMAC server and the command line interface using templates included with an application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- If the aggregation switches are supported by Oracle, the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the 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 (MOS) for assistance.
- Must be able to issue commands on the switch command line interface

Needed Material

- HP MISC Firmware ISO image

- Refer to the [4] Oracle Firmware Upgrade Pack Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

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.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 12. Configure HP 6120XG Switch

Step	Procedure	Result

1. ☐	**Virtual PMAC**: Prepare for switch configuration	If aggregation switches are supported by Oracle, log into the management server as admusr to the PMAC, then run:
		`$ /bin/ping -w3 <switch1A_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch1B_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch_mgmtVLAN_VIP>`
		If aggregation switches are provided by customer, log into the management server as admusr to the PMAC, then run:
		`$ /bin/ping -w3 <mgmtVLAN_gateway_address>`

2. ☐	**Virtual PMAC**: Verify network connectivity	For each 6120XG switch, verify network reachability. `$ /bin/ping -w3 <enclosure_switch_IP>`

Procedure 12. Configure HP 6120XG Switch

Step	Procedure	Result

3. ☐	**Virtual PMAC**: Reset switch to factory defaults	If the 6120XG switch has been configured before this procedure, clear 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 command fails, login using 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 fails.

4. ☐	**Virtual PMAC**: Copy switch configuration template from media to 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 of these files:
		• 6120XG_SingleUplink_configure.xml is for one uplink per enclosure switch topology
		• 6120XG_LAGUplink_configure.xml is for LAG uplink topology

Procedure 12. Configure HP 6120XG Switch

Step	Procedure	Result

5. ☐	**Virtual PMAC**: Verify switch configuration	Verify the switch initialization and configuration template files 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 PMAC**: Edit switch configuration file template for site-specific information	Modify values notated with a preceding dollar sign (for example, addresses and VLAN IDs). So a value with `$some_variable_name` needs to be modified. Remove the dollar sign and the less than, greater than sign.
		Note: Files created in this step can be prepared ahead of time using NAPD.
		`$ 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 PMAC**: Apply `include-credentials` command to the switch	Log into 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`

8. ☐	**Virtual PMAC**: Initialize the switch	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6120XG_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 5-10 minutes to complete.
		The user is returned to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS).

Procedure 12. Configure HP 6120XG Switch

Step	Procedure	Result
9. ☐	**Virtual PMAC**: Validate XML file	This script validates the XML file to a limited extent. It verifies: • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values To validate the XML file: `$ 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 above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.

10. ☐	**Virtual PMAC**: 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/6120XG_[single,LAG]Uplink_configure.xml`
		Note: This may take up to 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

11. ☐	**Virtual PMAC**: Apply QoS settings	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml` ***Note***: The switch reboots after this command. This step takes 2-5 minutes.

12. ☐	**Virtual PMAC**: Verify proper configuration of switches	Verify network reachability and configuration.
		`$ /bin/ping -w3 <enclose_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 and ensure it is configured per site requirements.

13. ☐	**Virtual PMAC**: Repeat	Repeat steps 3. through 12. for each HP 6120XG.
14. ☐	Back up HP for each switch	Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure.

Procedure 12. Configure HP 6120XG Switch

Step	Procedure	Result
15. ☐	**Virtual PMAC**: Clean up FW	Remove the FW image from the users' home directory and TFTP directory with the following command: `$ sudo /bin/rm -f ~<switch_backup_user>/<fw_filename>`

3.3.4 Configure HP 6125G Switch (netConfig)

This procedure configures the HP 6125G switches from the PMAC server and the command line interface using templates included with the application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- Must be able to issue commands on the switch command line interface
- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the 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 (MOS) for assistance.

Needed Material

- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 13. Configure HP 6125G Switch

Step	Procedure	Result

1. ☐	**Virtual PMAC**: Prepare for switch configuration	If the aggregation switches are supported by Oracle, login as **admusr** to the PMAC, 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 as **admusr** to the PMAC, then run:
		`$ /bin/ping -w3 <mgmtVLAN_gateway_address>`

2. ☐	**Virtual PMAC**: Verify network connectivity	For each OA, verify network reachability.
		`$ /bin/ping -w3 <OA1_IP>`
		`$ /bin/ping -w3 <OA2_IP>`

3. ☐	**Virtual PMAC**: Determine which OA is	Login to OA1 to determine if it is active: `$ /usr/bin/ssh root@<OA1_IP>` The OA is active if you see the following:

Procedure 13. Configure HP 6125G Switch

Step	Procedure	Result
	currently active	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 monitored 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 monitored 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 into 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 monitored 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 refers to the **active OA** and <active_OA_IP> refers to the **IP address** of the active OA. ***Note***: If no OA reports active, STOP and contact My Oracle Support (MOS). Exit the SSH session.
4. ☐	**Virtual PMAC**: Restore switch to factory	If the 6125G switch has been configured before this procedure, clear the configuration using the following command:

Procedure 13. Configure HP 6125G Switch

Step	Procedure	Result

	defaults	`$/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 monitored 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 automatically reboots. This takes 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 pressing **Ctrl + Shift + -**, then **d**.
		Note: If connecting to the virtual PMAC through the management server iLO then Appendix E.1 Access a Server Console Remotely applies. Disconnect from the console by pressing **Ctrl +v**.
		Exit from the OA terminal:
		`>exit`
		Note: The console connection to the switch must be closed or the initialization fails.

Procedure 13. Configure HP 6125G Switch

Step	Procedure	Result
5. ☐	**Virtual PMAC**: Copy switch configuration template from media to 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 PMAC**: Verify switch configuration	Verify the switch initialization and configuration template files are in the TFTP 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 PMAC**: Edit switch configuration file template for site-specific information	Modify values notated with a preceding dollar sign (for example, addresses and VLAN IDs). So a value with `$some_variable_name` needs to be modified. Remove the dollar sign and the less than, greater than sign.
		Note: Files created in this step can be prepared ahead of time using NAPD.
		`$ 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 PMAC**: Initialize the switch	***Note***: The console connection to the switch must be closed or the initialization fails. `$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6125G_init.xml` ***Note***: This step takes 5-10 minutes to complete.

9. ☐	**Virtual PMAC**: Verify switch initialized	`$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_hostname>`
		`Hostname: <switch_hostname>`
		Note: This step takes 2-3 minutes to complete.
		The user is returned to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS).

10. ☐	**Virtual PMAC**	Execute Appendix J Downgrade Firmware on a 6125G Switch to verify the existing firmware version and downgrade if required

Procedure 13. Configure HP 6125G Switch

Step	Procedure	Result
11. ☐	**Virtual PMAC**: Validate XML file	This script validates the XML file to a limited extent. It verifies: • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values To validate the XML file: `$ 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 above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.

12. ☐	**Virtual PMAC**: Configure the switch	Configure the switch by issuing the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6125G_configure.xml`
		`Processing file: /usr/TKLC/smac/etc/switch/xml/6125G_configure.xml`
		Note: This may take up to 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

13. ☐	**Virtual PMAC**: Add 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 PMAC**: Verify proper configuration of 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 it is configured as per site requirements.

15. ☐	**Virtual PMAC**: Repeat	Repeat steps 4. through 14. for each HP 6125G switch.
16. ☐	**Virtual PMAC**	Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure.

Procedure 13. Configure HP 6125G Switch

Step	Procedure	Result
17. ☐	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>`

3.3.5 Configure HP 6125XLG Switch (netConfig)

This procedure configures the HP 6125XLG switches from the PMAC server and the command line interface using templates included with the application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- Must be able to issue commands on the switch command line interface
- If the aggregation switches are supported by Oracle, the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the 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 (MOS) for assistance.

Needed Material

- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 14. Configure HP 6125XLG Switch

Step	Procedure	Result

1. ☐	**Virtual PMAC**: Prepare for switch configuration	If the aggregation switches are supported by Oracle, login as **admusr** to the PMAC, 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 as **admusr** to the PMAC, then run:
		`$ /bin/ping -w3 <mgmtVLAN_gateway_address>`

2. ☐	**Virtual PMAC**: Verify network connectivity	For each OA, verify network reachability.
		`$ /bin/ping -w3 <OA1_IP>`
		`$ /bin/ping -w3 <OA2_IP>`

3. ☐	**Virtual PMAC**: Determine which OA is	Login to OA1 to determine if it is active: `$ /usr/bin/ssh root@<OA1_IP>` The OA is active if you see the following:

Procedure 14. Configure HP 6125XLG Switch

Step	Procedure	Result

	currently active	`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 monitored 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 monitored 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 into 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 monitored 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 refers to the **active OA** and <active_OA_IP> refers to the **IP address** of the active OA.
		Note: If no OA reports active, STOP and contact My Oracle Support (MOS).
		Exit the SSH session.

4. ☐	**Virtual PMAC**: Restore switch to factory defaults	If the 6125XLG switch has been configured before this procedure, clear 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 monitored and can result in criminal or civil prosecution under applicable law.`

Procedure 14. Configure HP 6125XLG Switch

Step	Procedure	Result
		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 automatically reboots. This takes 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 pressing **Ctrl + Shift + -**, then **d**. ***Note***: If connecting to the virtual PMAC through the management server iLO then Appendix E.1 Access a Server Console Remotely applies. Disconnect from the console by pressing **Ctrl +v**. Exit from the OA terminal: >exit ***Note***: The console connection to the switch must be closed or the initialization fails.
5. ☐	**Virtual PMAC**: Copy switch configuration template from media to TFTP 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

Procedure 14. Configure HP 6125XLG Switch

Step	Procedure	Result

6. ☐	**Virtual PMAC**: Verify switch configuration	Verify the switch initialization and configuration template files are in the TFTP 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 PMAC**: Edit switch configuration file template for site-specific information	Modify values notated with a preceding dollar sign (for example, addresses and VLAN IDs). So a value with `$some_variable_name` needs to be modified. Remove the dollar sign and the less than, greater than sign.
		Note: Files created in this step can be prepared ahead of time using NAPD.
		`$ 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 PMAC**: Initialize the switch	***Note***: The console connection to the switch must be closed or the initialization fails. `$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6125XLG_init.xml` ***Note***: This step takes 5-10 minutes to complete.

9. ☐	**Virtual PMAC**: Verify switch initialized	`$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_hostname>`
		`Hostname: <switch_hostname>`
		Note: This step takes 2-3 minutes to complete.
		The user is returned to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS).

10. ☐	**Virtual PMAC**: Validate XML file	This script validates the XML file to a limited extent. It verifies: • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values To validate the XML file: `$ 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 above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.

Procedure 14. Configure HP 6125XLG Switch

Step	Procedure	Result

11. ☐	**Virtual PMAC**: Configure the switch	Configure the switch by issuing the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml`
		`Processing file: /usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml`
		Note: This may take up to 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 My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

12. ☐	**Virtual PMAC**: Add 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 PMAC**: Verify proper configuration of 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 it is configured as per site requirements.

14. ☐	**Virtual PMAC**	For HP 6125XLG switches connected by 4x1GE LAG uplink perform Utility procedure 3.4.9 Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig); otherwise, for deployments with 10GE uplink, continue to the next step.
15. ☐	**Virtual PMAC**: Repeat	Repeat steps 4. through 14. for each HP 6125XLG switch.
16. ☐	**Virtual PMAC**	For HP 6125XLG switches linking 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 14. For HP 6125XLG switches linking with 4x1GE LAG to product Cisco 4948/E/EF aggregation switches, perform Utility Procedure 3.4.10 Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig), to match speed and duplex settings from 14.
17. ☐	**Virtual PMAC**	Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure.

Procedure 14. Configure HP 6125XLG Switch

Step	Procedure	Result
18. ☐	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>`

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

This procedure configures a replacement HP switch.

Prerequisite: User has determined which switch has failed.

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] HP Solutions Firmware Upgrade Pack.

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

Needed Material: HP MISC firmware ISO image

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

Step	Procedure	Result
1. ☐	**Cabinet**: Replace switch	Remove failed switch and replace with new switch of same model.

2. ☐	**Virtual PMAC**: 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:
		`$ sudo /bin/mv -i <switch_backup_directory/<FW_image> ~<switch_backup_user>/`
		Note: If the file does not exist on the server, copy it from the firmware media.
		`$ sudo /bin/chmod 644 <tftp_directory>/<FW_image>`

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

Step	Procedure	Result
3. ☐	**Virtual PMAC**: Initialize switch	For a 6120XG: Perform 3.3.3 Configure HP 6120XG Switch (netConfig), steps 3. -4. , 6. (init.xml only), and 8. Return to this procedure, and continue with the next step. For a 6125G: Perform 3.3.4 Configure HP 6125G Switch (netConfig), steps 3. -4. , 6. (init.xml only), and 8. Return to this procedure, and continue with the next step. For a 6125XLG: Perform 3.3.5 Configure HP 6125XLG Switch (netConfig), steps 3. , 4. -6. (init.xml only), and 8. Return to this procedure, and continue with the next step.
4. ☐	**Virtual PMAC**: Copy switch backup file	Copy the switch backup files to the home directory of the <switch_backup_user> by performing the following command: `$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup* ~<switch_backup_user>/`
5. ☐	**Virtual PMAC**: Prepare to restore	`$ cd ~<switch_backup_user>` `$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*`

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

Step	Procedure	Result

6. ☐	**Virtual PMAC**: Prepare to restore	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 that does not currently exist on the switch ahead of the restore operation. Identify any port channels 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 port channel 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 PMAC**: Restore	`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> restoreConfiguration service=ssh_service filename=<switch_hostname>-backup` ***Note***: The switch reboots. It takes approximately 120-180 seconds before connectivity is restored.
8. ☐	**Cabinet**: Attach cable to new switch	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.

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

Step	Procedure	Result
9. ☐	**Virtual PMAC**: Verify connectivity	For a 6120XG: Refer to 3.3.3 Configure HP 6120XG Switch (netConfig), steps 10. -12. Apply QoS policy and verify connectivity. For a 6125G: Refer to 3.3.4 Configure HP 6125G Switch (netConfig), step 17. For a 6125XLG: Refer to 3.3.5 Configure HP 6125XLG Switch (netConfig), step 11.

10. ☐	**Virtual PMAC**: Clean up 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>`

3.4 Utility Procedures

3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch

Execute this procedure after every change to a switch configuration or after completing 3.3.3 Configure HP 6120XG Switch (netConfig), 3.3.4 Configure HP 6125G Switch (netConfig), or 3.3.5 Configure HP 6125XLG Switch (netConfig).

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

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 these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

Variable	Value
<switch_name> Hostname of switch	
<switch_backup_user>	admusr
<FW_image> FW file used in firmware upgrade/switch replacement/or initial install	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 16. Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch

Step	Procedure	Result

1. ☐	**Target Server**: Ensure directory 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`
		Change the directory permissions:
		`$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/switch/backup`
		Change directory ownership:
		`$ sudo /bin/chown –R pmacd:pmacbackup /usr/TKLC/smac/etc/switch/backup`

2. ☐	Execute backup command	`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup` Note: If the command failed with error message same as or similar to "Error saving to service", and the TPD version is 7.6.0.0.0_88.50.0 or later, please refer to **Error! Reference source not found.**.
3. ☐	Copy files to backup directory	`$ sudo /bin/mv -i ~<switch_backup_user>/<switch_name>-backup* /usr/TKLC/smac/etc/switch/backup`

4. ☐	Verify	Verify switch configuration was backed up by cat <switch_name> and inspect 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	Repeat steps 2. through 4. for each HP switch to back up.

6. ☐	**Virtual PMAC**: Clean up 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>`

3.4.2 Configure SNMP Communities and Trap Servers

This procedure configures SNMP communities and trap servers.

Prerequisites:

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

- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and/or
- 3.3.1 Configure Cisco 3020 Switch (netConfig) and/or
- 3.3.3 Configure HP 6120XG Switch (netConfig) and/or
- 3.3.4 Configure HP 6125G Switch (netConfig) and/or
- 3.3.5 Configure HP 6125XLG Switch (netConfig) and/or

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 these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

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	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 17. Configure SNMP Communities and Trap Servers

Step	Procedure	Result
1. ☐	**Virtual PMAC**: Login	Log into the PMAC Guest.

Procedure 17. Configure SNMP Communities and Trap Servers

Step	Procedure	Result

2. ☐	**Virtual PMAC**	1. Determine which devices require SNMP configuration.
		`$ 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.
		Refer to application documentation to determine which switches to add/remove the community string. Note the DEVICE NAME of each switch. This is used as <switch_name>. In the example output above, DEVICE NAME = 6120XG_IOBAY3, C3020_IOBAY1, and cClassswitch1A.

3. ☐	**Virtual PMAC**: Configure 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>`

Procedure 17. Configure SNMP Communities and Trap Servers

Step	Procedure	Result

4. ☐	**Virtual PMAC**: Configure the SNMP trap server	To ADD a trap server:
		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`
		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:
		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`
		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 PMAC**: 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 PMAC**: Back up the switch configuration	For Cisco, perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig). For 6120XG, perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch.
7. ☐	**Virtual PMAC**: Repeat	Repeat steps 3. through 6. for each device.

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

This procedure configures QoS on HP 6120XG switches.

Prerequisites:

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

- 3.3.3 Configure HP 6120XG Switch (netConfig)

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within **<>**. Refer back to this table for the proper value to insert depending on your system type.

Variable	Value
<switch_name> See Application Documentation and step 2.	
<dscp value> See Application Documentation (if available)	
<cos value> See Application Documentation (if available)	
<switch_platform_username> See Application Documentation	
<VLANID> See Application Documentation	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 18. Configure QoS (DSCP and/or CoS) on HP 6120XG Switches

Step	Procedure	Result
1. ☐	**Virtual PMAC**: Login	Log into the PMAC Guest.

Procedure 18. Configure QoS (DSCP and/or CoS) on HP 6120XG Switches

Step	Procedure	Result

2. ☐	**Virtual PMAC**	1. Determine which devices require QoS policies.
		`$ 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.
		Refer to application documentation to determine which switches or pairs of switches to configure with QoS.. Note the DEVICE NAME of each 6120XG switch. This is used as <switch_name>. In the example output above, DEVICE NAME = 6120XG_IOBAY3, C3020_IOBAY1, and cClassswitch1A.

3. ☐	**Virtual PMAC**: Add DSCP and/or CoS policy	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>`

Procedure 18. Configure QoS (DSCP and/or CoS) on HP 6120XG Switches

Step	Procedure	Result

4. ☐	**Virtual PMAC**: Verify 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 PMAC**: Repeat	Repeat steps 3. through 4. for each policy that needs to be applied to the switch.
6. ☐	**Virtual PMAC**: Back up the switch configuration	Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch.
7. ☐	**Virtual PMAC**: Repeat	Repeat steps 3. through 6. for each switch.

3.4.4 Configure Port Mirroring

This procedure configures port mirroring.

Prerequisites:

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

- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and/or
- 3.3.1 Configure Cisco 3020 Switch (netConfig) and/or
- 3.3.3 Configure HP 6120XG Switch (netConfig) and/or
- 3.3.4 Configure HP 6125G Switch (netConfig) and/or
- 3.3.5 Configure HP 6125XLG Switch (netConfig) and/or

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within **<>**. Refer back to this table for the proper value to insert depending on your system type.

Variable	Value
<switch_name> See Application Documentation and step 2.	
<switch_model> Value from step 2.	

Variable	Value
<switch_IP> Value from step 2.	
<srcInterface> See Application Documentation	
<destInterface> See Application Documentation	
<switch_platform_username> See Application Documentation	
<srcVLANID> See Application Documentation	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 19. Configure Port Mirroring

Step	Procedure	Result
1. ☐	**Virtual PMAC**: Login	Log into the PMAC Guest.

2.
☐
	Virtual PMAC	1. Determine which devices require port mirroring configuration.
		`$ 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`

Procedure 19. Configure Port Mirroring

Step	Procedure	Result
		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. Refer to application documentation to determine which switches to add/remove the community string. Note the DEVICE NAME, MODEL, and IP ADDRESS of each switch. These are used as <switch_name>, <switch_model>, and <switch_IP>.

3. ☐	**Virtual PMAC**: Configure port mirroring	For VLAN Monitoring (Cisco Devices Only):
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addPortMirrorsession=1 vlan=<srcVlanid> destInterface=<mirrorPort> direction=both`
		For Port Mirroring:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addPortMirrorsession=1 sourceInterface=<srcInterface> destInterface=<mirrorPort> direction=both`
		Notes:
		• The interface option allows for more than one source interface. The value can be entered as a single interface, for example, GE1 (1Gb port) or tenGE1 (10Gb port) or it can be entered as a range of interfaces separated by commas and dashes, for example, GE1-5,GE7,tenGE9-10.
		• The only direction supported by the HP switches is **both**. If the direction option is used on an HP switch, it is ignored and **both** is applied.
		VLAN Example:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=C3020_IOBAY1 addPortMirrorsession=1 vlan=2 destInterface=GE10 direction=both`
		Port Example:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY3 addPortMirrorsession=1 sourceInterface=tenGE1,tenGE3 destInterface=tenGE2`

Procedure 19. Configure Port Mirroring

Step	Procedure	Result

4. ☐	**Virtual PMAC**: Verify port mirroring configuration	`$ 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 may vary slightly from one device type to another.

5. ☐	**Virtual PMAC**: Back up the switch configuration	For Cisco, perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig). For HP, perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch.
6. ☐	**Virtual PMAC**: Repeat	Repeat steps 3. through 5. for each device.

3.4.5 SwitchConfig to netConfig Repository Configuration

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

Prerequisites:

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC
- Application management network interfaces must be configured on the management servers before executing this procedure.
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within **<>**. Refer back to this table for the proper value to insert depending on your system type.

Variable	Value
<serial console type>	U=USB, c=PCIe
<switch_hostname> From NAPD or output from `listDevices` command	
<switch_platform_username> See 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_mgmtVLANID>	
<switch1A_mgmtVLAN_IP_address>	
<switch1B_mgmtVLAN_IP_address>	
<mgmt_VLAN_subnet_ID	
<netmask>	
<switch_Internal_VLAN_list>	
<management_server1A_iLO_IP>	
<management_server1B_iLO_IP>	
<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	

Notes:

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

- 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.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results
1. ☐	**Management Server iLO**: Login and start the integrated remote console	1. On Server1A, log into iLO with Internet Explorer using the password provided by the application: `http://<management_server1A_iLO_IP>` 2. Click the Remote Console tab and start the Integrated Remote Console on the server. 3. If the Security Alert displays, click **Yes**. 4. If not already done so, login as **admusr**.

2. ☐	**Management Server**: 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 is the value for <ethernet_inteface_1> and the second line is the value for <ethernet_interface_2> .
		For example, from the sample output provided, <ethernet_inteface_1> is eth01. If the output from the above command is not successful, refer back to the application documentation.

3. ☐	**Management Server**: 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**: Pre-check. Verify virtual PMAC is installed	1. Verify virtual PMAC 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`
		2. If this command provides no output, it is likely that a virtual instance of PMAC is not installed. Refer to application documentation or My Oracle Support (MOS).

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results

5. ☐	**Virtual PMAC**: Run conserverSetup command	`$ sudo /usr/TKLC/plat/bin/conserverSetup -<serial console type> -s <management_server_mgmt_ip_address>`
		You are asked 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 My Oracle Support (MOS).
		Verify the output of the script.
		Verify your product release is based on Platform 7.2 (versions 7.2.x.x.x_x.x.x).
		Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results

6. ☐	**Virtual PMAC**: Log into the console of the virtual PMAC	***Note***: On a TVOE host, if you open the virsh console, for example, `$ 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, run `ps -ef |grep virsh`, and 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.
		`$ 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 PMAC is not installed. Refer to application documentation or contact My Oracle Support (MOS).

7. ☐	**Virtual PMAC**: Verify PMAC release version	`$ /usr/TKLC/plat/bin/appRev`
		If the following is shown in the output, the PMAC 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.

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results

8. ☐	**Virtual PMAC**: Set up netConfig repository with TFTP information	Use netConfig to create a repository entry that uses the tftp service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not 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=tftp_service`
		`Service type? [dhcp, oa, oobm, ssh, tftp, conserver] tftp`
		`TFTP host IP? <pmac_mgmtVLAN_IP_address>`
		`Directory on host? /var/TKLC/smac/image/`
		`Add service for tftp_service successful`
		To make sure you entered the information correctly, use the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=tftp_service`
		Check the output, which is similar to the one shown below.
		Note: Only the TFTP service information 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`

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results

9. ☐	**Virtual PMAC**: Set up netConfig repository with ssh information	1. Use netConfig to create a repository entry that uses the ssh service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <PMAC_mgmtVLAN_IP_address>`
		`SSH password: <switch_backup_user_password>`
		`Verify Password: <switch_backup_user_password>`
		`Add service for ssh_service successful`
		2. To ensure you entered the information correctly, use the following command and inspect the output, which is 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`

10. ☐	**Virtual PMAC**: 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. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		Note: 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 My Oracle Support (MOS).
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? 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]`

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results

		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 you entered the information correctly, use the following command:
		$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=switch1A
		and check the output, which is similar to the one shown:
		$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
		
		Device: switch1A
		Vendor: Cisco
		Model: 4948E
		Access: Network: 10.240.64.34
		Access: OOB:

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results
		Service: console_service Console: switch1A_console Init Protocol Configured Live Protocol Configured

11. ☐	**Virtual PMAC**: Set up netConfig repository with switch information	***Notes***:
		• If there are no new 3020s to be configured, go to the next step.
		• The Cisco 3020 is not compatible with IPv6 management configuration.
		Use netConfig to create a repository entry for each 3020. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		• If you do not know any of the required answers, stop now and contact My Oracle Support (MOS).
		• The device name must be 20 characters or less.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? Cisco`
		`Device Model [3020, 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`

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results
		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 you entered the information correctly, use the following command: $ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices and check the output, which is similar to the one shown below. $ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices Devices: Device: C3020_IOBAY1 Vendor: Cisco Model: 3020 Access: Network: 10.240.8.7Init 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. or 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.
12. ☐	**Virtual PMAC**: 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 provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here. • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. $ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? HP Device Model? 6120 What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>/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:

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results
		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 takes approximately 4 minutes. Once the unpacking, validation, and rebooting have completed, you are returned to the normal prompt. Proceed with the next step. To verify 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 is similar to the one shown: `$ 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 Repeat this step for each 6120, using appropriate values for those 6120s.

Procedure 20. SwitchConfig to netConfig Repository Configuration

Step	Procedure	Results
13. ☐	**Virtual PMAC**: Migration	Perform the Procedure 21 Cisco Switch SwitchConfig to netConfig Migration procedure for all switches in the system.

3.4.6 Cisco Switch SwitchConfig to netConfig Migration

This procedure configures Cisco switch to migrate from switchConfig to netConfig.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within **<>**. Refer back to these tables for the proper value to insert depending on your system type.

Variable	Serial Port
<switch1A_serial_port>	ttyS4
<switch1B_serial_port>	ttyS5

Fill in the blanks with values for this site.

Variable	Value
<switch_platform_username>	
<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_VLAN_list>	
<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> Check application documentation	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 21. Cisco Switch SwitchConfig to netConfig Migration

Step	Procedure	Results
1. ☐	**Virtual PMAC**: Verify network connectivity to the switch	`$ /bin/ping -w3 <switch_mgmt_IP_address>`
2. ☐	**Virtual PMAC**: Login	Log into the switch using Telnet. `$ /usr/bin/telnet <switch_mgmt_IP_address>`

3. ☐	**Switch CLI**: Apply netConfig commands	From the switch CLI, apply the following commands required by netConfig:
		`Switch# config`
		`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`

Procedure 21. Cisco Switch SwitchConfig to netConfig Migration

Step	Procedure	Results
4. ☐	**Switch CLI**: Reload the switch and verify configuration	If a command was not applied, repeat. `Switch# reload` If prompted, answer **Yes**.
5. ☐	**Virtual PMAC**: Verify netConfig connectivity	Verify that netConfig can communicate with the switch. `$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_name>` Hostname: <switch_name>
6. ☐	**Virtual PMAC**: Back up the switch configuration	Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig).
7. ☐	**Virtual PMAC**: Reset switch to factory defaults	For the 4948 series switches: `sudo /usr/TKLC/plat/bin/netConfig setFactoryDefault --device=<switch_name>` For the 3020 series switches, perform 3.3.1 Configure Cisco 3020 Switch (netConfig), steps 3. through 9. and 12. , replacing the values for the switch being replaced.
8. ☐	**Virtual PMAC**: Restore configuration	For the 4948 series switches, perform 3.2.4 Replace a Failed 4948/4948E/4948E-F Switch (PMAC Installed) (netConfig), steps 6. through 20. For the 3020 series switches, perform 3.3.2 Replace a Failed 3020 Switch (netConfig), steps 5. through 10.
9. ☐	**Virtual PMAC**: Repeat	Repeat steps 2. through 8. for each switch being migrated.

3.4.7 HP 6120XG SwitchConfig to netConfig Migration

This procedure configures 6120XG switch to migrate from switchconfig to netConfig.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 22. HP 6120XG SwitchConfig to netConfig Migration

Step	Procedure	Results
1. ☐	**Management Server**: Verify network connectivity to the 6120XG switch	`$ /bin/ping -w3 <enclosure_switch_IP>`

2. ☐	**Management Server**: Login	Log into the 6120XG switch using SSH or 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 commands	From the 6120XG switch 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. ☐	**Management Server**: Reload the switch and verify configuration	If a command was not applied, repeat. `Switch# reload` If prompted, answer **Yes**.

5. ☐	**Management Server**: Verify netConfig connectivity	Verify that netConfig can communicate with the switch.
		`$ sudo /usr/TKLC/plat/bin/netConfig getFirmware --device=<switch_name>`
		`Version: Z.14.32`
		`Image: Secondary`

6. ☐	**Management Server**: Back up the switch configuration	Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig).

Procedure 22. HP 6120XG SwitchConfig to netConfig Migration

Step	Procedure	Results
7. ☐	**Management Server**: Restore configuration	Perform 3.2.4 Replace a Failed 4948/4948E/4948E-F Switch (PMAC Installed) (netConfig), steps 3. through 8.

8. ☐	**Management Server**: Verify 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.

3.4.8 Configure DSCP Marking Using iptablesADM

This procedure configures DSCP marking using iptablesADM.

Note: DSCP marking set using the QOS procedure 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 is 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 set up this command creates 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 using 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 –setdscp
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 –setdscp
25'
```

3.4.9 Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig)

This 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 autonegotiation for the individual links, and must be performed on both switches for all participating LAG links. This procedure addresses a known weakness with autonegotiation on 1GE SFPs and the 6125XLG that causes 1GE links to take longer than expected to become active.

Prerequisites:

- 3.1 Configure netConfig Repository
- 3.3.5 Configure HP 6125XLG Switch (netConfig)

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 23. Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig)

Step	Procedure	Results

1. ☐	**Virtual PMAC**	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 PMAC**	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 PMAC**	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`

Procedure 23. Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig)

Step	Procedure	Results

4. ☐	**Virtual PMAC**	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> 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`

3.4.10 Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

This 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 autonegotiation for the individual links, and must be performed on both switches for all participating LAG links. This procedure addresses a known weakness with autonegotiation on 1GE SFPs and the 6125XLG that causes 1GE links to take longer than expected to become active.

Prerequisites:

- 3.1 Configure netConfig Repository
- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)
- 3.3.5 Configure HP 6125XLG Switch (netConfig)

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 24. Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

Step	Procedure	Results

1. ☐	**Virtual PMAC**	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`

Procedure 24. Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

Step	Procedure	Results

2. ☐	**Virtual PMAC**	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 PMAC**	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 to **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 PMAC**	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>`

Procedure 24. Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

Step	Procedure	Results
5. ☐	**Virtual PMAC**: Repeat	Repeat steps 2. through 4. for each LAD ID.

4. Brocade Switch — SwitchConfig Procedures

4.1 Configure Brocade Switches

This procedure configures names, user passwords, and NTP settings for Brocade switches; and backs up the configuration to the management server hosting PMAC.

Prerequisites:

- 7.1 Configure Initial OA IP
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 25. Configure Brocade Switches

Step	Procedure	Results

1. ☐	**OA Shell**: Log into 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 monitored 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**, log into the other OA of the enclosure system.

Procedure 25. Configure Brocade Switches

Step	Procedure	Results

2. ☐	**OA Shell**: Log into 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** twice and login 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`

Procedure 25. Configure Brocade Switches

Step	Procedure	Results
6. ☐	**Brocade Switch Console**: Set user password	`swd77:root> passwd user`

7. ☐	**Brocade Switch Console**: Set switch name for the FC switch	The bay ID number is the same number 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, for example, c505_05_01. `swd77:root> chassisName <chassis_name>` ***Note***: The chassis name must begin with an 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`
		Make sure the change was applied.
		`swd77:root> tsclockserver`
		`Active NTPServer 10.250.32.10`
		`Configured NTPServer List 10.250.32.10`

10. ☐	**Brocade Switch Console**: Back up configuration	`swd77:root> configUpload`
		`Protocol (scp, ftp, local) [ftp]: scp`
		`Server Name or IP Address [host]: <PMAC_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**: Log out	`swd77:root> logout` Press **control + shift + underscore** and **D** to logout from the FC switch console.
12. ☐	Repeat	Repeat steps 2. through 11. for the second Brocade switch.
13. ☐	**OA**: Log out	`> exit`

4.2 Upgrade Brocade Switch Firmware

This procedure upgrades firmware for the Brocade switches. The procedure covers either 4/24 or 8/24 Brocade switches.

Prerequisites:

- 7.1 Configure Initial OA IP

Needed Material

- HP MISC firmware ISO image
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6 is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

4.3 Configure Zones in Brocade Switches

This optional procedure should be applied to both Brocade switches that are part of the same enclosure. Zone settings have to be the same for both switches.

This procedure is optional. Skipping this procedure allows 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:

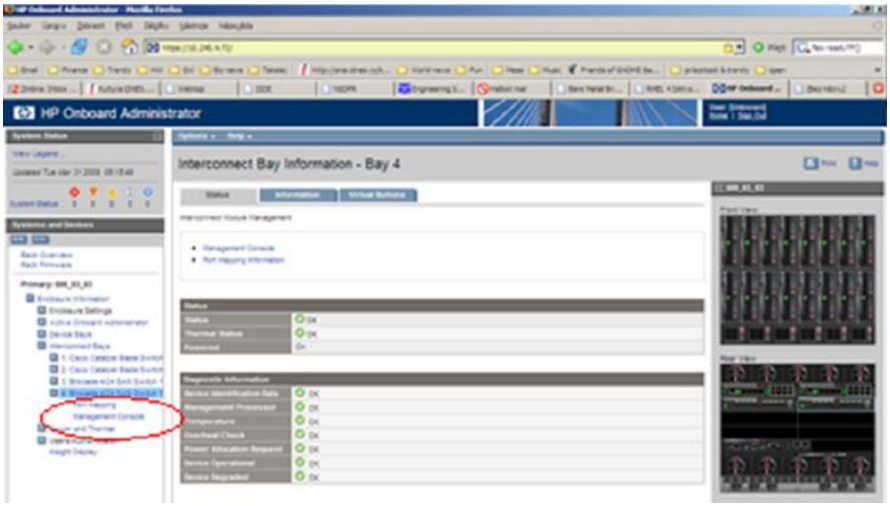
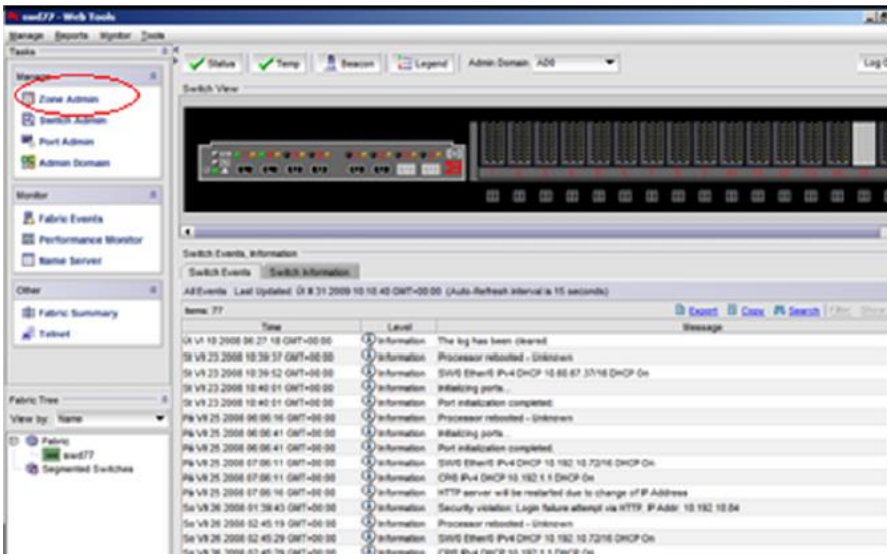
- The rules for the zone configuration: There should be one zone per one storage array in the fibre channel switch.
- Identical zones need to be created in each Brocade in the same enclosure.
- The members of such zone are all ports from the management storage array and all servers that need access to 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.

Prerequisites:

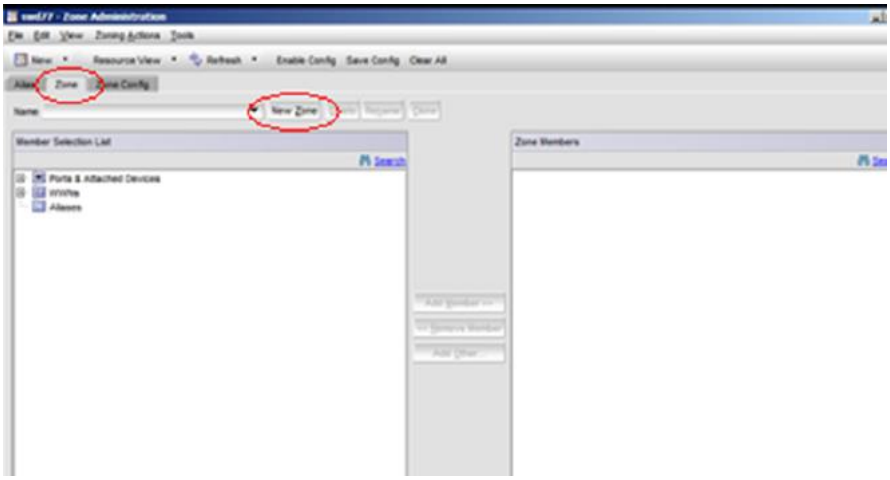
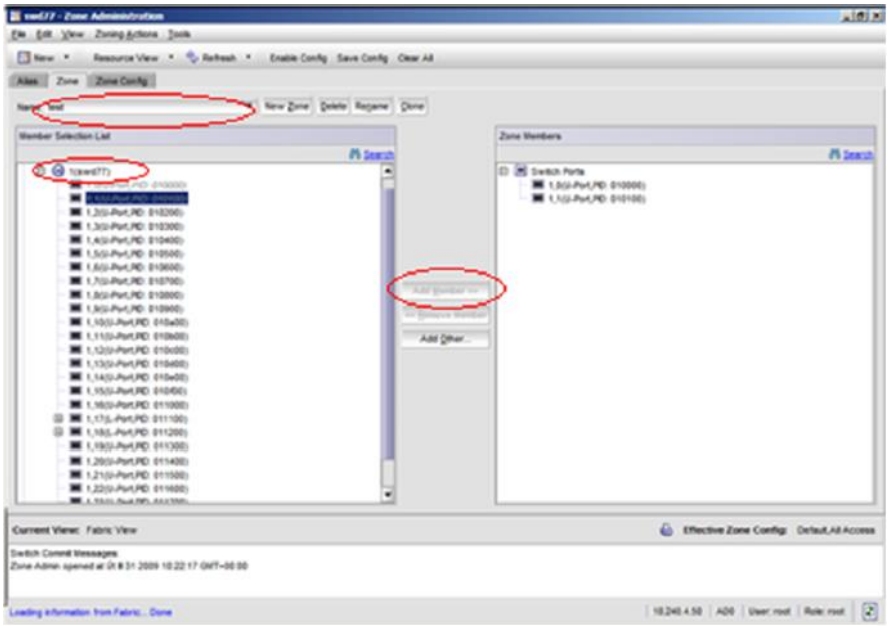
- 4.1 Configure Brocade Switches
- Know the network cabling and SAN requirements by blade server

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

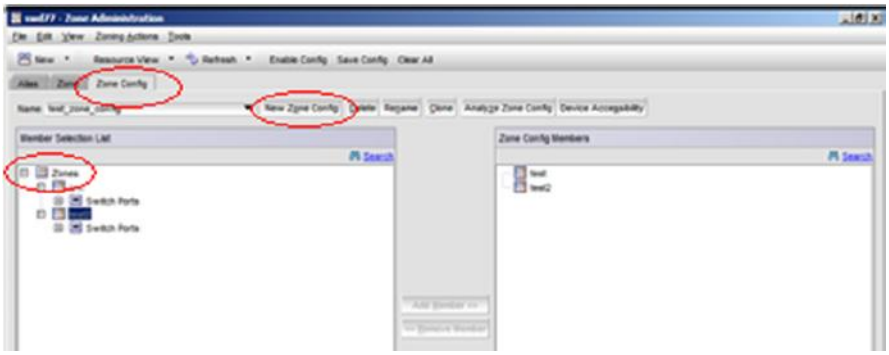
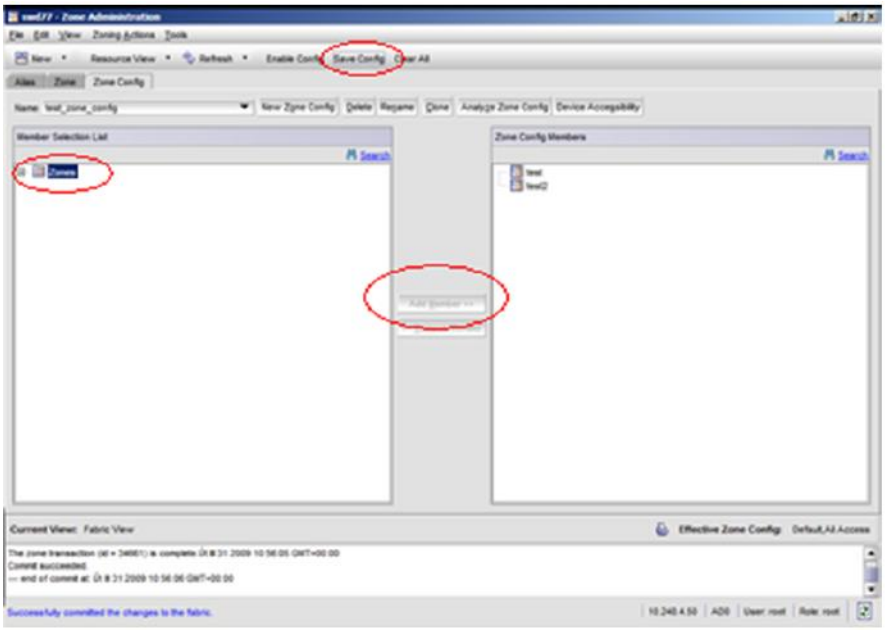
Procedure 26. Configure Zones in Brocade Switches

Step	Procedure	Results
1. ☐	**OA GUI**: Log into the OA and select the Fibre Channel switch	1. Navigate to Enclosure Information > Interconnect Bays > Brocade … > Management Console.  The Fibre Channel console loads. 2. Login as the administrative user.
2. ☐	**Fibre Channel Switch Console**	Navigate to Zone Admin. 

Procedure 26. Configure Zones in Brocade Switches

Step	Procedure	Results
3. ☐	**Fibre Channel Switch Console**: Create a new zone	1. Select the Zone tab.  2. Click **New Zone**. 3. Type an appropriate name and click **OK**.
4. ☐	**Fibre Channel Switch Console**: Add port members into the zone	1. Select the zone where ports should be added. 2. Expand the **Ports and Attached Devices** twice and select the ports under Ports and Attached Devices. 3. Click **Add Member**.  4. Create a **catch-all** zone that covers all remaining devices (such as blade servers and ports) that are not in the zone specified.

Procedure 26. Configure Zones in Brocade Switches

Step	Procedure	Results
5. ☐	**Fibre Channel Switch Console**: Create zone configuration	1. Select the Zone Config tab. 2. Click **New Zone Config**.  3. Type an appropriate name (for example, Production_Zone_Config) and click **OK**.
6. ☐	**Fibre Channel Switch Console**: Add zones into zone configuration	1. Expand the Zones Selection List. 2. Select all desired zones and click **Add Member**.  3. Click **Save Config** and **Yes**. 4. Observe the status at the bottom of the screen. Make sure the "Successfully committed the changes to the fabric" message displays in blue at the bottom of the screen.

Procedure 26. Configure Zones in Brocade Switches

Step	Procedure	Results
7. ☐	**Fibre Channel Switch Console**: Enable zone configuration	1. Click **Enable Config**. 2. Select **Zone Config** from the option list. 3. Click **OK**. 4. Click **Yes**. 5. Observe the status at the bottom of the screen. Make sure the "Successfully committed the changes to the fabric" message displays in blue at the bottom of the screen.
8. ☐	Repeat	Repeat steps 1. through 7. on second switch in the same enclosure. The two switches should have identical configurations.

4.4 Configure Brocade Switch XNMP Trap Target

This procedure configures SNMP settings for Brocade switches.

Prerequisites:

- 4.1 Configure Brocade Switches
- Know the network cabling and SAN requirements by blade server

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 27. Configure Brocade Switch XNMP Trap Target

Step	Procedure	Results

1. ☐	**OA**: Log into the Brocade switch console	Log into OA via ssh as root user. Run the following command to get the 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 connects the user to the FC switch console. Press **Enter** twice and login as the **admin** user.
		Note: The switch is configured to reject SNMP sets and gets. Only the hosts listed in step 4 are able to receive traps.

Procedure 27. Configure Brocade Switch XNMP Trap Target

Step	Procedure	Results

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 displays.
		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`

Procedure 27. Configure Brocade Switch XNMP Trap Target

Step	Procedure	Results

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`

Procedure 27. Configure Brocade Switch XNMP Trap Target

Step	Procedure	Results

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. ☐	Repeat	Repeats steps 1. through 7. to configure settings on the other Brocade switch in the enclosure.

5. SAN Storage Arrays Procedures

5.1 Set IP on Fibre Channel Disk Controllers

This procedure sets the IP address for fibre channel disk controllers.

Note: Execute this procedure for only one of the two controllers.

Needed Material

- Serial access cable that ships with the given controller and laptop running Microsoft Windows with USB port.
- If setting the IP address for P2000, you may need to install the P2000 MSAUSB driver on the laptop. Use the HP Solutions Firmware Upgrade Pack ISO image and follow Appendix B Install P2000 MSA USB Driver.
- If setting the IP address for P2000, you may need [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 28. Set IP on Fibre Channel Disk Controllers

Step	Procedure	Results

1. ☐	**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
		You may have to login 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`

2. ☐	**Disk Array Serial Console**: Verify the values were entered correctly	Run the following command and check the output:
		`# show network-parameters`
		Since you are currently logged in at the cli, execute the following command at this time to make sure the expansion disk arrays are identified correctly:
		`# rescan`

5.2 Configure Fibre Channel Disk Controllers

This procedure configures security and user settings for fibre channel disk controllers.

Prerequisite: 5.1 Set IP on Fibre Channel Disk Controllers

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 29. Configure Fibre Channel Disk Controllers

Step	Procedure	Results

1. ☐	**Fibre Channel Disk Controller**: Log in	Log into the fibre channel disk controller via ssh as a manage user.
		Output similar to the following displays:
		`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`

Procedure 29. Configure Fibre Channel Disk Controllers

Step	Procedure	Results
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	This step is required if the 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 time zone	`# set controller-date <month> <day> <hh>:<mm>:<ss> <year> <time-zone> ntp enabled ntpaddress <PMAC_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`

Procedure 29. Configure Fibre Channel Disk Controllers

Step	Procedure	Results

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 SNMP trap host	`# set snmp-parameters enable crit add-trap-host <target_IP>` This enables delivery of critical events to the target destination.
12. ☐	**Fibre Channel Disk Controller**: Log out	Log out from the fibre channel disk controller console. `# exit`

5.3 Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

This procedure configures advanced settings on each MSA 2012fc disk controller.

Prerequisites:

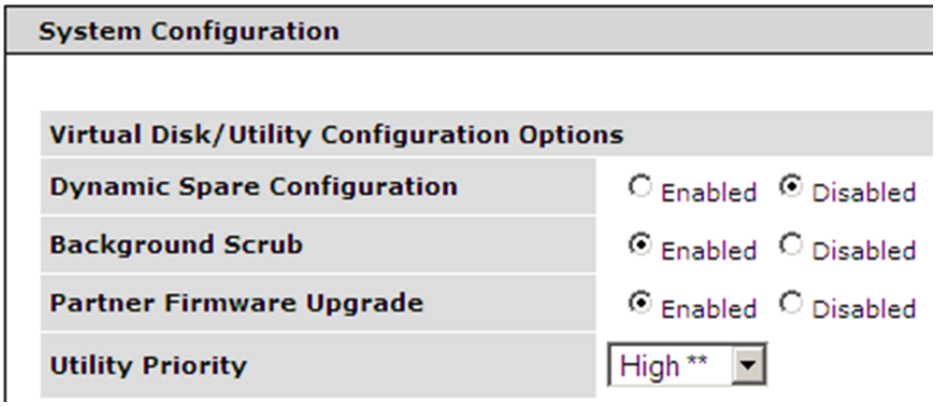
- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 30. Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

Step	Procedure	Results
1. ☐	**Fibre Channel Disk Controller GUI**: Log in	Log into the 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 **Manage > General Config > System Configuration**.

Procedure 30. Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

Step	Procedure	Results
3. ☐	**Fibre Channel Disk Controller GUI**: Change advanced settings	1. Make sure: Dynamic Spare Configuration is disabled. Background Scrub is enabled. Partner Firmware Upgrade is enabled.  2. Press Change System Configuration.
4. ☐	**Fibre Channel Disk Controller GUI**: Verify settings	Verify the **successful** message displays.
5. ☐	**Fibre Channel Disk Controller GUI**: Log out	Click **Log Off** on the left hand side.

5.4 Configure Advanced Settings on P2000 Fibre Channel Disk Controllers

This procedure configures advanced settings on each P2000 controller.

Prerequisites:

- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 31. Configure Advanced Settings on P2000 Fibre Channel Disk Controllers

Step	Procedure	Results

1. ☐	**Fibre Channel Disk Controller**: Login	Log into the fibre channel disk controller via ssh as a manage user.
		Output similar to the following displays:
		`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: L200R010`

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 setting	`# show advanced-settings`
4. ☐	**Fibre Channel Disk Controller**: Log out	Log out from the fibre channel disk controller console. `# exit`

5.5 Upgrade Firmware on MSA 2012 fc Disk Controllers

This procedure upgrades the firmware of the MSA 2012fc disk controller.

Prerequisite: 5.3 Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

Needed Material

- HP MISC firmware ISO image
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

Note: Execute this procedure only on the A controller; the B controller automatically upgrades after the A controller.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6 is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

5.6 Upgrade Firmware on MSA P2000 Disk Controllers

This procedure upgrades the firmware of the MSA P2000 disk controller.

Prerequisite: 5.4 Configure Advanced Settings on P2000 Fibre Channel Disk Controllers

Needed Material

- HP MISC firmware ISO image
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

Notes:

- Execute this procedure only on the A controller; the B controller automatically upgrades after the A controller.
- This procedure also upgrades any I/O modules of P2000 JBOD enclosures cascaded from the P2000 disk controller being upgraded.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6 is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

5.7 Replace a Failed Disk in MSA 2012fc Array

The MSA 2012fc arrays should be configured with spare disks. The designation and type of spare should always be recorded for future reference.

When a disk fails, the system looks for a dedicated spare first 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 with an appropriately sized disk and 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 a failure has occurred in several ways:

- SNMP trap is sent, if controller is configured to send SNMP traps (it should be).
- Failed drive has amber LED illuminated.
- If you log into the disk controller, a screen display to indicates which disk(s) failed.

Prerequisites:

- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

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.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 32. Replace a Failed Disk in MSA 2012fc Array

Step	Procedure	Results
1. ☐	**Fibre Channel Disk Controller GUI**: Log in	Log into the Fibre Channel Disk Controller GUI as a manage user using https: `https://<fibre_channel_disk_controller_IP>`
2. ☐	**Fibre Channel Disk Controller GUI**: Clear metadata	If the replacement disk has been used in another MSA 2012fc array, it has 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, are in a **Leftover** or **L** state. 1. Navigate to **Manage > Utilities > Disk Drive Utilities > Clear Metadata**. 2. Select the disk(s) in an **L** state. 3. Click **Clear Metadata for Selected Disk Drives**.
3. ☐	**Fibre Channel Disk Controller GUI**: Add global spare disk	1. To add a global spare to reconstruct a vdisk, navigate to **Manage > Virtual Disk Config**. 2. Click **Global Spare** menu and **Add Global Spares**. 3. Select the disk that was replaced by marking the checkbox. It should be bright green with an **A** on it. 4. Click **Add Global Spares** toward the bottom of the screen. 5. Verify the color of the disk changes and a **G** displays on the disk. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen.
4. ☐	**Fibre Channel Disk Controller GUI**: Add a dedicated spare disk	1. To add a dedicated spare to reconstruct a vdisk, navigate to **Manage > Virtual Disk Config**. 2. Click **vdisk configuration** and **Add Vdisk Spares**. 3. Select the vdisk at the top of the screen. It should be bright green with an **A** on it. 4. Ensure the disk is in the correct enclosure and select the disk by marking the checkbox. 5. Click the **Add Vdisk Spares** toward the bottom of the screen. The disk changes to the same shade of blue (grey) as the rest of the disks in the enclosure. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen. 6. Log off the disk controller by clicking **Log Off**.

5.8 Replace 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 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 a failure has occurred in several ways:

- SNMP trap is sent, if controller is configured to send SNMP traps (it should be).
- Failed drive has amber LED illuminated.
- If you log into the disk controller, a screen display to indicates which disk(s) failed.

Prerequisites:

- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

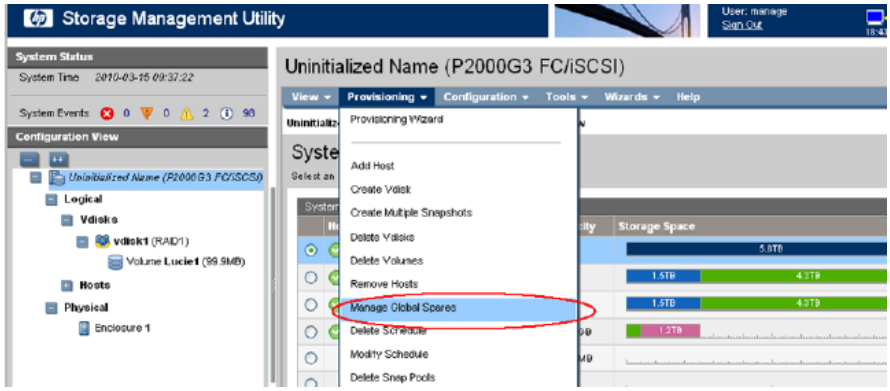
Note: The vdisk reconstruction can take hours or days to complete depending on the vdisk RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop reconstruction only by deleting the vdisk.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

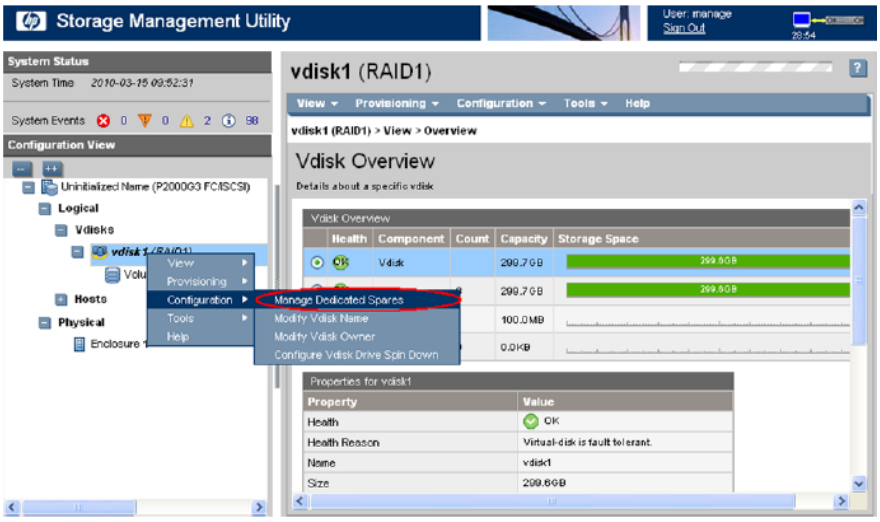
Procedure 33. Replace a Failed Disk in MSA P2000 Disk Array

Step	Procedure	Results
1. ☐	**Fibre Channel Disk Controller GUI**: Log in	Log into the Fibre Channel Disk Controller GUI as a manage user using https: `https://<fibre_channel_disk_controller_IP>`

Procedure 33. Replace a Failed Disk in MSA P2000 Disk Array

Step	Procedure	Results
2. ☐	**Fibre Channel Disk Controller GUI**: Clear metadata	If the replacement disk has been used in another P2000 array, it has 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, are in a **Leftover** state. 1. In the Configuration View panel, right-click the system and click **Tools > Clear Disk Metadata**. 2. In the main panel, select the disk(s) in an LEFTOVR state. 3. Click **Clear Metadata**. When processing is complete, a success screen displays. 4. Click **OK**.
3. ☐	**Fibre Channel Disk Controller GUI**: Add global spare disk	To add a global spare to reconstruct a vdisk, in the Configuration View panel, right-click on the system. On 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 marking the checkbox. It is labeled with an **AVAIL** on it. Click **Modify Spares**.  Verify the color of the disk changes to blue and a **GLOBALSP** displays on the disk. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen.

Procedure 33. Replace a Failed Disk in MSA P2000 Disk Array

Step	Procedure	Results
4. ☐	**Fibre Channel Disk Controller GUI**: Add a dedicated spare disk	To add a dedicated spare to reconstruct a vdisk, in the Configuration View panel, right-click on the vdisk and navigate to **Configuration > Manage Dedicated Spares**.  Switch to Graphical representation if needed. Ensure the disk is in the correct enclosure and select the disk by marking the checkbox. It is labelled with an **AVAIL** on it.  Click **Modify Spares**. Verify the color of the disk changes to green and **SPARE** displays on the disk. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen. Log off the disk controller by clicking **Log Off**.

6. Blade Server Procedures

6.1 Upgrade Blade Server Firmware

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 [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

This procedure upgrades the firmware on the blade servers.

The HP Support Pack for ProLiant installer automatically detects the firmware components available on the target server and only upgrades those components with firmware older than what is on the current ISO.

Prerequisite: TPD has to have been installed on the server.

Needed Material

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- USB Flash Drive (4GB or larger and formatted as FAT32) if upgrading with USB media.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6 is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

6.2 Confirm/Upgrade Blade Server BIOS Settings

6.2.1 BIOS Settings for HP Systems

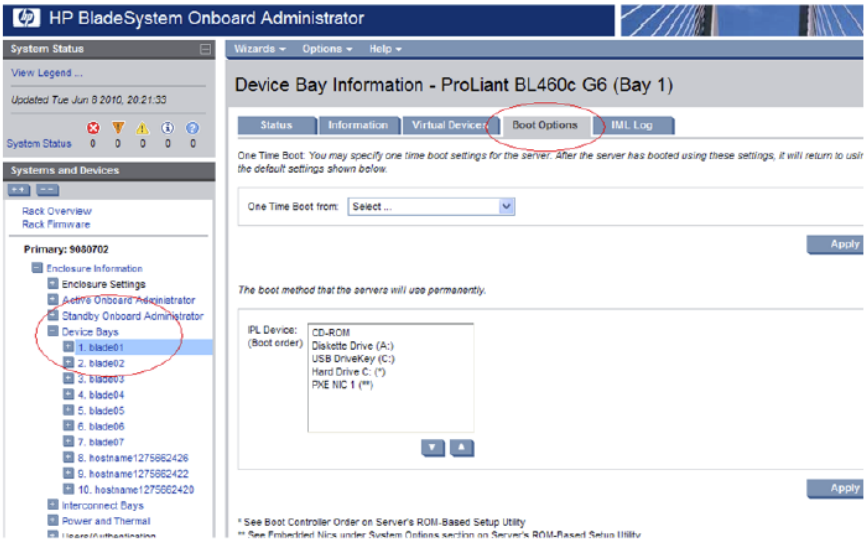
This procedure confirms and updates the BIOS boot order on the blade servers.

Prerequisite: 6.1 Upgrade Blade Server Firmware has been completed.

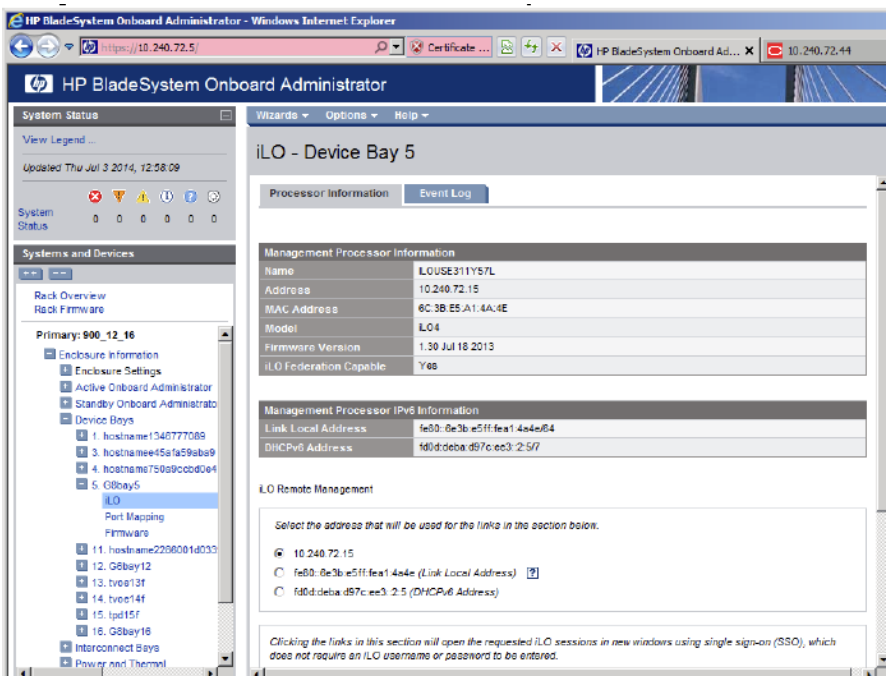
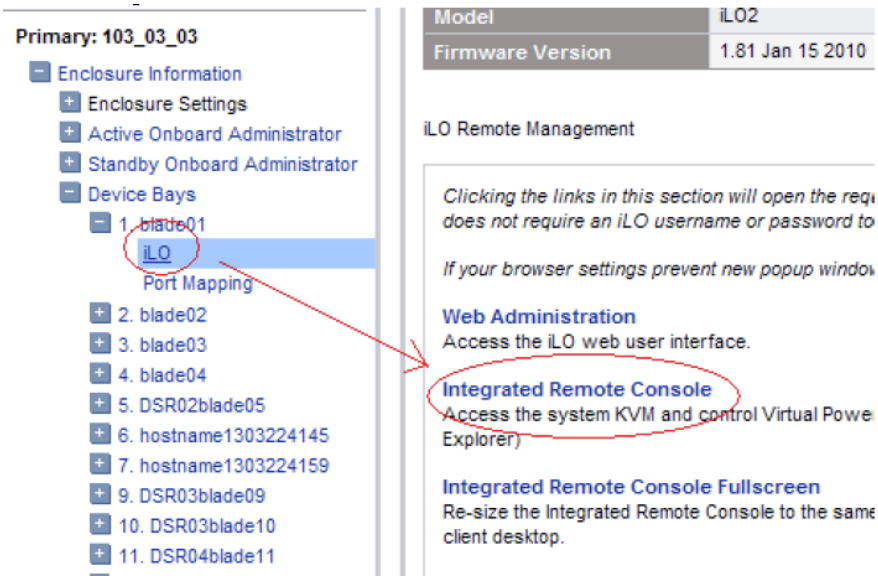
For instructions on configuring Gen9 BIOS settings, refer to [1] TPD Initial Product Manufacture Software Installation Procedure.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

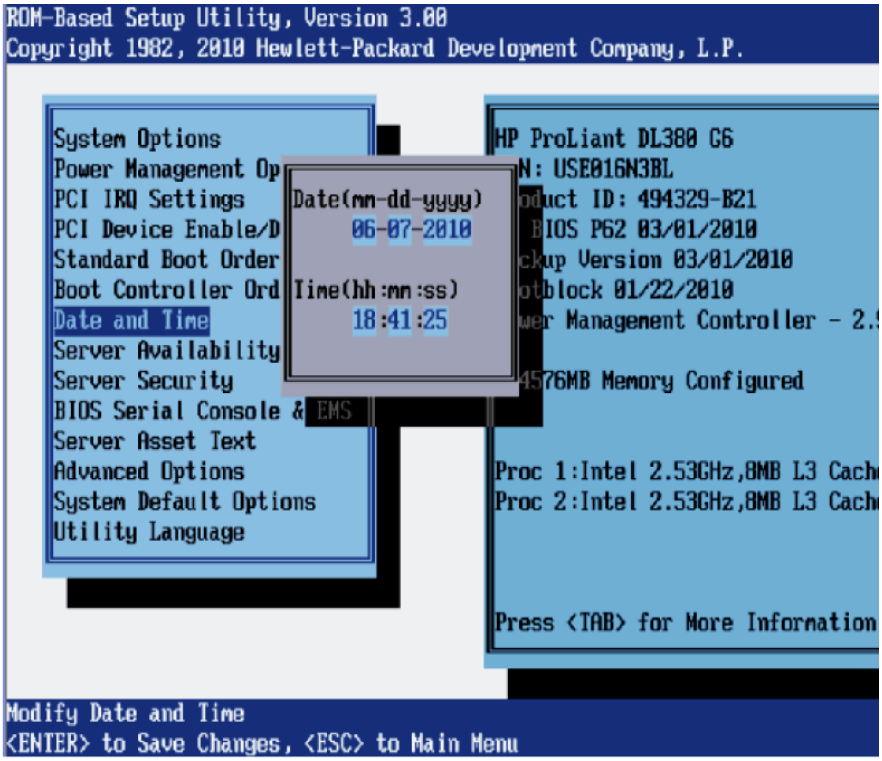
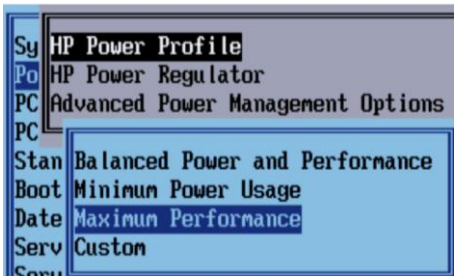
Procedure 34. BIOS Settings for HP Systems

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.
2. ☐	**OA Web GUI**: Verify boot device order	1. Navigate to **Enclosure Information > Device Bays > <Blade 1>**. 2. Click on the Boot Options tab.  3. Verify the boot order is: • CD-ROM • Diskette Drive (A:) • USB DriveKey (C:) • Hard Drive C: (*) • PXE NIC 1 (**) If it is not, use the arrows to adjust the order and click **Apply**.

Procedure 34. BIOS Settings for HP Systems

Step	Procedure	Results
3. ☐	**OA Web GUI**: Access the blade iLO	1. Navigate to **Enclosure Information > Device Bays > <[device]> > iLO**. 2. In **iLO Remote Management**, select the address. If the option to select from multiple addresses displays, select the appropriate static address.  3. Click **Integrated Remote Console**. This opens the iLO interface for that blade. If this is the first time the iLO is being accessed, you are asked to install and add on to your web browser. Follow the instructions to do so. 

Procedure 34. BIOS Settings for HP Systems

Step	Procedure	Results
4. ☐	**Server iLO**: Update BIOS settings	1. If a certificate security warning displays, click **continue**. 2. Log into the blade as the **admusr**. 3. Reboot the server and press **F9** during the power-up sequence to access the BIOS setup screen. 4. Navigate to **Date and Time** and press **Enter**. 5. Set the current date and UTC time, and press **Enter**.  6. Press **Esc** to go back to the main menu. 7. Navigate to **Power Management Options** and press **Enter**. 8. Select the **HP Power Profile** and press **Enter**. 9. Navigate to **Maximum Performance** and press **Enter**.  10. Press **Esc** twice to exit the BIOS setup screen and **F10** to confirm exiting the utility. The blade reboots.

Procedure 34. BIOS Settings for HP Systems

Step	Procedure	Results
5. ☐	**OA Web GUI**: Repeat	Repeat steps 2. through 4. for remaining blades and then exit the OA GUI.

6.2.2 BIOS Settings for Oracle Sun Systems

This procedure configures the BIOS power management and UEFI settings.

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/DVDROM.

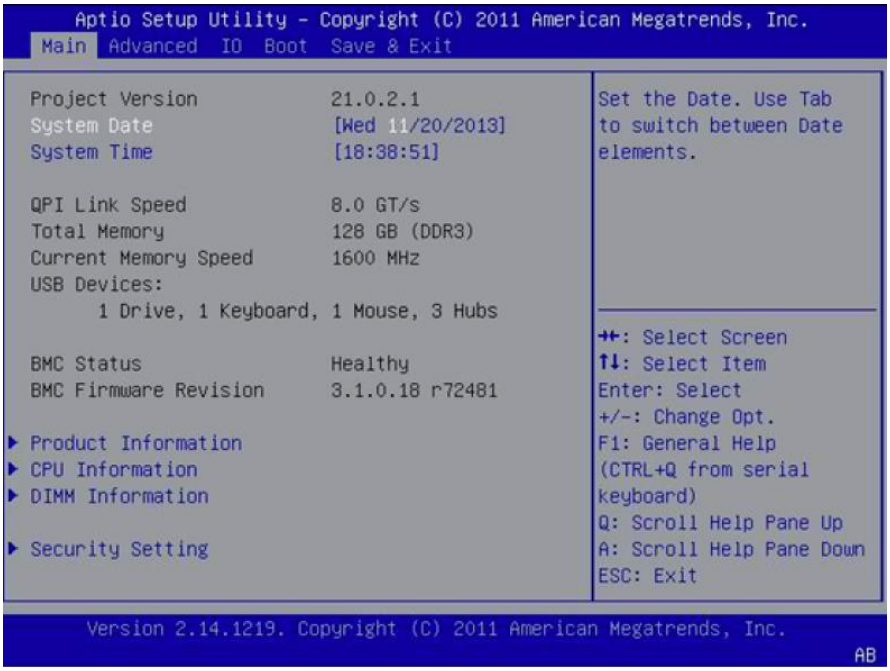
Note: In the following steps, unless stated otherwise, **X5-2**, **X6-2**, and **X7-2** refer to all versions of the X5-2, X6-2, X7-2 servers supported by TPD. For example, the Netra X5-2 server, Oracle X5-2 server, and Oracle X5-2M server apply for all mentions of X5-2.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

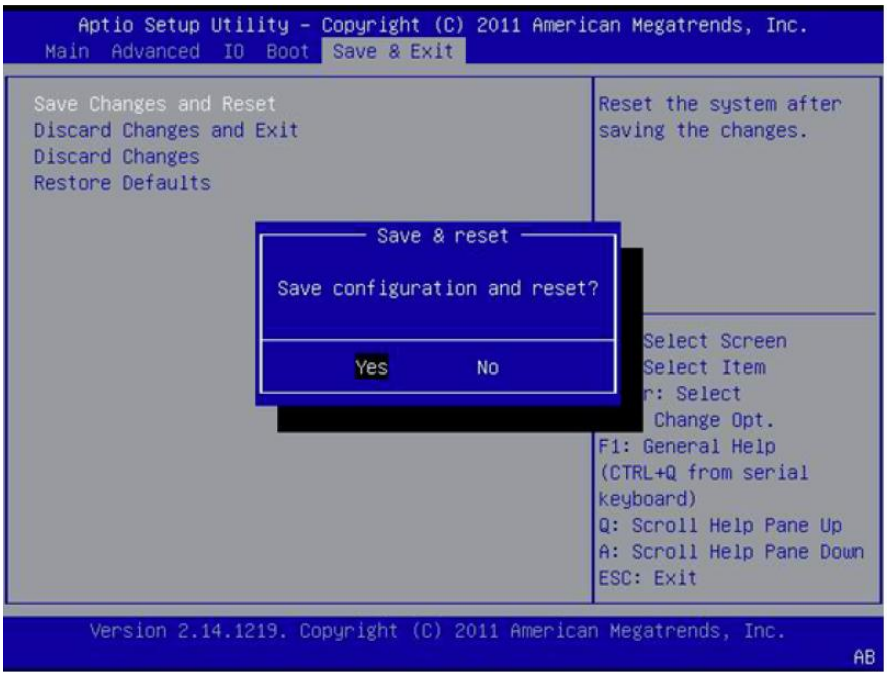
Procedure 35. BIOS Settings for Oracle Sun Systems

Step	Procedure	Results
1. ☐	**Oracle ILOM**: Login	Connect to the ILOM as described in and Appendix E.1 Access a Server Console Remotely login.

Procedure 35. BIOS Settings for Oracle Sun Systems

Step	Procedure	Results
2. ☐	**Oracle ILOM**: Update BIOS settings	1. Reboot the server and press **F2** during the power-up sequence to access the BIOS setup screen. 2. Set the current date and UTC time.  3. For X4-2, from the Advanced tab, select **Processors**. ***Note***: If the server is an X5-2, X6-2, or X7-2, skip this step and go to the next step. 4. Select **CPU Power Management Configuration**. 5. If the Energy Performance field is not set to **Performance**, select **Energy Performance** and press **Enter**. ***Note***: For X5-2 and X6-2, set **ENERGY_PERF_BIAS_CFG** mode to **PERF**. Press **Enter** and skip to step 7. 6. Select the **Performance** option and press **Enter**. 7. Press **Esc** twice (just once on the X5-2 and X6-2) to return to the Advanced menu.
3. ☐	**Oracle ILOM**: Update BIOS setting for the X4-2 only	1. Select **UEFI Configuration Synchronization** and press **Enter**. 2. If Synchronization Late is not **Disable**, press **Enter** to modify the option. Select **Disabled** and press **Enter**. 3. Press **Esc** to return to the Advanced menu.

Procedure 35. BIOS Settings for Oracle Sun Systems

Step	Procedure	Results
4. ☐	**Oracle ILOM**: Boot	1. Navigate to the Boot tab. 2. For X4-2, X5-2, and X6-2, under Legacy Boot Option Priority, verify the RAID Adapter is listed first. If not, highlight it and press the **+** key to move it to the top of the list. For X7-2, under UEFI Boot Option Priority, verify the **TPD XX.XX** is listed first. If not, highlight it and press **Enter** to move it to Boot Option #1. 3. Select **Exit** or from the Save & Exit tab, and select **Save Changes and Exit**. Answer **Yes** when asked to confirm. 

6.3 Configure Blade Server iLO Password for Administrator Account

This procedure changes the blade server iLO password for the Administrator account for blade servers in an enclosure.

Prerequisites:

- 7.1 Configure Initial OA IP
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 36. Configure Blade Server iLO Password for Administrator Account

Step	Procedure	Results

1. ☐	**PMAC**: Login	SSH into the PMAC and login as **admusr**.
		`login as: admusr`
		`Password: <admusr_password>`

2. ☐	**PMAC**: Create XML file	1. 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>`
		2. Save this file as change_ilo_admin_passwd.xml.
		3. Change the permission of the file.
		`$ sudo chmod 644 change_ilo_admin_passwd.xml`

3. ☐	**OA Shell**: Log into 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 monitored 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**, log into the other OA of the enclosure system.

4. ☐	**OA Shell**: Run hponcfg	`> hponcfg all https://<pmac_ip>/public-configs/change_ilo_admin_passwd.xml`
5. ☐	**OA Shell**: Check output	Monitor the output for error messages. Refer to the HP *Integrate Lights-Out Management processor Scripting and Command Line Resource Guide* for troubleshooting.
6. ☐	**OA Shell**: Log out	Log out from the OA.

Procedure 36. Configure Blade Server iLO Password for Administrator Account

Step	Procedure	Results
7. ☐	**PMAC**: Remove temporary file	On the PMAC, 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`

6.4 Access the Server Virtual Serial Port

This procedure accesses iLO or ILOM VSP.

Prerequisite: For HP servers, complete 6.3 Configure Blade Server iLO Password for Administrator Account.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 37. Access the Server Virtual Serial Port

Step	Procedure	Results

1. ☐	**For HP Servers**
	HP iLO: Access VSP
		Login 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**
	Oracle ILOM: Login and connect
		Login 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`
		`-> 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.

6.5 Configure Syscheck Default Route Ping Test

This procedure configures a ping test on the blade system.

Prerequisite: TPD must be installed on the blade server.

Note: Repeat this test for every blade server in the blade system.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 38. Configure Syscheck Default Route Ping Test

Step	Procedure	Results

1. ☐	**Blade Server**: Configure syscheck default route test	1. Log into the blade server as **admusr**.
		2. Enable syscheck default router test.
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net defaultroute -enable`
		3. Run syscheck to verify 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`
		4. Restart syscheck.
		`$ sudo /sbin/initctl/syscheck restart`
		5. Repeat for each blade server.

6.6 Prepare a System for Extended Power Outage

This procedure shuts down a system properly for an extended period such as shipping from one site to another site.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 39. Prepare a System for Extended Power Outage

Step	Results
1. ☐	Refer to instructions provided by the application to correctly power down all blade servers.
2. ☐	Verify each server has shut down.
3. ☐	Login via SSH into one fibre channel controller in each MSA as the manage user and run: `# shutdown both`
4. ☐	Power down disk arrays using power switches on each array.
5. ☐	Login to each management server via SSH as admusr and run: `$ sudo /sbin/shutdown -h now`

Procedure 39. Prepare a System for Extended Power Outage

Step	Results
6. ☐	If the aggregation switches are provided by Oracle, power off the 4948/4948E switches. If the aggregation switches are provided by the customer, request the customer follow their policies for preparing devices for an extended power outage.

6.7 Bring Up a System After Extended Power Outage

This procedure powers up the HP blade system properly.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 40. Bring Up a System After Extended Power Outage

Step	Results
1. ☐	Power on the cabinets that house the devices.
2. ☐	If the aggregation switches are provided by Oracle, power on the 4948/4948E switches.
3. ☐	Turn on the management server by depressing the power button on the front of the server.
4. ☐	Turn **on** power switches on all disk arrays.
5. ☐	Power on remaining cabinets. Ensure all power supply LEDs are green on all equipment.
6. ☐	Power up each blade server.

7. C7000 Enclosure Procedures

7.1 Configure Initial OA IP

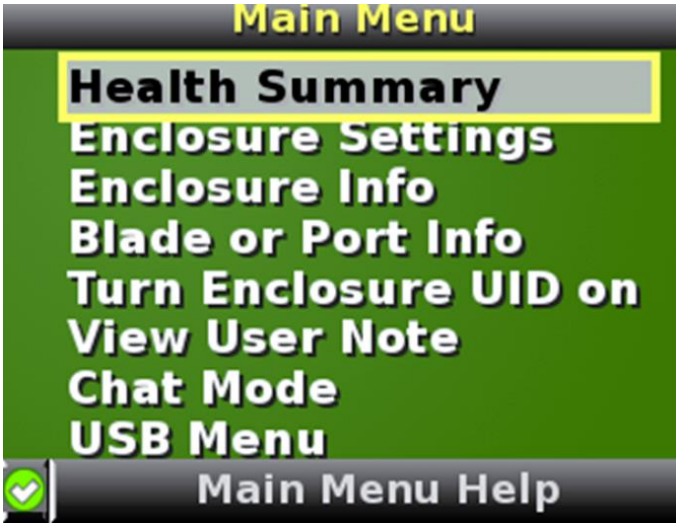
This procedure sets the initial IP address for the onboard administrator in location OA Bay 1 (left as viewed from the rear) and Bay 2 using the front panel display.

Prerequisite: Onboard administrator must be preset in the OA Bay 1 location.

Note: The enclosure should be provisioned with two onboard administrators. This procedure needs to be executed only for OA Bay 1 regardless of the number of OAs installed in the enclosure.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 41. Configure Initial OA IP

Step	Procedure	Results
1. ☐		Configure OA Bay1 IP address using insight display on the front side of the enclosure. 
2. ☐		1. Navigate to **Enclosure Settings** and click **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. 2. Navigate to the **OA1 IP** menu settings and click **OK**.

Procedure 41. Configure Initial OA IP

Step	Procedure	Results
3. ☐	For IPv4 addresses	1. Navigate to the OA1 IPv4 and click **OK**. 2. On the OA1 Network Mode screen, select **Static** and click **OK**. 3. Select **Accept** and click **OK**. 4. On the Change:OA1 IP address screen, fill in data below, and click **OK**. • IP • MASK • gateway 5. Select **Accept** and click **OK**. 6. Navigate to OA2 IP menu setting on the Insight display and repeat the above steps to assign the IP parameters of OA2.
4. ☐	For IPv6 addresses	1. Navigate to the OA1 IPv6and click **OK**. 2. On the Change: OA1 IPv6 Status menu, select the **Enabled** option and click **OK**. 3. Select **Accept** and click **OK**. 4. On the Change:OA1 IPv6 Settings screen, fill in appropriate data, and click **OK**. a. Set the **Static IPv6 address** to the globally scoped address and prefix and click **OK**. b. If not already disabled, set the DHCPv6 option to **Disabled**. c. If not already disabled, set the SLAAC option to **Disabled**. d. If a static Gateway address is to be configured, navigate to **Static Gateway,** and click **OK**. • Select the **Static Gateway IPv6 Address** and click **OK**. • Select **Set** and click **OK**. e. Navigate to OA2 IP menu setting on the Insight display and repeat the above steps to assign the IP parameters of OA2. f. Select **Accept All** and click **OK**. The Main Menu displays.

7.2 Configure Initial OA Settings Using the Configuration Wizard

This procedure configures 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:

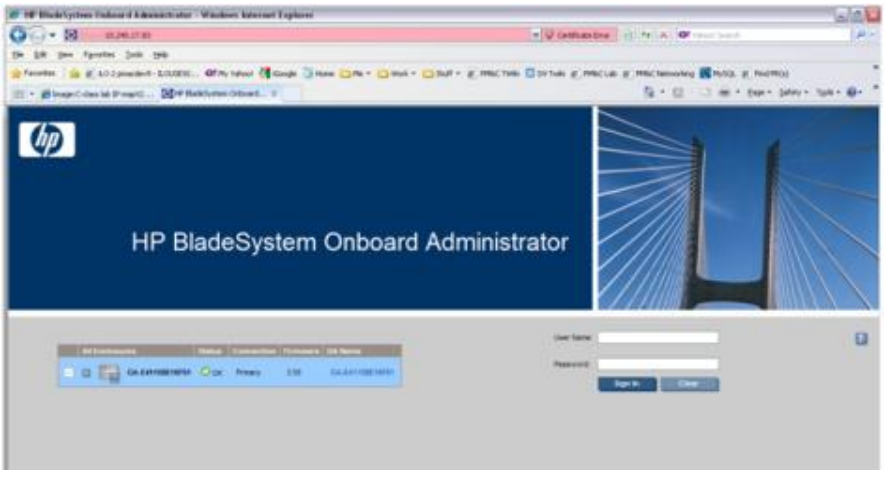
- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured 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 (MOS) for assistance.
- 7.1 Configure Initial OA IP
- Both OAs are installed

Notes:

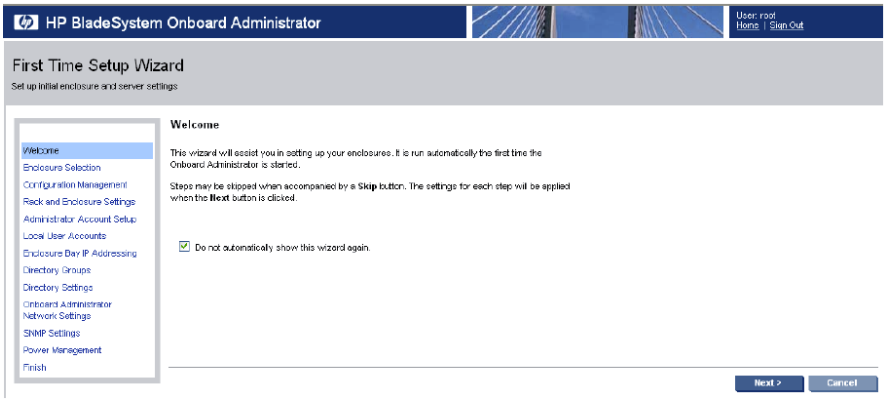
- The enclosure should be provisioned with two onboard administrators. The OA in Bay 2 automatically acquires its configuration from the OA in Bay 1 after the configuration is complete.
- Use this procedure for initial configuration only. Follow 7.7 Replace Onboard Administrator to learn how to replace one of the onboard administrators correctly.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

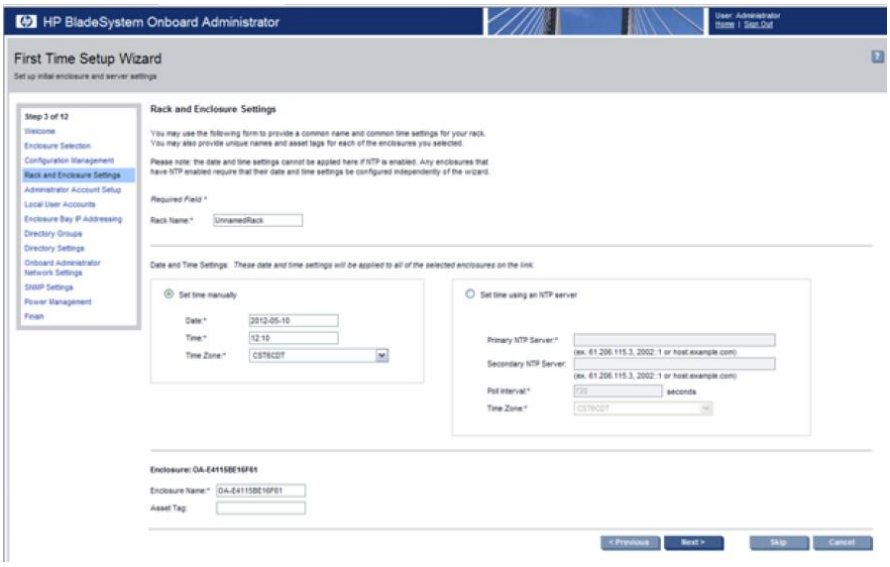
Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results
1. ☐	**OA GUI**: Login	From a web browser, navigate to the OA Bay1 IP address assigned in 7.1 Configure Initial OA IP. `http://<OA_IP>` Login as an administrative user. The original password is on a paper card attached to each OA. 

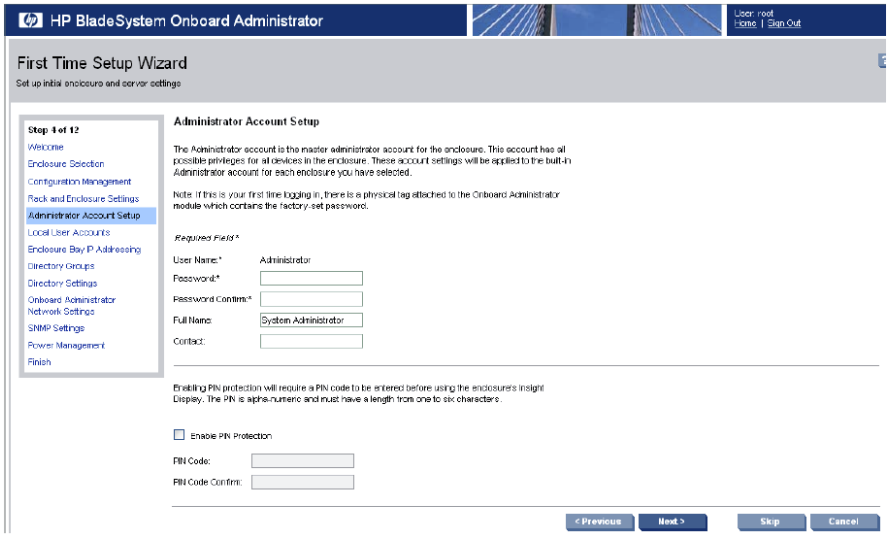
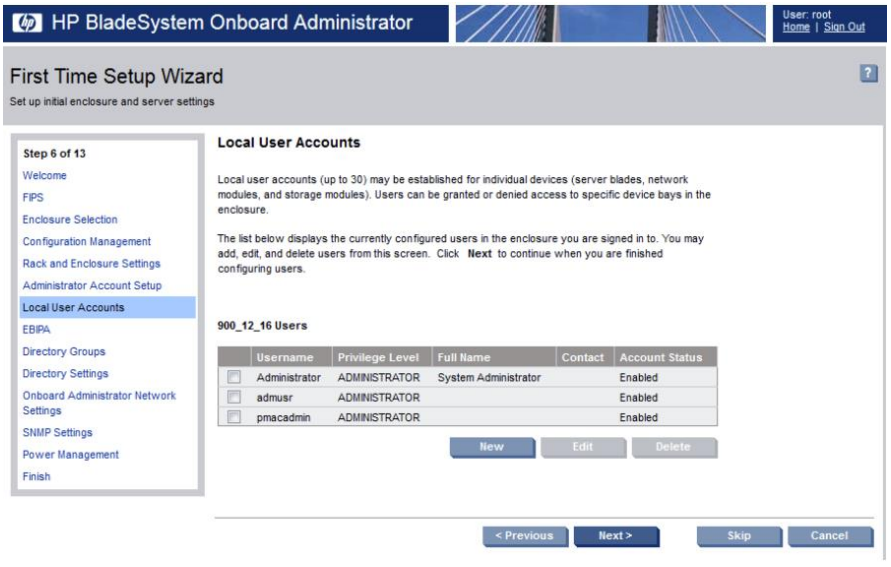
Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results
2. ☐	**OA GUI**: Run First Time Setup Wizard	Run the First Time Setup Wizard.  If needed, navigate to **Wizards > First Time Setup**.
3. ☐	**OA GUI**: Select the enclosure	Click **Next** to select the enclosure to configure. 
4. ☐	**OA GUI**: FIPS screen	Click **Next**. FIPS mode is not currently supported.
5. ☐	**OA GUI**: Enclosure Selection screen	Click **Next** and select the enclosure.
6. ☐	**OA GUI**: Configuration Management screen	Click **Next**. Skip Configuration management.

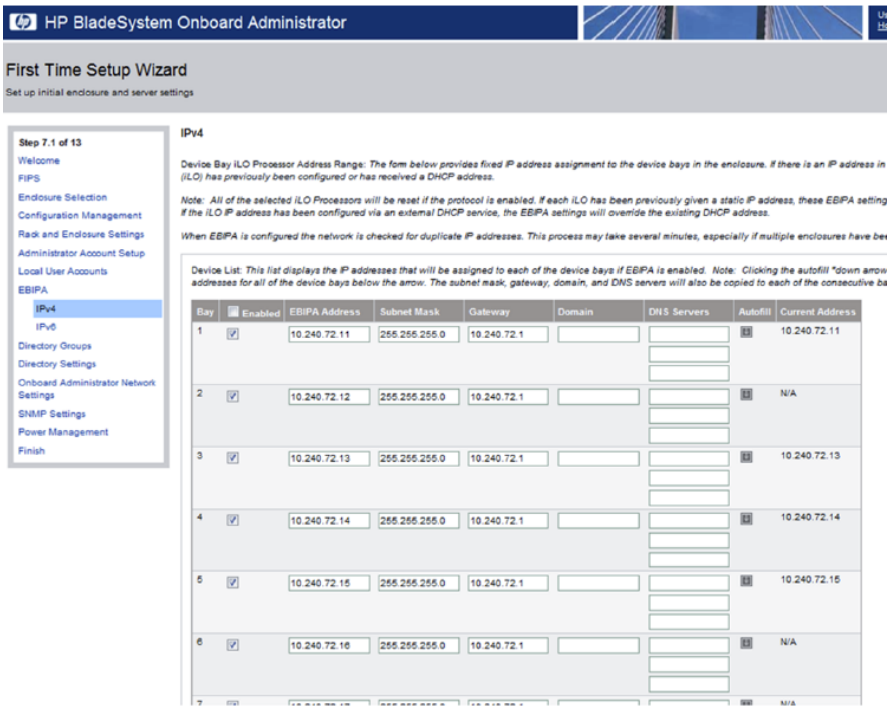
Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results
7. ☐	**OA GUI**: Rack and Enclosure Settings screen	Click **Next** and type: • The **Rack Name** in format xxx_xx. • The **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. • Mark the **Set time using an NTP server** option. • Type the **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. 

Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results
8. ☐	**OA GUI**: Administrator Account Setup screen	Click **Next** and change the administrator password. 
9. ☐	**OA GUI**: Configure EBIPA settings	Click **Next** to create the pmacadmin and admusr user. • On the Local User Accounts screen, click **New** to add pmacadmin user. • Type the **User Name** and **Password**. • Set the Privilege Level to **Administrator**. Refer to the application documentation for the password. • Verify all of the blades have been checked before marking the **Onboard Administrator Bays** checkbox under the User Permissions section. • Click **Add User**. • Repeat to create the admusr user. 

Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results
10. ☐	**OA GUI**: Enclosure Bay IP Addressing	Click **Next** to configure the EBIPA settings. Click **Next** to continue or **Skip** if the EBIPA has been configured. ***Note***: The EBIPA address setup is required. 1. For IPv4, click **First Time Setup Wizard EBIPA: IPv4**. a. From the Device List pane, type the **iLO IP Address**, **Subnet Mask**, and **Gateway** fields for device bays 1-16. Do not fill in the **iLO IP Address**, **Subnet Mask**, and **Gateway** fields for device bays 1A-16A or 1B-16B. ***Note***: Bays 1A-16A and 1B-16B are used for double-density blades, for example, BL2x220c, which are not supported in this release. b. Click **Enabled** for each device bay 1 through 16 in use. ***Notes***: • Any unused slots should have an IP address assigned, but should not be disabled. • Do not use autofill as this will fill the entries for the Device Bays 1A through 16B.  c. Scroll to the Interconnect List (below Device Bay 16B). d. Type the **EBIPA Address**, **Subnet Mask**, and **Gateway** fields for each Interconnect Bay in use. e. Click **Enable** for each Interconnect Bay in use.

Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results

f. Click **Next** to apply settings.

The system may restart devices such as interconnect devices or iLOs to apply new addresses.

g. Check the IP address to ensure the settings are correct.

2. For IPv6, click **First Time Setup Wizard EBIPA: IPv6**.

a. From the Device List pane, type the **iLO IP Address/Prefix** or **Gateway** fields for device bays 1-16.

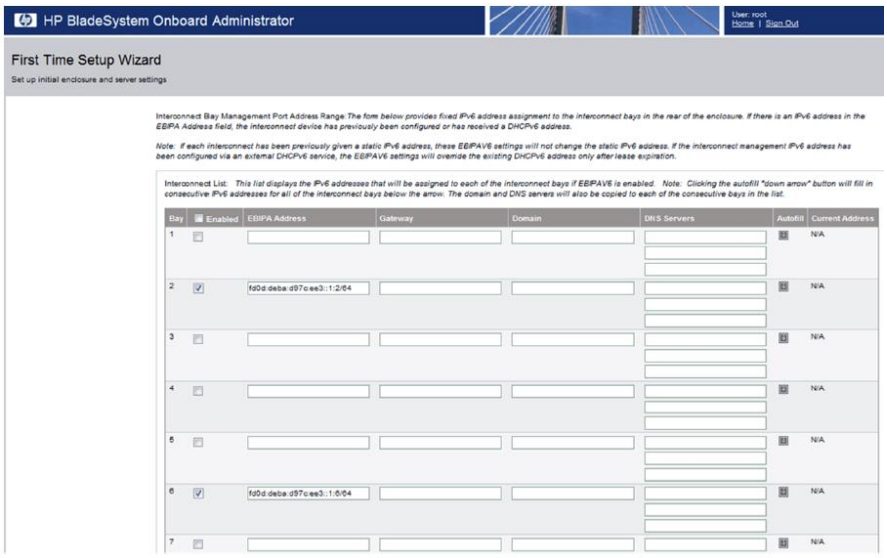
Do not fill in the **iLO IP Address/Prefix** and **Gateway** fields for device bays 1A-16A or 1B-16B.

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

b. Click **Enabled** for each device bay 1 through 16 in use.

Notes:

- Any unused slots should have an IP address assigned, but should not be disabled.
- Do not use autofill as this will fill the entries for the Device Bays 1A through 16B.



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

d. Type the **EBIPA Address/Prefix** and **Gateway** fields for each Interconnect Bay in use.

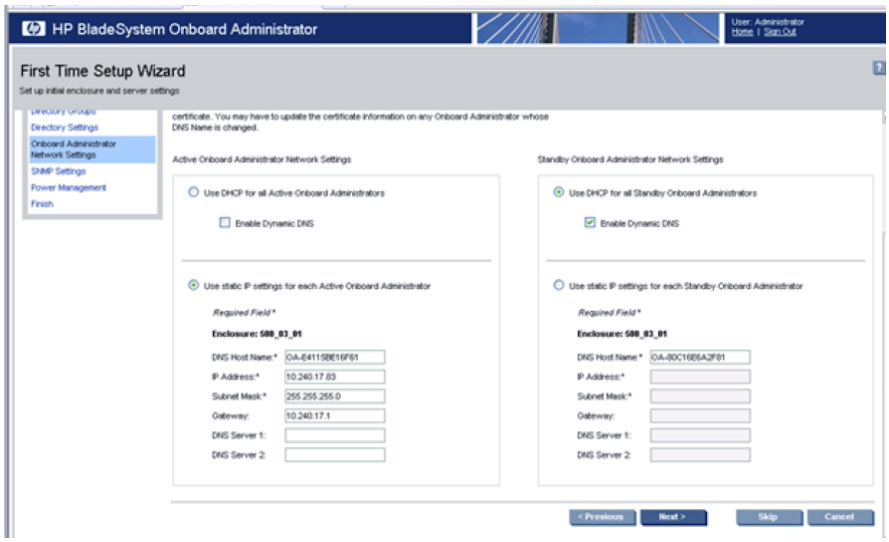
e. Click **Enable** for each Interconnect Bay in use.

f. Click **Next** to apply settings.

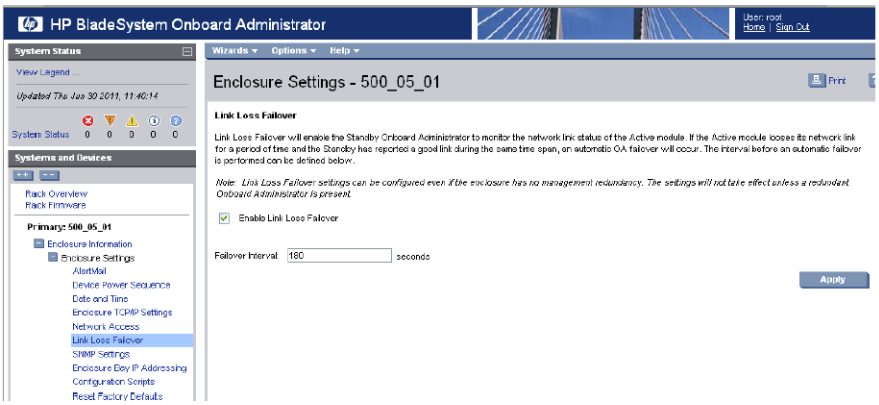
The system may restart devices such as interconnect devices or iLOs to apply new addresses.

g. Check the IP address to ensure the settings are correct.

Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results
11. ☐	**OA GUI**: Directory Groups screen	Skip Directory Group setup.
12. ☐	**OA GUI**: Directory Settings screen	Click **Next**. Skip Directory Settings setup.
13. ☐	**OA GUI**: Onboard Administrator Network Settings screen	Click **Next**. On the Onboard Administrator Network Settings screen, 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 also display. 1. Click **Use static IP settings for each Standby Onboard Administrator**. 2. Type the **IP Address**, **Subnet Mask**, and **Gateway** for the standard OA.  3. Click **Next**. If you changed the IP address of the active OA, you are disconnected. Close your browser and login again using the new IP address.
14. ☐	**OA GUI**: SNMP Settings screen	By default, the **Enable SNMP** checkbox is marked. If you do not want to have SNMP enabled, see Appendix I Disable SNMP on the OA. ***Note***: This step does not set an SNMP Trap Destination. To do this, see 7.10 Add SNMP Trap Destination on OA.

Procedure 42. Configure Initial OA Settings Using the Configuration Wizard

Step	Procedure	Results
15. ☐	**OA GUI**: Power Management screen	Click **Next**. 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 is either **AC Redundant** or **Redundant**, depending on whether the Enclosure is powered by AC or DC. In either case, click **Power Supply Redundant** option. For all other settings on the Power Management screen, leave the default settings unchanged.
16. ☐	**OA GUI**: Finish screen	Click **Next**. Click **Finish**.
17. ☐	**OA GUI**: Set link loss failover	Navigate to **Enclosure Information > Enclosure Settings > Link Loss Failover**. Mark the **Enable Link Loss Failover** checkbox and specify the **Failover Interval** to be **180** seconds. Click **Apply**. 

7.3 Configure OA Security

This procedure disables telnet access to OA.

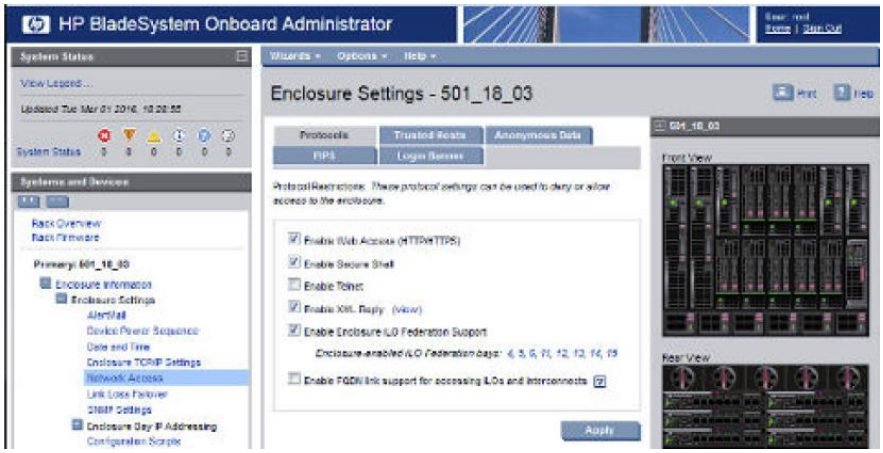
Prerequisite: 7.2 Configure Initial OA Settings Using the Configuration Wizard

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 43. Configure OA Security

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.

Procedure 43. Configure OA Security

Step	Procedure	Results
2. ☐	**OA GUI**: Disable telnet	1. Navigate to **Enclosure Information > Enclosure Settings > Network Access**. 2. Unmark the **Enable Telnet** checkbox. 
3. ☐	**OA GUI**: Apply changes	Click **Apply**.

7.4 Upgrade or Downgrade OA Firmware

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 upgrades or downgrades the firmware on the OAs. The procedure also ensures both OAs have the same firmware version. When the firmware update begins, the standby OA automatically updates first.

Prerequisite: Obtain 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
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

Note: The enclosure should be provisioned with two onboard administrators. This procedure installs the same firmware version on both onboard administrators.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6 is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

7.5 Store OA Configuration on Management Server

This procedure backs up OA settings on the management server.

Prerequisites:

- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the 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 (MOS) for assistance.
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 44. Store OA Configuration on Management Server

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.
2. ☐	**OA GUI**: Store configuration file	1. Navigate to **Enclosure Information > Enclosure Settings > Configuration Scripts**. 2. Open the first configuration file (current settings for enclosure).  3. Store file on the local disk. 4. Click **Show Config**. Copy all text on the screen and save it in a text file or navigate to **File > Save As** and select a filename and path. Select **Text file** as the type. For example, you may select the following syntax for the configuration file name: <enclosure ID>_<timetag>.conf

Procedure 44. Store OA Configuration on Management Server

Step	Procedure	Results

3. ☐	**PMAC**: Back up configuration file	1. Under **/usr/TKLC/smac/etc** directory, you can create your own subdirectory structure. Log into the management server using ssh as admusr and create the target directory:
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/OA_backups/OABackup`
		2. 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`
		3. 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 Appendix A Using WinSCP to copy the file to the management server.
		4. On the PMAC, move the configuration file to the OA Backup folder 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. ☐	**PMAC**: Use PMAC application backup to capture the OA backup	`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
		`PMAC backup been successfully initiated as task ID 7`
		Notes:
		• The backup runs as a background task. To check the status of the background task, use the PMAC GUI Task Monitor screen, or the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
		• The `pmacadm backup` command uses a naming convention that includes a date/time stamp in the file name (for example: backupPmac_20111025_100251.pef). In the example, the backup file name indicates it was created on 10/25/2011 at 10:02:51 am server time.

Procedure 44. Store OA Configuration on Management Server

Step	Procedure	Results

5. ☐	**PMAC**: Verify backup was successful	If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
		The output of `pmaccli getBgTasks` should look similar to this:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`2: Backup PMAC COMPLETE - PMAC 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. ☐	**PMAC**: Save the backup	If the NetBackup feature has not been configured for this PMAC or the Redundant PMAC is not configured in this system, the PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility) the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the **/var/TKLC/smac/backup** directory.
7. ☐	**OA GUI**: Log out	Log out from the OA by clicking **Sign Out** at the top right corner.

7.6 Restore OA Configuration from Management Server

This procedure restores configuration backup from the management server and applies it on the OAs.

Prerequisites:

- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the 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 (MOS) for assistance.
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

It is assumed that:

- 7.5 Store OA Configuration on Management Server has already been performed.
- 7.1 Configure Initial OA IP has been completed before this procedure.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

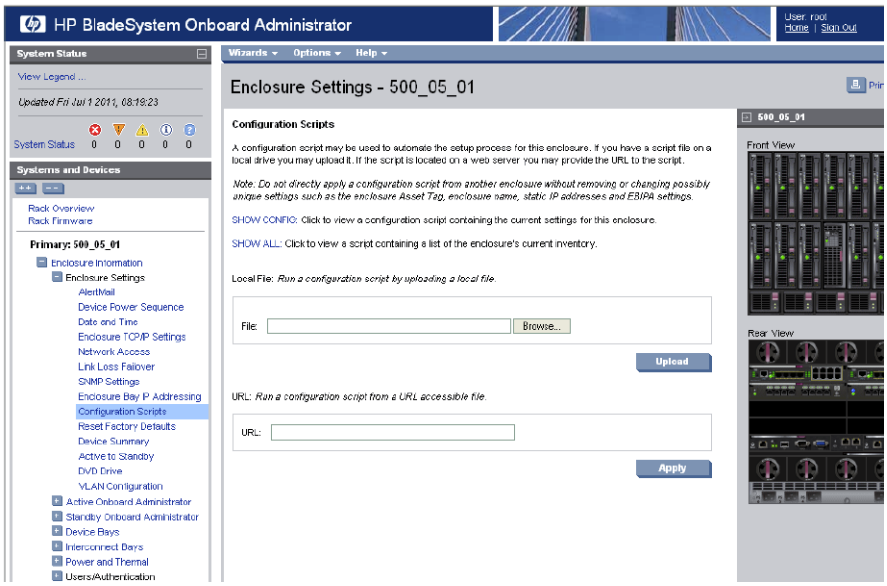
Procedure 45. Restore OA Configuration from Management Server

Step	Procedure	Results

1. ☐	Obtain configuration files from the management server	1. Log into the PMAC server as the **admusr** user.
		2. 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`
		3. Make the file readable by admusr:
		`$ sudo chown admusr /home/admusr/<backup_config_filename>`
		`$ sudo chmod 400 /home/admusr/<backup_config_filename>`
		4. From the PC, use scp or WinSCP to copy the file from admusr@<PMAC 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 Using WinSCP to copy the file to your PC.
		5. On the PMAC, remove the file copied above:
		`$ sudo rm /home/admusr/<backup_config_filename>`
		6. Log out of the PMAC server.

2. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.

Procedure 45. Restore OA Configuration from Management Server

Step	Procedure	Results
3. ☐	**OA GUI**: Restore configuration	1. Navigate to **Enclosure Information > Enclosure Settings > Configuration Scripts**. 2. Use Local file to upload and run the configuration script.  The restore can take 5-10 minutes. A screen displays when the restore is complete that contains logs from the restoration process. Make sure there are no errors. ***Note*** If both OAs were reset to factory defaults and have 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.
4. ☐	**OA GUI**: Log out	Log out from the OA by clicking **Sign Out** at the top right corner.

7.7 Replace Onboard Administrator

This procedure replaces OA in an enclosure with redundant OA.

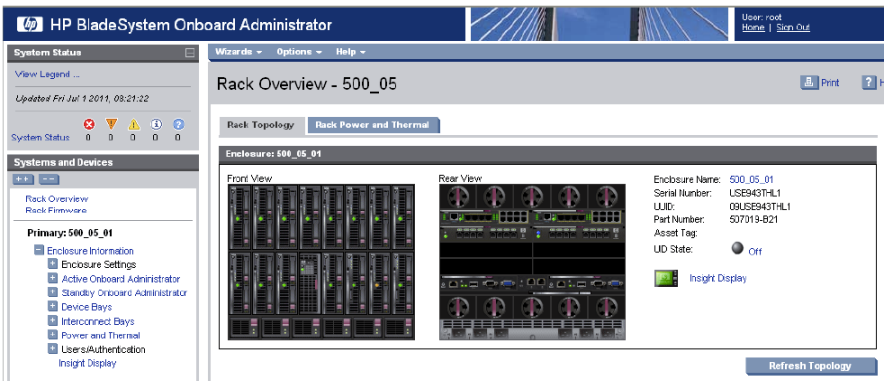
Prerequisites:

- Obtain customer approval needed for OA firmware updates. This procedure can change the version of firmware installed in one or both OAs.
- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the 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 (MOS) for assistance.
- 7.3 Configure OA Security

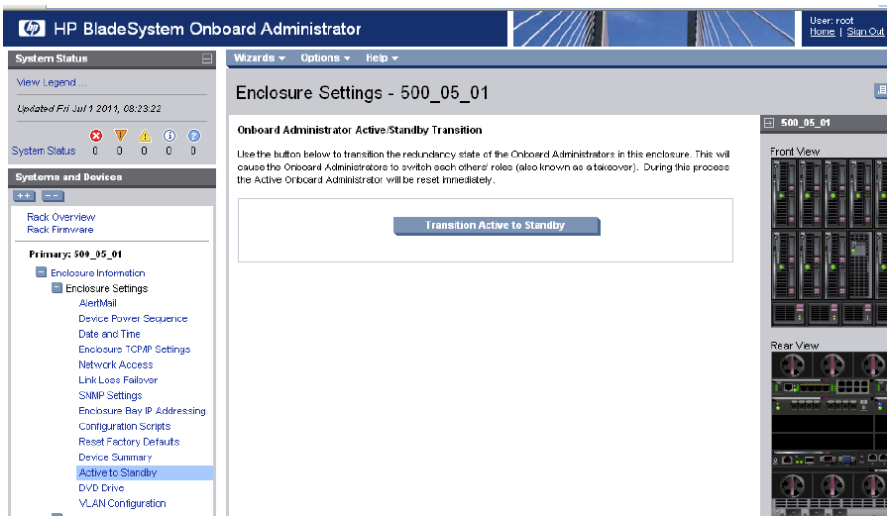
Note: The transfer of configuration occurs only from OA in Bay 1 to OA in Bay 2. Therefore, to keep the current configuration of the system, the insertion of new OA into the OA Bay 1 location should be avoided.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 46. Replace Onboard Administrator

<table>
<tr><th>Step</th><th>Procedure</th><th>Results</th></tr>
<tr><td>1.
☐</td><td>OA GUI: Login</td><td>Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as root.
 
</td></tr>
<tr><td>2.
☐</td><td>OA GUI: Record the IP configuration of the active and standby OAs</td><td>1. Navigate to Enclosure Information > Active Onboard Administrator > TCP/IP Settings.
2. Record the Active OA's IP Address, Subnet Mask, and Gateway.
3. Navigate to Enclosure Information > Standby Onboard Administrator > TCP/IP Settings.
4. Record the Standby OA's IP Address, Subnet Mask, and Gateway.
<table>
<tr><th></th><th>Active</th><th>Standby</th></tr>
<tr><td>OA IP Address</td><td></td><td></td></tr>
<tr><td>OA Subnet Mask</td><td></td><td></td></tr>
<tr><td>OA Gateway</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>3.
☐</td><td>OA GUI: Note the location of the active OA</td><td>Note the location of the active onboard administrator within the enclosure. The active OA has the active LED on. You may also hover over the OA to see its role.
If the OA to be replaced is not the active OA for the enclosure, skip to step 5. ; otherwise, continue with the next step.</td></tr>
</table>

Procedure 46. Replace Onboard Administrator

Step	Procedure	Results
4. ☐	**OA GUI**: Force active OA into standby mode	1. Navigate to **Enclosure Information > Enclosure Settings > Active to Standby** and click **Transition Active to Standby**.  2. Click **OK** when it asks if you are sure. 3. Wait about five minutes until the application reloads and login screen displays.
5. ☐	**OA GUI**: 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 the next step.
6. ☐	**OA GUI**	Move the OA from OA Bay 2 location into the OA Bay 1 location. Wait five minutes so the Onboard Administrator can initialize.
7. ☐	**OA GUI**: 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 initialize.
8. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.
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 7.1 Configure Initial OA IP.
10. ☐	**OA GUI**: Verify the status of the OA	On the Rear View, hover over each OA and verify the Status is **OK**. If the status of one OA or the other is shown as **Degraded** because of a firmware version mismatch, perform 7.4 Upgrade or Downgrade OA Firmware.

Procedure 46. Replace Onboard Administrator

Step	Procedure	Results

11. ☐	**PMAC CLI**: Delete OA SSH keys	Log into the PMAC 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`
		PMAC established new SSH keys the next time it logs into each OA.

7.8 Update IPv4 Address

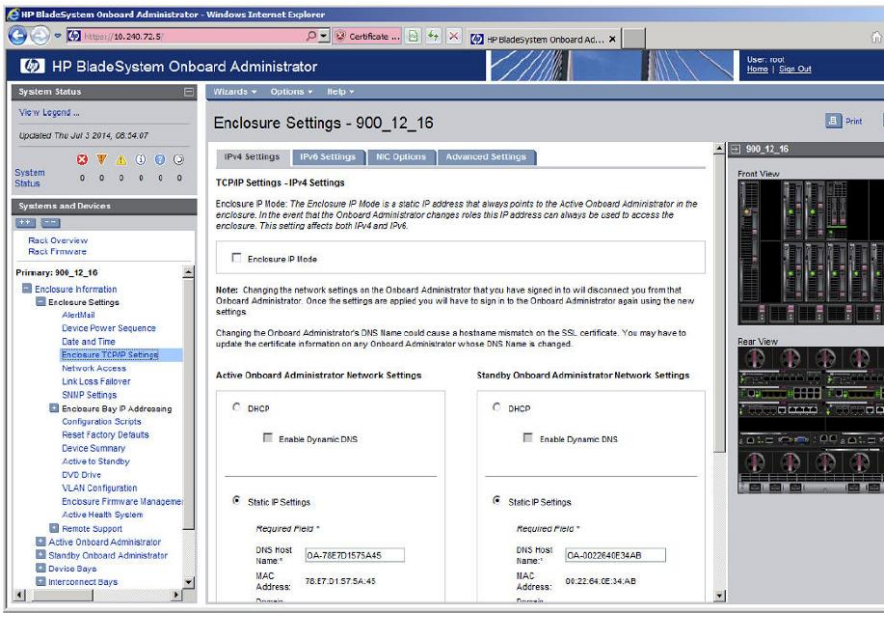
This procedure updates the IP address for a C7000 enclosure.

Prerequisites:

- Obtain address information from the customer.
- The enclosure has been previously configured and the PMAC GUI is reachable over the network.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

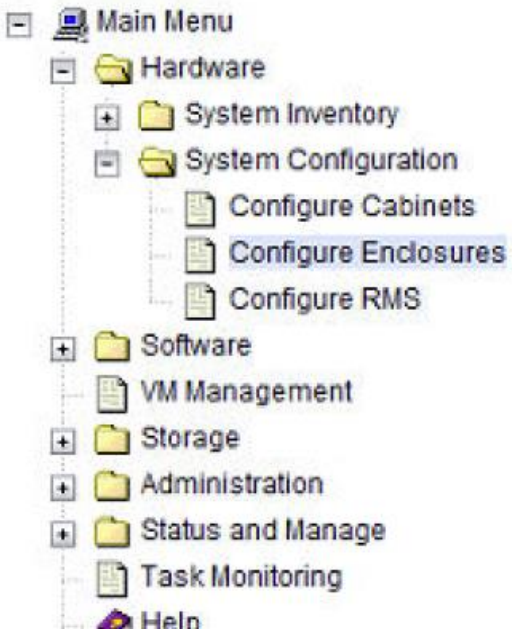
Procedure 47. Update IPv4 Address

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.
2. ☐	**OA GUI**: Update the IPv4 OA settings	Navigate to **Enclosure Information > Enclosure Settings > Enclosure TCP/IP Settings**. 

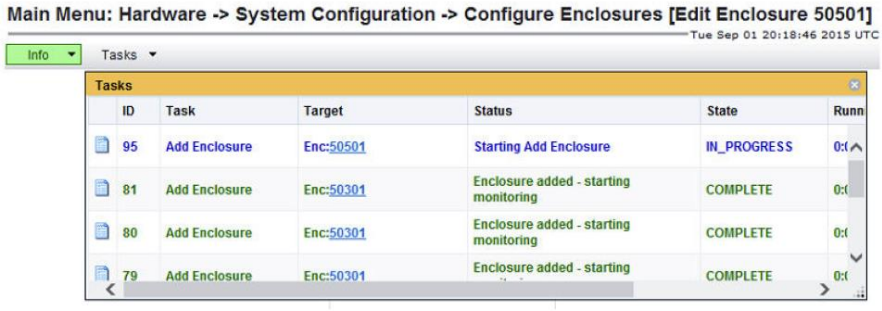
Procedure 47. Update IPv4 Address

Step	Procedure	Results
3. ☐	**OA GUI**: Update the static IP settings for both active and standby OA	Change the: • IP Address • Subnet Mask • Gateway Click **Apply**.
4. ☐	**OA GUI**: Update the EBIPA settings	4. Navigate to Enclosure Information > Enclosure Settings > Enclosure Bay IP Addressing > IPv4 > Device Bays tab. 5. Update the IP settings for the device bays by changing: a. EBIPA Address b. Subnet Mask c. Gateway 6. Click **Apply**. 7. Select the Interconnect Bays tab and update the IP settings for the interconnect device bays by changing: a. EBIPA Address b. Subnet Mask c. Gateway 8. Click **Apply**.
5. ☐	**OA GUI**: Log out	Log out from the OA by clicking **Sign Out** at the top right corner.

Procedure 47. Update IPv4 Address

Step	Procedure	Results
6. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Main Menu > Hardware > System Configuration > Configure Enclosures**. 
7. ☐	**PMAC GUI**: Select the enclosure to edit	On the Configure Enclosures panel, select the enclosure you are modifying and click **Edit Enclosure**.

Procedure 47. Update IPv4 Address

Step	Procedure	Results
8. ☐	**PMAC GUI**: Edit the enclosure address	On the Edit Enclosure panel, update the IP addresses, and click **Edit Enclosure**. The screen refreshes with a new background task entry. Click **Tasks** located on the toolbar under the Configure Enclosures heading.  When the task is complete, the text changes to green and the Progress column indicates 100%.

7.9 Update IPv6 Address

This procedure updates the IP address for a C7000 enclosure. It can be used to add IPv6 addresses or edit existing IPv6 addresses.

Prerequisites:

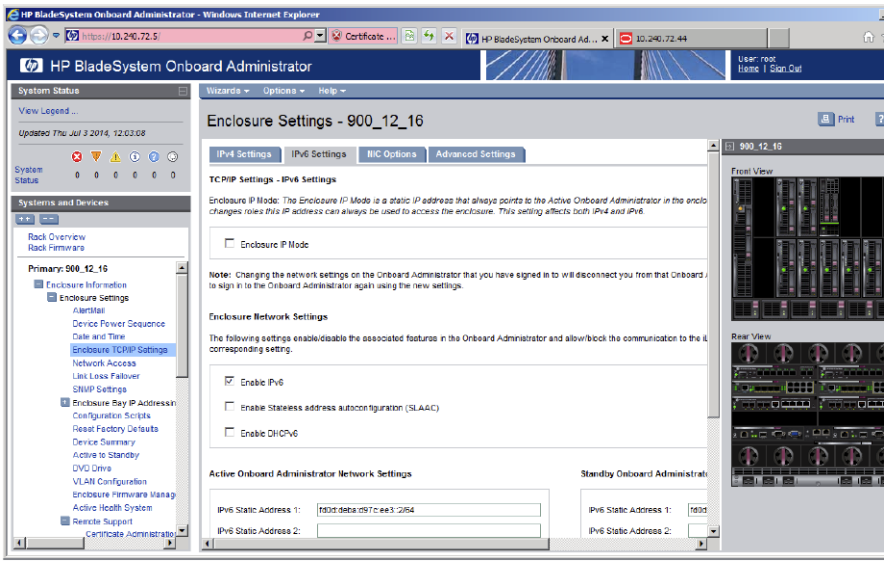
- Obtain address information from the customer.
- The enclosure has been previously configured and the PMAC GUI is reachable over the network.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

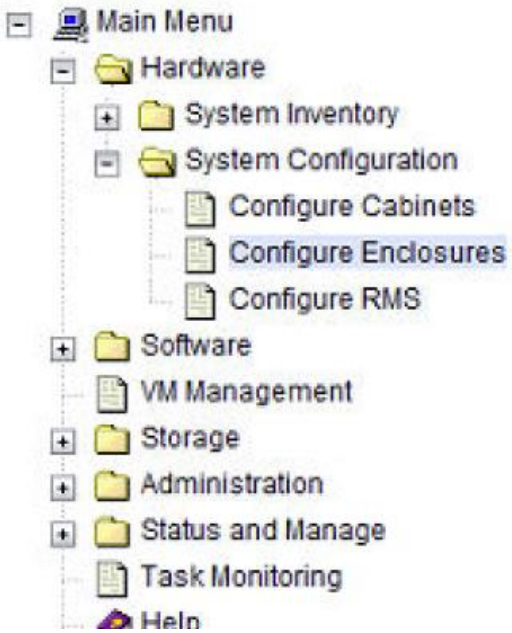
Procedure 48. Update IPv6 Address

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.

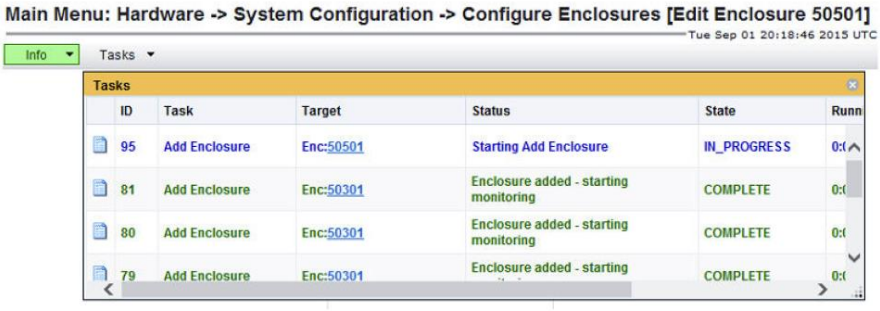
Procedure 48. Update IPv6 Address

Step	Procedure	Results
2. ☐	**OA GUI**: Update the IPv6 OA settings	Navigate to **Enclosure Information > Enclosure Settings > Enclosure TCP/IP Settings IPv6 Settings** tab. 
3. ☐	**OA GUI**: Verify	Under Enclosure Network Settings, verify the **Enable IPv6** checkbox is marked.
4. ☐	**OA GUI**: Update the static IP settings for both active and standby OA	Change the: • IPv6 Static Address a • Static Default Gateway Click **Apply**.
5. ☐	**OA GUI**: Update the EBIPA settings	1. Navigate to **Enclosure Information > Enclosure Settings > Enclosure Bay IP Addressing > IPv6 > Device Bays** tab. 2. Update the IP settings for the device bays by making sure **Enabled** is checked and changing: • EBIPA Address • Gateway 3. Click **Apply**. 4. Select the Interconnect Bays tab and update the IP settings for the interconnect device bays by making sure **Enabled** is checked and changing: • EBIPA Address • Gateway 5. Click **Apply**.
6. ☐	**OA GUI**: Log out	Log out from the OA by clicking **Sign Out** at the top right corner.

Procedure 48. Update IPv6 Address

Step	Procedure	Results
7. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Main Menu > Hardware > System Configuration > Configure Enclosures**. 
8. ☐	**PMAC GUI**: Select the enclosure to edit	On the Configure Enclosures panel, select the enclosure you are modifying and click **Edit Enclosure**.

Procedure 48. Update IPv6 Address

Step	Procedure	Results
9. ☐	**PMAC GUI**: Edit the enclosure address	On the Edit Enclosure panel, update the IP addresses, and click **Edit Enclosure**. The screen refreshes with a new background task entry. Click **Tasks** located on the toolbar under the Configure Enclosures heading.  When the task is complete, the text changes to green and the Progress column indicates 100%.

7.10 Add SNMP Trap Destination on OA

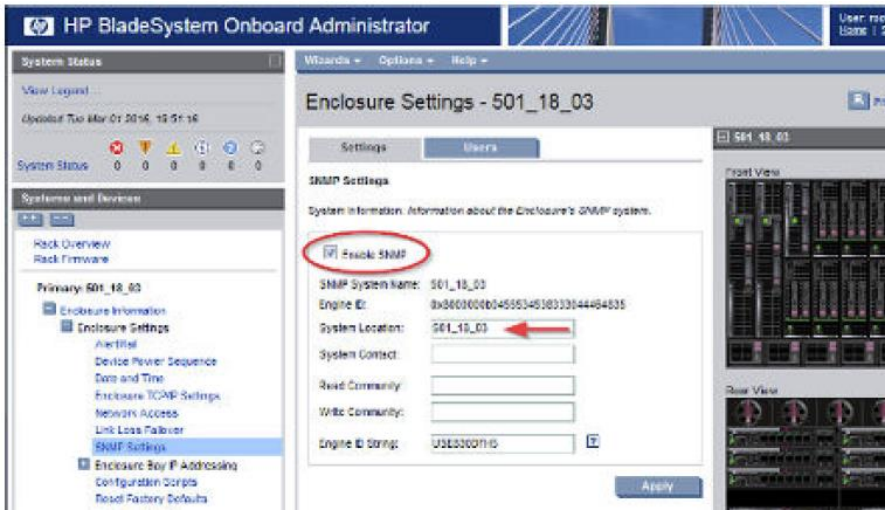
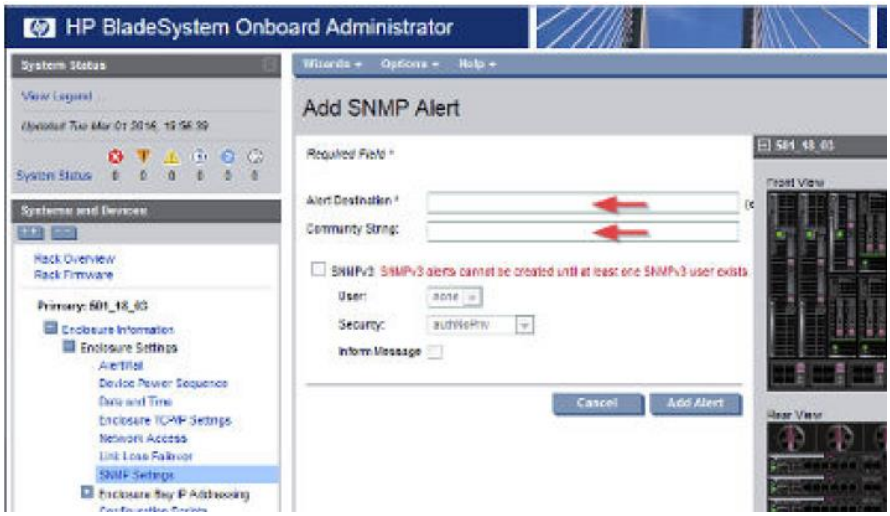
This procedure adds an SNMP trap destination and configures it using the OA.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 49. Add SNMP Trap Destination on OA

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.

Procedure 49. Add SNMP Trap Destination on OA

Step	Procedure	Results
2. ☐	**OA GUI**: SNMP Setting screen	1. Navigate to **Enclosure Information > Enclosure Settings > SNMP Settings**. 2. If SNMP is not already enabled, mark the **Enable SNMP** checkbox. 3. Type the enclosure name (shown in the title bar) or your preferred name as the **System Location**.  Do not set Read Community and Write Community. 4. Click **Apply**.
3. ☐	**OA GUI**: Add SNMP alert destination	1. Click **New**. 2. Type the destination information into the Alert Destination box (for example, 61.206.115.3, 2002::1 or host.example.com). 3. Type the **Community String**.  4. Click **Add Alert**. 5. Repeat for each required destination.

7.11 Disable SNMP Trap Destination on OA

This procedure disables an SNMP trap destination using the OA.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 50. Disable SNMP Trap Destination on OA

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.
2. ☐	**OA GUI**: SNMP Setting screen	1. Navigate to **Enclosure Information > Enclosure Settings > SNMP Settings**. 2. Unmark the **Enable SNMP** checkbox. 3. Click **Apply**.

7.12 Delete SNMP Trap Destination on OA

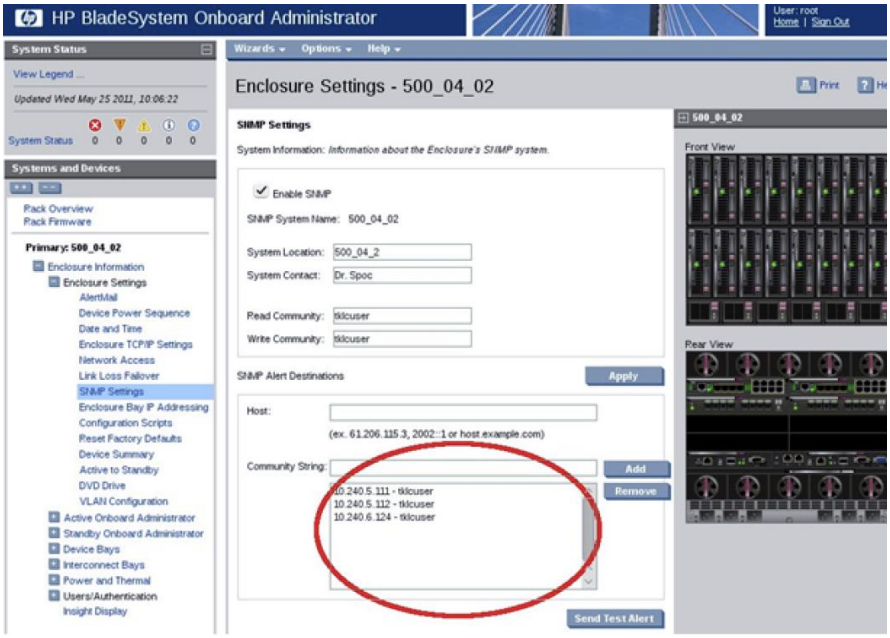
This procedure removes an SNMP trap destination from the OA.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 51. Delete SNMP Trap Destination on OA

Step	Procedure	Results
1. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.

Procedure 51. Delete SNMP Trap Destination on OA

Step	Procedure	Results
2. ☐	**OA GUI**: SNMP Setting screen	1. Navigate to **Enclosure Information > Enclosure Settings > SNMP Settings**. All configured SNMP trap destination display. 2. Select the trap destination and click **Remove**.  If no SNMP trap destinations display, then you may want to disable SNMP by unmarking the **Enable SNMP** checkbox. 3. Click **Apply** to activate the configuration. When the progress meter disappears the configuration has been applied.

8. Management Server Procedures

8.1 IPM Management Server

This procedure configures and IPMs the DL360, DL380, or Oracle rack mount server.

Needed Material: TPD Initial Product Manufacture Software Installation Procedure, E53017.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 52. IPM the Management Server

Step	Procedure	Results
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` ***Notes***: • If you are using a serial console for installation, do not use the `console=tty0` option. • 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.

8.2 Upgrade Management Server Firmware

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 [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

8.2.1 Upgrade DL360/DL380 Server Firmware

This procedure upgrades the DL360 or DL380 server firmware.

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

Prerequisite: 8.1 IPM Management Server

Needed Material

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- USB Flash Drive (4GB or larger) if upgrading with USB media.

Note: For the **Update Firmware Errata** step, check [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes to see if there are any firmware errata items that apply to the server being upgraded. If there is, there is 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.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6 is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

8.2.2 Upgrade Oracle Rack Mount Server Firmware

This procedure updates firmware on Oracle RMS.

Needed Material

- Oracle Firmware Upgrade Pack 3.x.x Release Notes
- Oracle Firmware Upgrade Pack 3.x.x Upgrade Guide

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

The minimum supported Oracle Firmware Upgrade Pack for Platform 7.6 is release 3.1.6. However, when upgrading firmware, it is recommended that the latest release be used. Refer to Oracle Firmware Upgrade Pack Release Notes for procedures on how to obtain the firmware, then follow the procedures in the Oracle Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

9. PMAC Procedures

Deploying a VM guest in the absence of a PMAC is complicated. To facilitate this, the PMAC media includes a guest archive and a script that deploys the running PMAC into a state where the Initialization process can begin. The general procedure is:

- Install TVOE 3.5 on the management server using the ILO.
- Create and configure the management bridge.
- Attach PMAC 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 PMAC.
- Perform Initial Configuration.

Needed Material

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 PMAC 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 into 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 uses the default MTU size.
  - If the PMAC NetBackup feature is enabled, and the backup service will be routed, with a source interface different from the management interface where the default route is applied, then define the route during PMAC initialization as a host route to the NetBackup server.
- The PMAC initialization profiles have been designed to configure the PMAC's networks and features. Profiles must identify interfaces. Existing profiles provided by PMAC use standard named interfaces (control, management). No VLAN tagging is expected on the PMAC's interfaces, all tagging should be handled on the TVOE management server configuration.

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 these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

Network Interface	DL360 (without HP NC364T 4pt Gb)	DL360 (with HP NC364T 4pt Gb in PCI Slot 2)	DL380 (with only LOM 4pt NICs) (G6)	DL380 (with HP 4pt Gb in PCI Slot 1) (Gen8, 9)	DL380 (with HP 4pt Gb 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	X7-2	
<ethernet_interface_1>	eth01	eth01	eth01	eth01	eth01	eth01	eth01	eth02	eth01
<ethernet_interface_2>	eth02	eth02	eth02	eth02	eth02	eth02	eth03	eth03	eth02
<ethernet_interface_3>		eth21		eth11	eth31	eth03	eth02	eth21	eth03
<ethernet_interface_4>		eth22		eth12	eth32	eth04	eth04	Eth23	eth04
<ethernet_interface_5>		eth23		eth04	eth04				eth05

PMAC Interface Alias	TVOE Bridge Name	TVOE Bridge Interface
control	control	<TVOE_Control_Bridge_Interface> _____ Default is bond0
management	<TVOE_Management_Bridge> _____	<TVOE_Management_Bridge_Interface> _____

PMAC Interface Alias	TVOE Bridge Name	TVOE Bridge Interface
NetBackup	<TVOE_NetBackup_Bridge> _____	<TVOE_NetBackup_Bridge_Interface> _____

Variable and Description	Value
<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> has 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 is 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 is on a tagged VLAN coming in on bond0.	
<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 PMAC for participation in the NetBackup network.	
<PMAC_NetBackup_IP_address> The IP address assigned to the PMAC 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.	

Variable and Description	Value
<PMAC_mgmt_IP_address> The PMAC 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 PMAC application's IP address on the control network.	
<control_netmask> The IP netmask for the control network.	

Network Bond Interface	Enslaved Interface 1	Enslaved Interface 2
bond0	For segregated networks only	
bond1		
bond2		Bonding used for abstraction only, not multiple interfaces

9.1 Install TVOE on the Management Server

Install the TVOE hypervisor platform on the management server. The PMAC is not available to do an IPM using TVOE on the management server. It is necessary to provide the TVOE media using a bootable USB drive.

Needed Material: TPD or TVOE installation media to be used for IPM.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

1. Configure the iLO IP address. For more information, refer to Appendix F in the [1] TPD Initial Product Manufacture Software Installation Procedure.
2. Configure and IPM the DLL360 or DL380 server by following 8.1 IPM Management Server.

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

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

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

9.2 Configure TVOE Network

This procedure configures the TVOE network.

Prerequisite: 9.1 Install TVOE on the Management Server

Note: The output shown in this procedure is for illustrative purposes only. The site information for the system determines the network interfaces (network devices, bonds, and bond-enslaved devices) to configure.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 53. Configure the TVOE Network

Step	Procedure	Results
1. ☐	**TVOE Management Server iLO**: Login	1. Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. `http://<management_server_iLO_IP>` 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click **Yes** if the Security Alert displays.
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. `$ 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	`$ 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.

4. ☐	**TVOE iLO**: Create a tagged control interface and bridge (optional)	If you are using a tagged control network interface on this PMAC, 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>`

Procedure 53. Configure the TVOE Network

Step	Procedure	Results

5. ☐	**TVOE Management Server**: Verify the non-segregated management network	This step only applies if the management network is tagged (non-segregated). This example 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.
		This example shows a PMAC management server configuration in a non-segregated network, untagged control network, and a tagged management network.
		Create a tagged device for the 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	This step only applies if the management network is untagged (segregated). This example shows the management bridge 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 bridge has been configured, skip to the next step.
		`$ 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`

Procedure 53. Configure the TVOE Network

Step	Procedure	Results

7. ☐	**TVOE Management Server**: Verify the management bridge	This example 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.
		For this example, create a tagged device for the management device.
		`$ 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>`

Procedure 53. Configure the TVOE Network

Step	Procedure	Results

8. ☐	**TVOE Management Server**: Verify the NetBackup network, if needed	If the NetBackup feature is not needed, skip to the next step.
		This example 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.
		This example shows a TVOE management server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size. 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>`

Procedure 53. Configure the TVOE Network

Step	Procedure	Results

9. ☐	**TVOE Management Server**: Set up 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`
		This example shows 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`
		This example shows 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	This example 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.
		This example adds the default route on a 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`

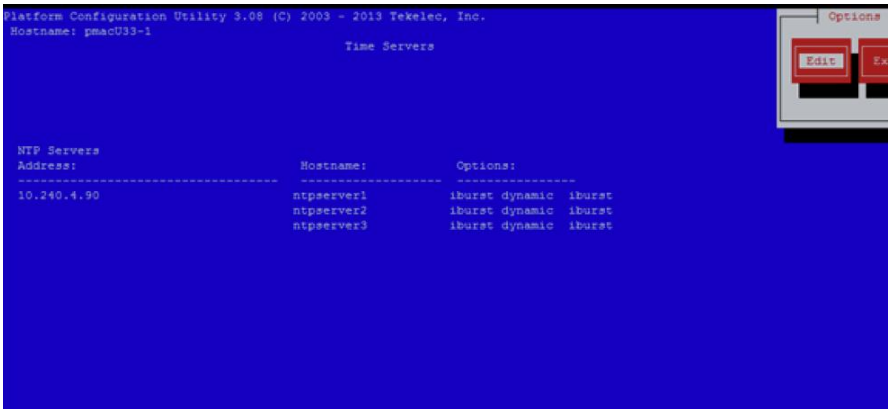
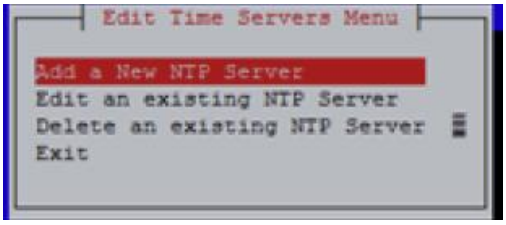
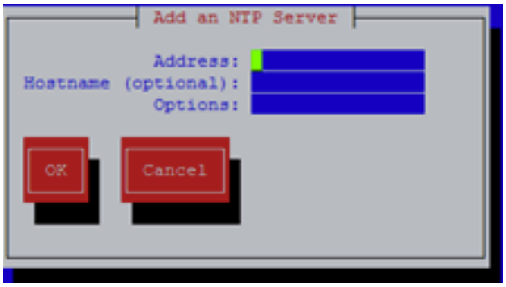
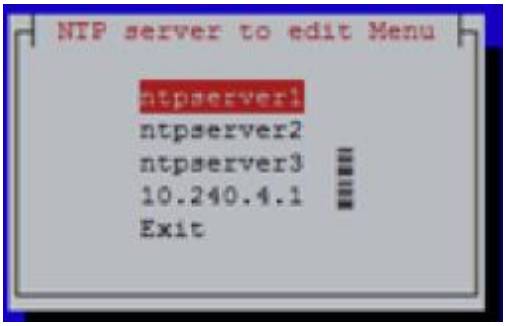
Procedure 53. Configure the TVOE Network

Step	Procedure	Results

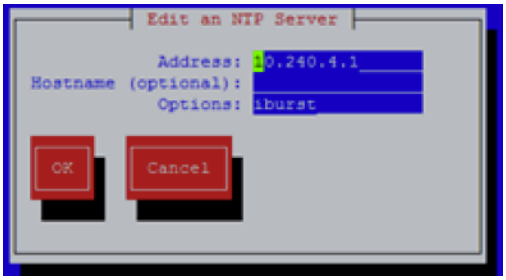
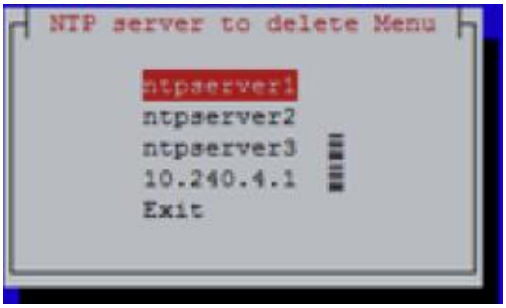
11. ☐	**TVOE Management Server**: Verify the NetBackup route (optional)	If the NetBackup network is a unique network for NetBackup data, verify the existence of the appropriate NetBackup route.
		This example shows the route on the NetBackup bridge is configured.
		If the NetBackup route is to be a network 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.
		This example adds 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`
		This example adds a host route on management network.
		Note: For the configuration of a host route, the <TVOE_NetBackup_Netmask> is 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. Click **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. Click **Edit**. 3. Set the time zone and/or hardware clock to GMT (Greenwich Mean Time). 4. Click **OK**. 5. Navigate out of Server Configuration.
14. ☐	**TVOE Management**	Three or more NTP sources are required. 1. Login as the **platcfg** user on the server.

Procedure 53. Configure the TVOE Network

Step	Procedure	Results
	Server: Configure NTP servers for a server based on TPD	2. Navigate to **Network Configuration > NTP**.  3. Click **Edit**. 4. Click **Add a New NTP Server**.  5. Type the appropriate data and click **OK**.  The default NTP option is iburst. Additional NTP options are listed on the ntp.conf man page, some of the valid options are burst, minpoll, and maxpoll. 6. Click **Edit an existing NTP Server**. 

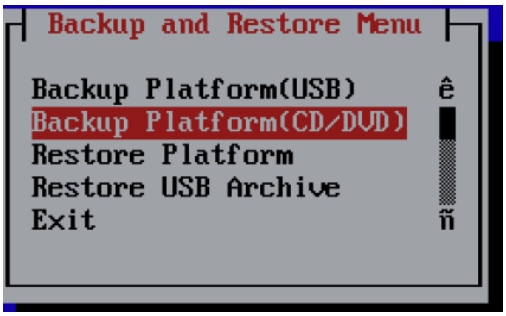
Procedure 53. Configure the TVOE Network

Step	Procedure	Results
		7. Select the NTP server and edit information as needed.  8. If deleting an existing NTP server, select **Delete an existing NTP Server**.  9. Select the NTP server and press **Enter**. 10. Click **Yes** to confirm deleting the NTP server. 11. Restart the NTP server. 12. Click **Exit** on each menu until platcfg exits.
15. ☐	**TVOE Management Server**: Set SNMP trap destination to a server based on TPD	All alarm information is sent to the NMS located at the destination. Follow 12.3 Add SNMP Trap Destination on TPD-Based Application. ***Note***: If NetBackup is to be configured, execute 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and then execute 13.2 Configure TVOE NetBackup Client on the TVOE host.
16. ☐	**TVOE Management Server**: Verify server health	`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus` Alarms may display if network connectivity has not been established.

17. ☐	**TVOE Management Server**: Set time based on NTP server	`$ sudo /sbin/service ntpd stop`
		`$ sudo /usr/sbin/ntpdate ntpserver1`
		`$ sudo /sbin/service ntpd start`
		Reboot the server.
		`$ sudo /sbin/init 6`

Procedure 53. Configure the TVOE Network

Step	Procedure	Results

18. ☐	**TVOE Management Server**: Back up system files to use when restoring a system	***Note***: The backup image is to be transferred to a customer device.
		1. Login as the **platcfg** user on the server.
		2. Navigate to **Maintenance > Backup and Restore**.
		3. Click **Backup Platform (CD/DVD)**.
		 
		Note: If this operation is attempted on a system without media (for example, the CD/DVD), a **No disk device available. This is normal on systems without a CD ROM device** message displays. Ignore the message and press any key to continue.
		4. Click **Build ISO file only**.
		The **Creating ISO Image. . .** message may display.
		After the ISO is created, platcfg returns to the Backup TekServer Menu screen. The ISO has now been created and is located in the **/var/TKLC/bkp/** directory. An example filename of a backup file created is **hostname1307466752-plat-app-201104171705.iso**.
		5. Click **Exit** on each menu until platcfg exits.
		The SSH connection to the TVOE server terminates.
		6. Log into the customer server and copy the 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**.
		`# 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 Appendix A Using WinSCP to copy the backup image to the customer system.

9.3 Deploy PMAC Guest

The pmac-deploy script deploys a PMAC guest in the absence of a PMAC to create the guest and install the OS and application. This is done at build time and the system disk image is kept on the PMAC media, along with this script. The media is either physical media (USB) or a disk image (.iso file) from OSDC. The media can be stored on a USB and mounted. It can be downloaded to the TVOE (usually /var/TKLC/upgrade), but that is recommended only for lab deployments and depends on the storage available on the TVOE host. Once the PMAC media is mounted, the pmac-deploy script can be found in the upgrade directory of the media.

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- PMAC Installation Media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 54. Deploy PMAC Guest

Step	Procedure	Results
1. ☐	**TVOE Management Server iLO**: Login	1. Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. `http://<management_server_iLO_IP>` 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click **Yes** if the Security Alert displays. ***Note***: Alternatively, you can log into the management console through PuTTY. Connect to the server using **<management_server_iLO_IP>** Start the virtual serial port by executing the **vsp** command. Log into the remote server using **admusr** credentials.

2. ☐	**TVOE Management Server**: Mount the PMAC 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-PMACx86_64.iso /mnt/upgrade`

Procedure 54. Deploy PMAC Guest

Step	Procedure	Results

3. ☐	**TVOE Management Server**: Validate the PMAC 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.

Procedure 54. Deploy PMAC Guest

Step	Procedure	Results

4. ☐	**TVOE Management Server**: Deploy PMAC instance	Using the pmac-deploy script, deploy the PMAC instance using the configuration detailed by the completed NAPD.
		For this example, a PMAC is deployed without NetBackup.
		`$ 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 PMAC with the NetBackup feature requires the **--netbackupVol** option, which creates a separate NetBackup logical volume on the TVOE host of PMAC. If the NetBackup feature's source interface is different from the management interface, include the **--bridge** and **--nic** as shown in this example.
		`$ cd /mnt/upgrade/upgrade`
		`$ sudo ./pmac-deploy --guest=<PMAC_Name>`
		`--hostname=<PMAC_Name>`
		`--controlBridge=<TVOE_Control_Bridge>`
		`--controlIP=<PMAC_Control_ip_address>`
		`--controlNM=<PMAC_Control_netmask>`
		`--managementBridge=<PMAC_Management_Bridge>`
		`--managementIP=<PMAC_Management_ip_address>`
		`--managementNM=<PMAC_Management_netmask_or_prefix>`
		`--routeGW=<PMAC_Management_gateway_address>`
		`--ntpserver=<TVOE_Management_server_ip_address>`
		`--netbackupVol`
		`--bridge=<TVOE_NetBackup_Bridge>`
		`--nic=netbackup`
		`--isoimagesVolSizeGB=20`
		Note: The NUMA settings can be configured using new options added to the pmac-deploy command. Please see section Configuring NUMA on pmac-deploy for instructions on using the new options.
		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>`

Procedure 54. Deploy PMAC Guest

Step	Procedure	Results

5. ☐	**TVOE Management Server**: Unmount the media and remove	After the PMAC deploys and boots, the management and control network comes up. At that point unmount the media and remove the PMAC media.
		`$ cd /`
		`$ sudo /bin/unmount /mmmnt/upgrade`

9.4 Set Up PMAC

This procedure configures the PMAC application environment on the management server TVOE host; and initializes the PMAC application. When this procedure is complete, the PMAC application environment is configured to allow configuration of system network assets associated with the management server.

Prerequisite: 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 55. Set Up PMAC

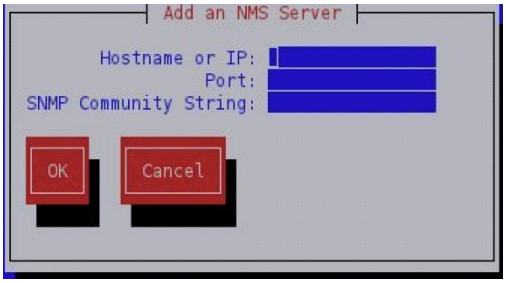
Step	Procedure	Results
1. ☐	**TVOE Management Server iLO**: Login	1. Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. `http://<management_server_iLO_IP>` 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click **Yes** if the Security Alert displays.

2. ☐	**TVOE Management Server iLO**: Login	Log into PMAC with **admusr** credentials.
		Note: On a TVOE host, if you open the virsh console, for example, `$ 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, run `ps -ef |grep virsh`, and 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 7.5 (Final)`
		`Kernel 2.6.32-358.6.1.el6prerel6.5.0_82.16.0.x86_64 on an x86_64`
		`pmacU17-1 login:`

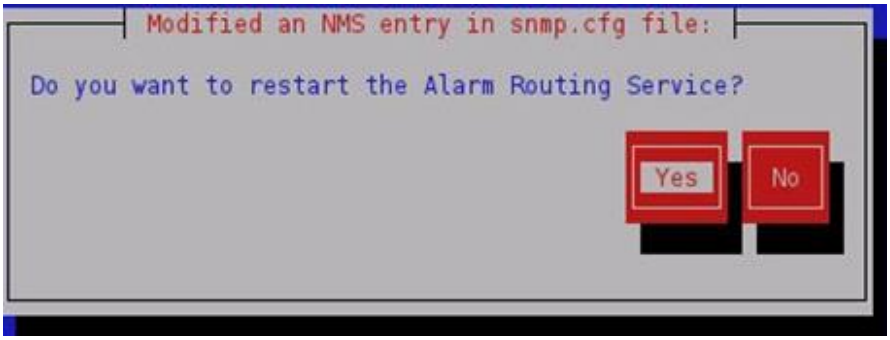
Procedure 55. Set Up PMAC

Step	Procedure	Results
3. ☐	**TVOE Management Server iLO**: Verify PMAC configure correctly	Run the following command (there should be no output): `$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/`

4. ☐	**TVOE Management Server iLO**: Determine and set the time zone	Valid time zones can be found on the server in the /usr/share/zoneinfo directory. Only time zones within the sub-directories (for example, America, Africa, Pacific, Mexico, etc.) are valid with platcfg.
		To set the time zone, run:
		`$ sudo /usr/TKLC/smac/bin/set_pmac_tz.pl <timezone>`
		For Example:
		`$ sudo set_pmac_tz.pl America/New_York`
		Verify the time zone has been updated by running:
		`$ sudo /bin/date`

5. ☐	**TVOE Management Server**: Set SNMP trap destination to a server based on TPD	All alarm information is sent to the NMS located at the destination. 1. Login as the **platcfg** user on the server. 2. Navigate to the NMS Server Configuration screen. 3. Navigate to **Network Configuration > SNMP Configuration > NMS Configuration**.  4. Click **Edit**. 5. Click **Add a New NMS Server**. 6. Type the appropriate data and click **OK**. 

Procedure 55. Set Up PMAC

Step	Procedure	Results
		7. Click **Exit** and **Yes**.  8. Click **Exit** on each menu until platcfg exits.
6. ☐	**TVOE Management Server iLO**: Login	Log into the PMAC as the **admusr** user.
7. ☐	**TVOE Management Server iLO**: Reboot	Reboot the server to ensure all processes are started with the new time zone. `$ sudo /sbin/init 6`

8. ☐	**PMAC** (optional)	Gather and prepare configuration files that must be located on the PMAC. These may be required to proceed with the application installation after the PMAC has been deployed, but before it has been initialized. These files are usually located within a given ISO on the physical media.
		Note: This is an optional step only required if needed by an application.
		Needed Material
		• HP Misc. Firmware DVD
		• [2] HP Solutions Firmware Upgrade Pack
		1. Once the PMAC has completed rebooting, but before initializing, log into the PMAC as **admusr** using virsh on the management server iLO.
		2. Create any necessary destination subdirectories in the PMAC **/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.
		`$ 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>`
		3. Make the media available to the TVOE host server. Mount the media on the TVOE host using the following method:
		a. Insert the USB into an available USB slot on the TVOE host server and execute the following command to determine its location and the

Procedure 55. Set Up PMAC

Step	Procedure	Results

		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 added to the list of media devices once it is inserted into a USB slot on the TVOE host server.
		b. 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.
		c. 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`
		4. Execute the following commands on the PMAC guest to copy the required files from the TVOE host to the PMAC 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>`
		5. Remove the application media from the TVOE host:
		`$ sudo /bin/unmount /mnt/upgrade`

9. ☐	**PMAC Application**: Initialize	If performing the setup on a redundant PMAC, do not initialize, skip this step, and continue with step 12.
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`1: Initialize PMAC COMPLETE - PMAC 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:`
		The command displays **IN_PROGRESS** for a short time. Run the command until a **COMPLETE** or **FAILED** response displays.

Procedure 55. Set Up PMAC

Step	Procedure	Results

10. ☐	**PMAC**: Perform a system health check	`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`
		This command should return no output on a healthy system.
		Note: An NTP alarm is 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:
		`PMAC 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.`

11. ☐	**PMAC Application**: Verify release	Verify the PMAC application product release is as expected.
		Note: If the PMAC application product release is not as expected, STOP and contact My Oracle Support (MOS).
		`$ 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`

12. ☐	**Virsh Console**: Log out	Exit the virsh console session using Appendix E.2 Exit a Guest Console Session on an iLO.
13. ☐	**Management Server iLO**: Exit the TVOE console	`$ logout` Close the iLO browser screen.
14. ☐	**Management Server iLO**	If NetBackup needs to be configured on this PMAC, execute 9.22.2 Initialize PMAC Application Using the GUI and enable NetBackup.

9.5 Configure PMAC Application

Configuration of the PMAC application is typically performed using the PMAC 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 PMAC configuration.

Prerequisites:

- PMAC has been deployed and initialized, but possibly not fully configured.
- Aggregation switches have been properly configured.

Note: The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 56. Configure PMAC Application

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Administration > PMAC Configuration**.
2. ☐	**PMAC GUID**: Select a profile	Click **Feature Configuration**.

Procedure 56. Configure PMAC Application

Step	Procedure	Results
3. ☐	**PMAC GUID**: Configure optional features	If NetBackup is to be used, enable the NetBackup feature; otherwise, use the selected features as is. This image is for reference only.  The **Enabled** checkbox selects the desired features. The **Role** field provides a list of known network roles with which the feature may be associated. The **Description** may be edited if desired. If the feature should be applied to a new network role (e.g., NetBackup), click **Add Role**. Enter the name of the new role and click **Add**. ***Note***: Role names are not significant, they are only used to associate features with networks. The new role name displays in the **Role** list for features. When done, click **Apply**. This foreground task takes a few moments, and then refreshes the view with an Info or Error notice to verify the action. To discard changes, navigate away from the view.

Procedure 56. Configure PMAC Application

Step	Procedure	Results
4. ☐	**PMAC GUI**: Reconfigure PMAC networks	***Note***: The network reconfiguration enters a tracked state. After you click Reconfigure, click **Cancel** to abort. 1. Click **Network Configuration** and follow the wizard through the configuration task. 2. Click **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 address and netmasks, or with IPv6 colon hex address and a prefix. When complete, click **Next**. 3. Click **Network Roles** to change the role of a network. Network associations can be added (for example, NetBackup) or deleted. You cannot add a new role since roles are driven from features. When complete, click **Next**. 4. Click **Network Interfaces** to add or delete interfaces, and change the IP address within the defined network space. If you add a network (for example, NetBackup), the Add Interface view displays when you click Add. This view provides an editable list 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 **Next**. 5. Click **Routes** to add or delete route destinations. The initial PMAC deployment does not define routes. Most likely, you want to add a default route — the route already exists, but this action defines it to PMAC so it may be displayed by PMAC. Click **Add**. The Add Route view provides an editable list 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. Click **Add Route**. When complete, click **Next**. 6. Click **DHCP Ranges** to define DHCP pools used by servers that PMAC manages. Click Add. Enter the starting and ending IPv4 address for the range on the network used to control servers (by default, the control network). Click **Add DHCP Range**. Only one range per network may be defined. When all pools are defined, click **Next**. 7. Click **Configuration Summary** for a view of your reconfigured PMAC. Click **Finish** to open the background task that reconfigures the PMAC application. A Task and Info or Error notice displays to verify your action. 8. Verify your reconfiguration task completes. Navigate to **Task Monitoring**. As the network reconfigures, you have a brief network interruption. From the Background Task Monitoring view, verify the Reconfigure PMAC task succeeds.
5. ☐	**PMAC GUI**: Set site settings	Navigate to **Administration > GUI Site Settings**. Set the **Site Name** to a descriptive name, set the **Welcome Message** to display when logging in.

Procedure 56. Configure PMAC Application

Step	Procedure	Results

6. ☐	**PMAC**: Application backup	`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
		`PMAC backup has 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 PMAC GUI Task Monitor screen, or issue the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
		Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.

7. ☐	**PMAC**: Verify backup was successful	***Note***: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
		The output of pmaccli getBgTasks should look similar to the example below:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`2: Backup PMAC COMPLETE - PMAC 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. ☐	**PMAC**: Save the backup	The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.

9.6 Add Cabinet and Enclosure to the PMAC System Inventory

This procedure adds a cabinet and an enclosure to the PMAC inventory.

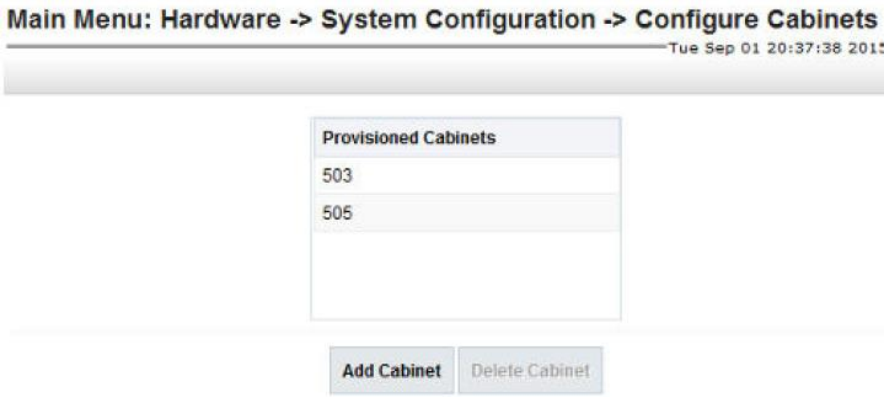
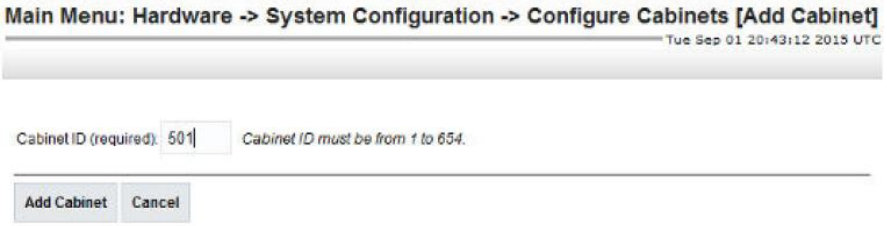
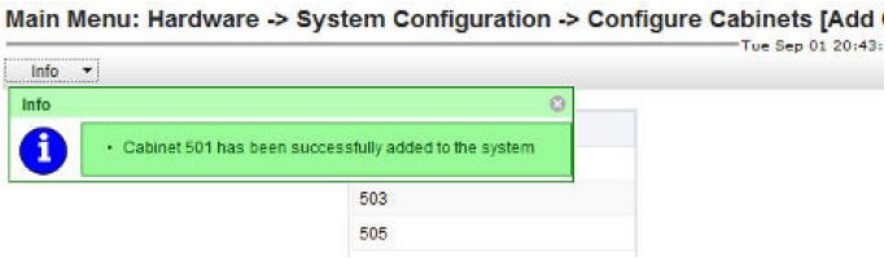
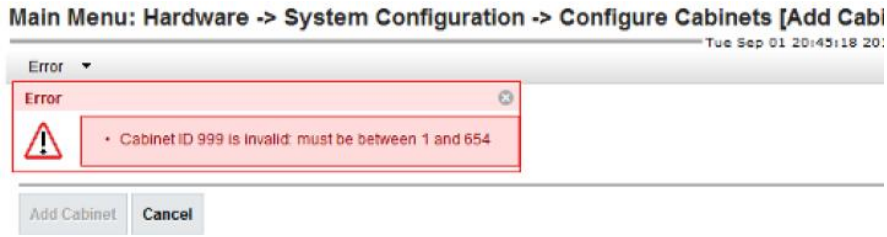
Prerequisite: 9.5 Configure PMAC Application

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

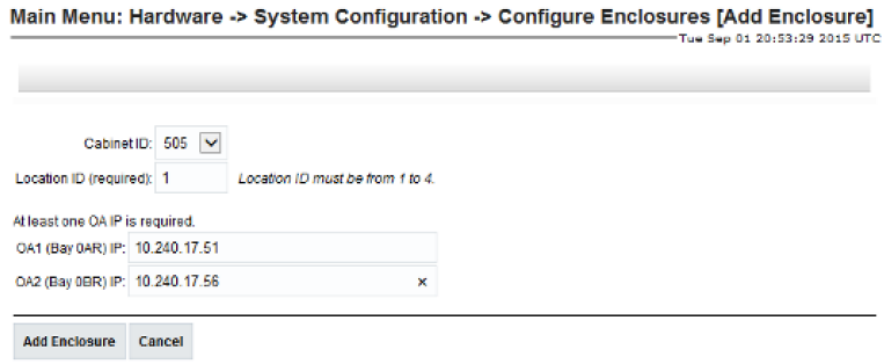
Procedure 57. Add Cabinet and Enclosure to the PMAC System Inventory

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 

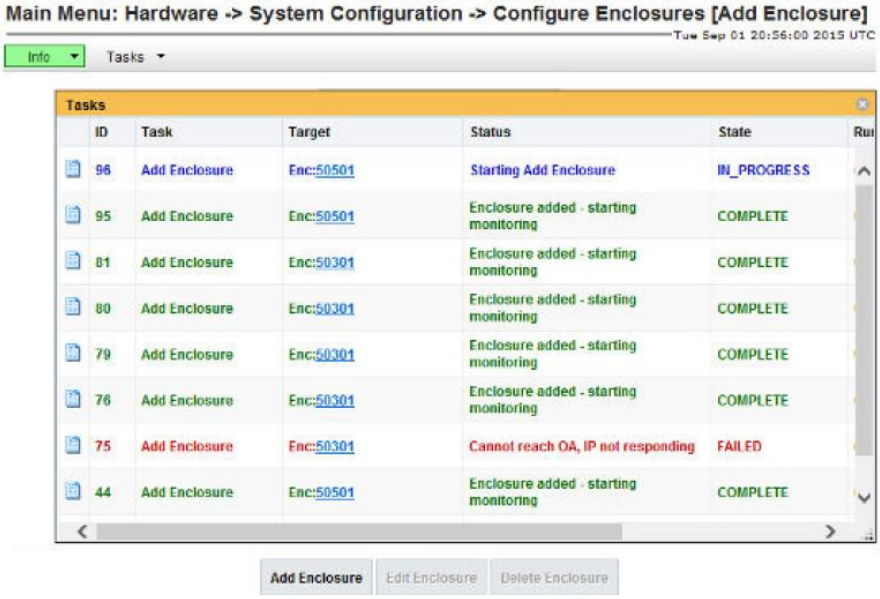
Procedure 57. Add Cabinet and Enclosure to the PMAC System Inventory

Step	Procedure	Results
2. ☐	**PMAC GUI**: Add cabinet	1. Navigate to **Hardware > System Configuration > Configure Cabinets**. 2. Click **Add Cabinet**.  3. Type the **Cabinet ID** and click **Add Cabinet**.  4. Check for errors. Success:  Error: 
3. ☐	**PMAC GUI**: Configure enclosures	1. Navigate to **Hardware > System Configuration > Configure Enclosures**. 2. Click **Add Enclosure**.

Procedure 57. Add Cabinet and Enclosure to the PMAC System Inventory

Step	Procedure	Results
		 3. Type the **Cabinet ID**, **Location ID**, and two **OA IP** addresses (the enclosure's active and standby OAs). 4. Click **Add Enclosure**.  ***Note*** Location ID is used to identify an enclosure within a cabinet. It can have a value of 1, 2, 3, or 4. The cabinet ID and location ID are combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 502 at location 1, has an enclosure ID of 50201). 5. The screen refreshes with a new background task entry. Click **Tasks** located on the toolbar under the Configure Enclosures heading.

Procedure 57. Add Cabinet and Enclosure to the PMAC System Inventory

Step	Procedure	Results
		 When the task is complete, the text changes to green and the Progress column indicates 100%.

9.7 Edit an Enclosure in the PMAC System Inventory

This procedure edits an existing enclosure configuration in the PMAC system inventory. This is used to notify PMAC of enclosure OA IP address changes.

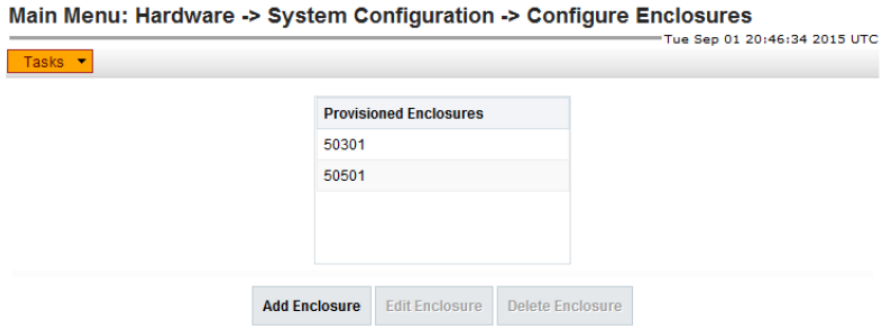
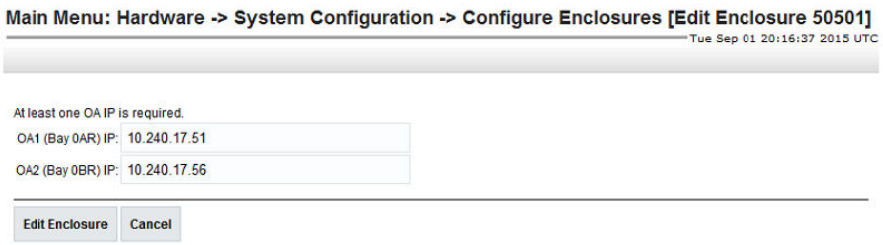
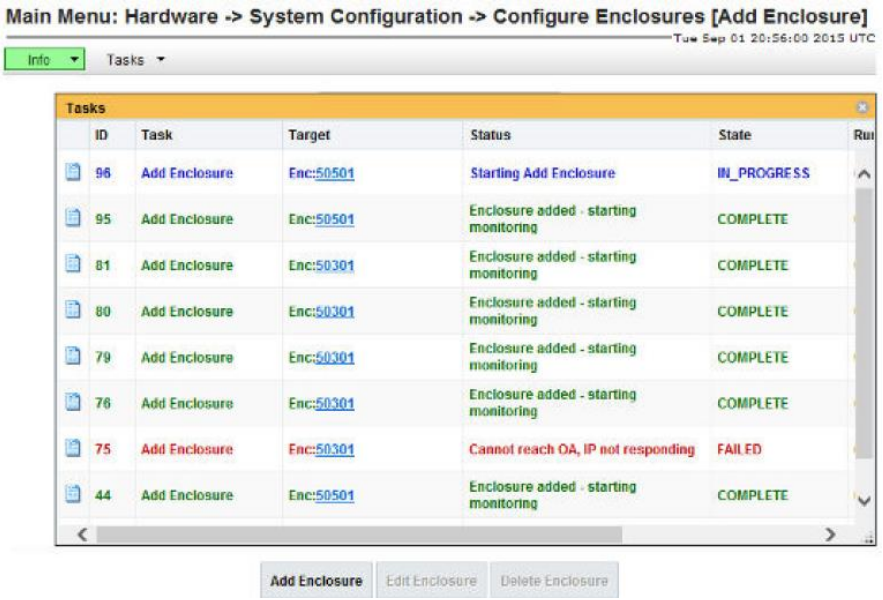
Prerequisite: 9.6 Add Cabinet and Enclosure to the PMAC System Inventory

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 58. Edit an Enclosure in the PMAC System Inventory

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 

Procedure 58. Edit an Enclosure in the PMAC System Inventory

Step	Procedure	Results
2. ☐	**PMAC GUI**: Edit enclosures	1. Navigate to **Hardware > System Configuration > Configure Enclosures**. 2. Select a row from the list of provisioned enclosures and click **Edit Enclosure**.  3. Modify the **OA IP** addresses as needed and click **Edit Enclosure**.  4. The screen refreshes with a new background task entry. Click **Tasks** located on the toolbar under the Configure Enclosures heading.  When the task is complete, the text changes to green and the Progress column indicates 100%.

9.8 Add ISO Images to the PMAC Image Repository

This procedure adds ISO images to the PMAC repository.

Prerequisite: 9.5 Configure PMAC Application

Note: If the ISO image has already been added to the PMAC software inventory in a previous procedure, skip this procedure.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

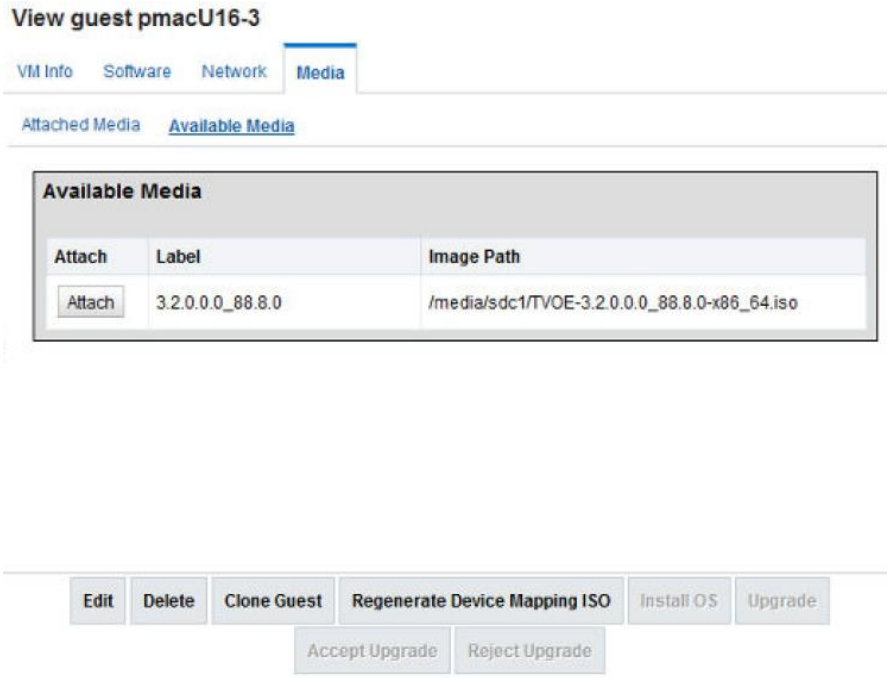
Procedure 59. Add ISO Images to the PMAC Image Repository

Step	Procedure	Results

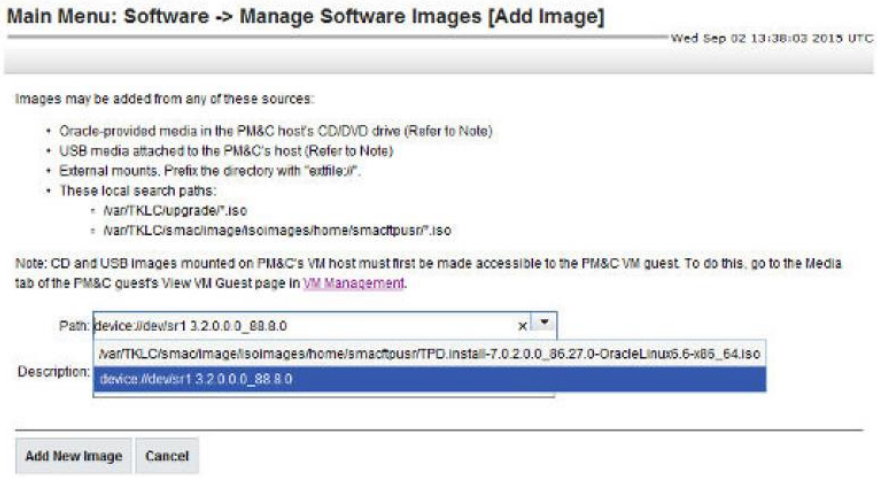
1. ☐	Make the image available to PMAC	There are two ways to make an image available to PMAC:
		• Attach the USB device containing the ISO image to a USB port of the management server.
		• Use SFTP to transfer the iso image to the PMAC server in the **/var/TKLC/smac/image/isoimages/home/smacftpusr/** directory as **pmacftpusr** user:
		  • cd into the directory where your ISO image is located (not on the PMAC server)
		  • Using SFTP, connect to the PMAC 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. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 

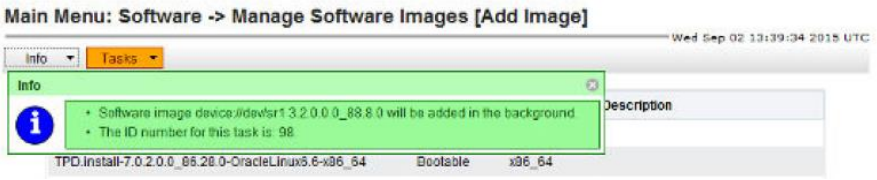
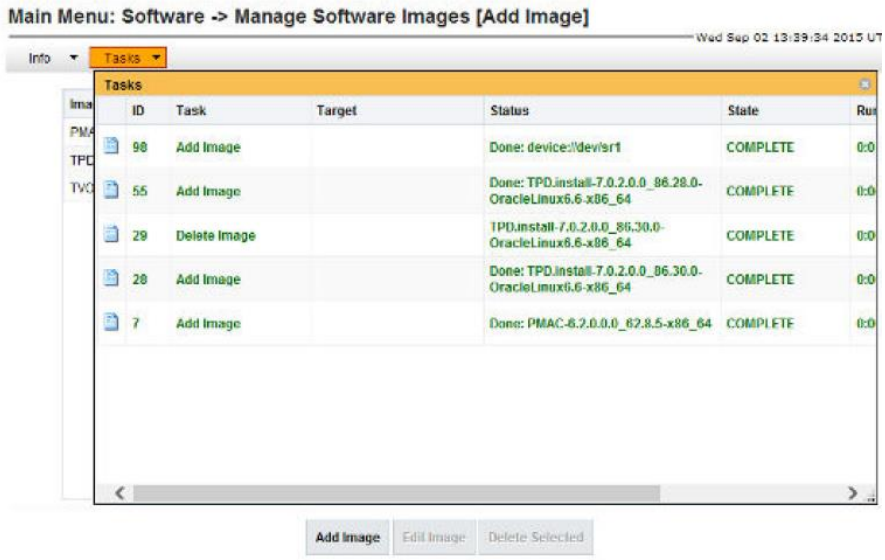
Procedure 59. Add ISO Images to the PMAC Image Repository

Step	Procedure	Results
3. ☐	**PMAC GUI**: Attach software image to the PMAC guest	If in step 1 the ISO image was transferred directly to the PMAC guest using SFTP, skip this step and continue with the next step. If the image is on a USB device, continue with this step. 1. Navigate to **Main Menu > VM Management**.. Select PMAC guest from the VM Entities list. 2. Click the Media tab. 3. Locate the ISO image in the Available Media list, and click **Attach** next to it. After a pause, the image displays in the Attached Media list. 

Procedure 59. Add ISO Images to the PMAC Image Repository

Step	Procedure	Results
4. ☐	**PMAC GUI**: Manage Software Image screen	1. Navigate to **Main Menu > Software > Manage Software Images**. 2. Click **Add Image**. If in step 1 the ISO image was transferred directly to the PMAC guest using SFTP, it displays as a local file **/var/TKLC/…** If the image was supplied on a USB drive, it displays 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 PMAC; therefore, the ISO image of interest is normally present on the second device, **device://dev/sr1**. If one or more USB-based images was already present on the management server before you started this procedure, select a correspondingly higher device number. 3. Type an image description and click **Add New Image**. 

Procedure 59. Add ISO Images to the PMAC Image Repository

Step	Procedure	Results
5. ☐	**PMAC GUI**: Monitor the status	Click **Info** to access the status and confirm a background task has been started to add the image.  Click **Tasks** located on the toolbar. Make sure the correct image or source device name displays in the Status column.  When the task is complete, the text changes to green and the Progress column indicates 100%.
6. ☐	**PMAC GUI**: Detach image from PMAC guest	If the image was supplied on USB, return to the PMAC guest's Media tab, locate the image in the Attached Media list, and click **Detach** next to it. To confirm the new image has been detached, reload the page by reselecting the VM guest in the VM Entities list and navigate to **Media > Attached Media** subtab. This releases the virtual device for future use. Remove the USB device from the management server.
7. ☐	Repeat	If there are additional ISO images to be provisioned on the PMAC, repeat the procedure with the appropriate ISO image data.

9.9 IPM Servers Using PMAC Application

This procedure installs TPD or TVOE using an image from the PMAC image repository.

Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for IPM have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for IPM have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- A bootable image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.
- The BIOS settings on the servers have been verified using 6.2 Confirm/Upgrade Blade Server BIOS Settings or Section 3.2 of [1] TPD Initial Product Manufacture Software Installation Procedure.

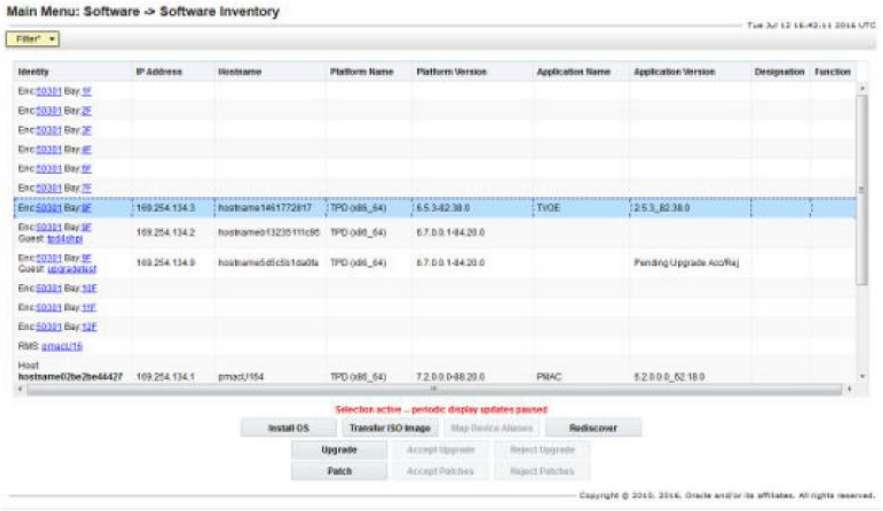
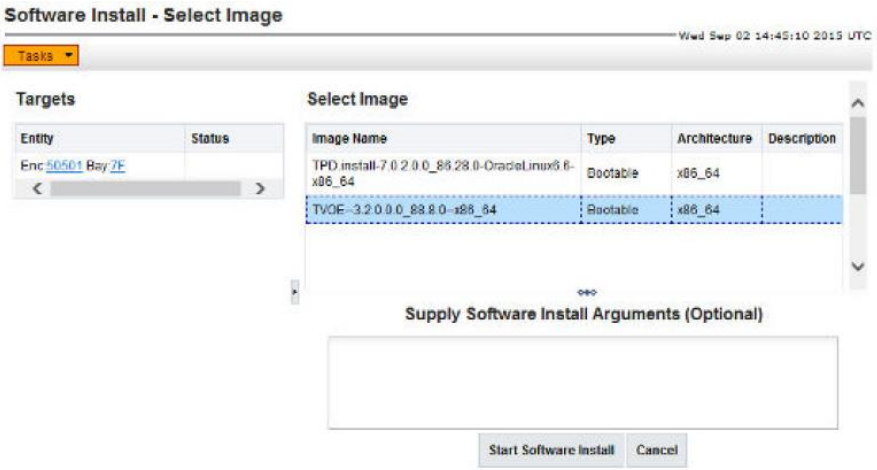
Note: If you are about to IPM as preparation for SAN configuration, follow 10.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 60. IPM Servers Using PMAC Application

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 

Procedure 60. IPM Servers Using PMAC Application

Step	Procedure	Results
2. ☐	**PMAC GUI**: Select servers	1. Navigate to **Software > Software Inventory**. 2. Select the servers you want to IPM. If you want to install the same OS on more than one server, press **Ctrl** while selecting multiple rows. 3. Click **Install OS**. 
3. ☐	**PMAC GUI**: Select image	1. Select the OS image to install on the servers. 2. (Optional) Install arguments can be supplied by entering them into the text box displayed under the list of bootable images. These arguments are 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 [1] TPD Initial Product Manufacture Software Installation Procedure. 3. Click **Start Software Install**.  4. Click **OK** to confirm the install.

Procedure 60. IPM Servers Using PMAC Application

Step	Procedure	Results
4. ☐	**PMAC GUI**: Monitor install OS	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Install OS** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.
5. ☐	Repeat	Repeat this procedure for additional rack mount servers.

9.10 Install/Upgrade Applications Using PMAC

This procedure installs upgrades an application using an image from the PMAC image repository.

Prerequisites:

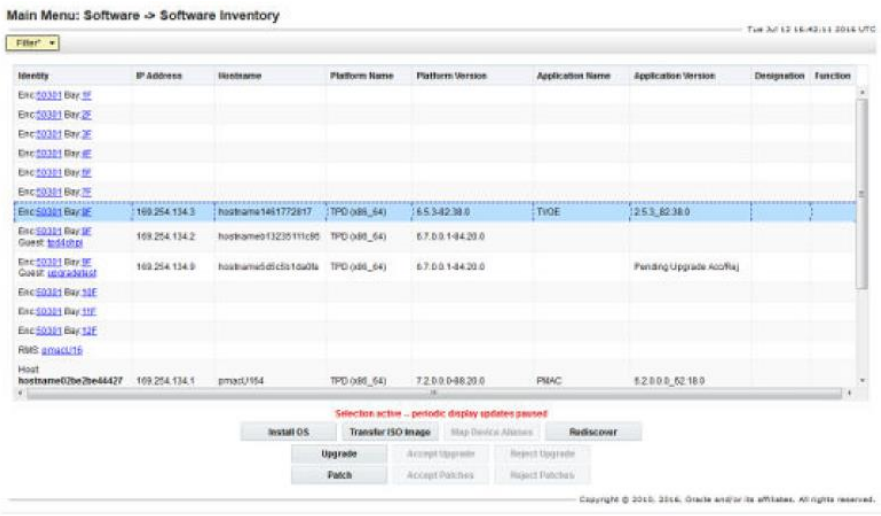
- Enclosures containing the blade servers or servers containing a TVOE host targeted for IPM have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for IPM have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- An upgradable image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.

Notes:

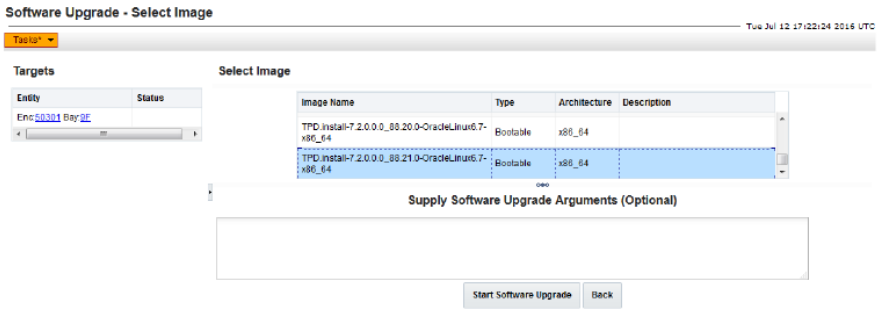
- Firmware update is only supported for HP c-Class blades and Rack Mount Servers.
- Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 61. Install/Upgrade Applications Using PMAC

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	**PMAC GUI**: Select servers	1. Navigate to **Software > Software Inventory**. 2. Select the servers you want to upgrade. If you want to upgrade more than one server, press **Ctrl** while selecting multiple rows. 3. Click **Upgrade**.  ***Note***: Until the target servers are fully discovered by PMAC, you are 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 screen (no IP address, hostname, plat name, plat version, etc., displays).

Procedure 61. Install/Upgrade Applications Using PMAC

Step	Procedure	Results
3. ☐	**PMAC GUI**: Select image	1. Select the OS image to install on the servers. 2. (Optional) Install arguments can be supplied by entering them into the text box displayed under the list of bootable images. These arguments are 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***: PMAC does not validate firmware update arguments. 3. Click **Start Software Upgrade**.  4. Click **OK** to confirm the upgrade.
4. ☐	**PMAC GUI**: Monitor upgrade	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Upgrade** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.
5. ☐	**PMAC GUI**	Verify the installed/upgraded application is fully functional. The application must provide the steps for verifying its functionality.
6. ☐	**PMAC GUI**: Accept or reject upgrade (platform 6.x applications only)	If the application you just upgraded or installed is based on a TPD release supported by PMAC 6.6, you must either accept or reject the upgrade. To accept an upgrade using PMAC, perform 9.18 Accept Upgrades Using PMAC . Likewise, to reject an upgrade using PMAC, perform 9.19 Reject Upgrades Using PMAC.

9.11 Patch Applications Using PMAC

This procedure patches an application using an image from the PMAC image repository.

Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host for an application patch have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for an application patch have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- A patch image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.
- Target servers have been IPM'd with an application based on a TPD 7.2 release.

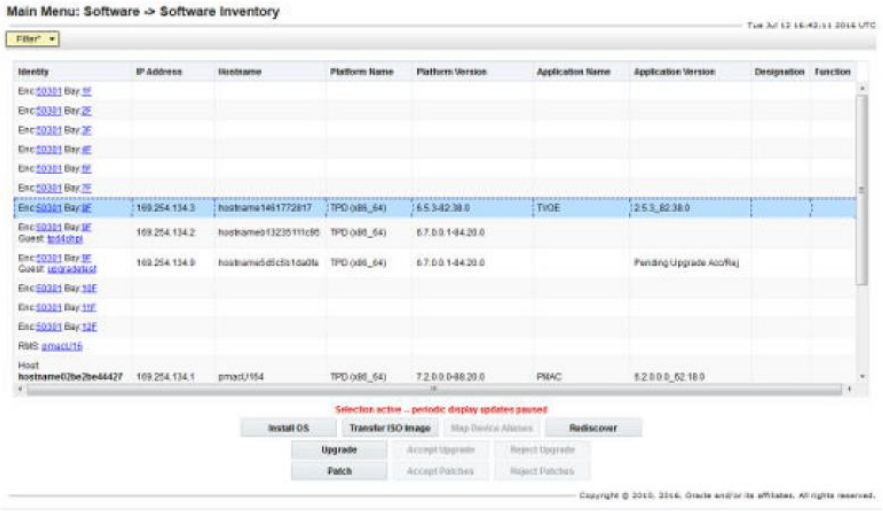
Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

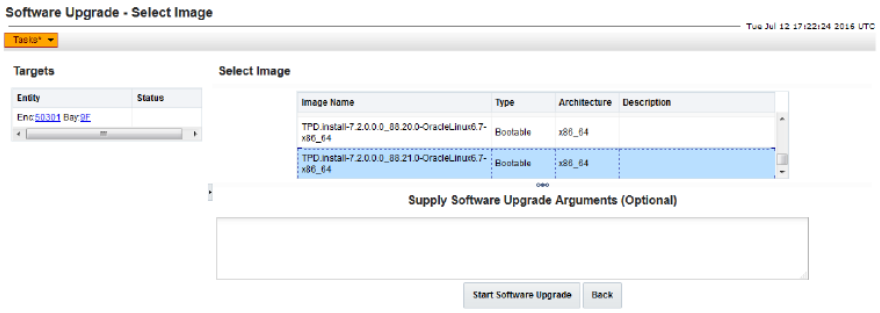
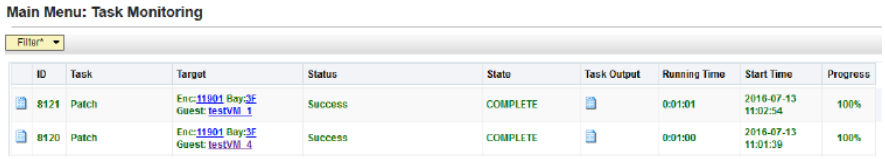
Procedure 62. Patch Applications Using PMAC

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 

Procedure 62. Patch Applications Using PMAC

Step	Procedure	Results
2. ☐	**PMAC GUI**: Select servers	1. Navigate to **Software > Software Inventory**. 2. Select the servers you want to upgrade. If you want to upgrade more than one server, press **Ctrl** while selecting multiple rows. 3. Click **Patch**.  ***Note***: Until the target servers are fully discovered by PMAC, you are 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 screen (no IP address, hostname, plat name, plat version, etc., displays).

Procedure 62. Patch Applications Using PMAC

Step	Procedure	Results
3. ☐	**PMAC GUI**: Select image	1. Select the OS image to install on the servers. 2. (Optional) There are three optional arguments that can be specified as part of a patch. The first option is **Reboot**. If this is enabled, the patched server reboots once the patch installation has completed. The second option is **No runlevel change required**. If this is enabled, the patched server does not transition from runlevel 4 to 3 before installing the patch. This means applications running on the server are not 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 waits 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. ***Note***: PMAC does not validate firmware update arguments. 3. Click **Start Patch Installation**.  4. Click **OK** to confirm proceeding with the patch.
4. ☐	**PMAC GUI**: Monitor patch	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Patch** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.
5. ☐	**PMAC GUI**	Verify the patch installation. The application must provide the steps for verifying its functionality.

Procedure 62. Patch Applications Using PMAC

Step	Procedure	Results
6. ☐	**PMAC GUI**: Accept or reject patch	If the application you just patched is based on a TPD 7.2 release or later, you must accept or reject the upgrade. To accept a patch using PMAC, perform 9.20 Accept Patches Using PMAC. Likewise, to reject an upgrade using PMAC, perform 9.21 Reject Patches Using PMAC.

9.12 Install PMAC on Redundant DL360 or DL380

This procedure installs and configures TVOE on a redundant DL360 or DL380 server, deploys a redundant PMAC, and creates the first backup from the primary PMAC.

This procedure is optional and required only if the redundant PMAC server feature is to be deployed.

Prerequisites:

- 9.8 Add ISO Images to the PMAC Image Repository has been completed using the TVOE media.
- 9.8 Add ISO Images to the PMAC Image Repository has been completed using the PMAC media. Note the PMAC image name; it is used during the procedure as <PMAC_Image_Name>.
- 9.9 IPM Servers Using PMAC Application has been completed on the redundant management server using the TVOE media.
- 9.2 Configure TVOE Network has been completed on the redundant management server.

Notes:

- In the event a disaster recovery is required, refer to the recovery procedure in 909-2210-001.
- It is assumed that the use of a redundant PMAC means the NetBackup feature is not in use.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 63. Install PMAC on Redundant DL360 or DL380

Step	Procedure	Results
1. ☐	**Redundant Management Server iLO**: Login	1. Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. `http://<redundant_management_server_iLO_IP>` 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click **Yes** if the Security Alert displays.

Procedure 63. Install PMAC on Redundant DL360 or DL380

Step	Procedure	Results

2. ☐	**Primary Management Server iLO**: Log into the primary management server on the remote console	Log into PMAC with **admusr** credentials.
		Note: On a TVOE host, if you open the virsh console, for example, `$ 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, run `ps -ef |grep virsh`, and 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]`
		`pmacU17-1 login:`

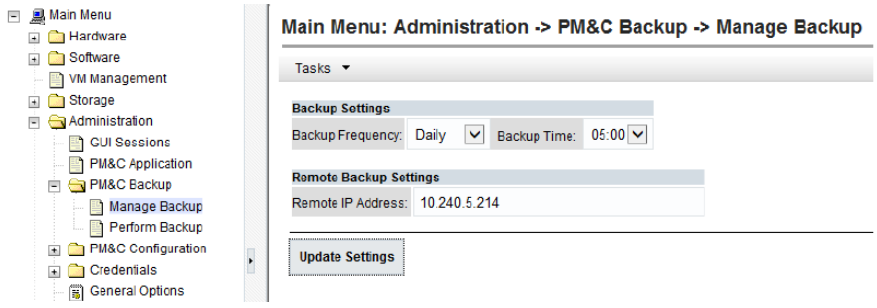
3. ☐	**Primary PMAC**: Export ISO image	Export the PMAC ISO image to the redundant management server's address on the control network. `$ sudo /usr/sbin/exportfs <redundant_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name>`
4. ☐	**Redundant Management Server TVOE**: Mount media	Mount the PMAC upgrade media from the PMAC server. `$ sudo /bin/mount <primary_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name> /mnt/upgrade`

5. ☐	**Redundant Management Server TVOE**: Deploy PMAC instance	Using the pmac-deploy script, deploy the PMAC instance using the configuration detailed by the completed NAPD. All configuration options (NetBackup or isoimagesVolSizeGB) should match the configuration of the primary PMAC.
		For this example, a PMAC is deployed without NetBackup.
		`$ 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`

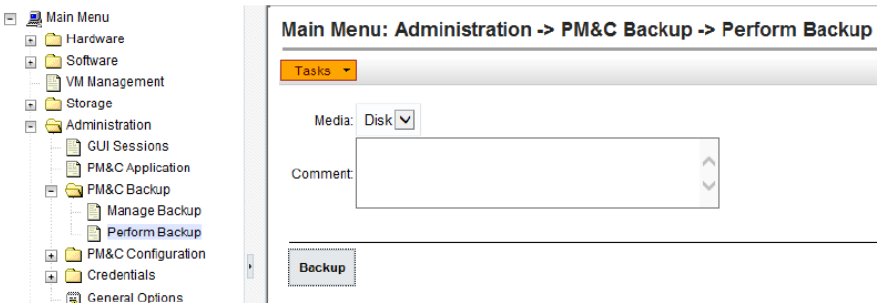
Procedure 63. Install PMAC on Redundant DL360 or DL380

Step	Procedure	Results

6. ☐	**Redundant Management Server TVOE**: Unmount the media and remove	After the PMAC deploys and boots, the management and control network comes up. At that point unmount the media and remove the PMAC media.
		`$ cd /`
		`$ sudo /bin/unmount /mmmnt/upgrade`

7. ☐	**Redundant PMAC**	Perform 9.4 Set Up PMAC. **WARNING**: Initialization of the redundant PMAC is to be avoided at all costs.
8. ☐	**Primary PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Administration > PMAC Backup > Manage Backup**.
9. ☐	**Primary PMAC GUI**: Configure primary PMAC to send backup to the redundant PMAC	Type the **Remote IP Address** of the redundant PMAC (redundant_management_server_mgmtVLAN_IP) and click **Update Settings**. 
10. ☐	**Primary PMAC GUI**: Verify update was successful	Navigate to **Task Monitoring**. From the Background Task Monitoring view, verify the Update PMAC Backup Data task succeeds.

Procedure 63. Install PMAC on Redundant DL360 or DL380

Step	Procedure	Results
11. ☐	**Primary PMAC GUI**: Perform initial backup to the redundant PMAC server	Navigate to **Administration > PMAC Backup > Perform Backup**. Select **Remote Server** from the Media options, type any comments, and click **Backup**. 
12. ☐	**Primary PMAC GUI**: Verify update was successful	Navigate to **Task Monitoring**. From the Background Task Monitoring view, verify the Backup PMAC task succeeds. This backup copies the existing PMAC backup files and all of the images added to the PMAC image repository from the primary PMAC server to the redundant PMAC server.
13. ☐	**Primary PMAC**: Unexport the PMAC ISO image	`$ sudo /usr/sbin/exportfs -u <redundant_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name>`

9.13 Configure Management Server SNMP Trap Target

This procedure configures SNMP settings for the management server.

Prerequisites:

- 9.5 Configure PMAC Application
- Know IP address of the target NMS for SNMP traps

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 64. Configure Management Server SNMP Trap Target

Step	Results
1. ☐	Perform 12.3 Add SNMP Trap Destination on TPD-Based Application logging into the management server and providing the IP address of each trap destination.
2. ☐	Ensure the PMAC specific MIB files are located in the **/usr/TKLC/smac/etc/mib** directory on the management server. The file of interest is pmacAppAlarms.mib.

9.14 Install and Configure PMAC NetBackup Client

This procedure installs and configures the NetBackup client software on a PMAC application.

Prerequisite: The PMAC 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.

9.22 Initialize PMAC Application or 9.5 Configure PMAC Application

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 65. Install and Configure PMAC NetBackup Client

Step	Procedure	Results
1. ☐	**PMAC GUI**	Verify the PMAC application guest has been configured with NetBackup virtual disk by following 9.22 Initialize PMAC Application.
2. ☐	**TVOE Management Server iLO**: Login	1. Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. `http://<management_server_iLO_IP>` 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click **Yes** if the Security Alert displays.

3. ☐	**TVOE Application Server iLO**: Login	Log into PMAC with **admusr** credentials.
		Note: On a TVOE host, if you open the virsh console, for example, `$ 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, run `ps -ef |grep virsh`, and 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]`
		`pmacU17-1 login:`

Procedure 65. Install and Configure PMAC NetBackup Client

Step	Procedure	Results

4. ☐	**PMAC**	Perform 12.5 Install the NetBackup Client Application. The following data is required:
		• Netbackup support:
		  • PMAC 5.7.0 supports NetBackup client software versions 7.1 and 7.5.
		  • PMAC 5.7.1 through PMAC 6.6 supports NetBackup client software versions 7.1, 7.5, and 7.6.
		• The PMAC is a 64-bit application.
		• The PMAC application NetBackup user is **NetBackup**. See appropriate documentation for the password.
		• The paths to the PMAC application software NetBackup notify scripts are:
		  • /usr/TKLC/smac/sbin/bpstart_notify
		  • /usr/TKLC/smac/sbin/bpend_notify
		• For the PMAC application the following is the NetBackup server policy files list:
		  • /var/TKLC/smac/image/repository/*.iso
		  • /var/TKLC/smac/backup/backupPmac*.pef
		At the NetBackup server, the NetBackup policy(ies) can now be created to perform the NetBackup backups of the PMAC application.

9.15 Add Rack Mount Server to the PMAC System Inventory

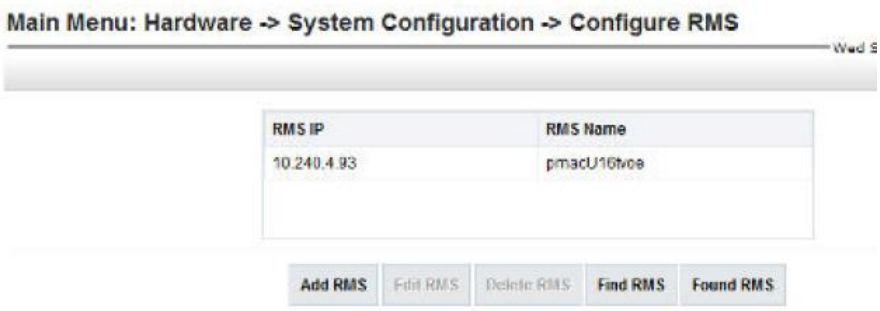
This procedure adds a rack mount server to the PMAC system inventory.

Prerequisite: 9.5 Configure PMAC Application

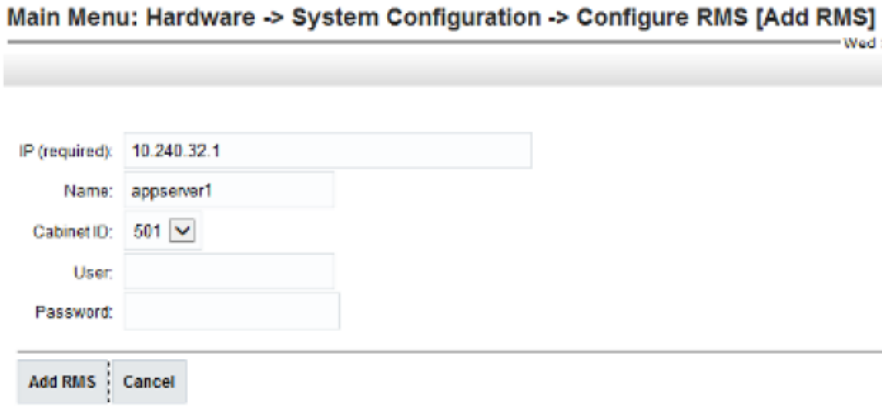
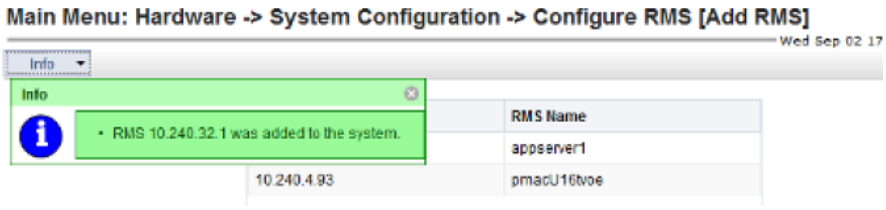
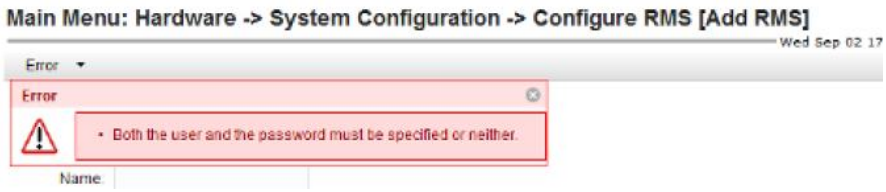
Note: You cannot edit the RMS iLO IP address. To change this address, delete and then add the RMS with the correct address.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

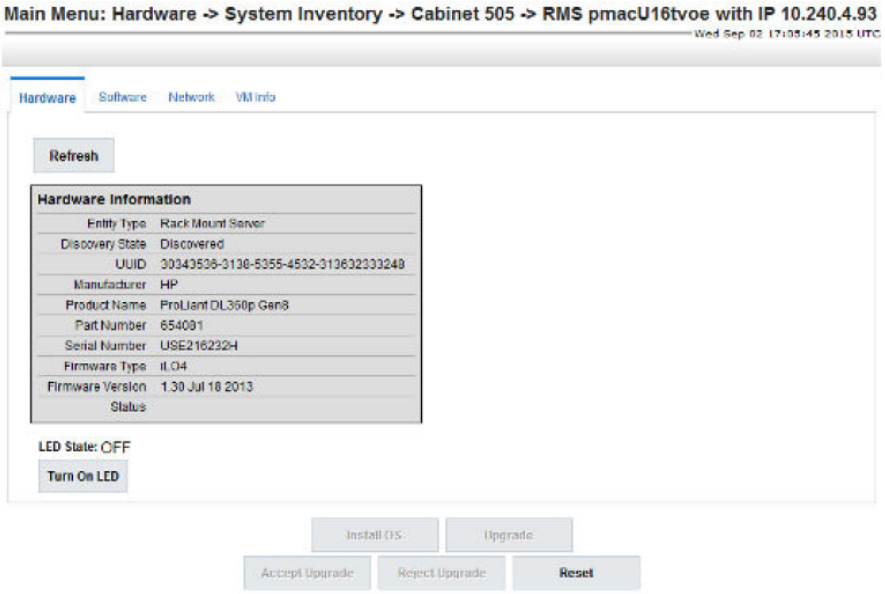
Procedure 66. Add Rack Mount Server to the PMAC System Inventory

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **pmacadmin** user. 
2. ☐	**PMAC GUI**: Add cabinet (optional)	If this is a RMS installation only or a cabinet has not been previously configured, perform step 2. of 9.6 Add Cabinet and Enclosure to the PMAC System Inventory to add one or more cabinets.
3. ☐	**PMAC GUI**: Add RMS	1. Navigate to **Hardware > System Configuration > Configure RMS**. 2. Click **Add RMS**.  3. Type the **IP** address of the rack mount server management port (iLO) in the specified field. Type **root** as the **User**, type the **Password** for the iLO root user. All the other fields are optional. 4. Click **Add RMS**.

Procedure 66. Add Rack Mount Server to the PMAC System Inventory

Step	Procedure	Results
		 ***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. 5. Check for errors. Success:  Error: 

Procedure 66. Add Rack Mount Server to the PMAC System Inventory

Step	Procedure	Results
4. ☐	**PMAC GUI**: Verify RMS discovered	Navigate to **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.  Click **Refresh** to refresh the hardware information periodically until the Discovery state changes from **Undiscovered** to **Discovered**. If **Status** displays an error, contact My Oracle Support (MOS) for assistance.

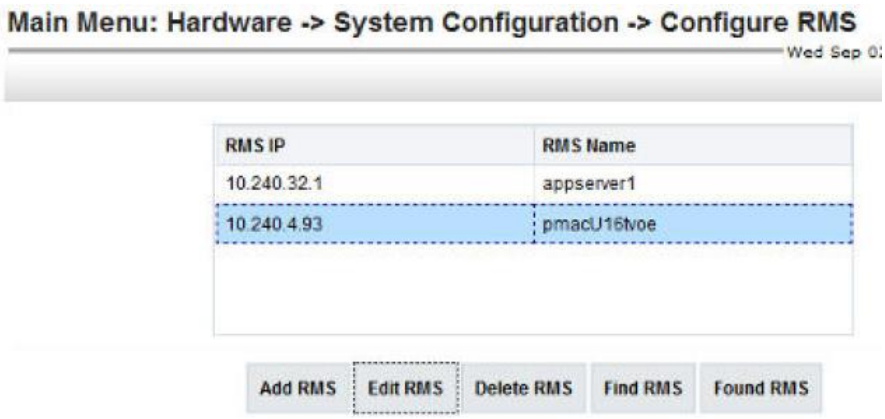
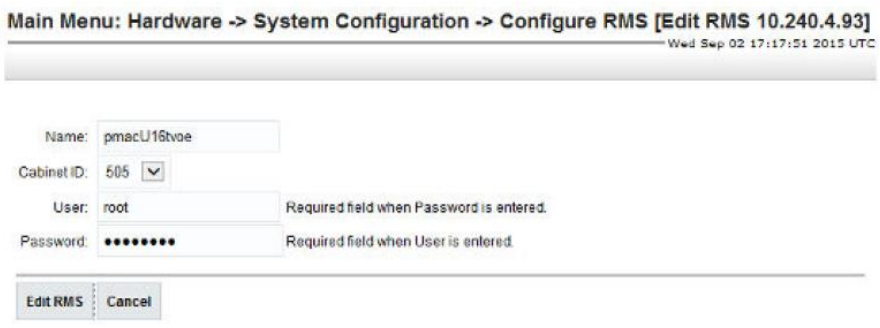
9.16 Edit Rack Mount Server in the PMAC System Inventory

This procedure edits a rack mount server in the PMAC system inventory. This procedure modifies the name, cabinet, or credentials of a provisioned RMS.

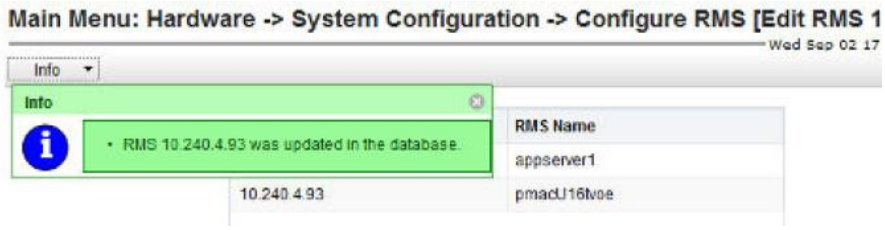
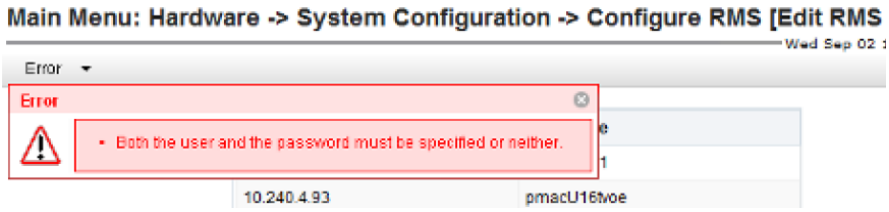
Prerequisite: 9.15 Add Rack Mount Server to the PMAC System Inventory

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 67. Edit Rack Mount Server in the PMAC System Inventory

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **pmacadmin** user. 
2. ☐	**PMAC GUI**: Edit RMS	1. Navigate to **Hardware > System Configuration > Configure RMS**. 2. Select one row in the list of rack mount servers and click **Edit RMS**.  3. Modify the fields that need to be changed. 4. Click **Edit RMS**. 

Procedure 67. Edit Rack Mount Server in the PMAC System Inventory

Step	Procedure	Results
		5. Check for errors. Success:  Error: 

9.17 Find and Add a Rack Mount Server to the PMAC System Inventory

This procedure locates and adds a RMS to the PMAC system inventory. Use this procedure to find rack mount servers running a Tekelec OS or within a specified IP address range and then add those to the PMAC system inventory.

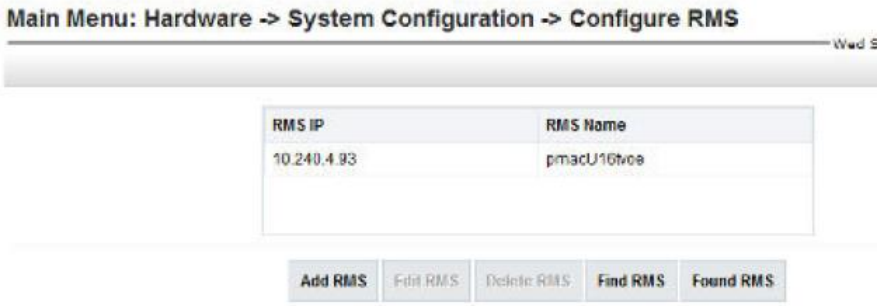
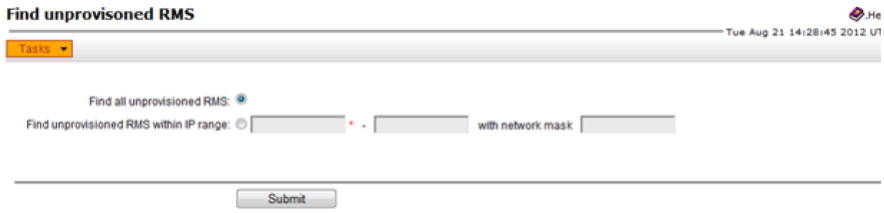
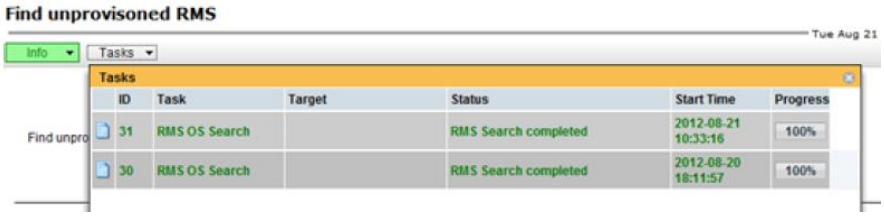
Prerequisite: 9.5 Configure PMAC Application

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

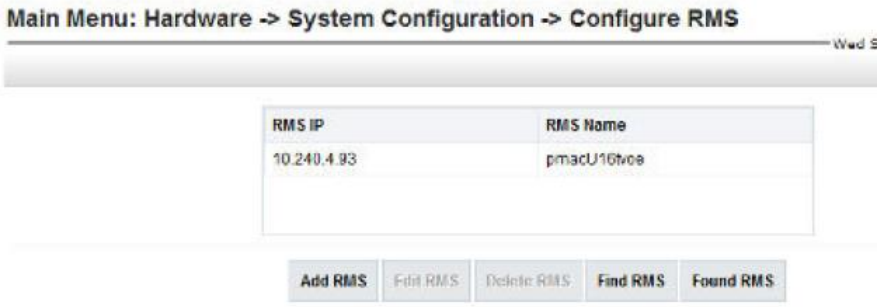
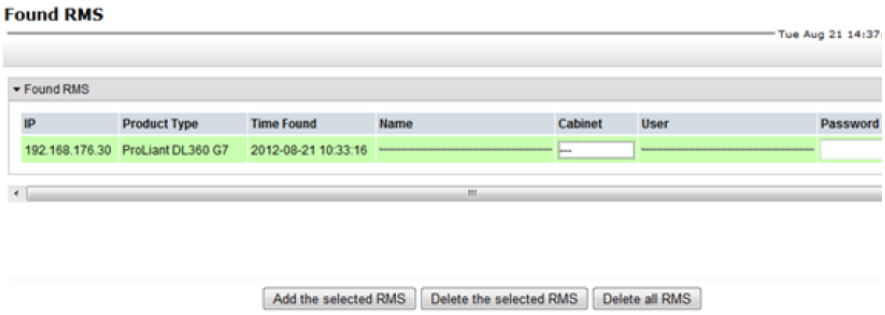
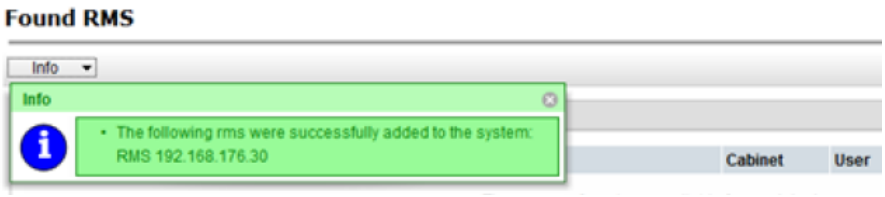
Procedure 68. Find and Add a Rack Mount Server to the PMAC System Inventory

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **pmacadmin** user.  Navigate to **Administration > PMAC Configuration**.

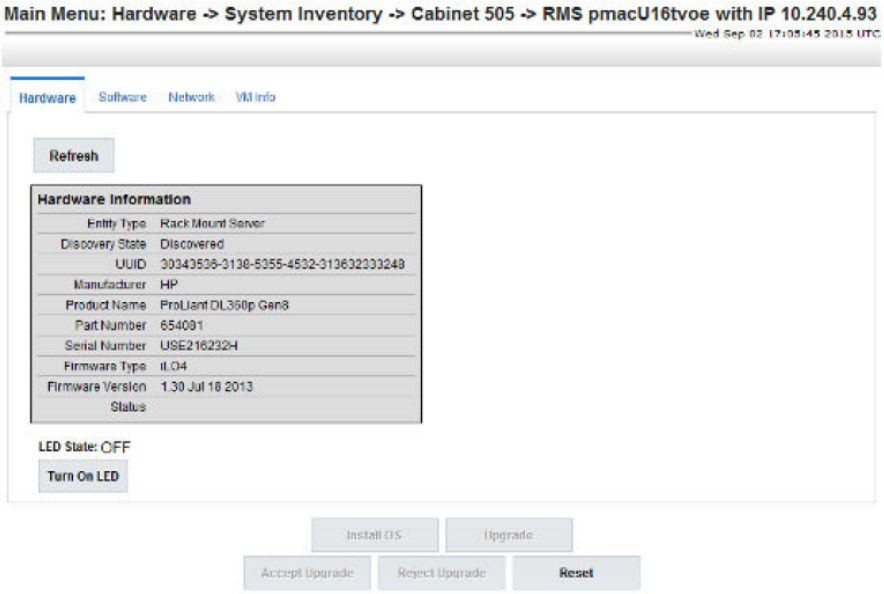
Procedure 68. Find and Add a Rack Mount Server to the PMAC System Inventory

Step	Procedure	Results
2. ☐	**PMAC GUI**: Find RMS	1. Navigate to **Hardware > System Configuration > Configure RMS**. 2. Click **Find RMS**.  3. Select the type of find to perform. If the RMS has a Tekelec OS installed, then select the default **Find all unprovisioned RMS**. If the RMS does not have a Tekelec OS installed, then PMAC can search a range of IP addresses for a valid management port (for example, iLO) connection. 4. Click **Submit**.  5. Monitor screen. The screen refreshes with a new background task entry. Click **Tasks** located on the toolbar under the Find unprovisioned RMS heading.  When the task is complete, the text changes to green and the Progress column indicates 100%.

Procedure 68. Find and Add a Rack Mount Server to the PMAC System Inventory

Step	Procedure	Results
3. ☐	**PMAC GUI**: Add found RMS	1. Click **Found RMS**.  2. Select one of the servers and enter values for any optional fields, as needed 3. Click **Add the selected RMS**.  4. Check for errors. 

Procedure 68. Find and Add a Rack Mount Server to the PMAC System Inventory

Step	Procedure	Results
4. ☐	**PMAC GUI**: Verify RMS discovered	Navigate to **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.  Click **Refresh** to refresh the hardware information periodically until the Discovery state changes from **Undiscovered** to **Discovered**. If **Status** displays an error, contact My Oracle Support (MOS) for assistance.

9.18 Accept Upgrades Using PMAC

This procedure accepts upgrades using PMAC.

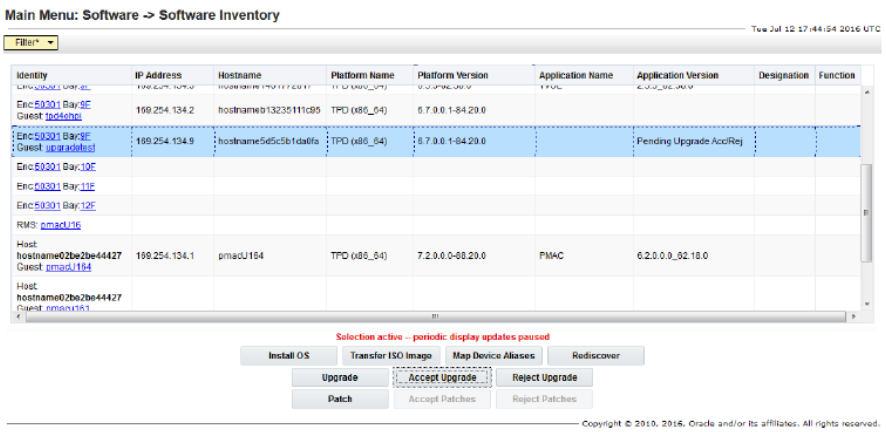
Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for accept upgrade have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for accept upgrade have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- The BIOS settings on the target servers have been verified using 6.2 Confirm/Upgrade Blade Server BIOS Settings or Section 3.2 of [1] TPD Initial Product Manufacture Software Installation Procedure.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

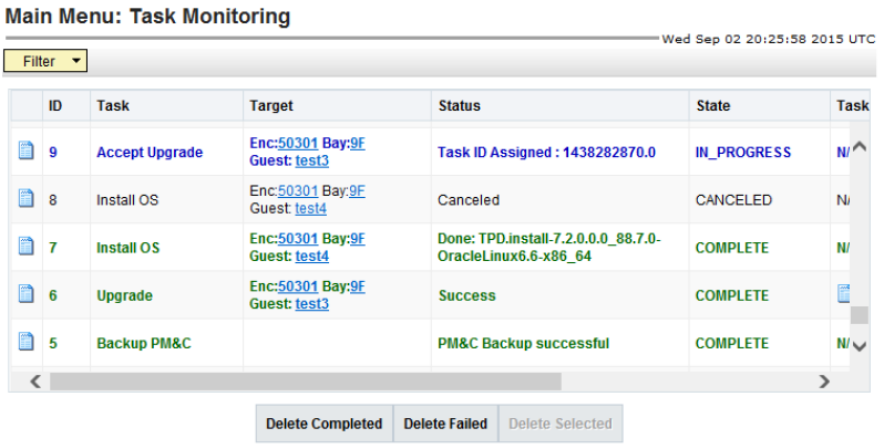
Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 69. Accept Upgrades Using PMAC

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Software > Software Inventory**.
2. ☐	**PMAC GUI**: Select servers	To accept upgrades, the servers must be in the pending accept/reject upgrade state. Servers in this state have **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after an upgrade completes. 1. Select the servers you want to upgrade. If you want to upgrade more than one server, press **Ctrl** while selecting multiple rows. 2. Click **Accept Upgrade**.  ***Note***: The servers may reboot if a migration of the file system is required. 3. Click **OK** to confirm proceeding with the upgrade.

Procedure 69. Accept Upgrades Using PMAC

Step	Procedure	Results
3. ☐	**PMAC GUI**: Monitor upgrade	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Upgrade** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.

9.19 Reject Upgrades Using PMAC

This procedure rejects upgrades using PMAC.

Prerequisites:

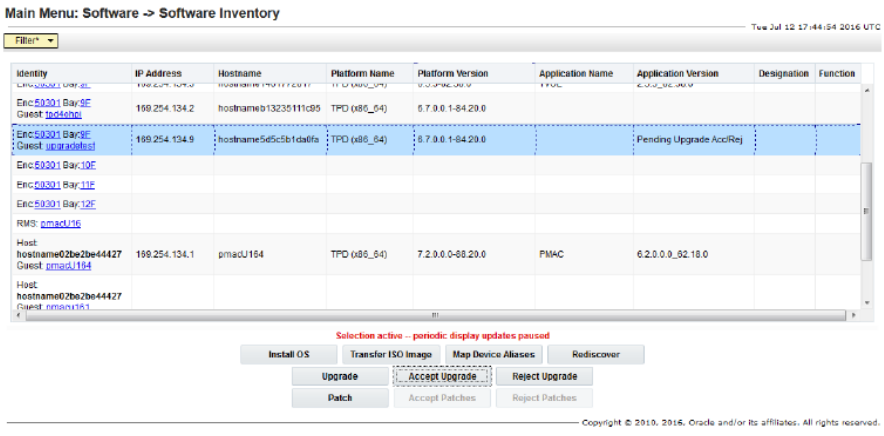
- Enclosures containing the blade servers or servers containing a TVOE host targeted for reject upgrade have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for reject upgrade have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

Notes:

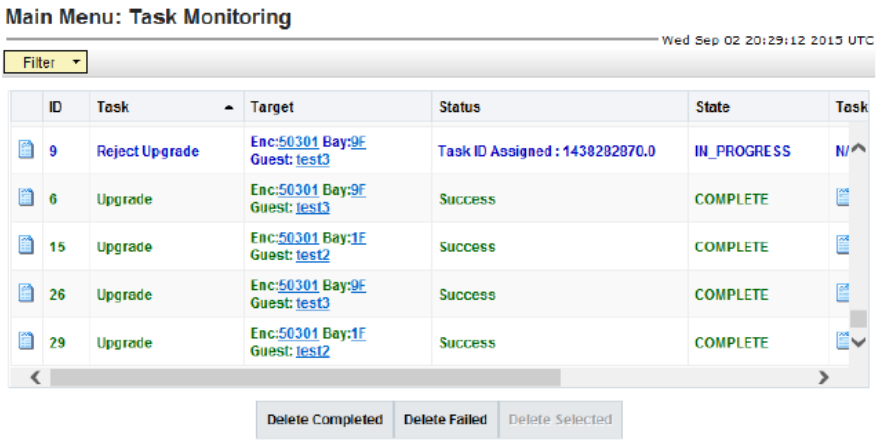
- Until the target servers are fully discovered by PMAC, you are unable to reject upgrades on the servers (this may take up to 15 minutes after the upgrades complete).
- The image transfer is only supported for discovered entities (IP address is known)

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 70. Reject Upgrades Using PMAC

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Software > Software Inventory**.
2. ☐	**PMAC GUI**: Select servers	To reject upgrades, the servers must be in the pending accept/reject upgrade state. Servers in this state have **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after an upgrade completes. 1. Select the servers with upgrades you want to reject. If you want to reject an upgrade on more than one server, press **Ctrl** while selecting multiple rows. 2. Click **Reject Upgrade**.  3. Click **OK** to confirm proceeding with rejecting the upgrade.

Procedure 70. Reject Upgrades Using PMAC

Step	Procedure	Results
3. ☐	**PMAC GUI**: Monitor upgrade	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Reject Upgrade** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.

9.20 Accept Patches Using PMAC

This procedure accepts patches using PMAC.

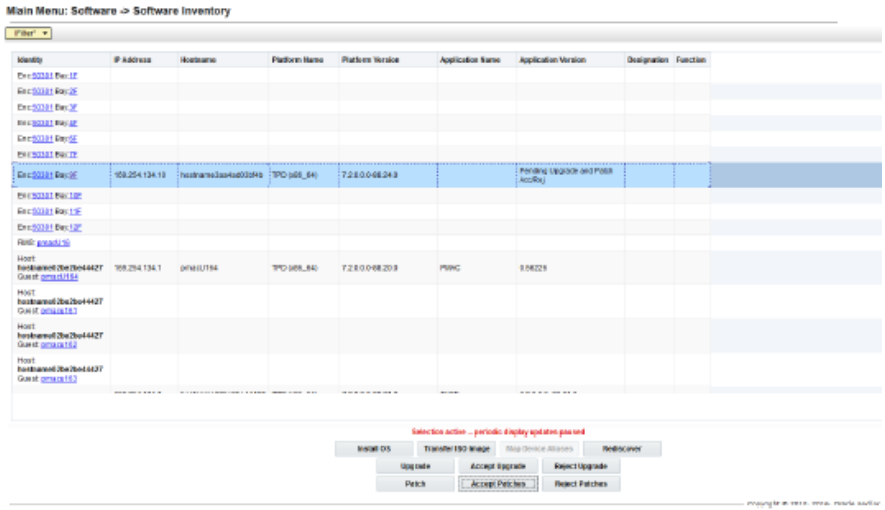
Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for the application patch have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for the application patch have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

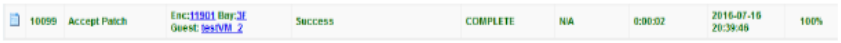
Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 71. Accept Patches Using PMAC

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Software > Software Inventory**.
2. ☐	**PMAC GUI**: Select servers	To accept patches, the servers must be in the pending accept/reject state. Servers in this state have **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after an upgrade completes. 1. Select the servers you want to patch. If you want to patch more than one server, press **Ctrl** while selecting multiple rows. 2. Click **Accept Patches**.  3. Click **OK** to confirm proceeding with the patch.

Procedure 71. Accept Patches Using PMAC

Step	Procedure	Results
3. ☐	**PMAC GUI**: Monitor accept patch	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Patch** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.

9.21 Reject Patches Using PMAC

This procedure rejects patches using PMAC.

Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for the application patch have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for the application patch have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

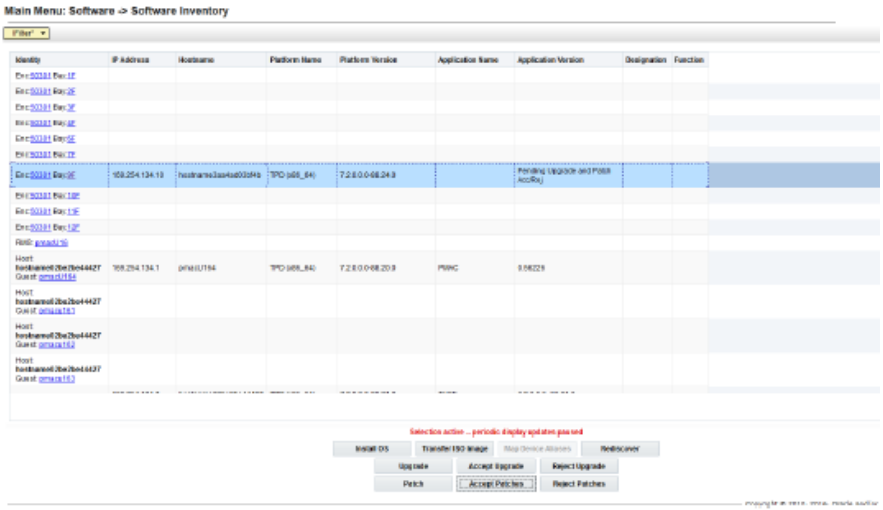
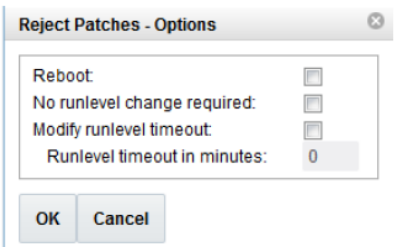
Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 72. Reject Patches Using PMAC

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Software > Software Inventory**.

Procedure 72. Reject Patches Using PMAC

Step	Procedure	Results
2. ☐	**PMAC GUI**: Select servers	To reject patches, the servers must be in the pending accept/reject state. Servers in this state have **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state after an upgrade completes. 1. Select the servers with patches you want to reject. If you want to reject a patch on more than one server, press **Ctrl** while selecting multiple rows. 2. Click **Reject Patches**.  3. (Optional) There are three optional arguments that can be specified as part of a patch rejection. The first option is **Reboot**. If this is enabled, the patched server reboots once the patch rejection has completed. The second option is **No runlevel change required**. If this is enabled, the patched server does not transition from runlevel 4 to 3 before rejecting the patch. This means applications running on the server are not 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 patch rejection process waits 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.  4. Click **OK** to confirm proceeding with the rejecting the patch.

Procedure 72. Reject Patches Using PMAC

Step	Procedure	Results
3. ☐	**PMAC GUI**: Monitor reject patch	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Reject Patch** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.

9.22 Initialize PMAC Application

This procedure initializes the PMAC application and network resources.

Initialization of the PMAC application can be performed using the PMAC CLI if an initialization profile exists with the desired features. In the case where a PMAC feature needs to be enabled or modified, the PMAC GUI is used to initialize the application.

Prerequisites:

- PMAC has been deployed and is not initialized or fully configured.
- Aggregation switches have been properly configured.

Notes:

- The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.
- If the NetBackup feature is to be configured on this PMAC, perform 9.22.2 Initialize PMAC Application Using the GUI.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

If the PMAC application is to be initialized using the PMAC CLI, perform 9.22.1 Initialize PMAC Application Using CLI; otherwise, perform 9.22.2 Initialize PMAC Application Using the GUI.

9.22.1 Initialize PMAC Application Using CLI

This procedure initializes the PMAC application and network resources using CLI.

Prerequisites:

- PMAC has been deployed and is not initialized or fully configured.
- Aggregation switches have been properly configured.

Notes: The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 73. Initialize PMAC Application Using CLI

Step	Procedure	Results
1. ☐	**TVOE Management Server iLO**: Login	1. Log into the management server iLO with Internet Explorer as TVOE **admusr** user. `http://<management_server_iLO_IP>` 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click **Yes** if the Security Alert displays.

2. ☐	**TVOE Application Server iLO**: Login	Log into PMAC with **admusr** credentials.
		Note: On a TVOE host, if you open the virsh console, for example, `$ 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, run `ps -ef |grep virsh`, and 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 PMAC 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:`

Procedure 73. Initialize PMAC Application Using CLI

Step	Procedure	Results

3. ☐	**PMAC**: Initialize	Initialize the PMAC application with the PMAC profile.
		`$ 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`
		Wait for the background task to complete successfully. The command displays **IN_PROGRESS** for a short time.
		Run the following command until a **COMPLETE** or **FAILED** response is seen similar to the following:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`1: Initialize PMAC COMPLETE - PMAC 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:`

4. ☐	**PMAC**: Perform a system health check	`$ 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:
		`PMAC 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.`

5. ☐	**Virsh Console**: Log out	Exit the virsh console session using Appendix E.2 Exit a Guest Console Session on an iLO.
6. ☐	**Management Server iLO**: Exit the TVOE console	`$ logout`

9.22.2 Initialize PMAC Application Using the GUI

This procedure initializes the PMAC application and network resources using the GUI.

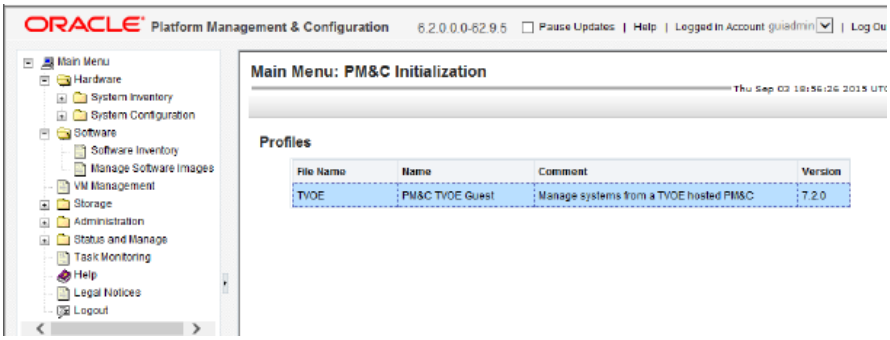
Prerequisites:

- PMAC has been deployed and is not initialized or fully configured.
- Aggregation switches have been properly configured.

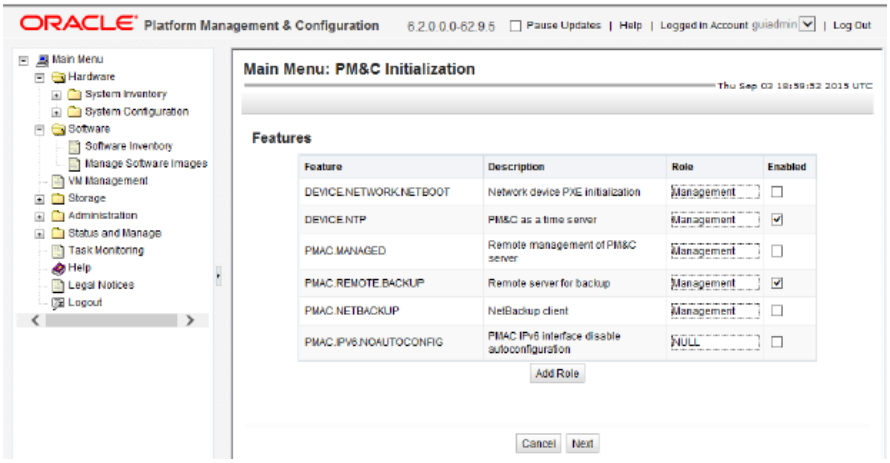
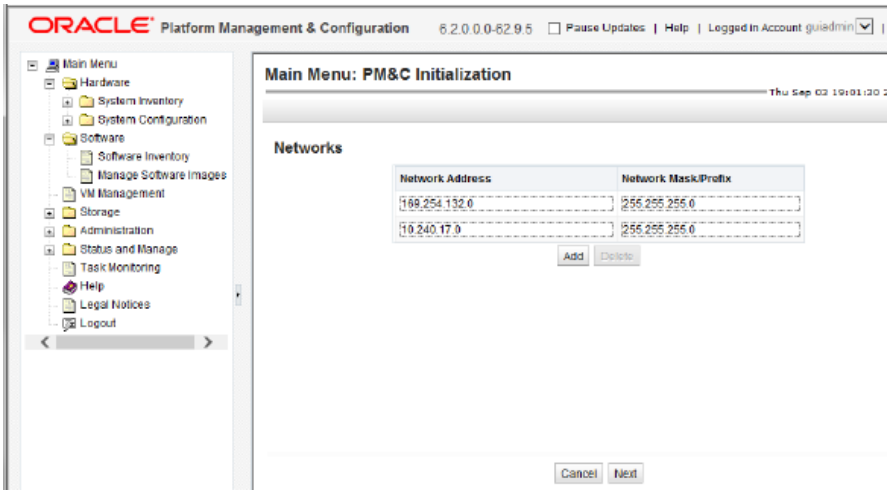
Notes: The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

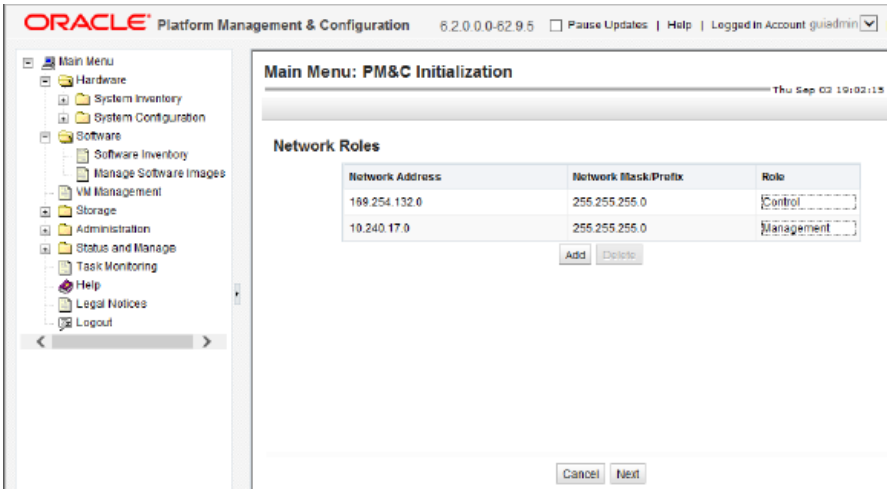
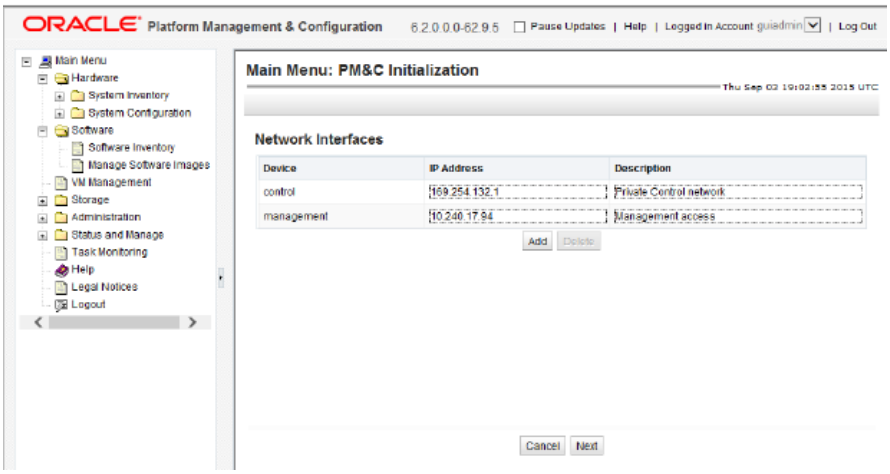
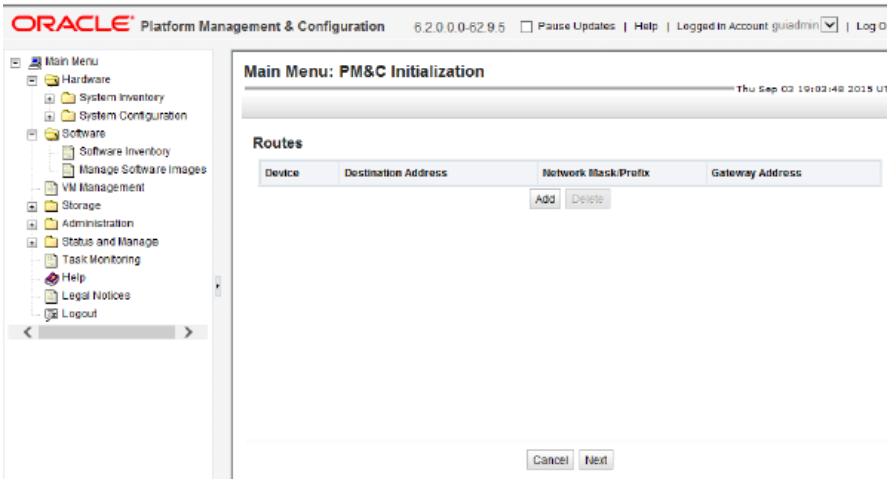
Procedure 74. Initialize PMAC Application Using the GUI

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Administration > PMAC Configuration**.
2. ☐	**PMAC GUI**: Select initialization profile	Select the appropriate PMAC initialization profile. 

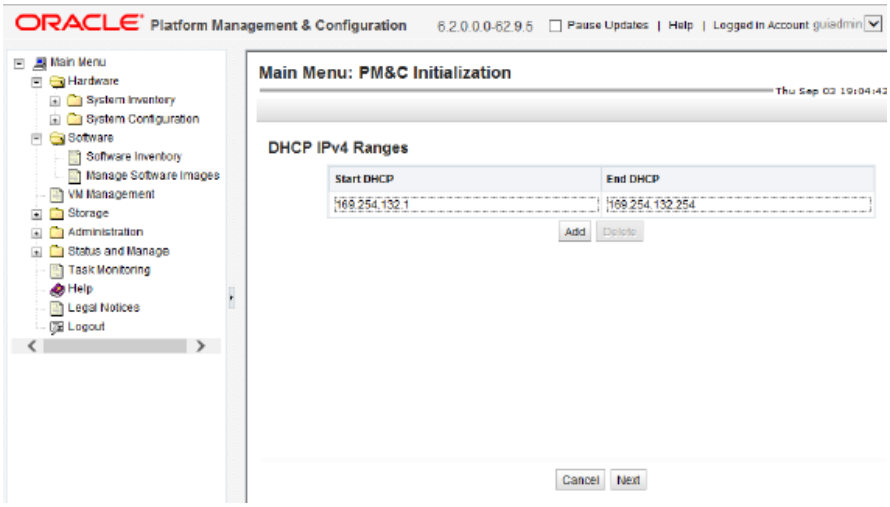
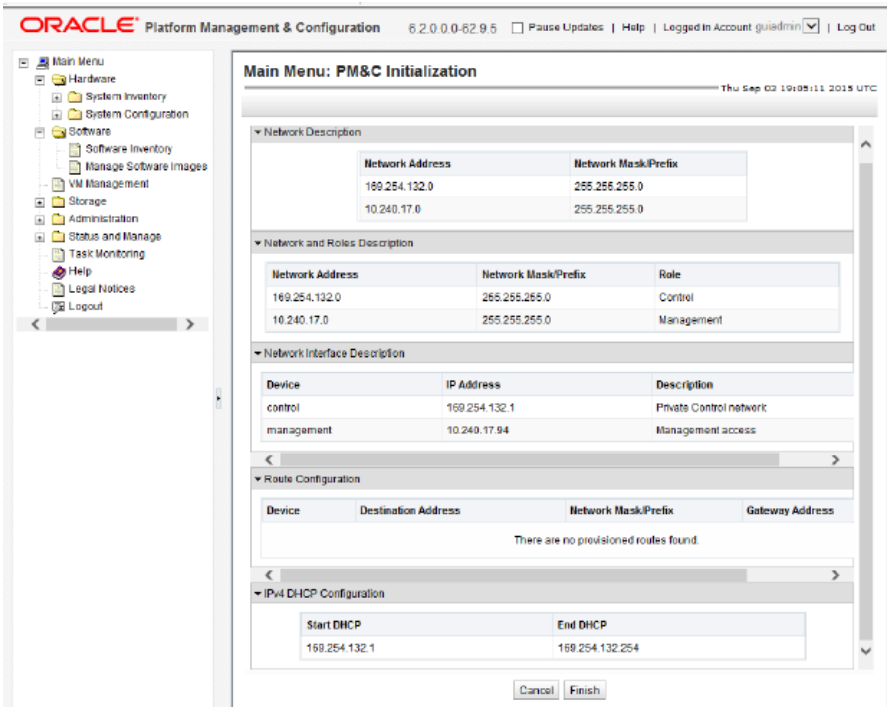
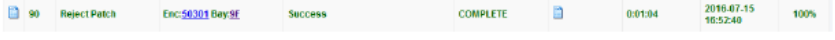
Procedure 74. Initialize PMAC Application Using the GUI

Step	Procedure	Results
3. ☐	**PMAC GUI**: Select features and roles	Select and enable, appropriate PMAC features and, if required, add new Roles. Click **Next**. 
4. ☐	**PMAC GUI**: Provision network	Provision the PMAC application networks and click **Next**. 

Procedure 74. Initialize PMAC Application Using the GUI

Step	Procedure	Results
5. ☐	**PMAC GUI**: Provision network roles	Provision the PMAC application network roles and click **Next**. 
6. ☐	**PMAC GUI**: Provision network interfaces	Provision the PMAC application network interface and click **Next**. 
7. ☐	**PMAC GUI**: Provision application routes	Provision the PMAC application routes and click **Next**. 

Procedure 74. Initialize PMAC Application Using the GUI

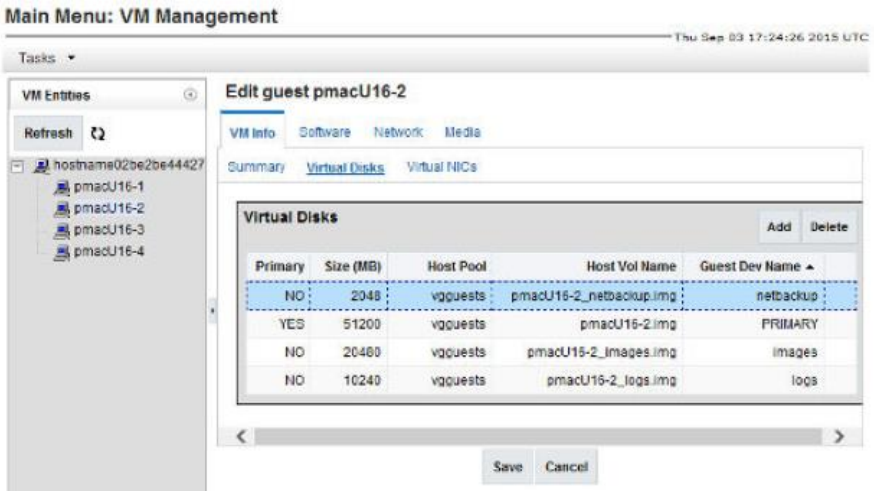
Step	Procedure	Results
8. ☐	**PMAC GUI**: Provision application DHCP ranges	Provision the PMAC application DHCP ranges and click **Next**. 
9. ☐	**PMAC GUI**: Verify	Verify the PMAC application initialization is correct on the Configuration Summary screen and click **Finish**. 
10. ☐	**PMAC GUI**: Monitor and verify	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Initialize PMAC** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.

9.23 Configure PMAC Application Guest NetBackup Virtual Disk

This procedure configures the PMAC application guest NetBackup virtual disk.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 75. Configure PMAC Application Guest NetBackup Virtual Disk

Step	Procedure	Results
1. ☐	**PMAC GUI**: Determine if the PMAC application guest is configured with a NetBackup virtual disk	Navigate to the Virtual Machine Management screen and select the PMAC application guest from the VM Entities list. From the VM Info tab, select the Virtual Disks sub-tab. Determine if the Virtual Disks list contains the NetBackup device. If the NetBackup device exists for the PMAC application guest, then the NetBackup Virtual Disk has already been configure; otherwise, continue to the next step
2. ☐	**PMAC GUI**: Edit the guest to add the NetBackup virtual disk	Click **Edit** and **Add**, then type the following data for the new NetBackup virtual disk. • Size (MB): 2048 • Host Pool: vgguests • Host Vol Name: <pmacGuestName>_netbackup.img • Guest Dev Name: netbackup ***Note***: The Guest Dev Name must be set to **netbackup** for the PMAC application to mount the appropriate host device. The <pmacGuestName> variable should be set to this PMAC guest's name to create a unique volume name on the TVOE host of the PMAC.
3. ☐	**PMAC GUI**: Verify	Verify the new NetBackup virtual disk data and click **Save**. 
4. ☐	**PMAC GUI**: Confirm the PMAC application guest list	Click **OK** on the confirmation screen.

Procedure 75. Configure PMAC Application Guest NetBackup Virtual Disk

Step	Procedure	Results
5. ☐	**PMAC GUI**: Monitor and verify	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Guest Edit** background task. When the task is complete, the text changes to green and the Progress column indicates 100%.
6. ☐	**TVOE Management Server iLO**: Shut down	Shut down the PMAC application guest. ***Note***: To configure the PMAC application with the new NetBackup virtual disk the PMAC application guest needs to be shut down and restarted. Refer to *PMAC Incremental Upgrade*, Release 6.6, E91174-01, Appendix O, Shutdown PMAC 5.5 or Later Guest.

7. ☐	**TVOE Management Server iLO**: Start the PMAC application guest	Using virsh utility on TVOE host of the PMAC guest, start the PMAC guest. Query the list of guests until the PMAC 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`

9.24 PMAC Guest Migrate NetBackup Client to New File System

If the NetBackup client software was installed on a PMAC application guest before the NetBackup virtual disk required for a PMAC deploys with NetBackup, execute 9.23 Configure PMAC Application Guest NetBackup Virtual Disk. This creates a new NetBackup virtual disk for the PMAC guest. The PMAC guest is shut down and restarted. The content of the **/usr/openv** directory is moved to the new NetBackup virtual disk, and mounted at **/usr/openv**.

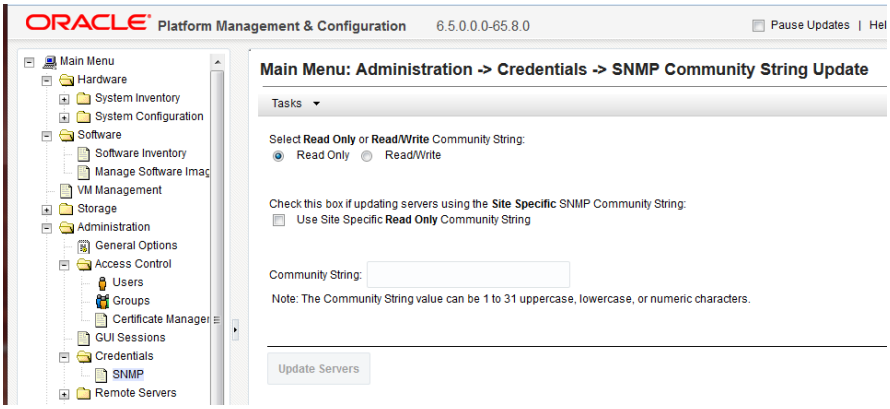
9.25 Update the TVOE Host SNMP Community String from the GUI

This procedure uses the PMAC GUI to update the read only or read/write SNMP community string on all TVOE hosting servers and the PMAC guest TPD, which are known to the PMAC control network.

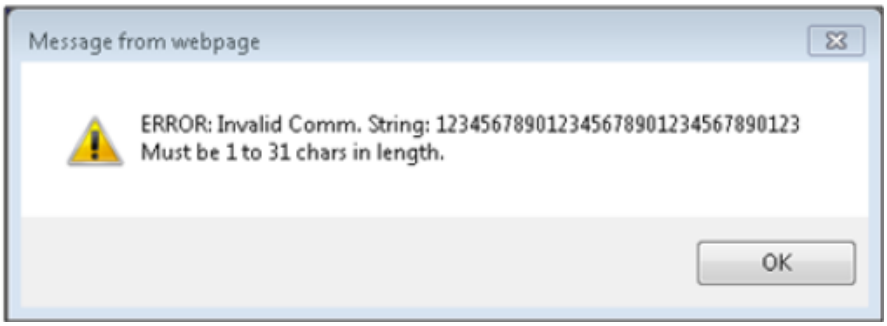
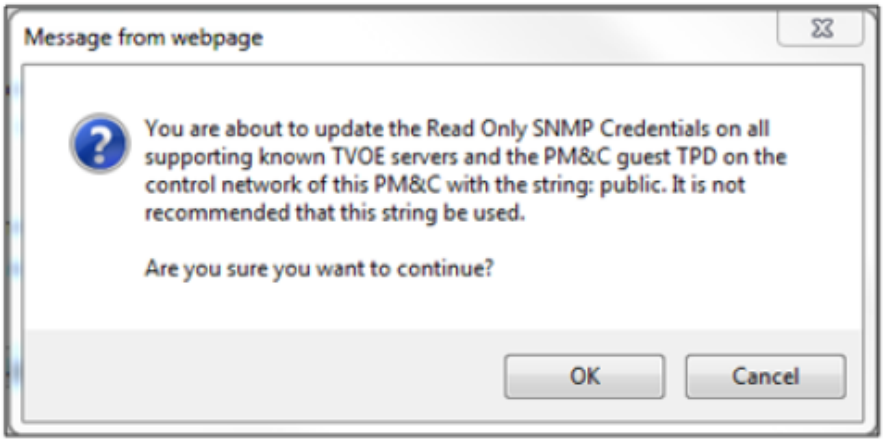
Prerequisite: You must be logged in as the Admin user to access this page.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

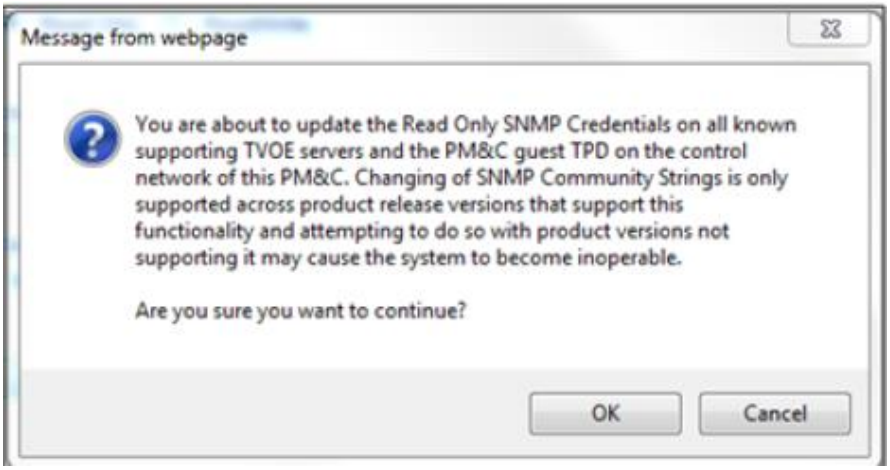
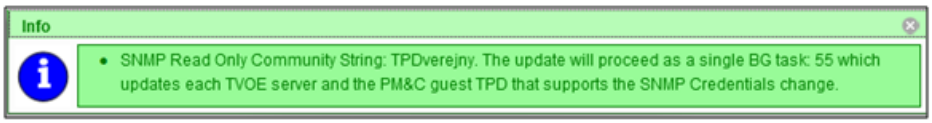
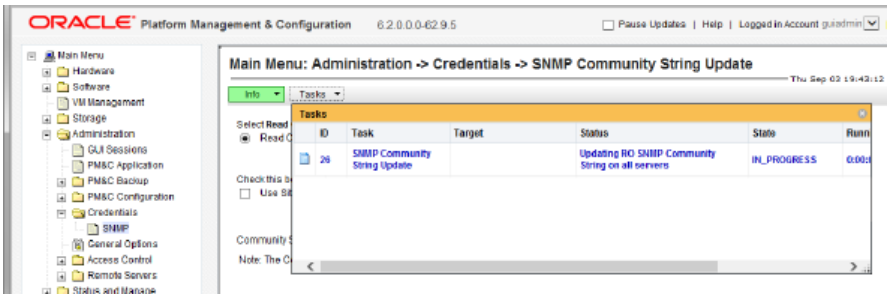
Procedure 76. Update the TVOE Host SNMP Community String from the GUI

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	**PMAC GUI**: Configure	1. Navigate to **Administration > Credentials > SNMP**. 2. Select the **Read Only** or **Read/Write** option depending on which SNMP Community String needs to updated. 3. If this the first time the SNMP Community Strings have been updated for this PMAC, then leave the **Use Site Specific** checkbox unmarked and type 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. If you want 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 disables the **Community String** textbox and enables the **Update Servers** button because the string to be used is the one stored in the PMAC database. 

Procedure 76. Update the TVOE Host SNMP Community String from the GUI

Step	Procedure	Results
3. ☐	**PMAC GUI**	Click **Update Servers**. The following error or warning messages may display depending on the Community String entered: • 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 the string to be set. • Valid Community String general warning.

Procedure 76. Update the TVOE Host SNMP Community String from the GUI

Step	Procedure	Results
		 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 inoperable if other components are not changed to reflect what is entered here. Click **OK**. ***Note***: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest TPD on the PMAC control network update. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.
4. ☐	**PMAC GUI**: Monitor the status	Click **Info** to access the status and watch for a successful or failed update.  Click **Tasks** located on the toolbar to monitor the progress.  Or navigate to **Main Menu > Task Monitoring** screen. When the task is complete, the text changes to green and the Progress column indicates 100%.
5. ☐	Validate the task	If the update needs to be validated, the user can type the pmaccli `getCommStrStatus` command at a SSH terminal connection to the PMAC to display the status of the Community Strings on all servers on the PMAC control network. Execution loops over all known servers on the PMAC control network and

Procedure 76. Update the TVOE Host SNMP Community String from the GUI

Step	Procedure	Results
		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 are queried. It uses the values set in the PMAC database to determine the status of each Community String. The status can be any 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 PMAC database. • Default - Matches the default (non-editable) Read Only or Read/Write Community String stored in the PMAC database. • Unknown - Was able to retrieve the Read Only or Read/Write Community String but it does not match what is maintained in the PMAC database. Usually indicates the Community String was updated manually from an interface other than the PMAC. • 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 PMAC, 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:

Procedure 76. Update the TVOE Host SNMP Community String from the GUI

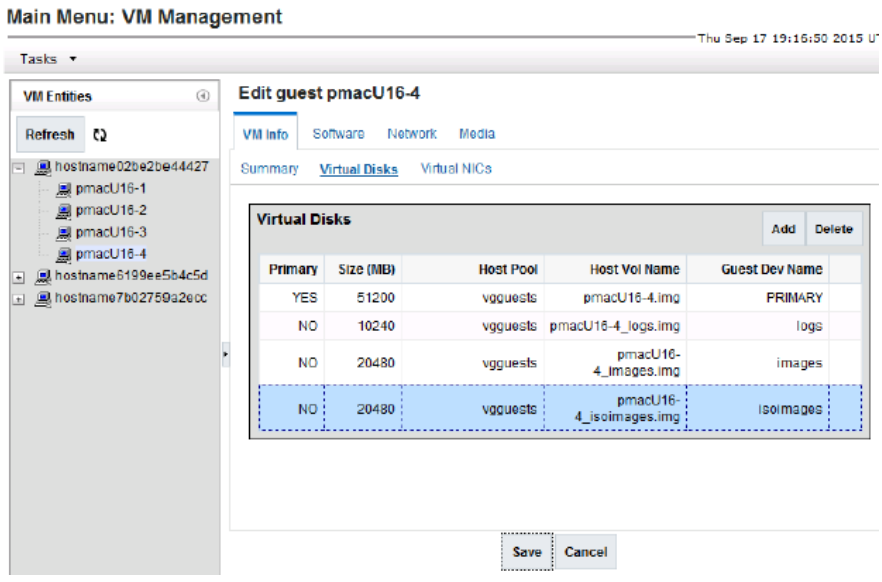
Step	Procedure	Results
		pmaccli getCommStrStatus SNMP Credentials Status Info: --- Server IP Address (IPv4 - IPv6) : 169.254.131.6 - fe80::b699:baff:fea8:b860 Server Release Info (Host - App): TPD: 6.0.0-80.28.1 - Unknown: Unknown Server Update Supported : Not Supported SNMP Read Only Community String : 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: 6.0.0-80.20.0 - 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:fce0 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

9.26 Configure PMAC Application Guest Isoimages Virtual Disk

This procedure expands the PMAC temporary area for importing software images using sftp in cases where PMAC already exists and larger ISO images need to be imported. The preferred method is to designate the extra space during PMAC deployment, refer to 9.3 Deploy PMAC Guest.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 77. Configure PMAC Application Guest Isoimages Virtual Disk

Step	Procedure	Results
1. ☐	**PMAC GUI**: Determine if the PMAC application guest is configured with a isoimages virtual disk	Navigate to the Virtual Machine Management screen and select the PMAC application guest from the VM Entities list. From the VM Info tab, select the Virtual Disks sub-tab. Determine if the Virtual Disks list contains the isoimages device. If the isoimages device exists for the PMAC application guest, then the isoimages Virtual Disk has already been configure; otherwise, continue to the next step
2. ☐	**PMAC GUI**: Edit the guest to add the isoimages virtual disk	Click **Edit** and **Add**, then type the following data for the new NetBackup virtual disk. • Size (MB): 2048 • Host Pool: vgguests • Host Vol Name: <pmacGuestName>_isoimages.img • Guest Dev Name: isoimages ***Note***: The Guest Dev Name must be set to **isoimages** for the PMAC application to mount the appropriate host device. The <pmacGuestName> variable should be set to this PMAC guest's name to create a unique volume name on the TVOE host of the PMAC.
3. ☐	**PMAC GUI**: Verify	Verify the new isoimages virtual disk data and click **Save**. 

Procedure 77. Configure PMAC Application Guest Isoimages Virtual Disk

Step	Procedure	Results
4. ☐	**PMAC GUI**: Confirm the PMAC application guest list	Click **OK** on the confirmation screen.
5. ☐	**PMAC GUI**: Monitor and verify	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Guest Edit** background task. When the task is complete, the text changes to green and the Progress column indicates 100%.
6. ☐	**TVOE Management Server iLO**: Shut down	Shut down the PMAC application guest. ***Note***: To configure the PMAC application with the new isoimages virtual disk the PMAC application guest needs to be shut down and restarted. Refer to *PMAC Incremental Upgrade*, Release 6.6, E91174-01, Appendix O, Shutdown PMAC 5.5 or Later Guest.

7. ☐	**TVOE Management Server iLO**: Start the PMAC application guest	Using virsh utility on TVOE host of the PMAC guest, start the PMAC guest. Query the list of guests until the PMAC 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`

9.27 Certificate Management

9.27.1 Generate a New Certificate Signing Request

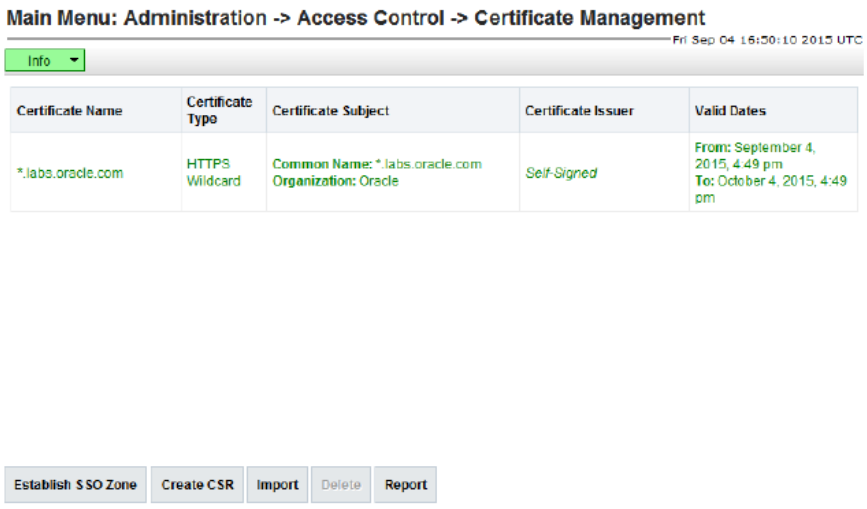
This procedure generates a new self-signed HTTPS certificate and a Certificate Signing Request to be submitted to the customer's Certificate Authority. The CA provides a signed certificate that can be used to replace the self-signed certificate using the procedure Update an HTTPS Certificate.

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 Import an HTTPS Certificate or Update an HTTPS Certificate instead.

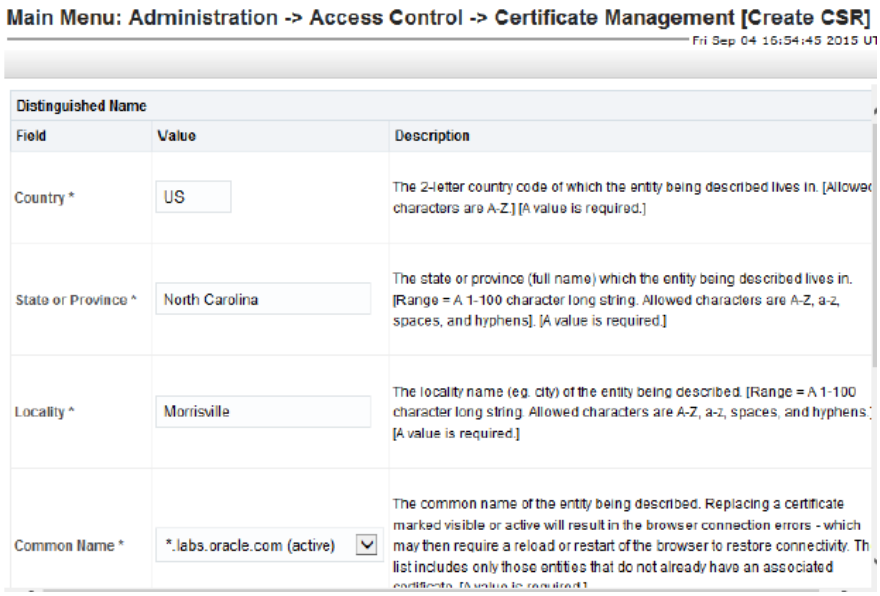
Prerequisite: 9.30 Configure PMAC Domain Name System

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 78. Generate a New Certificate Signing Request

Step	Results
1. ☐	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	1. Navigate to **Administration > Access Control > Certificate Management**. 2. Click **Create CSR**. 

Procedure 78. Generate a New Certificate Signing Request

Step	Results
3. ☐	Edit fields to describe the system for which the new certificate will be generated. All fields are required.  The **Common Name** determines whether the new certificate applies only to this PMAC host (for example, pmac1.office.company.com) or to any host in the same domain (for example, *.office.company.com). Use the host-specific option unless there are other hosts in the same domain sharing a single certificate. The Common Name only offer names for which no certificate is already present on this PMAC. To replace an existing certificate, first delete it as instructed in 9.27.4 Delete an HTTPS Certificate.
4. ☐	Click **Generate CSR**. This creates and installs a new (self-signed) HTTPS certificate in PMAC and writes the related Certificate Signing Request to a file. This file is available immediately using the **Status and Manage > Files** screen (refer to 9.27.2 Update an HTTPS Certificate). Because a new self-signed certificate is in use now, the user needs to re-establish the GUI session and accept the certificate.

9.27.2 Update an HTTPS Certificate

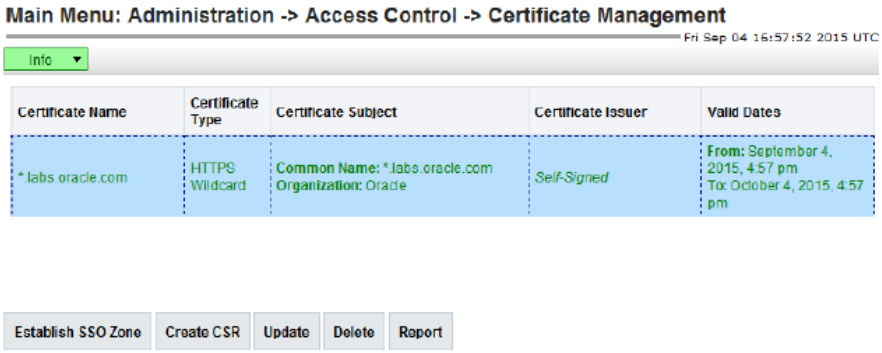
This procedure replaces a self-signed certificate generated by PMAC with a CA-signed certificate provided by the customer's Certificate Authority.

Prerequisites:

- 9.27.1 Generate a New Certificate Signing Request has been performed 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

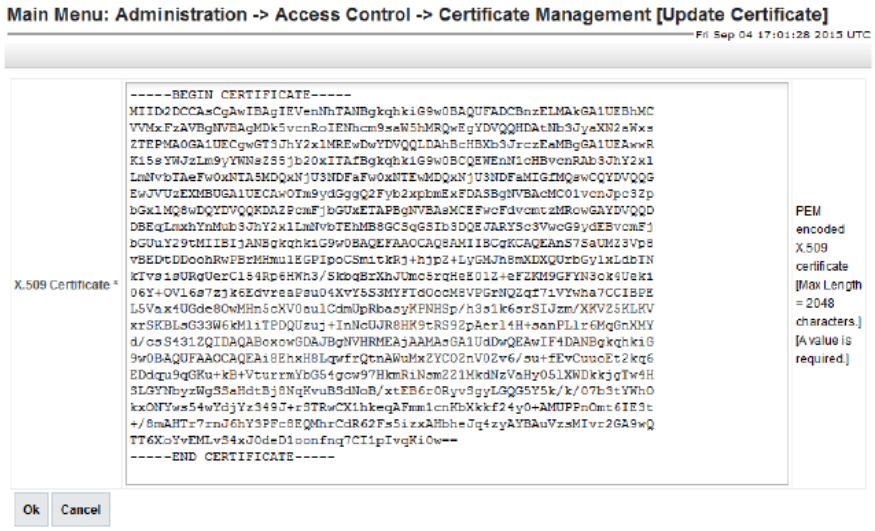
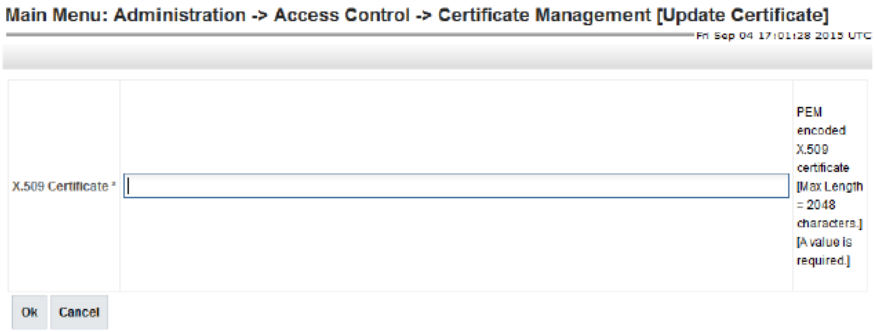
If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 79. Update an HTTPS Certificate

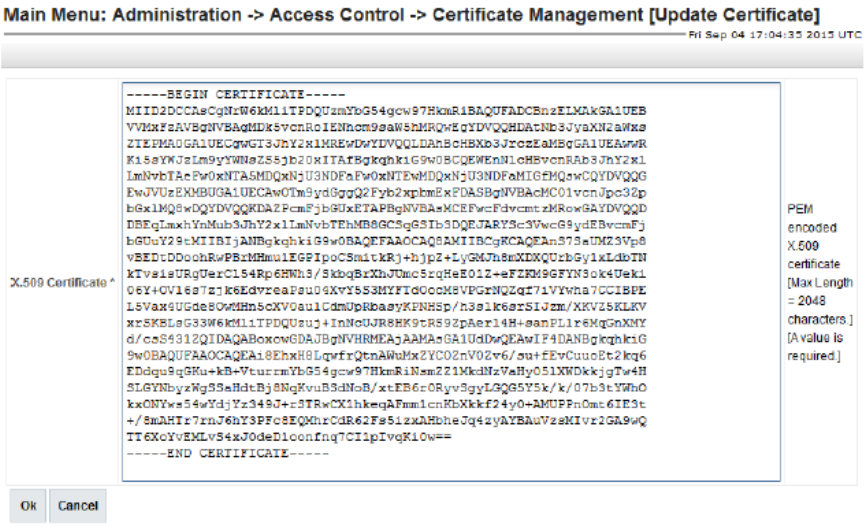
Step	Results
1. ☐	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	1. Navigate to **Administration > Access Control > Certificate Management**. 2. Select the certificate to update. 3. Click **Update**. 

Procedure 79. Update an HTTPS Certificate

Step	Results

3. ☐	1. Select the text and delete it.
	 
	
	 
	
	2. Using an ASCII text editor on the PC, open the signed certificate provided by the Certificate Authority.
	3. Copy the certificate from the editor to the **X.509 Certificate** field on the PMAC screen.
	Include the BEGIN and END lines and everything between:
	`-----BEGIN CERTIFICATE-----`
	`<encoded certificate data>`
	`-----END CERTIFICATE-----`

Procedure 79. Update an HTTPS Certificate

Step	Results
	
4.	Click **OK**. The PMAC web server restarts immediately to put the updated certificate into effect. If the signing CA is not known to the browser or the PMAC was not accessed by DNS name, the user has to re-establish the GUI session and accept the new certificate. Users are now able to access the PMAC GUI without having to acknowledge and accept the server's certificate if the following conditions are met: • The PMAC is accessed by DNS name, not by IP address. This requires either a customer-provided DNS server or configuration of the PMAC host name in the client PC's hosts file. • The browser recognizes the CA's signature on the certificate. This requires 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.

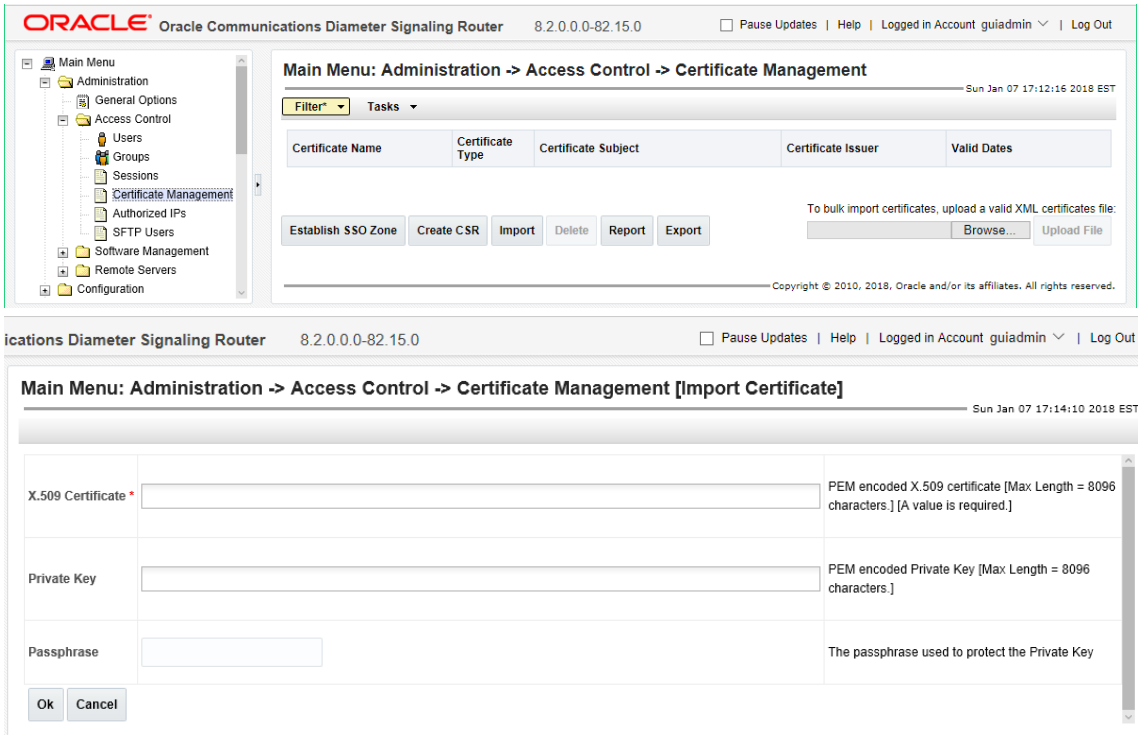
9.27.3 Import an HTTPS Certificate

This procedure 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 PMAC using its own passphrase. The customer's passphrase is not retained by PMAC.

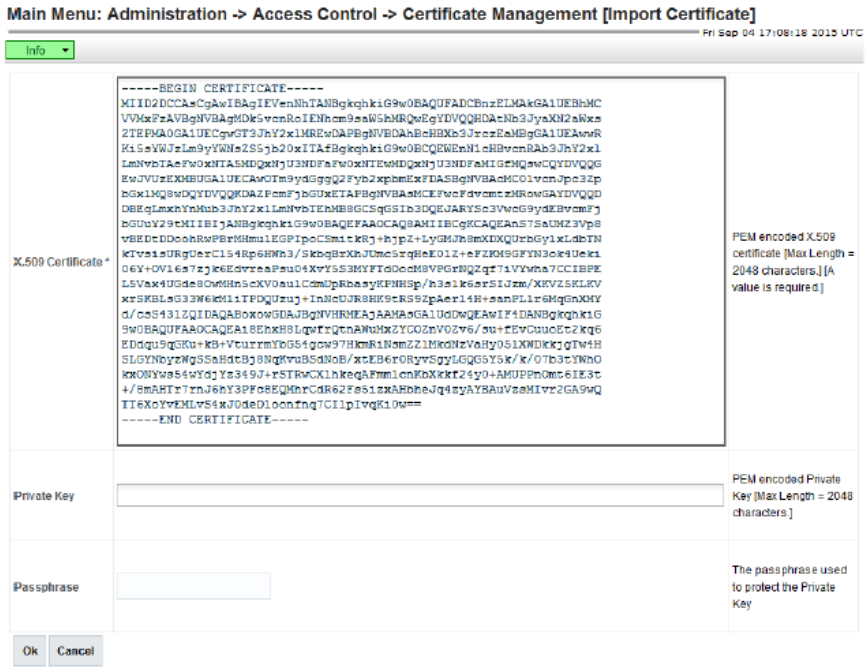
If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 80. Import an HTTPS Certificate

Step	Results
1. ☐	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	1. Navigate to **Administration > Access Control > Certificate Management**. 2. Click **Import**. 

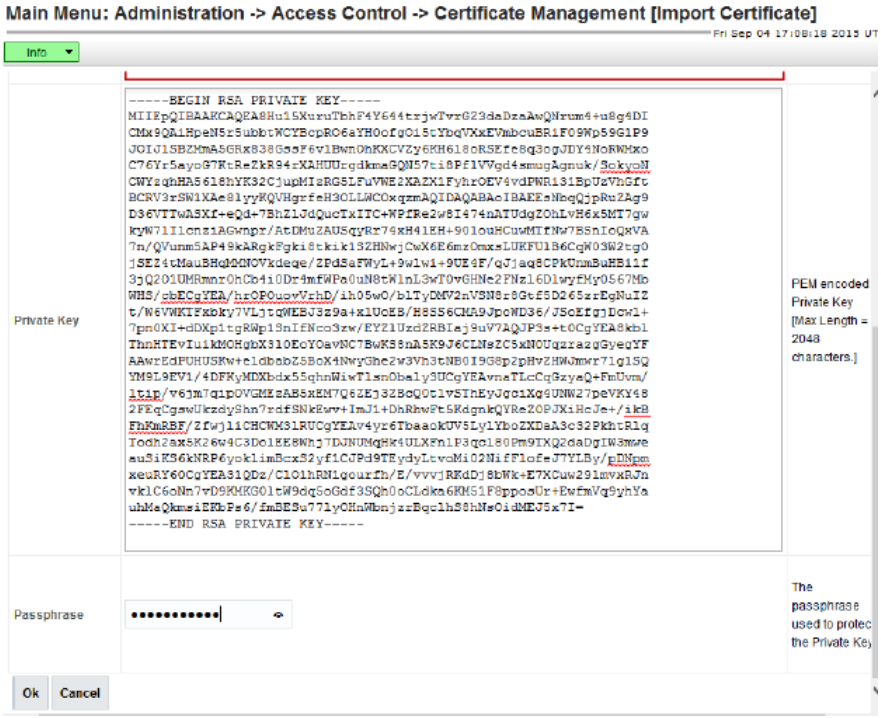
Procedure 80. Import an HTTPS Certificate

Step	Results

3. ☐	1. Using an ASCII text editor on the PC, open the signed certificate provided by the Certificate Authority.
	2. Copy the certificate from the editor to the **X.509 Certificate** field on the PMAC screen.
	Include the BEGIN and END lines and everything between:
	`-----BEGIN CERTIFICATE-----`
	`<encoded certificate data>`
	`-----END CERTIFICATE-----`
	 

Procedure 80. Import an HTTPS Certificate

Step	Results

4. ☐	1. Using an ASCII text editor on the PC, open the private key file.
	2. Copy the private key from the editor to the **Private Key** field on the PMAC screen.
	Include the BEGIN and END lines and everything between:
	`-----BEGIN RSA PRIVATE KEY-----`
	`<encoded key data>`
	`-----END RSA PRIVATE KEY-----`
	3. If the private key is encrypted, type or paste the passphrase into the **Passphrase** field.
	 

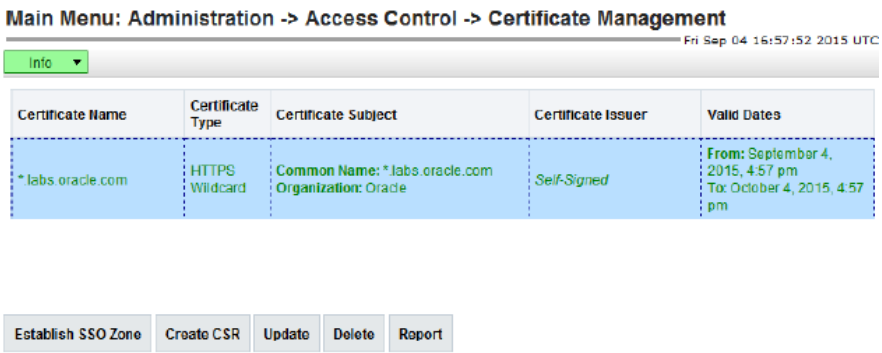
5. ☐	Click **OK**. The PMAC web server restarts immediately to put the updated certificate into effect. If the signing CA is not known to the browser or the PMAC was not accessed by DNS name, the user has to re-establish the GUI session and accept the new certificate. Users are now able to access the PMAC GUI without having to acknowledge and accept the server's certificate if the following conditions are met: • The PMAC is accessed by DNS name, not by IP address. This requires either a customer-provided DNS server or configuration of the PMAC host name in the client PC's hosts file. • The browser recognizes the CA's signature on the certificate. This requires 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.

9.27.4 Delete an HTTPS Certificate

This procedure removes a certificate from PMAC. PMAC then reverts to using e default HTTPS certificate. This requires the user to acknowledge and accept the certificate when accessing the PMAC GUI.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 81. Delete an HTTPS Certificate

Step	Results
1. ☐	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	1. Navigate to **Administration > Access Control > Certificate Management**. 2. Select the certificate to delete. 3. Click **Delete**.  The PMAC web server restarts immediately to put the default certificate into effect. Users now have to acknowledge and accept the certificate when accessing the PMAC GUI. For this reason, the current session may need to be re-established.

9.28 Use the PMAC File Management System

This procedure uses the PMAC GUI to manage files on the PMAC server. These files are stored locally in the **/var/TKLC/db/filemgmt/csr** directory (considered the FMA or File Management Area). Any files added to the FMA are visible from the **Status and Management > Files** screen on the PMAC GUI. 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 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.

Prerequisite: You must be logged in as the Admin user to access this page.

9.28.1 Use the PMAC File Management System to Delete Files

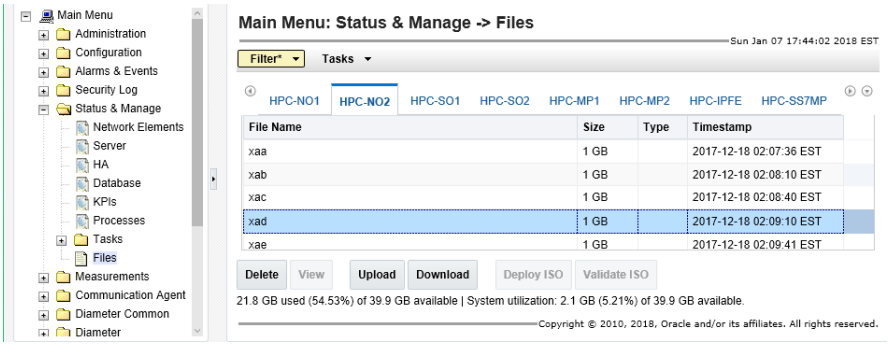
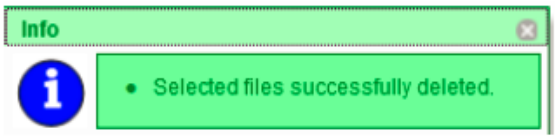
This procedure deletes one of more files on the PMAC server using the PMAC GUI.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 82. Use the PMAC File Management System to Delete Files

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 

Procedure 82. Use the PMAC File Management System to Delete Files

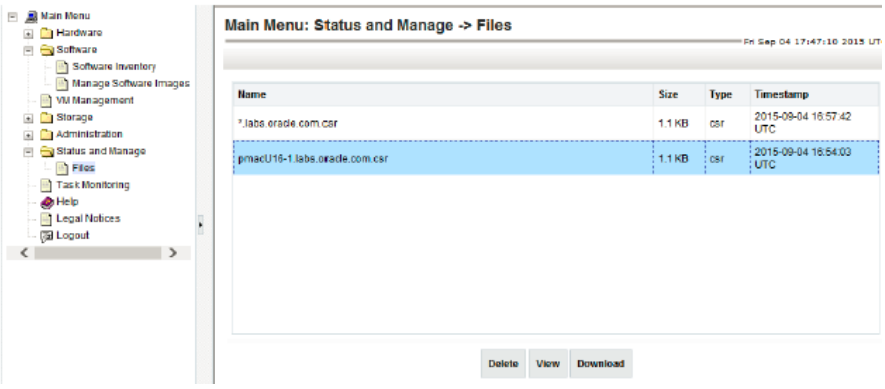
Step	Procedure	Results
2. ☐	Select a file	1. Navigate to **Status and Management > Files**. 2. Select one or more files to delete.  Upon initial display of the Files Management screen, all available files located within the FMA are visible. If no files are located within the FMA, **There are no files present** displays. If no files are selected, all buttons are visible but disabled. If a single file is selected all buttons are enabled. If more than one file is selected, the View and Download buttons are disabled.
3. ☐	Delete the file(s)	1. Click **Delete**. 2. Click **OK** to confirm. The Files Management screen refreshes with the selected file(s) no longer displayed and a status info box (which can be selected) indicating the action was successful. 

9.28.2 Use the PMAC File Management System to View Files

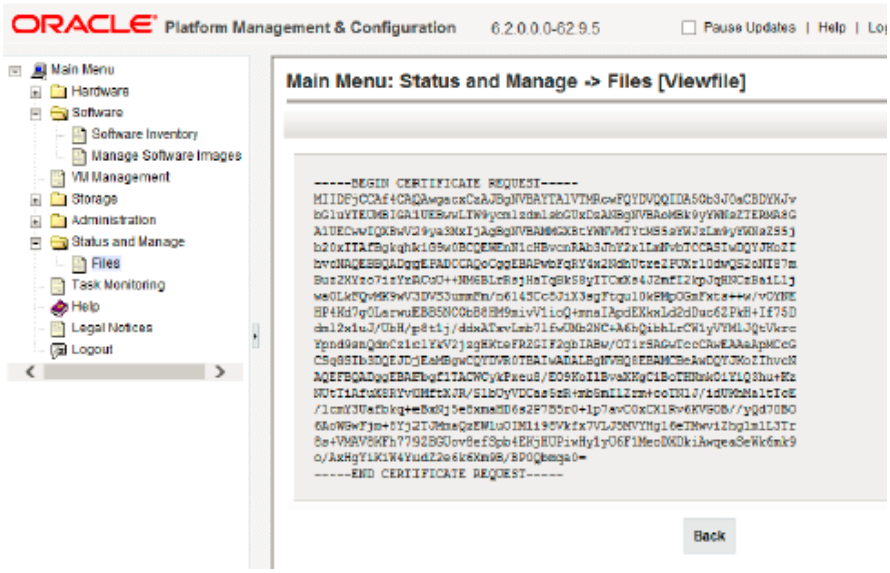
This procedure views a single file on the PMAC server using the PMAC GUI.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 83. Use the PMAC File Management System

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	Select a file	1. Navigate to **Status and Management > Files**. 2. Select one file to view.  Only one file may be selected for viewing. If more than one file is selected, the View and Download buttons are disabled.

Procedure 83. Use the PMAC File Management System

Step	Procedure	Results
3. ☐	View single file	The View File page displays.  Click the Back arrow to return to the original Files Management screen.

9.28.3 Use the PMAC File Management System to Download Files

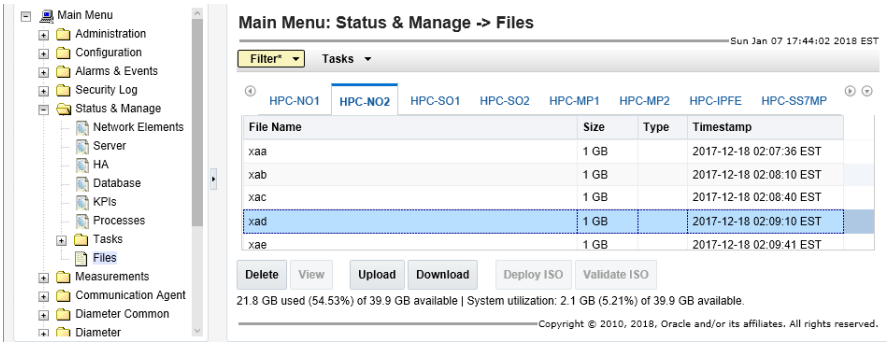
This procedure downloads a single file to the PMAC server using the PMAC GUI.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 84. Use the PMAC File Management System

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 

Procedure 84. Use the PMAC File Management System

Step	Procedure	Results
2. ☐	Select a file	1. Navigate to **Status and Management > Files**. 2. Select one file to download.  Only one file may be selected for downloading. If more than one file is selected, the View and Download buttons are disabled.
3. ☐	Download a single file	1. Click **Delete**. 2. Depending on the browser, you are asked to **Save** to a disk or **Open** the file. The default editor program (usually set to Notepad, which does not format files) 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.

9.29 Delete ISO Images from the PMAC Image Repository

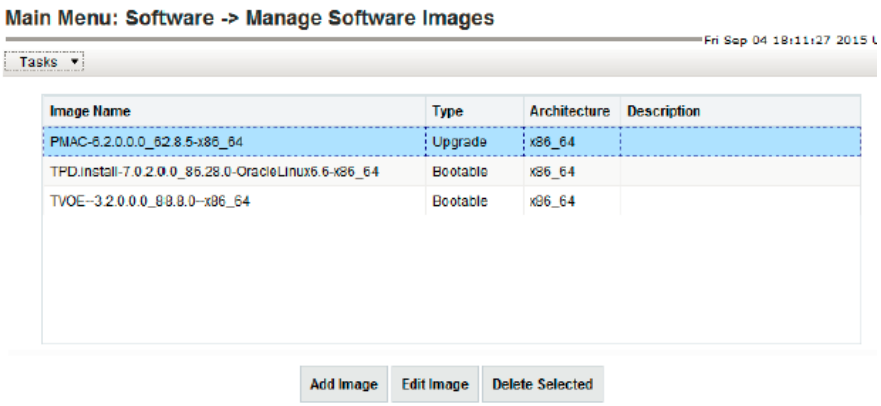
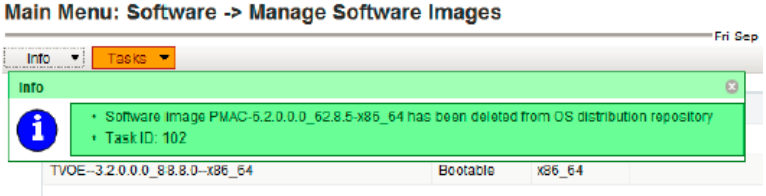
This procedure deletes ISO images from the PMAC repository.

Prerequisites:

9.8 Add ISO Images to the PMAC Image Repository

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 85. Delete ISO Images from the PMAC Image Repository

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user. 
2. ☐	**PMAC GUI**: Select an image	1. Navigate to **Software > Manage Software Images**. 2. Select the software image to delete. 
3. ☐	**PMAC GUI**: Delete the image	1. Click **Delete Image**. 2. Click **OK** to confirm. The Manage Software Images screen refreshes with the selected file(s) no longer displayed. Click **Info** to confirm the correct image file was deleted. 

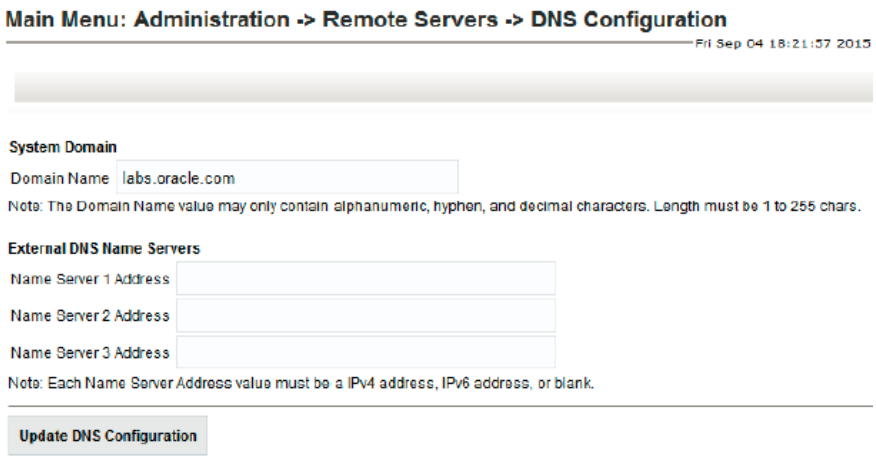
9.30 Configure PMAC Domain Name System

This procedure configures the PMAC Domain Name System (DNS).

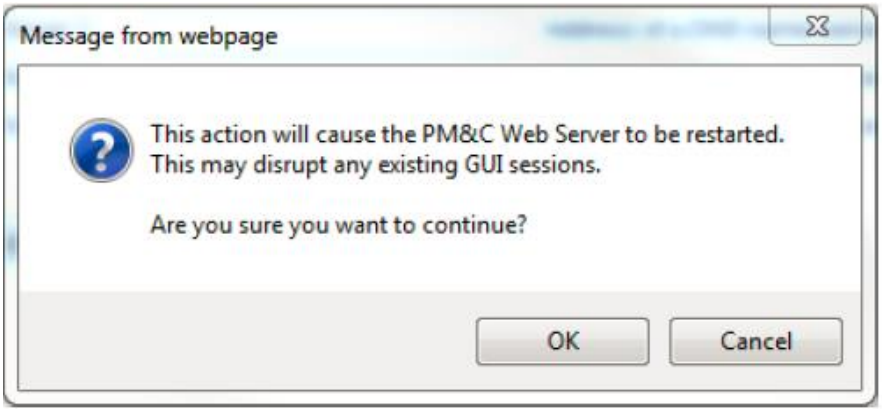
If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 86. Configure PMAC Domain Name System

Step	Procedure	Results

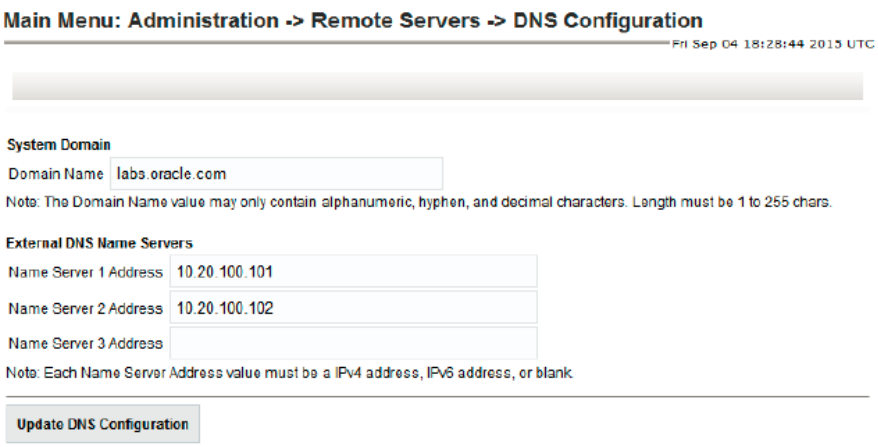
1. ☐	**PMAC GUI**: Update the domain server only	1. Navigate to **Administration > Remote Servers > DNS Configuration**.
		2. On initial setup, all fields should be empty. Enter the required **Domain** name.
		This should be a valid domain name consisting of 1 to 255 alphanumeric characters plus the "." and "-" characters.
		Leave all Name Server text boxes blank.
		3. Click **Update DNS Configuration**.
		 
		This saves the Domain Name into the PMAC database. It does not enable DNS for the PMAC. After the update, the DNS Configuration refreshes with the domain name displayed in the Domain textbox.
		It does not update the DNS **/etc/resolv.conf** file. This file is 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`
		4. Check for errors.
		Success:

Procedure 86. Configure PMAC Domain Name System

Step	Procedure	Results
		 Error:  5. Click **OK** to confirm the web server restart.  6. Refresh the DNS Configuration screen since the web server restarted.
2. ☐	**PMAC GUI**: Update the full DNS configuration	1. Navigate to **Administration > Remote Servers > DNS Configuration**. 2. On initial setup, all fields should be empty. Enter the required **Domain** name. This should be a valid domain name consisting of 1 to 255 alphanumeric characters plus the "." and "-" characters. Leave all Name Server text boxes blank. 3. Type a valid IPv4 or IPv6 address in each **Name Server** textbox. It is not required to type an IP into all three textboxes. 4. Click **Update DNS Configuration**.

Procedure 86. Configure PMAC Domain Name System

Step	Procedure	Results



This saves the Domain Name into the PMAC database and enables DNS for the PMAC. After the update, the DNS Configuration refreshes with the domain name displayed in the Domain textbox and all servers display.

It also updates the DNS **/etc/resolv.conf** file. This file is in the following format (TPD default):

```
# PMAC DNS Configuration File
# ------------------------------------------------------------
# WARNING: Do not make manual changes to this file.  This
file
# is auto generated by the PMAC 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
```

5. Check for errors.

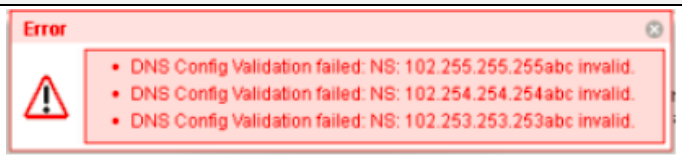
Success:

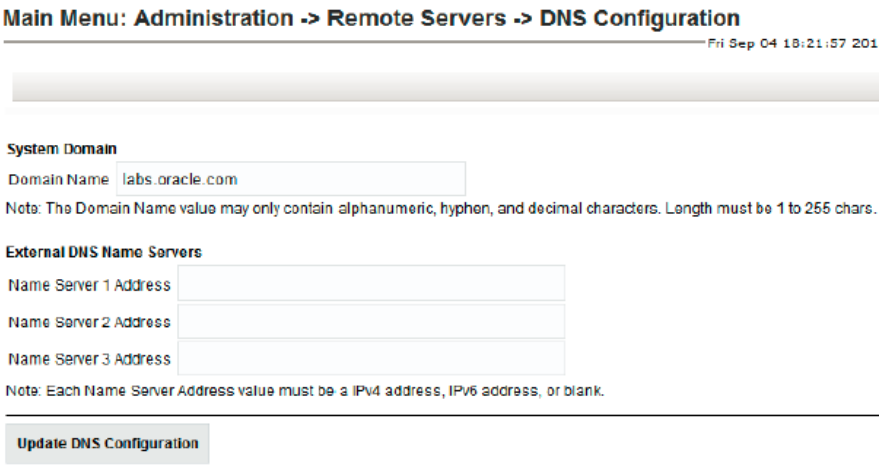
Errors:

- Domain Name validation failure

- Server Name validation failure. This error may display a failure for each incorrect Name Server.

Procedure 86. Configure PMAC Domain Name System

Step	Procedure	Results
		

3. ☐	**PMAC GUI**: Remove the current DNS configuration	1. Navigate to **Administration > Remote Servers > DNS Configuration**.
		2. Delete all entries from all Name Server textboxes.
		This assumes the Certificates Management screen is still using the Domain Name.
		3. Click **Update DNS Configuration**.
		 
		This saves the Domain Name into the PMAC database and disables DNS for the PMAC. After the update, the DNS Configuration refreshes with the domain name displayed in the Domain textbox and all servers are blank.
		It also updates the DNS **/etc/resolv.conf** file. This file is 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`

9.31 Set User Authentication on the PMAC

This procedure configures the authentication on a new or existing user from the **Main Menu > Administration > Access Control > Users** screen by clicking **Insert** for new users or selecting an existing user entry and clicking **Edit**. Remote Authentication can only be used if an LDAP server has been properly configured on the PMAC. Please see section 9.33 Configure an LDAP Server on the PMAC 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 marked. The user must apply the following rules when selecting the authentication type:

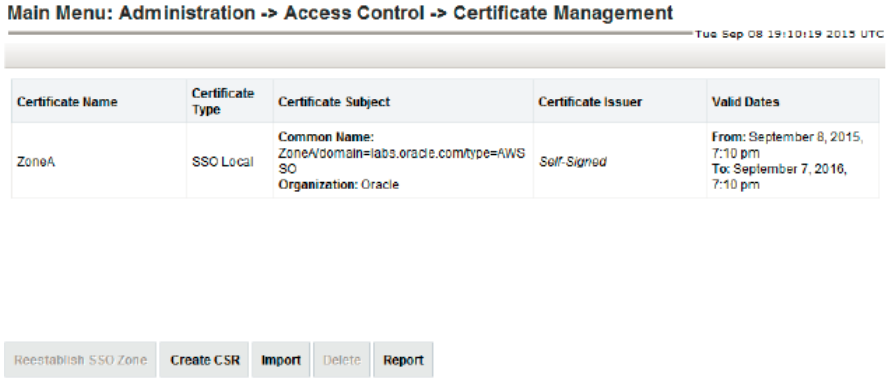
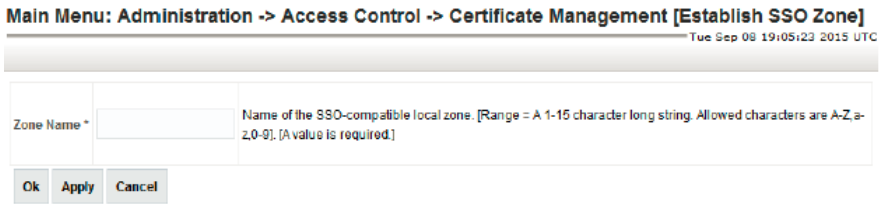
1. The three default users (guiadmin, pmacops, and guest) have a default setting of **Allow Local Authentication** selected and **Allow Remote Authentication** not selected. On upgrade, these settings are configured according to the setting of the **GUI Site Settings > Local Authentication Enabled** (if included in the **from** release).
2. The guiadmin user authentication settings cannot be changed and is 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, the user fails local authentication unless it is an admin group user. It does not attempt remote authentication.
5. If a new user is created with **Allow Remote Authentication** only selected, on first login, the password change request is not initiated. Once **Allow Local Authentication** is selected for the new user, the user is asked to change the password 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 attempts remote authentication first. If communication is established to the LDAP server for authentication and authentication fails, local authentication is not attempted. The login is rejected.
7. If both **Allow Local Authentication** and **Allow Remote Authentication** are selected, the system attempts remote authentication first. If communication is NOT established to the LDAP server for authentication, local authentication is attempted. The login request is accepted if the proper local credentials are 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 since it is maintained on the LDAP server.

9.32 Configure the PMAC into an Existing Single Sign-On (SSO) Domain

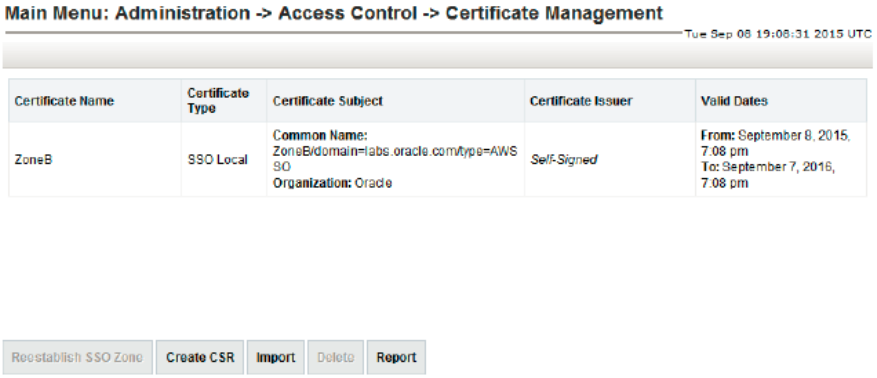
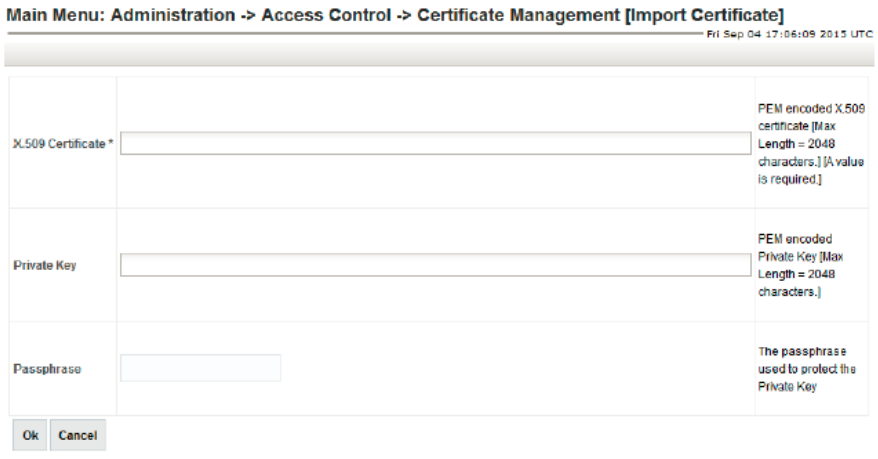
This procedure set up and incorporates the PMAC into an existing single sign-on domain. Within a given domain (SSO can only configured with a sing domain), the PMAC is defined within a different domain zone the NO/SO/MP. The SSO certificates of the different zones must be imported manually using the Certificate Management interface of the two zones (typically from the AppWorks GUI and the PMAC GUI). Once each zone includes the local and remote SSO certificates, the user can login from one zone management GUI, which then logs the user into the other zone management GUIs

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

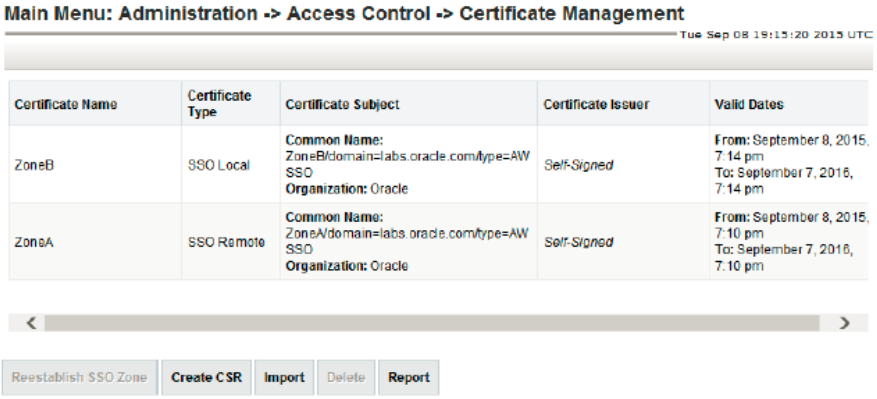
Procedure 87. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

Step	Results
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 9.31 Set User Authentication on the PMAC).
2. ☐	The current zone (ZoneA - consisting of the NO/SO/MP architecture) should already have an existing SSO certificate configured from the **Administration** > **Access Control** > **Certificate Management** screen using the **Establish SSO Zone** button. This is indicated as the **SSO Local** certificate type. 
3. ☐	1. From the ZoneB (PMAC) GUI, navigate to **Administration > Access Control > Certificate Management**. 2. Click **Establish SSO Zone**. 

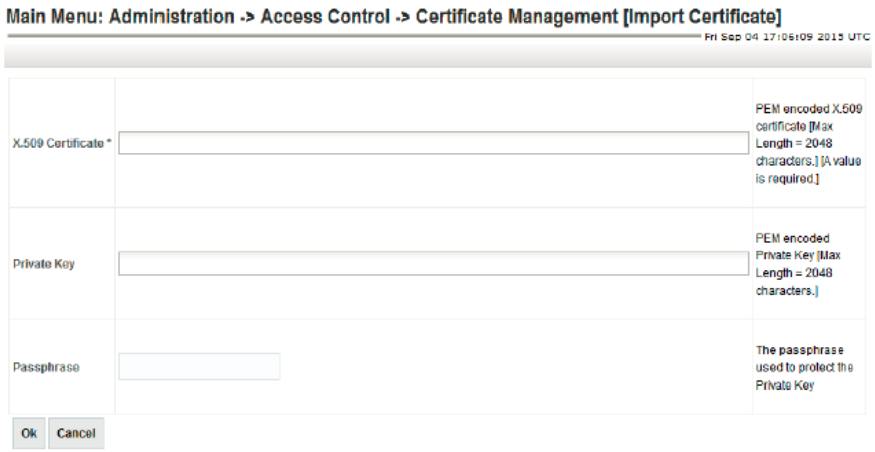
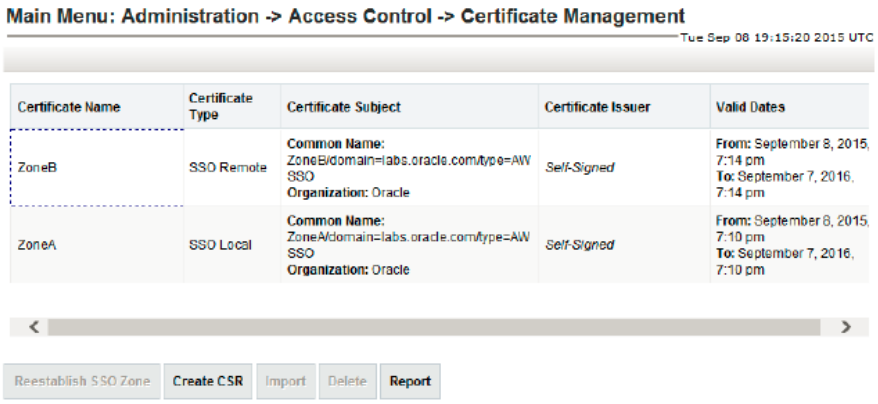
Procedure 87. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

Step	Results
4. ☐	1. Enter a valid **Zone Name**. 2. Click **OK**. This creates a **SSO Local** certificate on the PMAC and returns to **Administration > Access Control > Certificate Management**. 
5. ☐	1. From ZoneA (AppWorks) GUI, navigate to **Administration > Access Control > Certificate Management**. 2. Select the ZoneA SSO Local certificate and click **Report**. This displays a printable encrypted version of the certificate.
6. ☐	Copy the certificate from the `-----BEGIN CERTIFICATE-----` to the end of the `-----END CERTIFICATE-----`.
7. ☐	Click **Back** to return to **Administration > Access Control > Certificate Management**.
8. ☐	Navigate to the ZoneB (PMAC) GUI **Administration > Access Control > Certificate Management**.
9. ☐	Click **Import**. 

Procedure 87. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

Step	Results
10. ☐	Paste the copied certificate from ZoneA into the **X.509 Certificate** field. Leave the other fields blank.
11. ☐	Click **OK**. This creates a **Remote SSO** certificate and returns to **Administration > Access Control > Certificate Management** displaying ZoneB as the SSO Local certificate type and ZoneA as the SSO Remote certificate type. 
12. ☐	3. From ZoneB (PMAC) GUI, navigate to **Administration > Access Control > Certificate Management**. 4. Select the ZoneB SSO Local certificate and click **Report**. This displays a printable encrypted version of the certificate.
13. ☐	Copy the certificate from the `-----BEGIN CERTIFICATE-----` to the end of the `-----END CERTIFICATE-----`.
14. ☐	Click **Back** to return to **Administration > Access Control > Certificate Management**.
15. ☐	Navigate to the ZoneA (AppWorks) GUI **Administration > Access Control > Certificate Management**.

Procedure 87. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

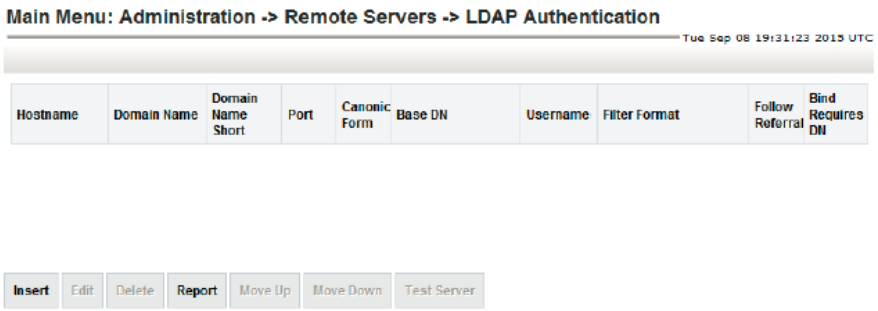
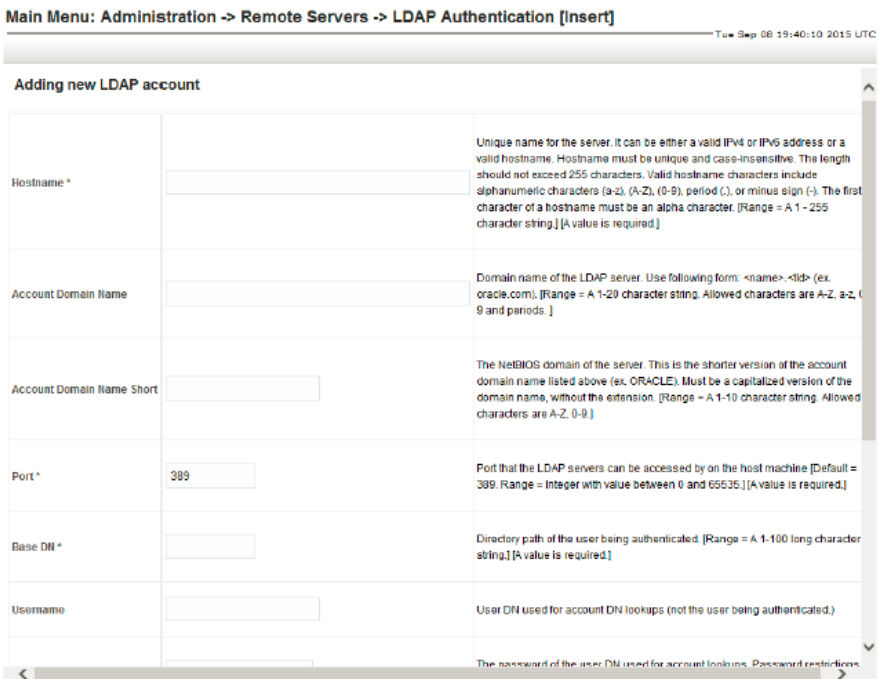
Step	Results
16. ☐	Click **Import**. 
17. ☐	Paste the copied certificate from ZoneB into the **X.509 Certificate** field. Leave the other fields blank.
18. ☐	Click **OK**. This creates a **Remote SSO** certificate and returns to **Administration > Access Control > Certificate Management** displaying ZoneA as the SSO Local certificate type and ZoneB as the SSO Remote certificate type.  Once both zones have their local and remote SSO certificates configured, the user is 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 logs in immediately. If the user logs out from either zone, both zones are logged out. 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 remains logged in. This works the same in either direction.

9.33 Configure an LDAP Server on the PMAC

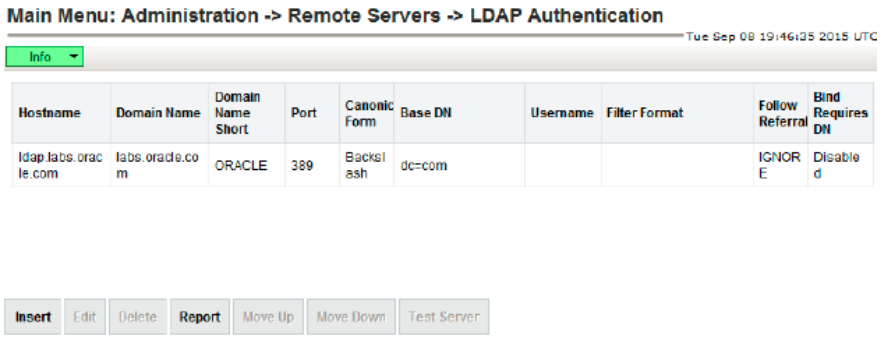
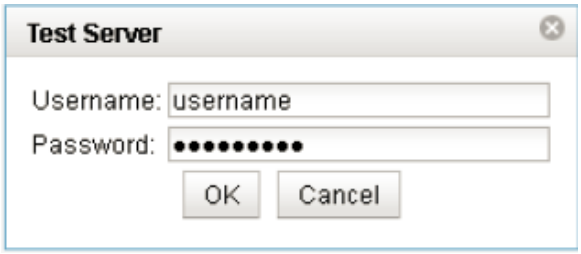
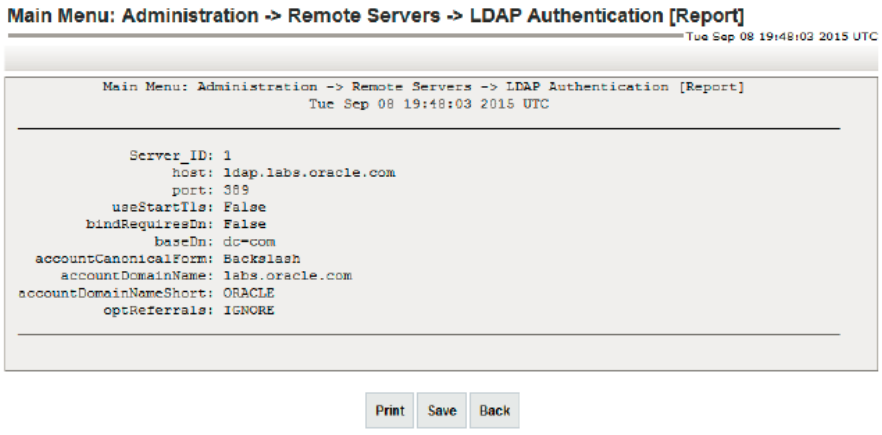
This procedure configures a LDAP server on the PMAC.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 88. Configure an LDAP Server on the PMAC

Step	Results
1. ☐	Navigate to **Administration > Remote Servers > LDAP Authentication**.  Only **Insert** and **Report** are available and no LDAP servers configured.
2. ☐	1. Click **Insert**.  ***Note***: Port 389 has been set as default. This is the standard port number for LDAP communication. Change it, if necessary. 2. Contact your LDAP Server Administrator for the proper values required to configure the LDAP server.

Procedure 88. Configure an LDAP Server on the PMAC

Step	Results
3. ☐	1. Click **OK**. The LDAP server configures and returns to **Administration > Remote Servers > LDAP Authentication**. ***Note***: Click **Apply** to remain on the Insert screen.  2. Click **Test Server**.  Type a valid username and password configured on the LDAP server to verify the user and communication to the LDAP server. 3. Click **Report** to display the configuration data of the LDAP. 

9.34 Transfer Image from PMAC Repository to Other Servers

This procedure transfers a software image from the PMAC image repository to servers managed by PMAC.

Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for application install/upgrade have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for application install/upgrade have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- An image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.

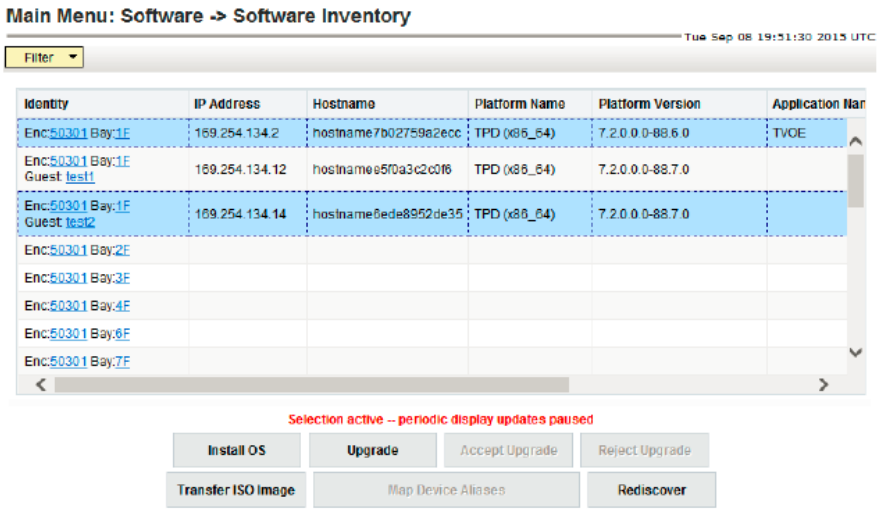
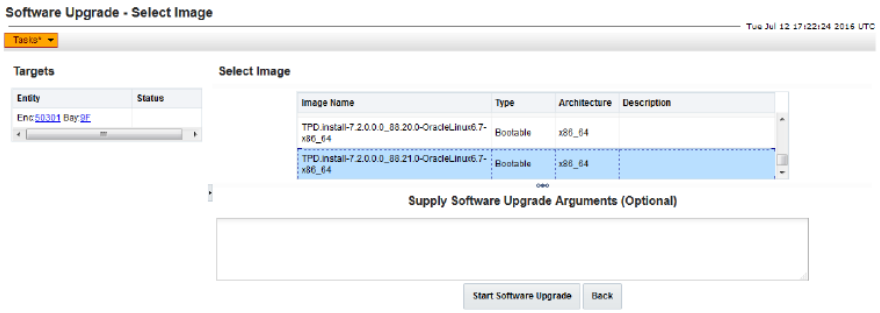
Note: The image transfer is only supported for discovered entities (IP address is known)

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

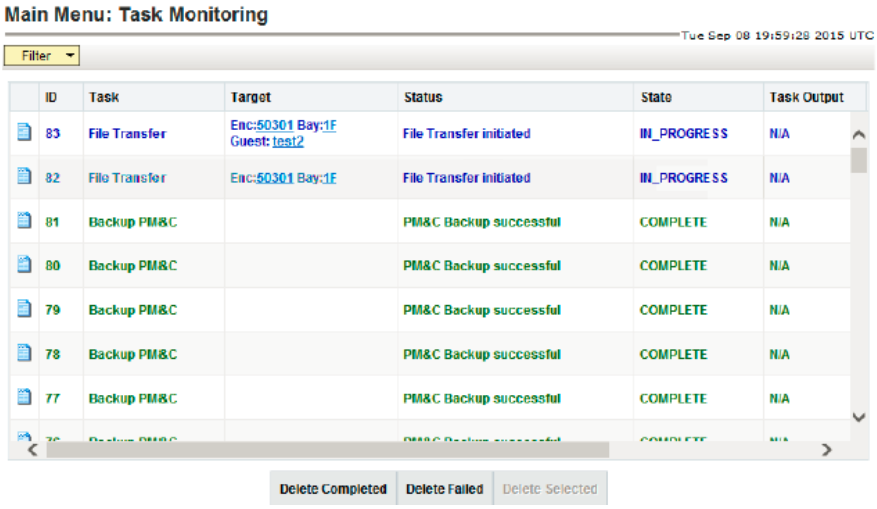
Procedure 89. Transfer Image from PMAC Repository to Other Servers

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as **guiadmin** user.  Navigate to **Software > Software Inventory**.

Procedure 89. Transfer Image from PMAC Repository to Other Servers

Step	Procedure	Results
2. ☐	**PMAC GUI**: Select servers	1. Select the servers where you want to transfer the image. If you want to perform an upgrade on more than one server, press **Ctrl** while selecting multiple rows. 2. Click **Transfer ISO Image**. 
3. ☐	**PMAC GUI**: Select image	1. Select the image to transfer to the servers. 2. Type the **Path**, **User**, and **Password** for the target entities. The credentials should be consistent with credentials used for SCP. The path should be accessible with the credentials provided. ***Note***: PMAC does not validate firmware update arguments. It only verifies they are all present. 3. Click **Start Image Transfer**.  4. Click **OK** to confirm the transfer.

Procedure 89. Transfer Image from PMAC Repository to Other Servers

Step	Procedure	Results
4. ☐	**PMAC GUI**: Monitor transfer	Navigate to **Main Menu > Task Monitoring** to monitor the progress of the **Transfer** background task. A separate task displays for each server.  When the task is complete, the text changes to green and the Progress column indicates 100%.

10. Configure SAN Procedures

10.1 Configure SAN Storage Using PMAC Application

This procedure configures a SAN storage using the PMAC application. You configure the SAN controller and corresponding host volumes using XML files uploaded by the PMAC application. The XML files allow you to:

- add virtual disks
- delete virtual disks without an associated volume
- add global spares
- delete global spares
- 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.

Prerequisites:

- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- 9.5 Configure PMAC Application
- 5.3 Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers
- 5.4 Configure Advanced Settings on P2000 Fibre Channel Disk Controllers for a given SAN storage type
- 4.1 Configure Brocade Switches

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

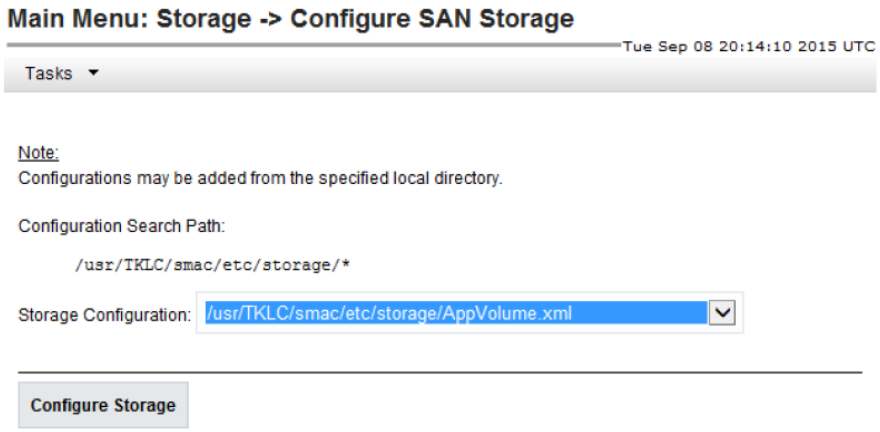
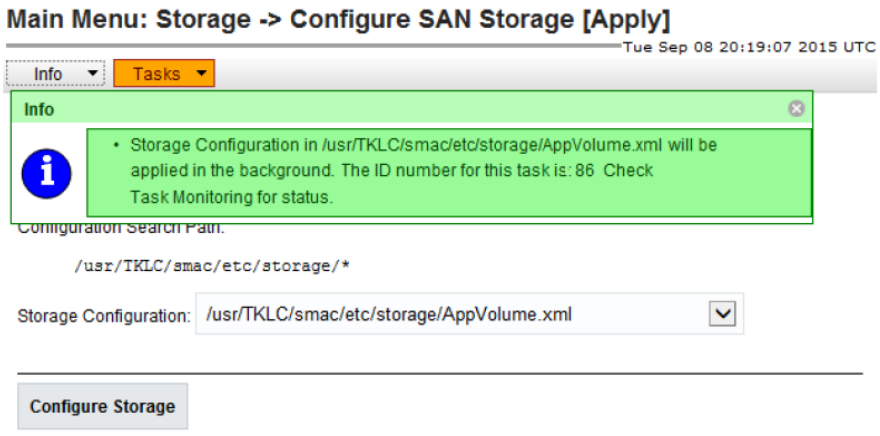
fail. Dedicating spares to vdisks is the most secure method, but it is also expensive to reserve spares for each vdisk. Alternatively, you can assign global spares. A properly sized spare is one whose capacity is equal to or greater than the largest disk in the vdisk.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 90. Configure SAN Storage Using PMAC Application

Step	Procedure	Results
1. ☐	Handle failed SAN configuration	If any attempt to add SAN storage components have failed, a partial configuration may exist. This needs to be cleaned-up before attempting again. 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 delete the partial configuration and clear the SAN controller or host volume. Note that after a host volume is deleted or cleared, PMAC automatically reboots the server blade. Once the XML file is obtained, continue following to correctly upload and execute the XML file using the PMAC application. If the end user desires to IPM the blade server to cleanup host volumes, refer to 9.9 IPM Servers Using PMAC Application.
2. ☐	**PMAC Server**: Provide SAN configuration XML files	Log into the management server as the **admusr** user. Copy all SAN configuration XML files into **/usr/TKLC/smac/etc/storage** directory.
3. ☐	**PMAC Server**: Update SAN controller password in PMAC	If default password has been changed on SAN controllers, then the stored password in PMAC must be changed to match. Run this script on PMAC and set the SAN controller password for the manage user: `$ sudo /usr/TKLC/smac/bin/updateCredentials --type=msa`
4. ☐	**PMAC GUI**: Login	If needed, open a web browser and type `https://<pmac_management_network_ip>` Login as the **guiadmin** user.

Procedure 90. Configure SAN Storage Using PMAC Application

Step	Procedure	Results
5. ☐	**PMAC GUI**: Configure SAN	Navigate to **Main Men > Storage > Configure SAN Storage**. From the Storage Configuration option, select **SAN configuration file** and click **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 PMAC automatically reboots 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. ☐	**PMAC GUI**: Monitor configuration status	The Configure SAN Storage screen displays with a new background task entry. Click **Tasks** located on the toolbar. 
7. ☐	Recovery from configuration errors	If PMAC is able to parse the XML configuration file successfully, the 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.

10.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation

This procedure removes volumes from the partially installed SAN. This can happen if the SAN configuration fails. Blade servers are IPMed again.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 91. Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation

Step	Procedure	Results
1. ☐	**Management Server**: Update SAN controller password	If default password has been changed on SAN controllers, then the stored password in PMAC must be changed to match. Run this script on PMAC and set the SAN controller password for the manage user: `$ sudo /usr/TKLC/smac/bin/updateCredentials --type=msa`
2. ☐	**Fibre Channel Controller GUI**: Login	Log into `https://<controller_IP_address>`.
3. ☐	**Fibre Channel Controller GUI**: Delete volumes and vdisks on MSA 2012	For MSA 2012 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**. Repeat this step for second controller.
4. ☐	**Fibre Channel Controller GUI**: Delete volumes and vdisks on P2000	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**, unselect all the global spare disks, and click **Modify Spares**. Repeat this step for second controller.
5. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.

Procedure 91. Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation

Step	Procedure	Results
6. ☐	**OA GUI**: Delete zones from Brocade switches	1. Select one of the Brocade switches and click **Management Console**. 2. Login as an administrative user. 3. Select **Zone Admin** and click **Clear All**. Wait for success message in bottom left of window and **Effective zone Config: Default, All Access** in bottom right of window. 4. Click **Save Config**. 5. Repeat for the second switch.
7. ☐	Run IPM on blade server	Run IPM on blade servers 9.9 IPM Servers Using PMAC Application. ***Note***: A new IP address is assigned to bond0 of each blade at the end of the IPM process, so the XML files need to be updated accordingly.

11. Virtualization Procedures

11.1 Create Guest Server Using PMAC Application

This procedure creates a virtualized guest server on a TVOE host using the PMAC web GUI.

Prerequisites:

- Enclosure containing the TVOE host blade server to host the guest has been configured using 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- The TVOE host has been installed using 9.9 IPM Servers Using PMAC Application.

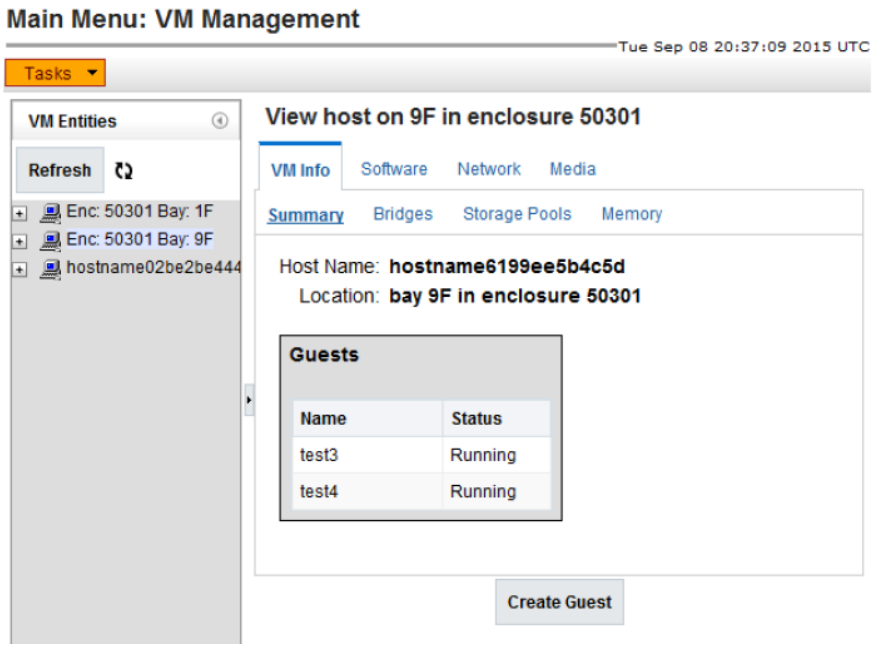
Note: PMAC does not prevent over-subscription of memory or CPU resources.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

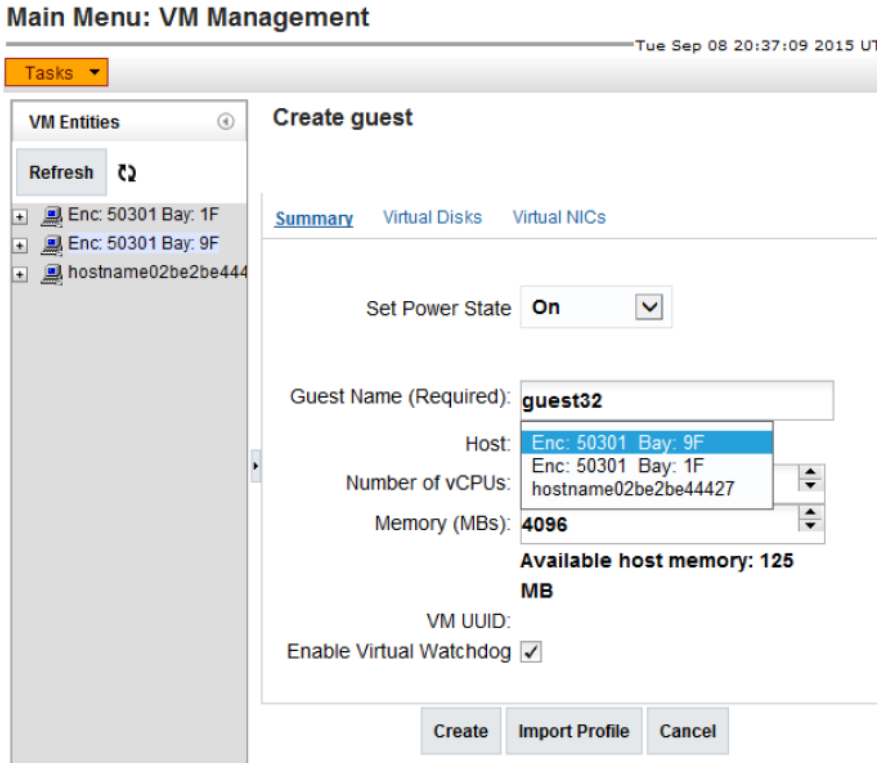
Procedure 92. Create Guest Server Using PMAC Application

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open a web browser and type: `https://<pmac_management_network_IP>` Login as **guiadmin** user.
2. ☐	**PMAC GUI**	Navigate to **Main Menu > VM Management**.

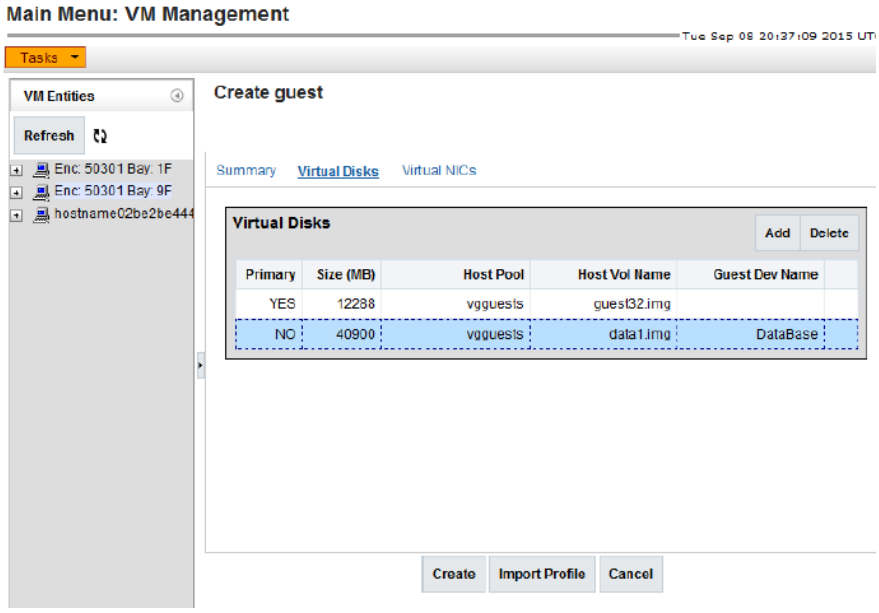
Procedure 92. Create Guest Server Using PMAC Application

Step	Procedure	Results
3. ☐	**PMAC GUI**	Click **Create Guest**. 

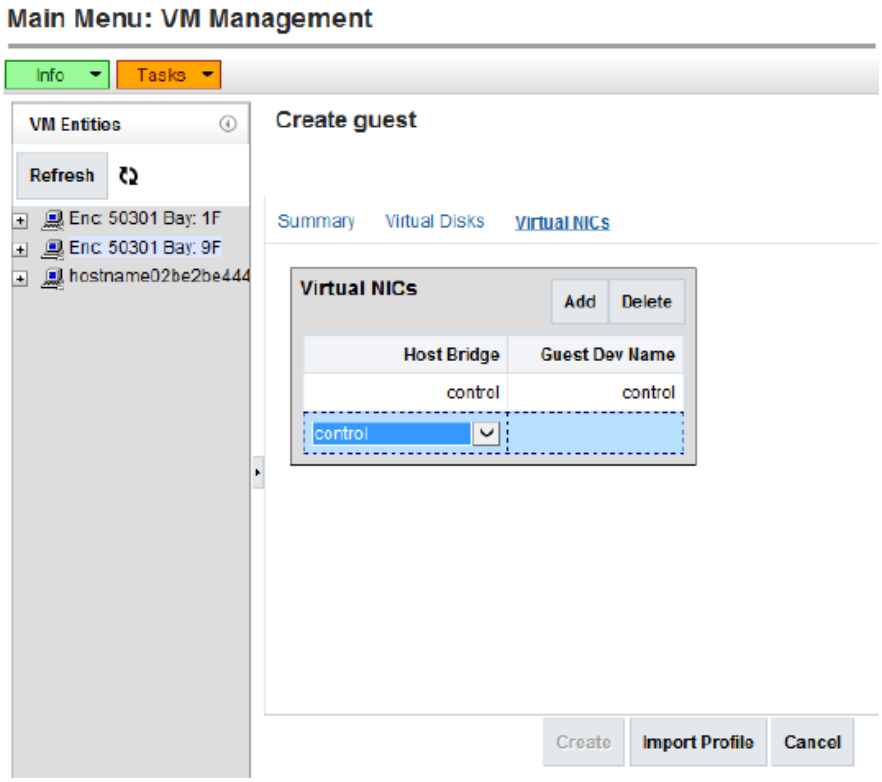
Procedure 92. Create Guest Server Using PMAC Application

Step	Procedure	Results
4. ☐	**PMAC GUI**	1. Type a **Name** (something unique to the TVOE host). The name can be identical to a guest on a different host. 2. From the **Host** options, select the TVOE host on which to create the guest.  3. From the **Set Power State** options, select the initial power state for the guest. In this context, **Shutdown** and **Destroy** both behave the same. The guest is not powered on upon creation. 4. Edit the **vCPU** count and **Memory** size. 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. PMAC does not prevent over-subscription of these resources. 5. If this Guest is being created on a version of TVOE having support for virtual guest watchdogs, the **Enable Virtual Watchdog** checkbox displays. Set this checkbox according to whether or not watchdog support is desired for this guest.

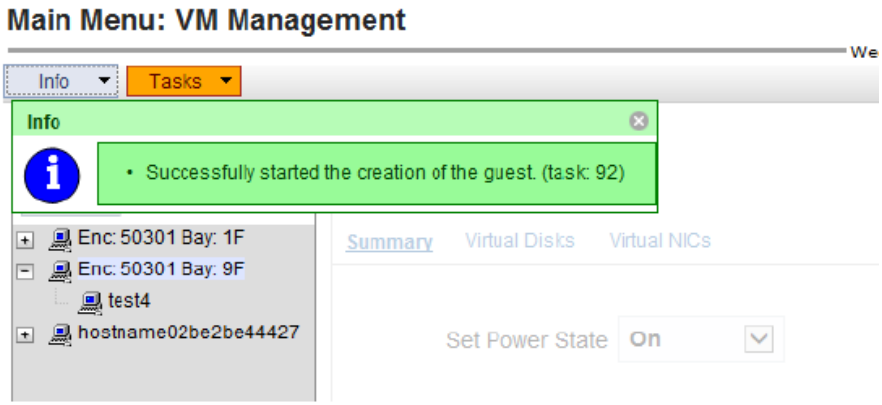
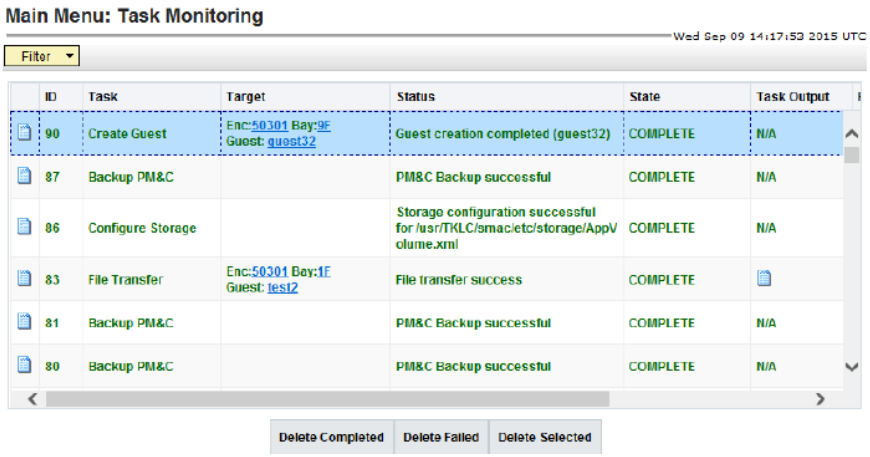
Procedure 92. Create Guest Server Using PMAC Application

Step	Procedure	Results
5. ☐	**PMAC 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 is 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. **Host Pool**: The default vgguests storage pool is selected. Other pools that have been configured on the TVOE can be selected from the options. **Host Vol Name**: For the primary disk, this is filled in automatically based on the guest name provided. It can be modified manually if needed. It must be unique among all disks on all guests hosted on the TVOE. **Guest Dev Name**: For the primary disk, this value is not set. For added disks, this is the alias used inside the TPD instance running on the guest. It helps the application identify the disk. Click **Add** at the top-right corner of the Virtual Disks pane if the application requires extra virtual disks to be specified. Repeat for each extra disk. 

Procedure 92. Create Guest Server Using PMAC Application

Step	Procedure	Results
6. ☐	**PMAC GUI**: Add virtual NICs	By default, the control network is configured, and is required for PMAC to install and upgrade the guest. If this is removed, one is added during the guest creation. To add additional NICs, repeat this step for each virtual NIC. Click **Add** at the top-right corner of the Virtual NICs pane. **Host Bridge**: Select the desired bridge that has been previously configured on the TVOE. **Guest Dev Name**: This is the alias used inside of the TPD instance running on the guest. It helps the application identify the network.  Repeat as needed for each vNIC.

Procedure 92. Create Guest Server Using PMAC Application

Step	Procedure	Results
7. ☐	**PMAC GUI**: Create the guest	Verify the guest configuration and click **Create**. If there was an immediate problem, an alert box displays to report the error, and the values can be corrected and retried. Otherwise, the Info box confirms the creation of a Background Task. 
8. ☐	**PMAC 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 changes to green and the Progress column indicates 100%.

11.2 Delete Guest Server Using PMAC Application

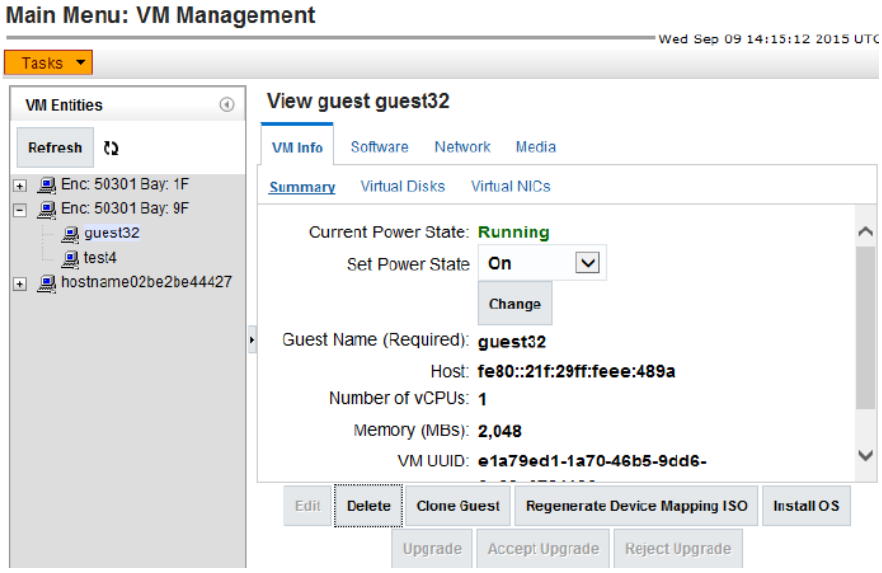
This procedure deletes a virtualized guest server on a TVOE host using the PMAC web GUI.

Prerequisite: Enclosure containing the TVOE host blade server to host the guest has been configured using 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.

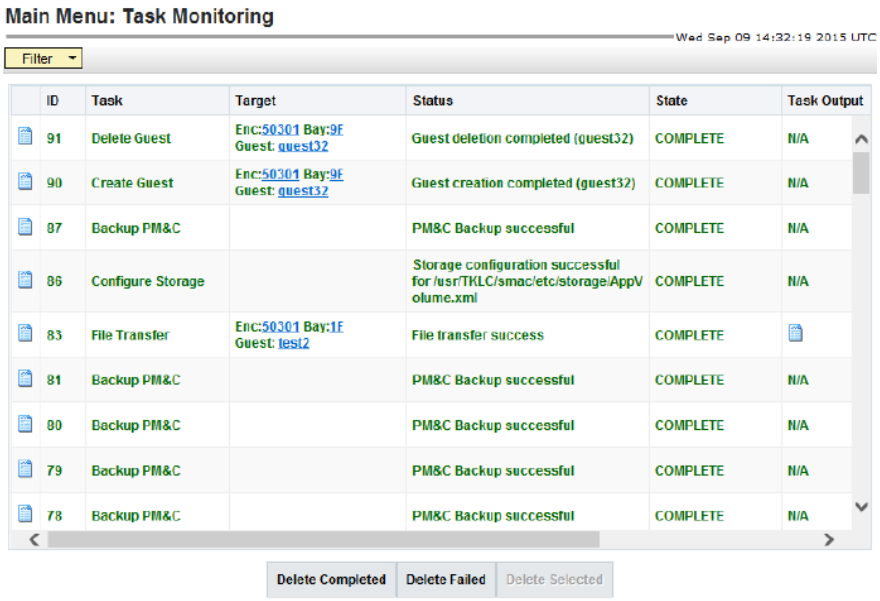
Note: All data belonging to the guest server is lost in the execution of this procedure.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 93. Delete Guest Server Using PMAC Application

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open a web browser and type: `https://<pmac_management_network_IP>` Login as **guiadmin** user.
2. ☐	**PMAC GUI**	Navigate to **Main Menu > VM Management**.
3. ☐	**PMAC GUI**	1. Click **+** to expand the TVOE host that contains the guest server to delete. 2. Select the guest to delete. The guest details display on the right.  3. Click **Delete**. 4. Click **OK** to confirm. Take a moment to double-check that the guest name is correct. There is no further confirmation and the delete is final.

Procedure 93. Delete Guest Server Using PMAC Application

Step	Procedure	Results
4. ☐	**PMAC GUI**: Monitor guest deletion	Navigate to **Main Menu > Task Monitoring** to monitoring the **VirtAction: Delete** background task.  When the task is complete, the text changes to green and the Progress column indicates 100%.

11.3 Create Guest Server from Guest Archive Using PMAC Application

This procedure creates virtualized guest server from a guest archive image on a TVOE host, using the PMAC web GUI.

Prerequisites:

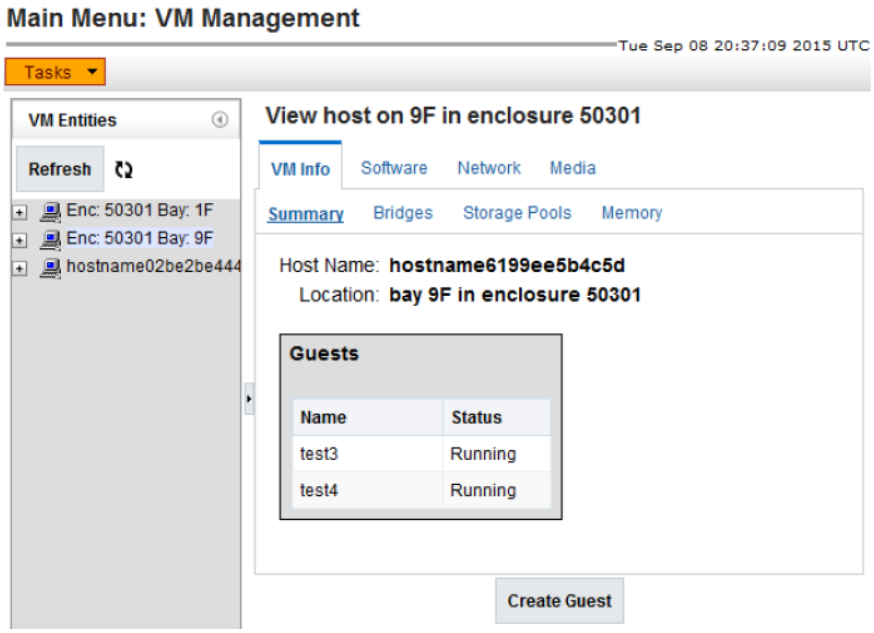
- Enclosure containing the TVOE host blade server to host the guest has been configured using 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- The TVOE host has been installed using 9.9 IPM Servers Using PMAC Application.
- The ISO image providing the guest archive image and profile has been provisioned using 9.8 Add ISO Images to the PMAC Image Repository.

Notes:

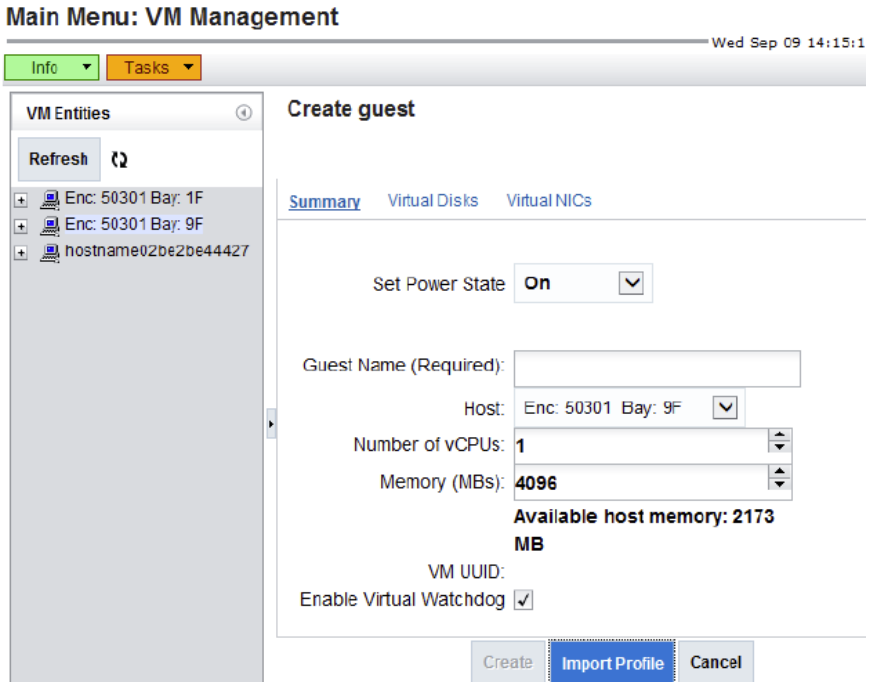
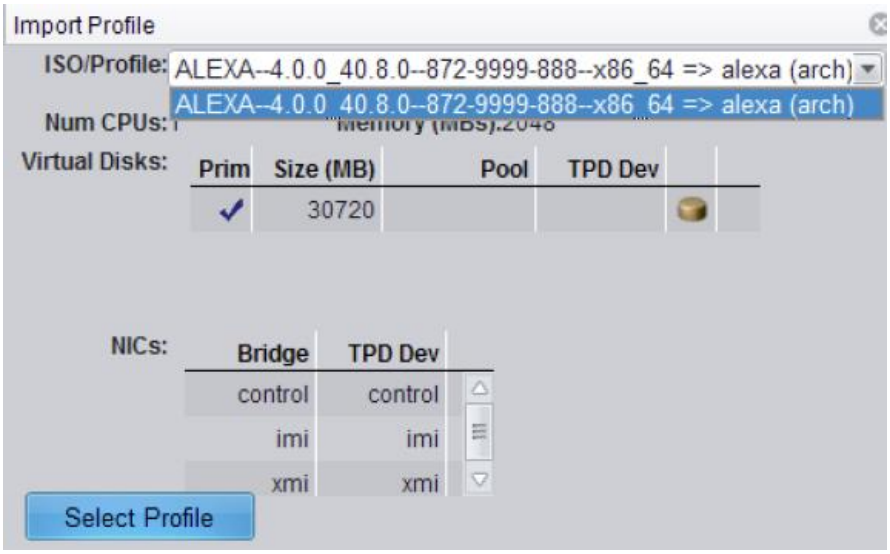
- PMAC does not prevent over-subscription of memory or CPU resources.
- The guest archive profiles might not contain values for all required fields.
- The values provided by the guest archive profile can be overridden before the guest is created.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

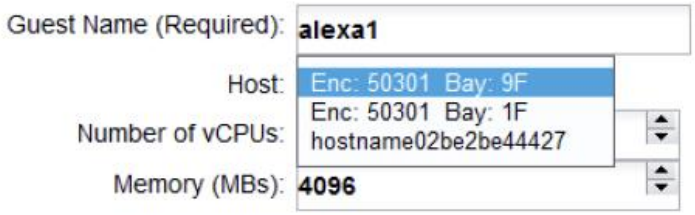
Procedure 94. Create Guest Server from Guest Archive Using PMAC Application

Step	Procedure	Results
1. ☐	**PMAC GUI**: Login	Open a web browser and type: `https://<pmac_management_network_IP>` Login as **guiadmin** user.
2. ☐	**PMAC GUI**	Navigate to **Main Menu > VM Management**.
3. ☐	**PMAC GUI**	Click **Create Guest**. 

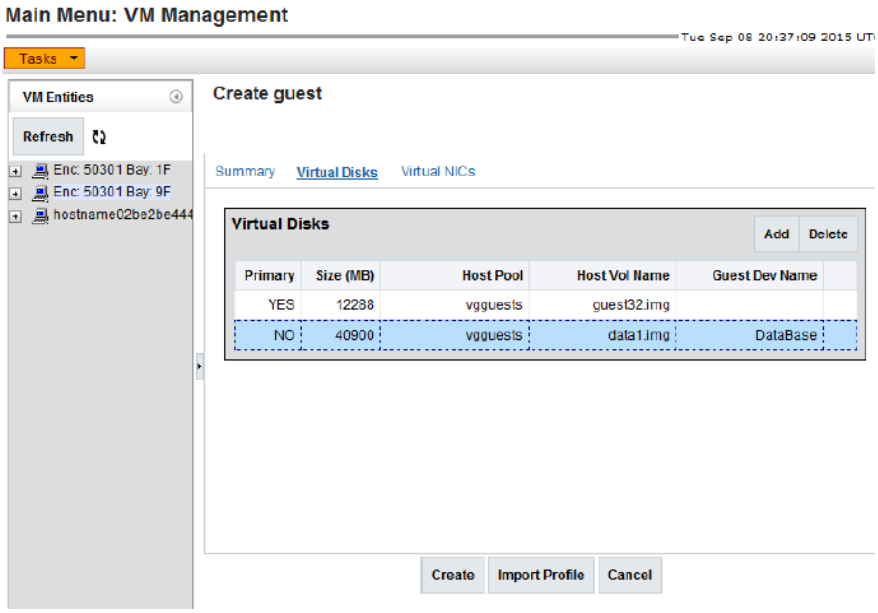
Procedure 94. Create Guest Server from Guest Archive Using PMAC Application

Step	Procedure	Results
4. ☐	**PMAC GUI**	Click **Import Profile**. 
5. ☐	**PMAC GUI**	Select the desired profile and click **Select Profile**.  There may be multiple profiles on an ISO. Verify the details.

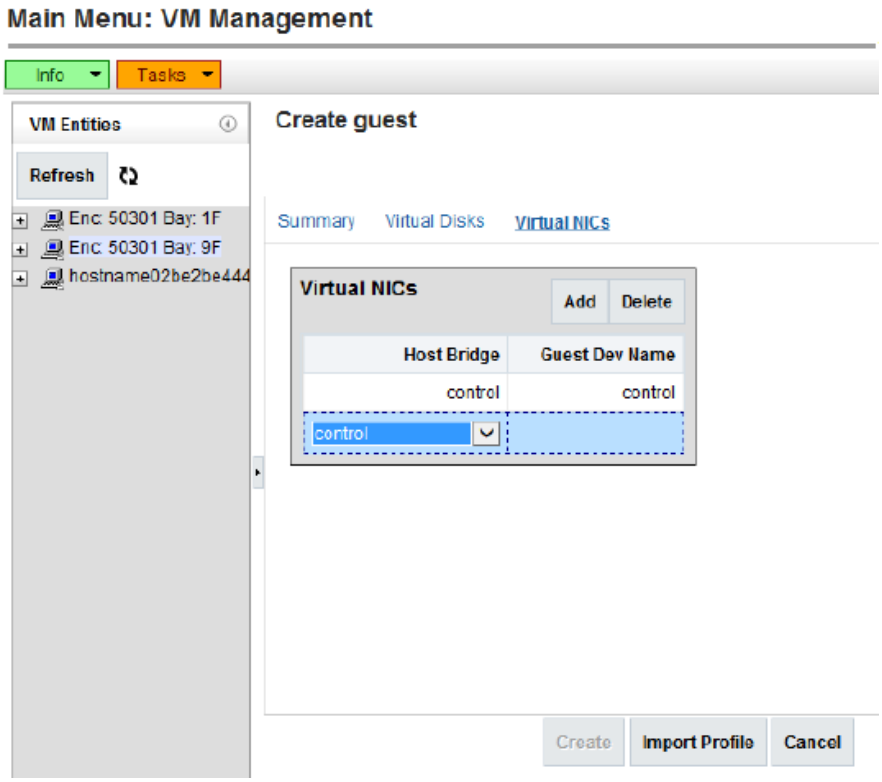
Procedure 94. Create Guest Server from Guest Archive Using PMAC Application

Step	Procedure	Results
6. ☐	**PMAC GUI**	1. The profile fills in the default name. If a different name is desired, type a **Name** that is something unique to the TVOE host. The name can be identical to a guest on a different host. 2. From the **Host** options, select the TVOE host on which to create the guest.  3. From the **Set Power State** options, select the initial power state for the guest. In this context, **Shutdown** and **Destroy** both behave the same. The guest is not powered on upon creation. 4. Edit the **vCPU** count and **Memory** size. 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. PMAC does not prevent over-subscription of these resources. 5. If this Guest is being created on a version of TVOE having support for virtual guest watchdogs, the **Enable Virtual Watchdog** checkbox displays. Set this checkbox according to whether or not watchdog support is desired for this guest.

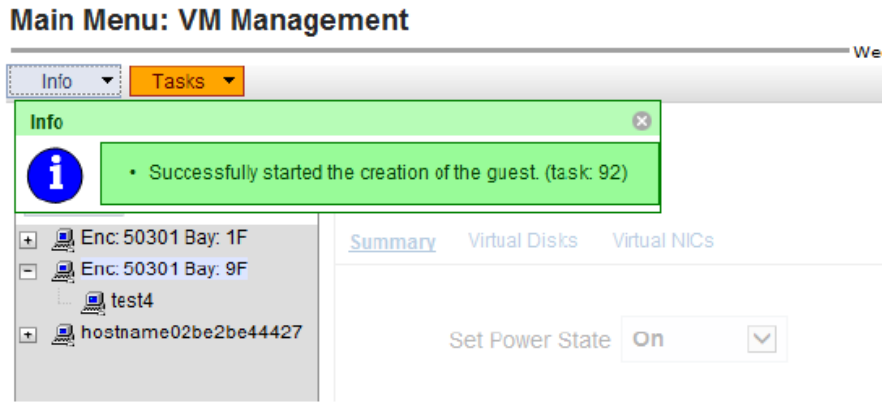
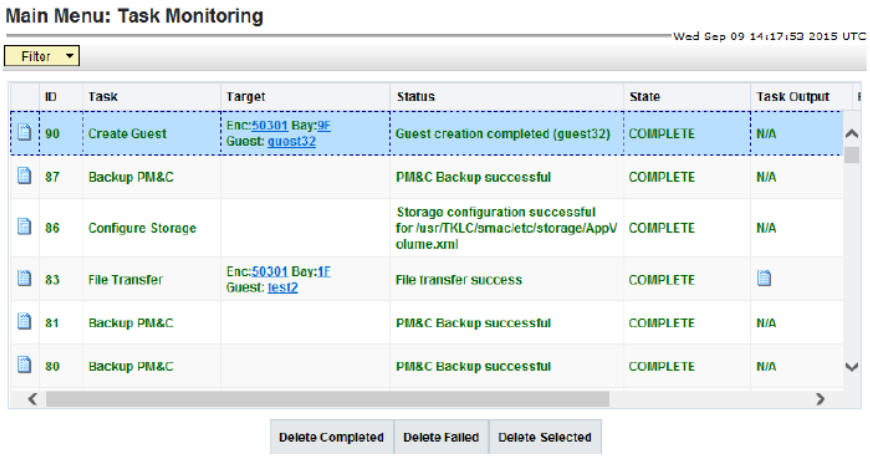
Procedure 94. Create Guest Server from Guest Archive Using PMAC Application

Step	Procedure	Results
7. ☐	**PMAC GUI**: Edit the primary virtual disk	A primary disk is specified by default. The disk image shows how the disk is populated with the archive's image. The only fields that should be modified are the Host Pool and Host Vol Name columns. **Size (MB)**: By default, a primary disk is specified with the minimum size supported by TPD. **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 does not allow you to continue until one is selected. When adding a new disk, the default vgguests storage pool is selected. **Host Vol Name**: For the primary disk, this is filled in automatically based on the guest name provided. It can be modified manually if needed. It must be unique among all disks on all guests hosted on the TVOE. **Guest Dev Name**: For the primary disk, this value is not set. For added disks, this is the alias used inside the TPD instance running on the guest. It helps the application identify the disk. Click **Add** at the top-right corner of the Virtual Disks pane if the application requires extra virtual disks to be specified. Repeat for each extra disk. 

Procedure 94. Create Guest Server from Guest Archive Using PMAC Application

Step	Procedure	Results
8. ☐	**PMAC GUI**: Edit virtual NICs	By default, the control network is configured, and is required for PMAC to install and upgrade the guest. If this is removed, one is added during the guest creation. To add additional NICs, repeat this step for each virtual NIC. Click **Add** at the top-right corner of the Virtual NICs pane. **Host Bridge**: Select the desired bridge that has been previously configured on the TVOE. **Guest Dev Name**: This is the alias used inside of the TPD instance running on the guest. It helps the application identify the network.  Repeat as needed for each vNIC.

Procedure 94. Create Guest Server from Guest Archive Using PMAC Application

Step	Procedure	Results
9. ☐	**PMAC GUI**: Create the guest	Verify the guest configuration and click **Create**. If there was an immediate problem, an alert box displays to report the error, and the values can be corrected and retried. Otherwise, the Info box confirms the creation of a Background Task. 
10. ☐	**PMAC 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 changes to green and the Progress column indicates 100%.

12. General TPD-Based Application Procedures

12.1 Back Up TVOE

This procedure backs up system files to use when restoring a failed system.

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

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 95. Back Up TVOE

Step	Procedure	Results
1. ☐	**TVOE Host**: Login	Login as the **platcfg** user.

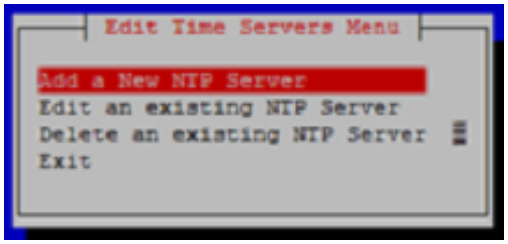
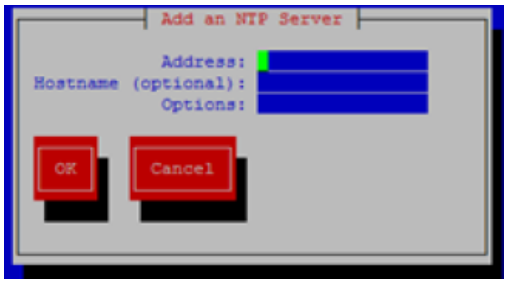
2. ☐	**TVOE Host**: Back up files	1. Navigate to **Maintenance > Backup and Restore > Backup Platform**.
		Note: If this operation is attempted on a system without media (for example, the CD/DVD), a **No disk device available. This is normal on systems without a CD ROM device** message displays. Ignore the message and press any key to continue.
		2. Click **Build ISO file only**.
		The **Creating ISO Image. . .** message may display.
		After the ISO is created, platcfg returns to the Backup TekServer Menu screen. The ISO has now been created and is located in the **/var/TKLC/bkp/** directory. An example filename of a backup file created is **hostname1307466752-plat-app-201104171705.iso**.
		3. Click **Exit** on each menu until platcfg exits.
		The SSH connection to the TVOE server terminates.
		4. Log into the customer server and copy the 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>:/var/TKLC/bkp/* /path/to/destination/`
		When prompted, enter the tvoexfer user password and press **Enter**.
		`# 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 Appendix A Using WinSCP to copy the backup image to the customer system.

12.2 Configure NTP on TPD-Based Application

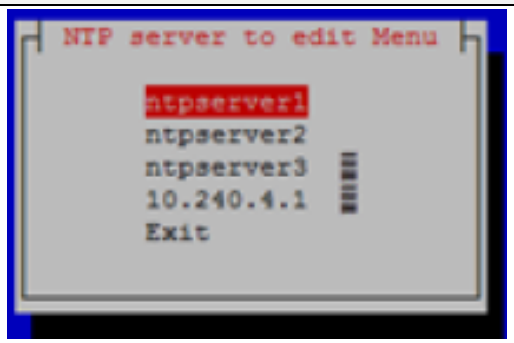
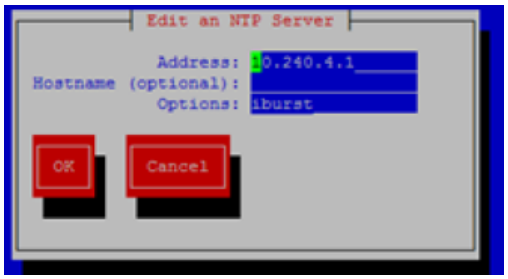
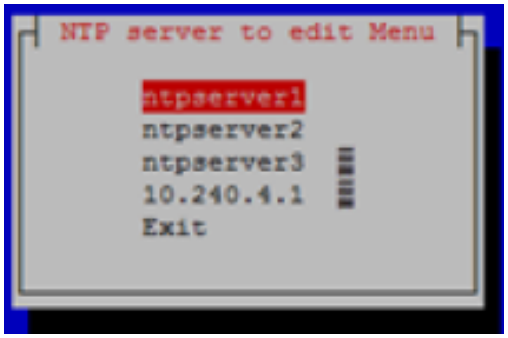
This procedure configures NTP servers for a server based on TPD.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 96. Configure NTP on TPD-Based Application

Step	Results
1. ☐	Login as the **platcfg** user on the server.
2. ☐	Navigate to **Network Configuration > NTP**. 
3. ☐	Click **Edit**. 
4. ☐	Add, edit, and delete NTP servers as needed. Remember that three (3) NTP sources are required. **Add an NTP server** 1. Click **Add a New NTP Server**. 2. Type the **Address**, **Hostname (optional)**, **Options**. 3. Click **OK**.  **Edit an NTP server** 1. Click **Edit an Existing NTP Server**. 2. Select the NTP server.

Procedure 96. Configure NTP on TPD-Based Application

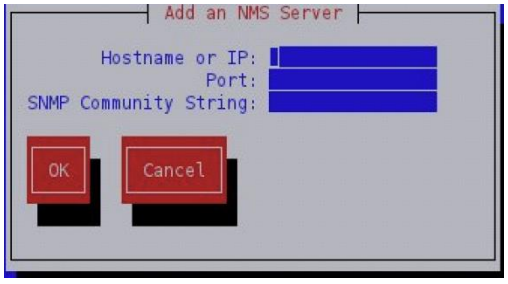
Step	Results
	 3. Edit the **Address**, **Hostname (optional)**, **Options**. 4. Click **OK**.  **Delete an NTP server** 1. Click **Delete an existing NTP Server**. 2. Select the NTP server and press **Enter**.  3. Click **Yes** to confirm deleting the NTP server.
5. ☐	Click **Exit** and **Yes** to restart the NTP server. 
6. ☐	Click **Exit** on each menu until platcfg exits.

12.3 Add SNMP Trap Destination on TPD-Based Application

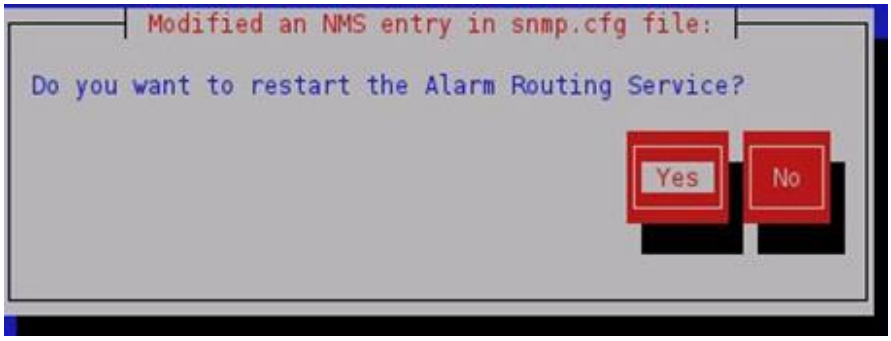
This procedure adds an SNMP trap destination to a server based on TPD. All alarm information is then sent to the NMS located at the destination.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 97. Add SNMP Trap Destination on TPD-Based Application

Step	Results
1. ☐	Login as the **platcfg** user on the server.
2. ☐	Navigate to **Network Configuration > SNMP Configuration > NMS Configuration**. 
3. ☐	Click **Edit**.
4. ☐	Click **Add a New NMS Server**.
5. ☐	Type the information related to SNMP trap destination and click **OK**. 

Procedure 97. Add SNMP Trap Destination on TPD-Based Application

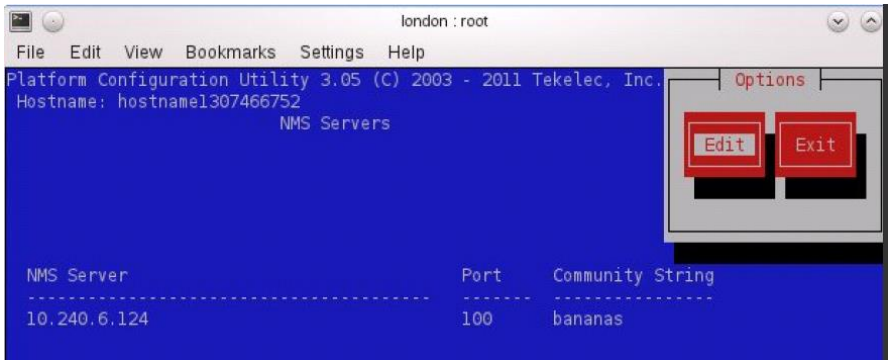
Step	Results
6. ☐	Click **Exit** and **Yes** to restart the service. 
7. ☐	Click **Exit** on each menu until platcfg exits.

12.4 Delete SNMP Trap Destination on TPD-Based Application

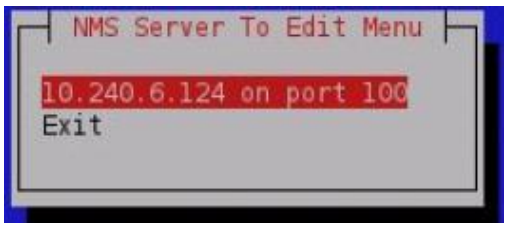
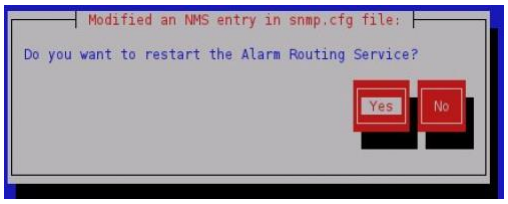
This procedure removes an SNMP trap destination on a server.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 98. Delete SNMP Trap Destination on TPD-Based Application

Step	Results
1. ☐	Login as the **platcfg** user on the server.
2. ☐	Navigate to **Network Configuration > SNMP Configuration > NMS Configuration**. 
3. ☐	Click **Edit**.
4. ☐	Click **Delete an Existing NMS Server**.

Procedure 98. Delete SNMP Trap Destination on TPD-Based Application

Step	Results
5. ☐	Select the NMS server and press **Enter**.  Click **Yes** to confirm deleting the NMS server.
6. ☐	Click **Exit** and **Yes** to restart the service. 
7. ☐	Click **Exit** on each menu until platcfg exits.

12.5 Install the NetBackup Client Application

This procedure installs or upgrades the NetBackup client software on an application server.

NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite supports disaster recovery at the customer site.

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.
- 12.11 Create LV and Filesystem for NetBackup Client Software.

  Note: For the PMAC application deployed with NetBackup Volume option `--netbackupVol` the guest virtual disk is created by deploy.
- Config file has been created if the version of NetBackup Client is not supported 12.13 Create NetBackup Client Config File.

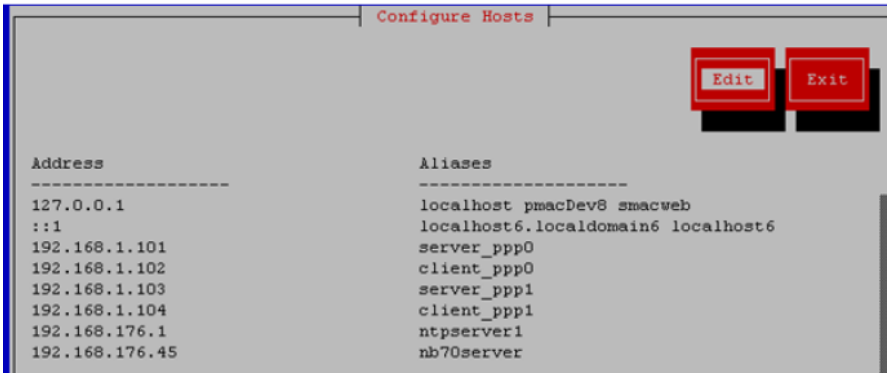
Notes:

- Platform 7.6 supports NetBackup 7.1, 7.5, and 7.6 clients. If the NetBackup Client being installed is not supported, contact My Oracle Support (MOS) for guidance on creating a config file that allows for installation of unknown NetBackup Clients. 12.13 Create NetBackup Client Config File can be used once the contents of the config are known.
- Failure to install the NetBackup Client properly (that is, by neglecting to execute this procedure) may result in the NetBackup Client being deleted during an Oracle software upgrade.

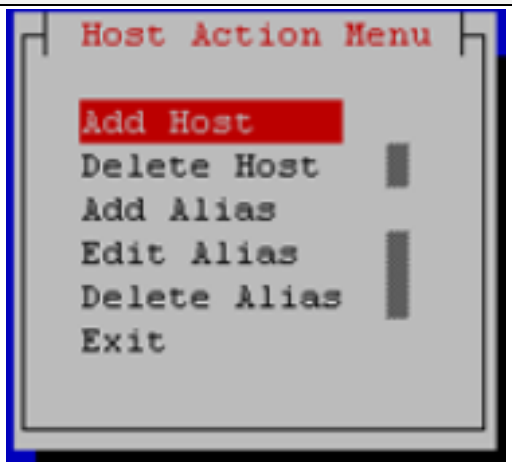
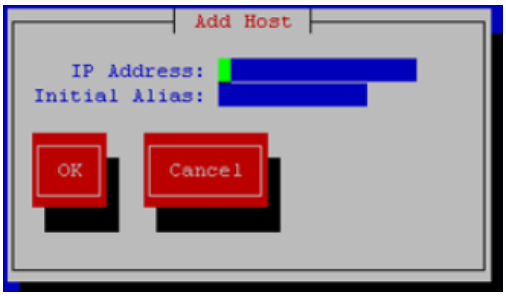
If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 99. Install the NetBackup Client Application

Step	Procedure	Results
1. ☐	Select and perform a NetBackup client installation path	There are two methods to install NetBackup Client. • If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools, then use Netbackup Client Install with nbAutoInstall. This is not common and if the answer is not known then do not use Netbackup Client Install with nbAutoInstall. • If you do not use Netbackup Client Install with nbAutoInstall, use NetBackup Client Install/Upgrade with platcfg.

2. ☐	**Application Console**: Modify the hosts file	1. Use platform configuration utility (platcfg) to modify the 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 is 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, the 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.
		2. Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.
		`$ sudo su - platcfg`
		a. Navigate to **Network Configuration > Modify Hosts File**.
		b. Click **Edit**.
		 
		c. Click **Add Host**.

Procedure 99. Install the NetBackup Client Application

Step	Procedure	Results
		 d. Type information and click **OK**.  e. Click **Exit** on each menu until platcfg exits.

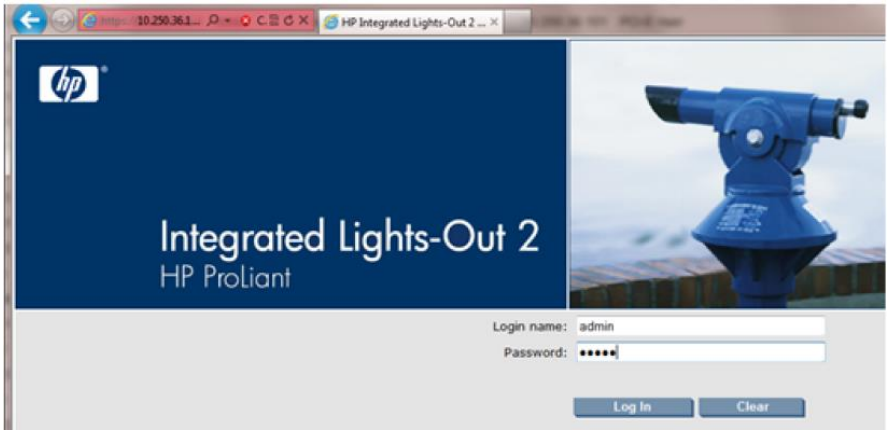
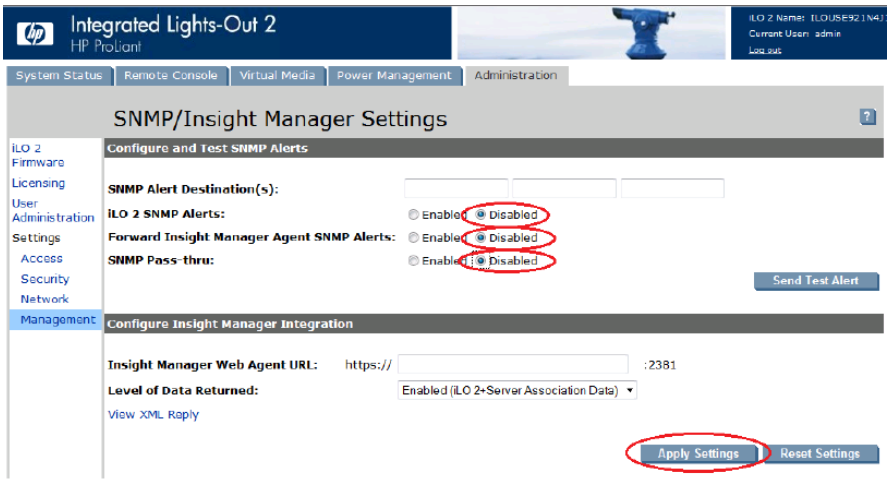
3. ☐	**Application Console**: Create to server	Create a link for the application provided NetBackup client notify scripts to path on application server where NetBackup expects to find them.
		Note: Link notify scripts from appropriate path on application server for given application.
		`$ sudo mkdir -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`

12.6 Change SNMP Configuration Settings for iLO2

This procedure changes the default SNMP settings for HP ProLiant iLO2 devices. Perform this procedure for every HP ProLiant G1/G5/G6 blade and rack mount server on the network

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 100.Change SNMP Configuration Settings for iLO2

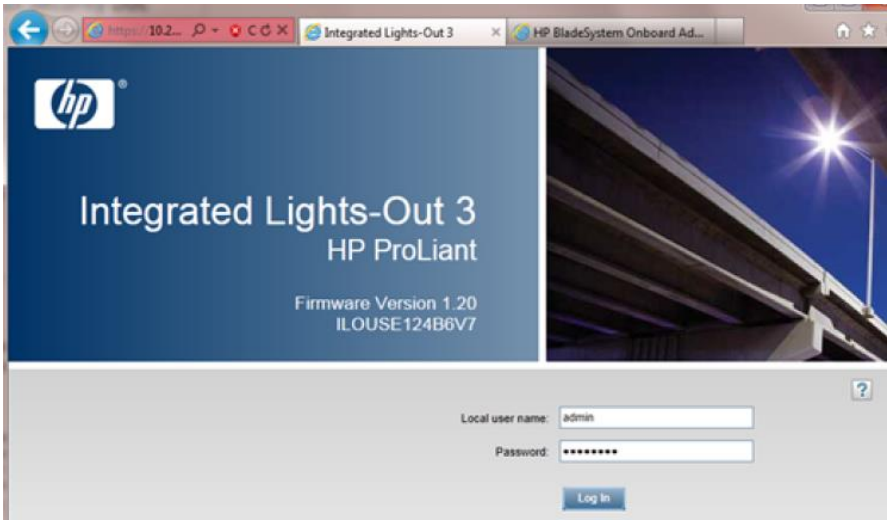
Step	Procedure	Results
1. ☐	**iLO Web UI**: Login	1. Open a web browser and navigate to the IP address of the iLO device. 2. Click **Continue to this website (not recommended)** if prompted. 3. Login using an account with administrative level privileges. 
2. ☐	**iLO Web UI**: Management screen	1. Navigate to **Administration > Management**. 2. Select **Disabled** for each of the three SNMP alerts. 3. Click **Apply Settings**. 
3. ☐	**iLO Web UI**: Verify settings	Navigate away from the SNMP Management page and then back to make sure the settings are correct. Click **Log Out**.
4. ☐	Repeat	Repeat for each iLO2 device on the network.

12.7 Change SNMP Configuration Settings for iLO3 and iLO4

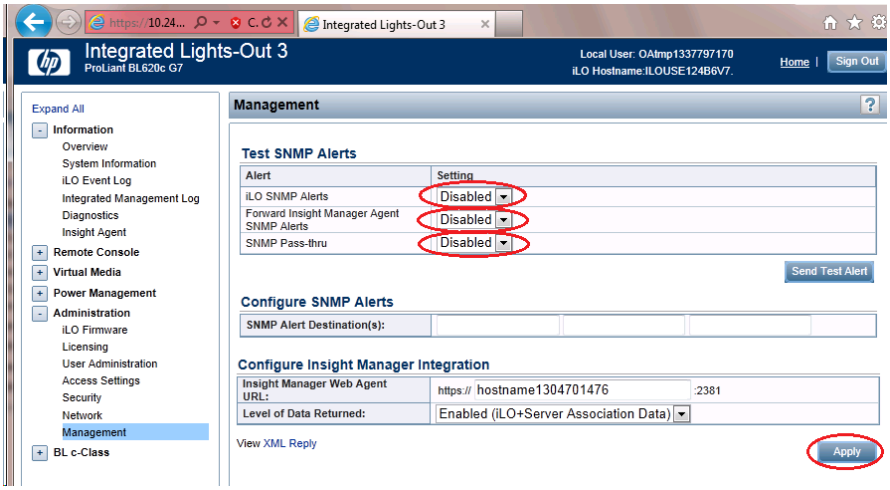
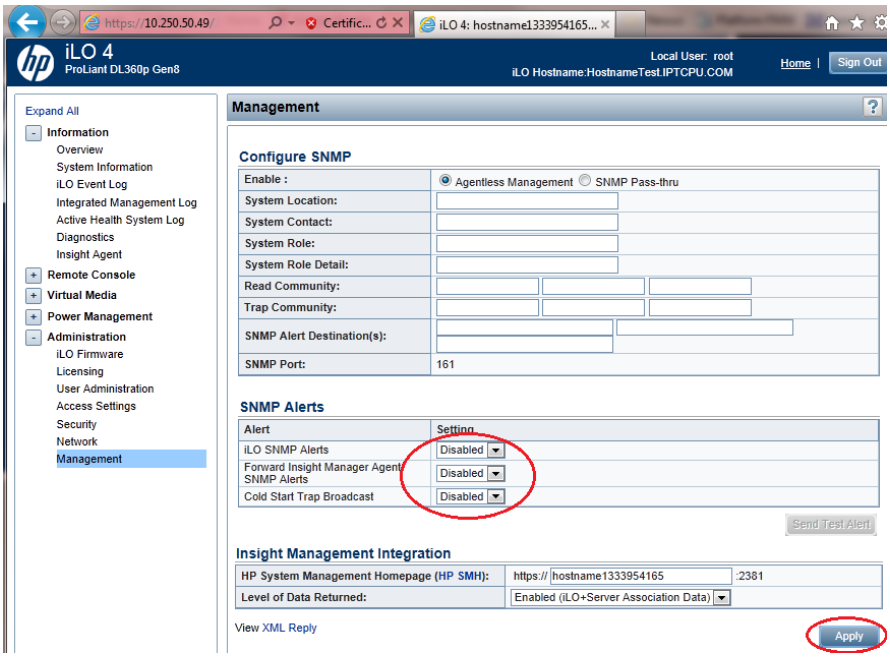
This procedure changes the default SNMP settings for HP ProLiant iLO3 devices. Perform this procedure for every HP ProLiant G7 blade and rack mount server on the network.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 101.Change SNMP Configuration Settings for iLO3 and iLO4

Step	Procedure	Results
1. ☐	**iLO Web UI**: Login	1. Open a web browser and navigate to the IP address of the iLO device. 2. Click **Continue to this website (not recommended)** if prompted. 3. Login using an account with administrative level privileges. 

Procedure 101. Change SNMP Configuration Settings for iLO3 and iLO4

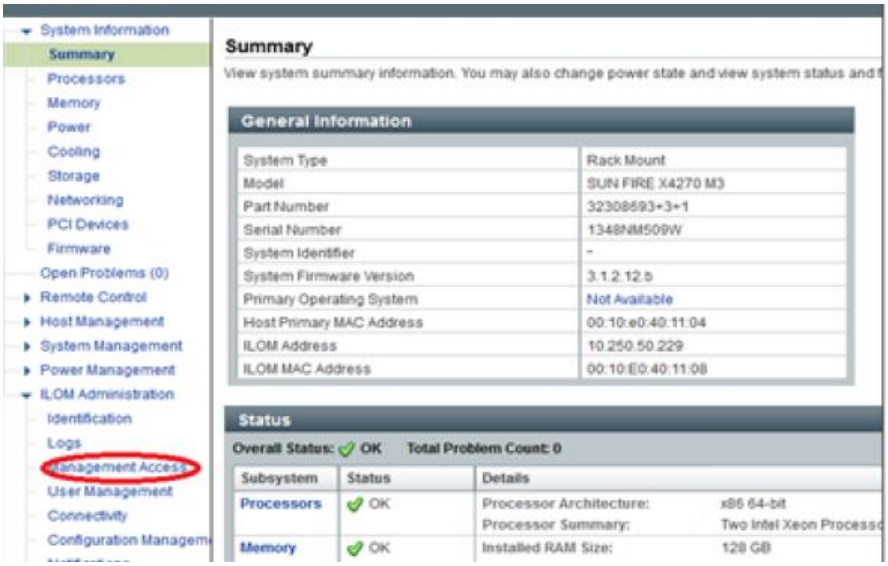
Step	Procedure	Results
2. ☐	**iLO Web UI**: Management screen	1. Navigate to **Administration > Management**. 2. Select **Disabled** for each of the three SNMP alerts. 3. Click **Apply**. iLO3 Web UI:  iLO4 Web UI: 
3. ☐	**iLO Web UI**: Verify settings	Navigate away from the SNMP Management page and then back to make sure the settings are correct. Click **Sign Out**.
4. ☐	Repeat	Repeat for each iLO3 and iLO4 device on the network.

12.8 Change SNMP Configuration Settings for iLOM

This procedure changes the default SNMP settings for ILOM devices. Perform this procedure for every ILOM device on the network.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 102.Change SNMP Configuration Settings for iLOM

Step	Procedure	Results
1. ☐	**ILOM Web UI**: Login	1. Open a web browser and navigate to the IP address of the ILOM device. 2. Click **Continue to this website (not recommended)** if prompted. 3. Login using an account with administrative level privileges. 
2. ☐	**ILOM Web UI**: Management Access screen	1. Navigate to **System Information > Summary**. 2. Click **Management Access**.  3. Click the SNMP tab. 4. Unmark the **Enabled** checkbox. 5. Click **Save**.

12.9 Install NetBackup Client with nbAutoInstall

This procedure enables TPD to detect automatically when a NetBackup client is installed and completes TPD-related tasks 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.

Notes:

- If the customer does not have a way to push and install the NetBackup client, then use 12.10 Install/Upgrade NetBackup Client with platcfg.
- This procedure must be 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 12.11 Create LV and Filesystem for NetBackup Client Software.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 103.Install NetBackup Client with nbAutoInstall

Step	Results
1. ☐	Complete workaround to prepare the server, if workaround is required as directed by My Oracle Support (MOS).
2. ☐	Enable nbAutoInstall. `$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable` The server periodically checks if a new version of the NetBackup client has been installed and performs necessary TPD configuration accordingly. At any time, you can now push and install a new version of the NetBackup Client.

12.10 Install/Upgrade NetBackup Client with platcfg

This procedure pushes and installs 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 12.11 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.

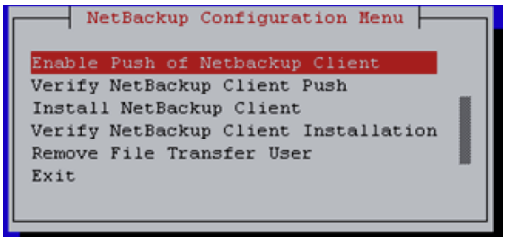
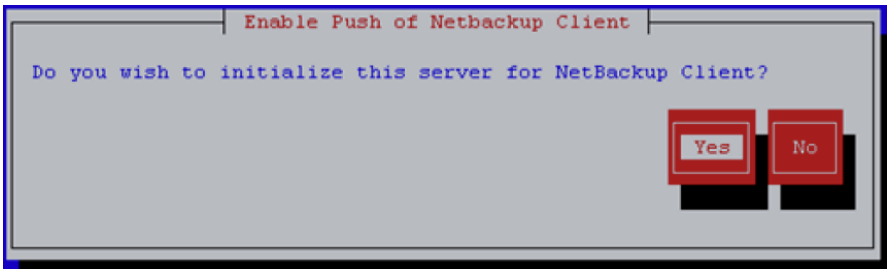
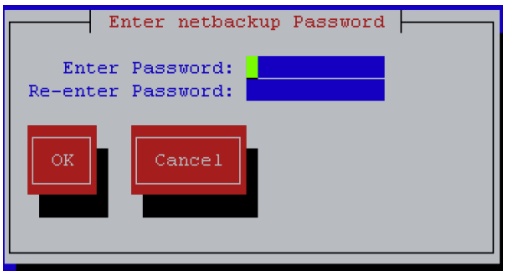
If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 104.Install/Upgrade NetBackup Client with platcfg

Step	Procedure	Results
1. ☐	**Application Server iLO**: Login and start the integrated remote console	1. Log into iLO with Internet Explorer using the password provided by the application. `http://<management_server_iLO_IP>` 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click **Yes** if the Security Alert displays.

2. ☐	**TVOE Application Server iLO**: Login	If the application is a guest on a TVOE host, login with application **admusr** credentials.
		Note: On a TVOE host, if you open the virsh console, for example, `$ 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, run `ps -ef |grep virsh`, and 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 the 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:`

Procedure 104.Install/Upgrade NetBackup Client with platcfg

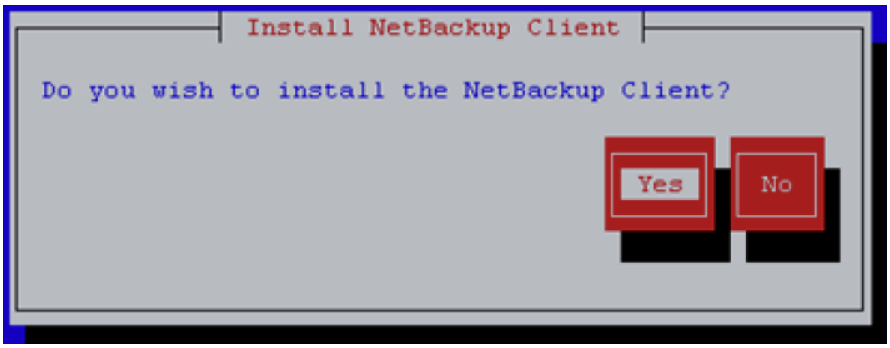
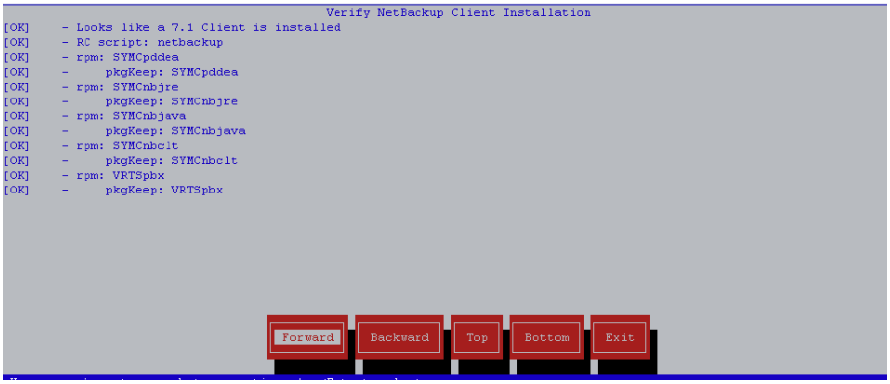
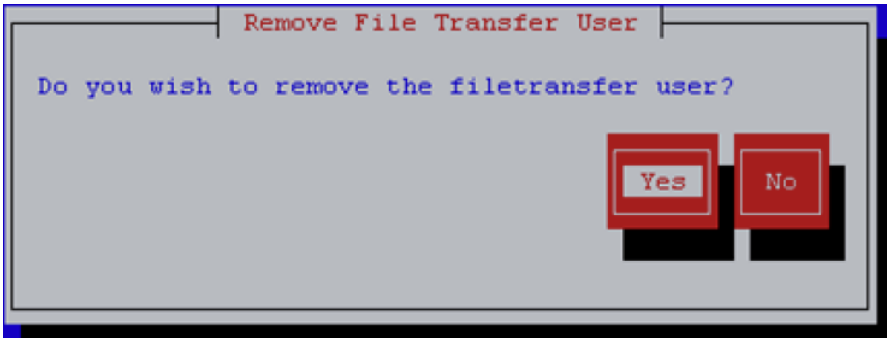
Step	Procedure	Results
3. ☐	**Application Console**: Configure NetBackup client on application server	`$ sudo su - platcfg` 1. Navigate to **NetBackup Configuration**. 2. Click **Enable Push of NetBackup Client**.  3. Click **Yes** to initialize the server and enable the Netbackup client software push.  4. Type the NetBackup password and click **OK**.  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. 5. Navigate to **NetBackup Configuration** > **Verify NetBackup Client Push**. 6. Verify the list of entries indicate **[OK]** for the NetBackup client software environment and click **Exit**.

Procedure 104.Install/Upgrade NetBackup Client with platcfg

Step	Procedure	Results

4. ☐	**NetBackup Server**: Push appropriate NetBackup client software to application server	***Notes***:
		• 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. These steps are required on the NetBackup server to push the NetBackup client software to the application server.
		• These steps assume the NetBackup server is executing in a Linux environment.
		• The backup server is supported by the customer, and the backup utility software provider. If this step, executed at the backup utility server, fails to execute successfully, STOP and contact My Oracle Support (MOS) for the backup and restore utility software provider being used at this site.
		• The NetBackup user on the client is a new user that requires the operator to change the password immediately. The operator should log into the client to change the initial password.
		1. Log into the NetBackup server with the password provided by customer.
		2. 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.`

Procedure 104.Install/Upgrade NetBackup Client with platcfg

Step	Procedure	Results
5. ☐	**Application Console**: Install NetBackup client software on the application server	1. Navigate to **NetBackup Configuration > Install NetBackup Client**. 2. Click **Yes** to install the NetBackup client software.  3. Click **Exit** to return to the NetBackup Configuration menu.
6. ☐	**Application Console**: Verify NetBackup client software installation on the application server	1. Navigate to **NetBackup Configuration** > **Verify NetBackup Client Installation**. 2. Verify list entries indicate **[OK]** for NetBackup client software installation.  3. Click **Exit** to return to the NetBackup Configuration menu.
7. ☐	**Application Console**: Disable NetBackup client software transfer to the application server	1. Navigate to **NetBackup Configuration** > **Remove File Transfer User**. 2. Click **Yes** to remove the NetBackup file transfer from the application server. 

Procedure 104.Install/Upgrade NetBackup Client with platcfg

Step	Procedure	Results

8. ☐	**Application Console**: Verify the server has been added to the **/user/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`

9. ☐	**Application Console iLO**	Exit platform configuration utility (platcfg).

12.11 Create LV and Filesystem for NetBackup Client Software

This procedure configures storage for the NetBackup client. This prevents a disk shortage in the **/usr/** filesystem.

Prerequisite: The volume group where the NetBackup logical volume resides 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 the volume group where the NetBackup LV should reside.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 105.Create LV and Filesystem for NetBackup Client Software

Step	Procedure	Results
1. ☐	**Server**: Login	Login as the **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=$VG" > /tmp/nb.lvm` This example uses the **$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 creates the LV, formats it with a filesystem, and mounts it under **/usr/openv/**. For example:
		`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.`

12.12 Migrate NetBackup Client to New Filesystem

This procedure migrates the installed files for NetBackup client from the **/usr/** filesystem to a filesystem dedicated to NetBackup client.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 106.Migrate NetBackup Client to New Filesystem

Step	Results
1. ☐	From the server, login as the **admusr** user.

2. ☐	Stop the NetBackup services.
	`$ sudo service netbackup stop`
	`$ sudo service vxpbx_exchanged stop`

3. ☐	Bind mount **/usr/openv** to a temporary mount point.
	`$ sudo mkdir /tmp/openv`
	`$ sudo mount --bind /usr/openv /tmp/openv`

4. ☐	Create the LV and filesystem using 12.11 Create LV and Filesystem for NetBackup Client Software.
5. ☐	Move all contents of **/tmp/openv** to **/usr/openv**. `$ sudo mv /tmp/openv/* /usr/openv`

6. ☐	Unmount bind mount and remove mount point.
	`$ sudo unmount /tmp/openv`
	`$ sudo rmdir /tmp/openv`

7. ☐	Start the NetBackup services.
	`$ sudo service vxpbx_exchanged start`
	`$ sudo service netbackup start`

12.13 Create NetBackup Client Config File

This procedure copies NetBackup Client config file into the appropriate location on the TPD based application server. This config file allows a customer to install previously unsupported versions of NetBackup Client by providing necessary information to TPD.

The contents of the config file are provided by My Oracle Support (MOS). Contact My Oracle Support (MOS) 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.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 107.Create NetBackup Client Config File

Step	Procedure	Results
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 **NB$ver.conf** conventions. Where **$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**

13. TVOE Host Procedures

13.1 Enable Virtual Guest Watchdogs as Appropriate for the Application

This procedure describes how to use the PMAC 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).

Prerequisite: One or more installations of TVOE have been upgraded to TVOE version 2.0.0_80.11.0 or later.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 108.Enable Virtual Guest Watchdogs as Appropriate for the Application

Step	Results
1. ☐	On the PMAC managing each newly upgraded TVOE server, navigate to **Main Menu > VM Management** on the PMAC GUI.
2. ☐	From the VM Entities list, locate the host just upgraded and click **+** to expand the list of VM guests.

Procedure 108.Enable Virtual Guest Watchdogs as Appropriate for the Application

Step	Results
3. ☐	Select each VM guest on the TVOE host where virtual watchdog support is needed: 1. Shut down the VM guest by setting its power state to **Shutdown** and clicking the adjacent **Change to**. Wait for the shutdown to complete as indicated by the Current Power State field of the GUI. 2. Click **Edit** to enter edit mode for this VM Guest. 3. Mark the **Enable Virtual Watchdog** checkbox. 4. Click **Save** and wait for the edit operation to finish. 5. Start the VM guest by setting the power state to **On** and clicking **Change to**. 6. When the VM Guest's power state indication shows **Running**, proceed to the next VM guest on this host.

13.2 Configure TVOE NetBackup Client

This procedure sets up and installs the NetBackup client on a TVOE host.

Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to back up the following file from the TVOE host.

/var/TKLC/bkp/*.iso

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 109.Configure TVOE NetBackup Client

Step	Procedure	Results
1. ☐	**TVOE Server**: Login	Login as the **admusr** user.

2. ☐	**TVOE Server**: Open firewall ports for NetBackup	`$ 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	`$ 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, execute 12.11 Create LV and Filesystem for NetBackup Client Software to create an LV and filesystem for the NetBackup client software.

Procedure 109. Configure TVOE NetBackup Client

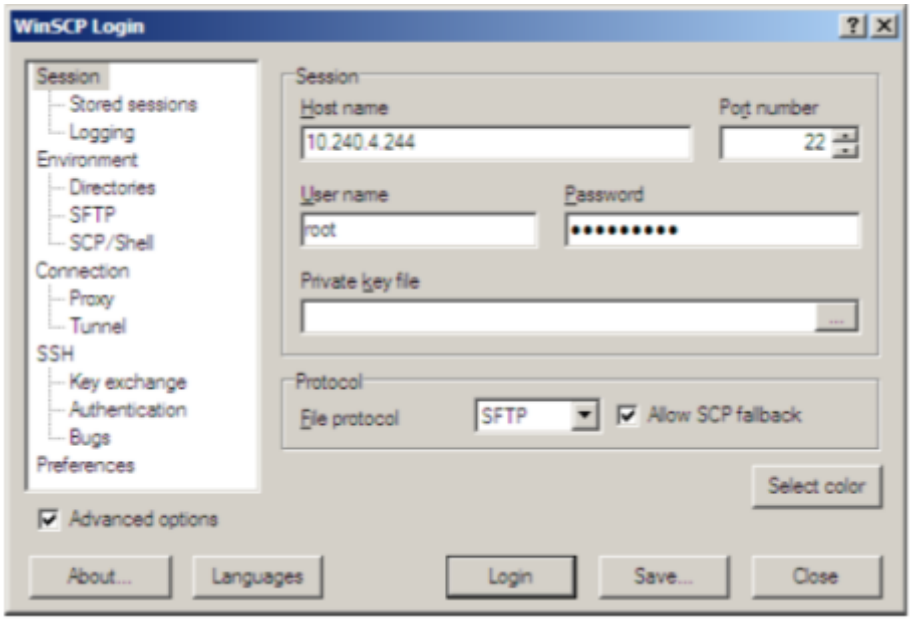
Step	Procedure	Results
5. ☐	**TVOE Server**: Install NetBackup client software	Execute 12.5 Install the NetBackup Client . ***Note***: Skip any steps relating to copying NetBackup **notify** scripts to /usr/openv/netbackup/bin. The TVOE NetBackup notify scripts are taken care of in the next step.
6. ☐	**TVOE Server**: Create soft links 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

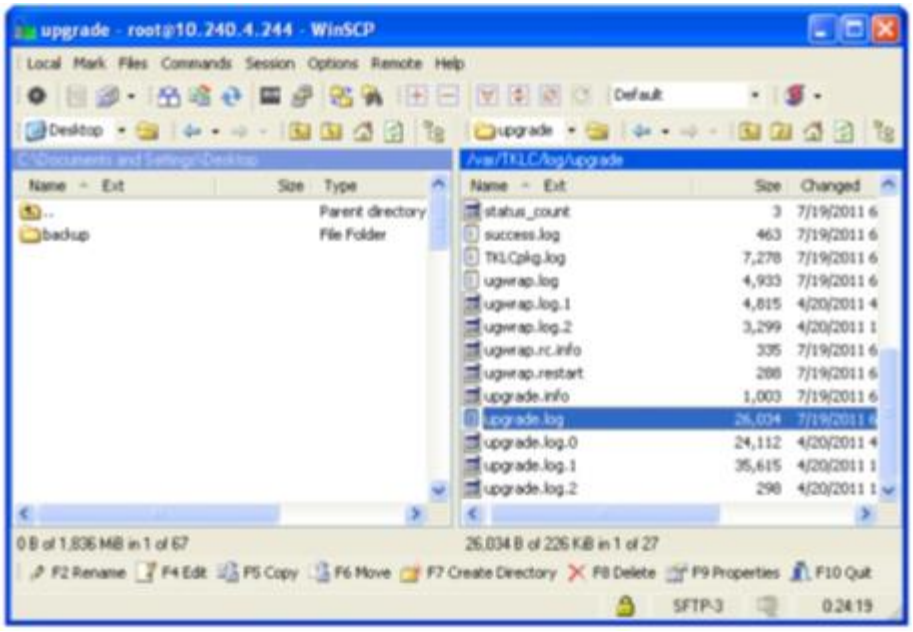
This procedure demonstrates how to copy a file from the management server to your PC desktop.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 110. Copy a File from the Management Server to the PC Desktop

Step	Procedure	Results
1. ☐	Download the WinSCP application	`http:winscp.net/eng/download.php`
2. ☐	Connect to the management server	After starting this application, navigate to Session and enter: **<management_server_IP>** into the **Host name** field, **root** into the **User name** field, and **<root_password>** into the **Password** field. Click **Login**. 

Procedure 110. Copy a File from the Management Server to the PC Desktop

Step	Procedure	Results
3. ☐	Copy the target file from the management server	On the left is your own desktop filesystem. Navigate within it to Desktop directory. On the right side is the management server file system. Within it, navigate into the location of the file you would like to copy to your desktop. Highlight the file in the management server file system by pressing the insert key, and then press **F5** to copy the file. 
4. ☐	Close the WinSCP application	Press **F10** and click **OK** to confirm terminating the session.

Appendix B. Install P2000 MSA USB Driver

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: 9.8 Add ISO Images to the PMAC Image Repository has been completed using the HP MISC firmware ISO image.

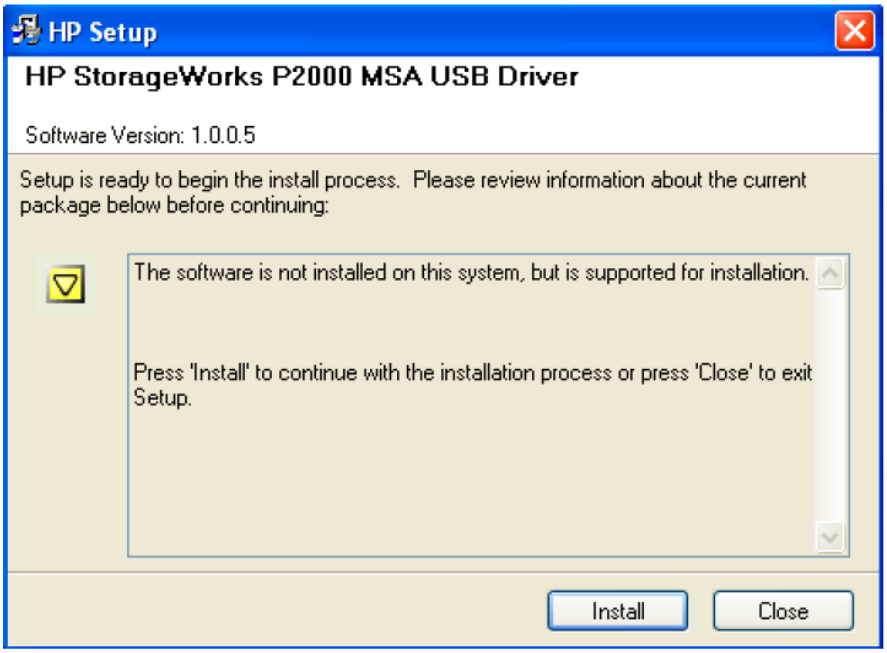
Note: If you are unable to detect the P2000 array after installing the USB driver, power cycle the P2000 array once.

Needed Material

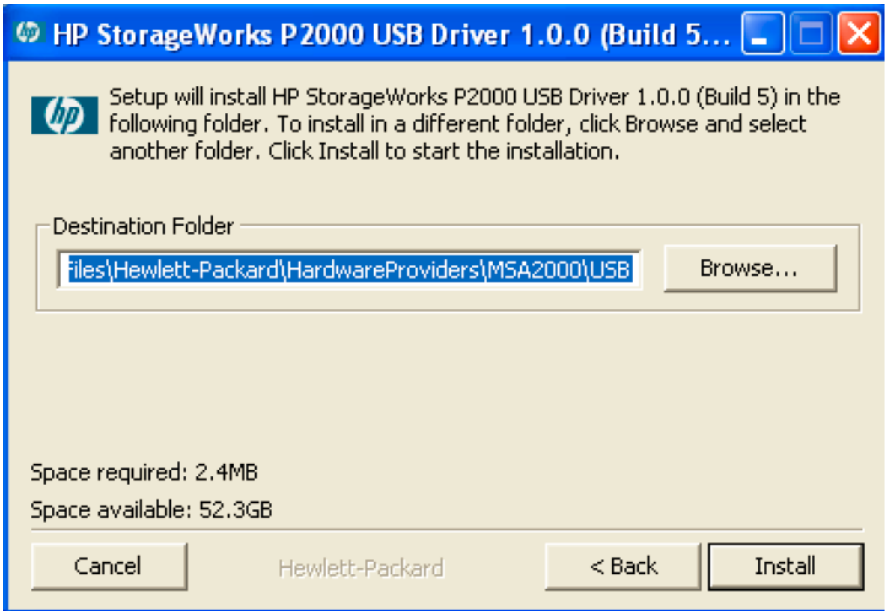
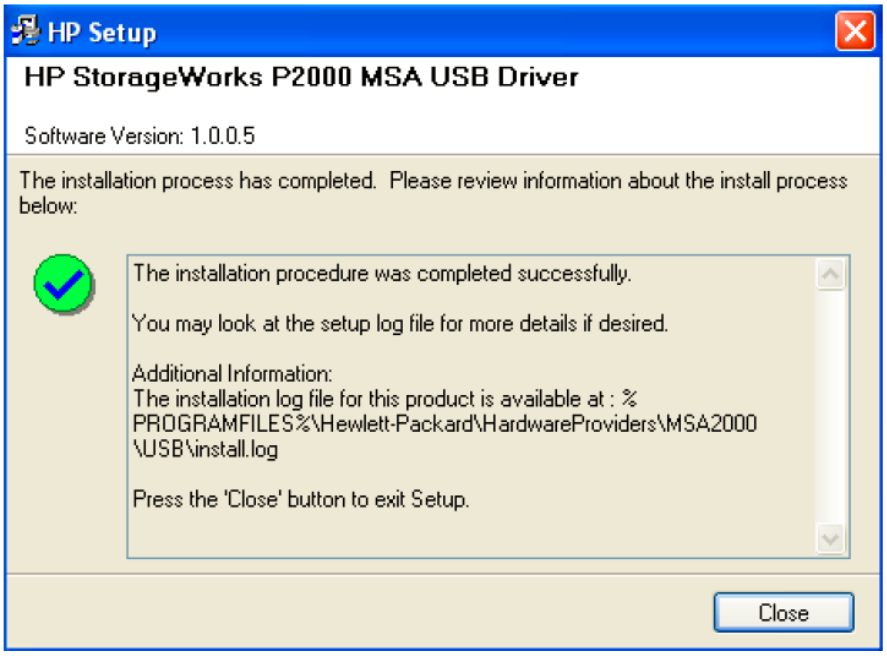
- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 111.Install P2000 MSA USB Driver

Step	Procedure	Results
1. ☐	**Management Server**: Obtain the USB driver executable	Copy the following from 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 need to refer to Appendix A Using WinSCP to copy the zip file to you PC. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 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 displays asking whether to run the executable, click **Run**. 
3. ☐	**Microsoft Windows Laptop**: Agree to installation	Click **Install**.  In the next window, click **I agree** to proceed with the installation.

Procedure 111.Install P2000 MSA USB Driver

Step	Procedure	Results
4. ☐	**Microsoft Windows Laptop**: Select installation directory	Click **Browse** to select the folder where to install.  Click **Install**.
5. ☐	**Microsoft Windows Laptop**: Verify installation	Click **Close**. 

Appendix C. Determine which Onboard Administrator is Active

This procedure determines which onboard administrator is active in an enclosure with two OAs.

Prerequisite: 7.2 Configure Initial OA Settings Using the Configuration Wizard

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 112. Determine which Onboard Administrator is Active

Step	Procedure	Results
1. ☐	**OA GUI**: Determine which OA is active	Open a web browser and navigate to the IP address of one of the administrators. `http://winscp.net/eng/download.php` If you see the following screen, you have navigated to a GUI of the standby OA as indicated by the red warning. In such a case, navigate to the other Onboard Administrator IP address.  If you navigate to the active Onboard Administrator GUI, the enclosure overview table is available in the left part of the login screen. 

Appendix D. PMAC Features Configuration

Appendix D.1 Overview

PMAC configuration manages identified software features. Features implemented by PMAC may be defined as editable in profiles used during PMAC 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 using the PMAC 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 a network interface basis.

Appendix D.2 Enabling Features

Enabling features may affect 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 block actions temporarily. 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 PMAC is restarted.

Appendix D.3 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. PMAC was designed to be flexible, so you are able to create roles and map them to interfaces as desired (that is, expanding a system may need to add new non-contiguous networks for control or management).

Appendix D.4 Features

Features are declared as user editable by profiles. The current PMAC 6.6 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 PMAC as an NTP server. By default, the port is blocked by the firewall.
- **PMAC.MANAGED** allows remote systems to access the SNMP service on PMAC.
- **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 PMAC interfaces.

To add features as editable, they must be declared in the profile during PMAC Initialization. If PMAC is in service, you must use the CLI to reset and re-initialize PMAC. To prevent profile changes from being lost during upgrade, you should avoid modifying profiles delivered with PMAC. Best practice is to copy the profile and edit this version.

Appendix D.5 GUI Usage

From the PMAC GUI, navigate to **Administration** > **PMAC Configuration** > **Feature Configuration**.

Click **Apply** to reconfigure the platform.

Appendix D.6 CLI Usage

The `pmacadm` CLI allows features to be modified also. This is the only interface to disable a feature administratively. 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 E. Access and Exit a Server Console Remotely Using iLO

This procedure accesses a server console remotely.

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

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Appendix E.1 Access a Server Console Remotely

Procedure 113. Access a Remote Server Console

Step	Procedure	Results
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 on the management server. Click **Continue to this website (not recommended)** if prompted. Log into the iLO as the **<iLO_admin_user>**.
2. ☐	If the iLO is an iLO2: Configure hot keys	The iLO GUI indicates 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 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. 5. Click **Save Hot Keys**. As a result, pressing **Ctrl-T** rather than **Ctrl-]** exits the console of a TVOE guest and returns to the console of the TVOE host. Pressing **Ctrl-v** disconnects the switch console session.

Procedure 113. Access a Remote Server Console

3. ☐	Open the remote console window	For HP servers: Click the Remote Console tab and select **Remote Console** to open the remote console in a new window. If prompted, click **Continue** on the Security Warning screen. For Oracle rack mount servers: Click **Launch** beside the Remote Console in the Actions frame. Click **Continue** if a Security Warning screen displays. Click **Run**.

4. ☐	Log into the console	In the Remote Console window, log into the console as the **admusr**.
		`Login as: admusr`
		`Password:`
		`Last login: Fri Oct 6 17:52:28 2017`
		`[admusr@tvo ~]$`

Appendix E.2 Exit a Guest Console Session on an iLO

This procedure exits a guest console session on an iLO.

Enter the control sequence for the iLO version.

If the main iLO GUI window indicates that this is an iLO2 (Integrated Lights-Out 2), press **Ctrl-T**. Otherwise, press **Ctrl-]**. This step corresponds to the configuration of iLO 2 Hot Keys performed in Appendix E.1, step 2.

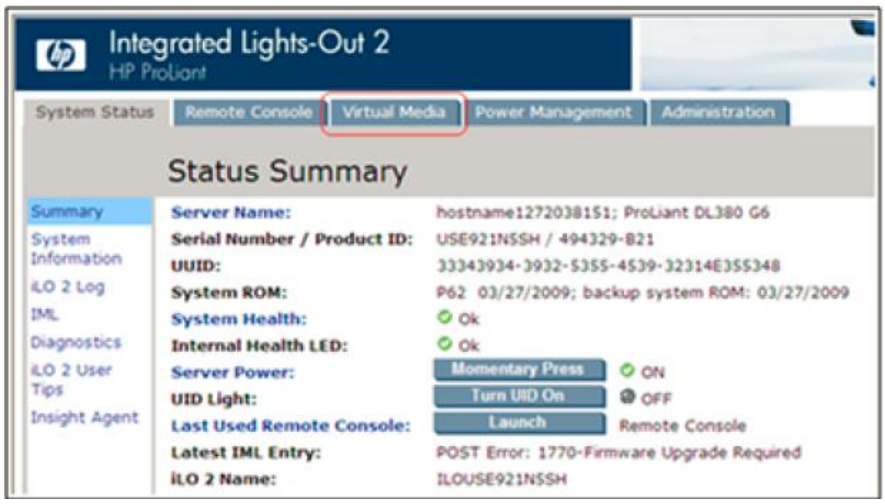
Appendix F. Attach an ISO Image to a Server Using iLO or iLOM

Appendix F.1 Attach an ISO Image to an HP Server Using iLO

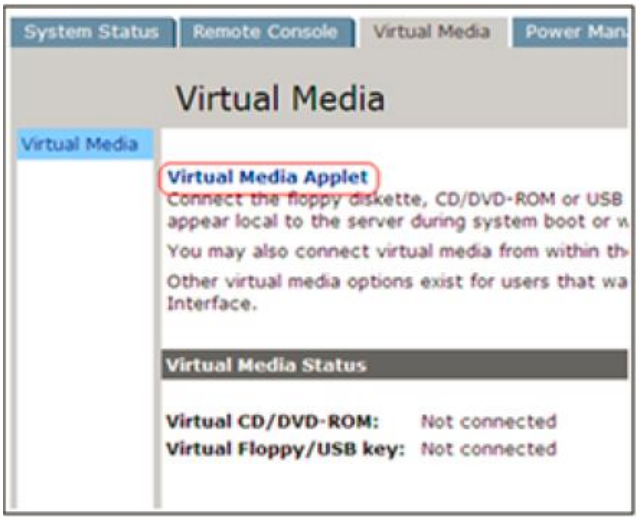
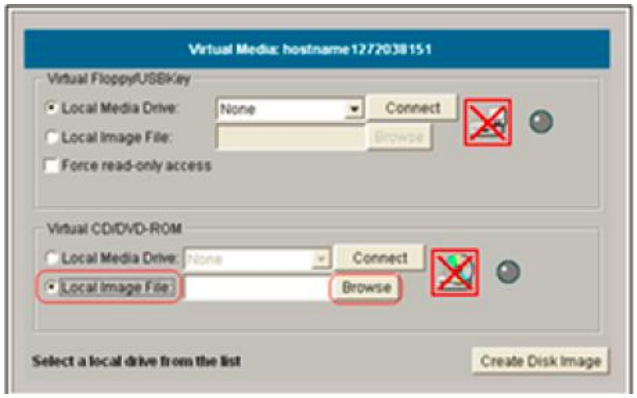
This procedure attaches an ISO image to an HP server.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

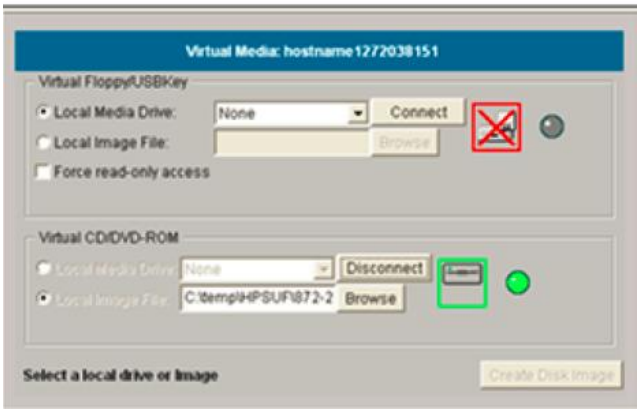
Procedure 114. Attach an ISO Image to an HP Server Using iLO

Step	Procedure	Results
1. ☐	**Local Workstation**: Access the ILO Web GUI and login	Log into the ProLiant Server using Internet Explorer: `https://<ilo_IP>/` Username: <ilo_admin_user> Password: <ilo_admin_password> 
2. ☐	**Local Workstation**: Determine iLO version	If the iLO GUI indicates **Integrated Lights-Out 2**, then continue to the next step. If the iLO GUI indicates **Integrated Lights-Out 3** or **Integrated Lights-Out 4**, then continue to step 8. .
3. ☐	**iLO2 Web GUI**: Access virtual media	Navigate to **Summary -> Virtual Media**. 

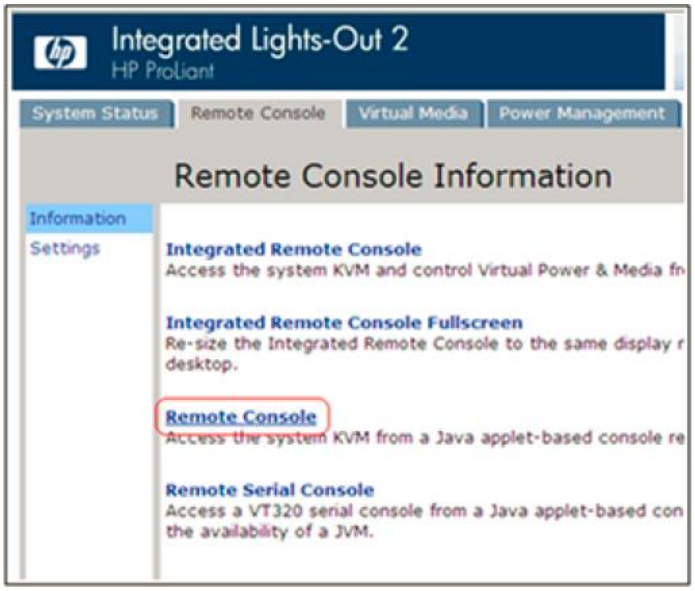
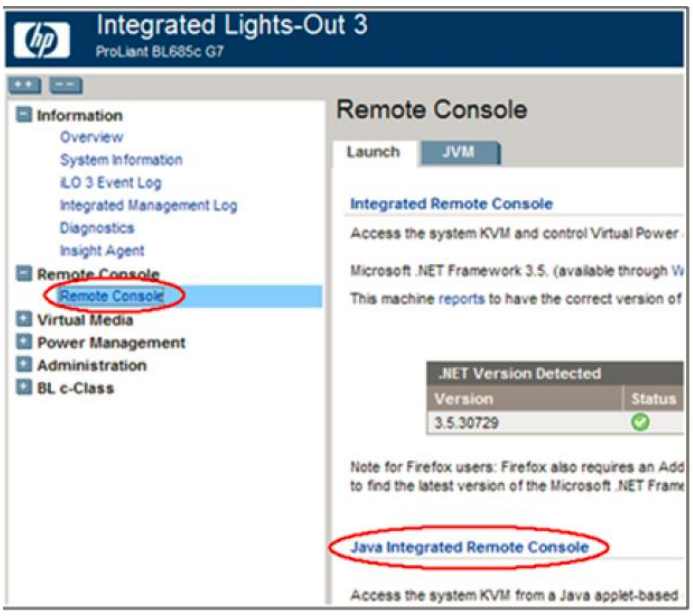
Procedure 114. Attach an ISO Image to an HP Server Using iLO

Step	Procedure	Results
4. ☐	**iLO2 Web GUI**: Open Virtual Media Applet	Click **Virtual Media Applet**.  Click **Yes** to acknowledge the security warning. If other screens display, acknowledge them as well.
5. ☐	**iLO 2 VM Applet**: Select ISO file	In the Virtual CD/DVD-ROM panel, select the **Local Image File** option and click **Browse**. Navigate to the ISO image file specified by the procedure that referenced this appendix.  Select the ISO image file and click **Open**.

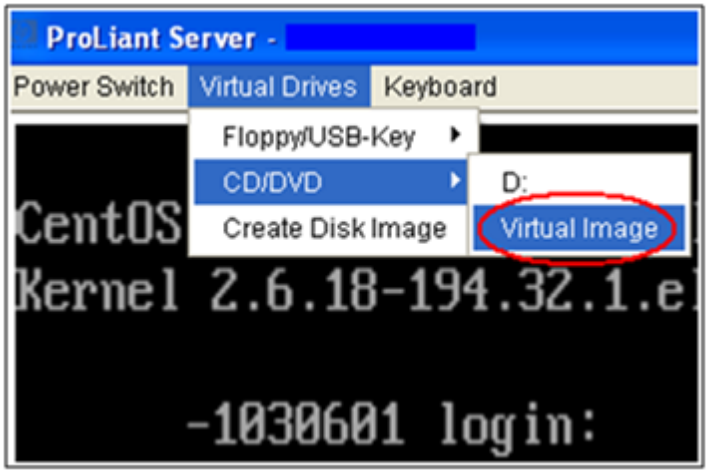
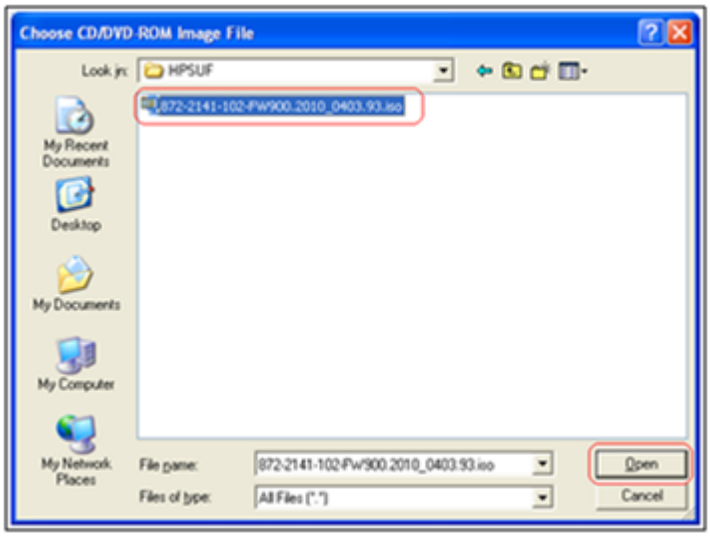
Procedure 114. Attach an ISO Image to an HP Server Using iLO

Step	Procedure	Results
6. ☐	**iLO 2 VM Applet**: Create a virtual drive connection	Click **Connect** to create a virtual DVD-ROM connection to the ISO image file.  The light icon turns green.  DO NOT close the applet and return to the browser window with the iLO Web GUI.

Procedure 114. Attach an ISO Image to an HP Server Using iLO

Step	Procedure	Results
7. ☐	**iLO2 Web GUI**: Open Remote Console applet	Click on the Remote Console tab. Click **Remote Console**.  Click **Yes** to acknowledge the security warning. If other screens display, acknowledge them as well. Return to procedure that referenced this appendix.
8. ☐	**iLO3/iLO4 Web GUI**: Open Remote Console applet	From the left side menu, click **Remote Console**. Click **Java Integrated Remote Console**.  Click **Yes** to acknowledge the security warning.

Procedure 114. Attach an ISO Image to an HP Server Using iLO

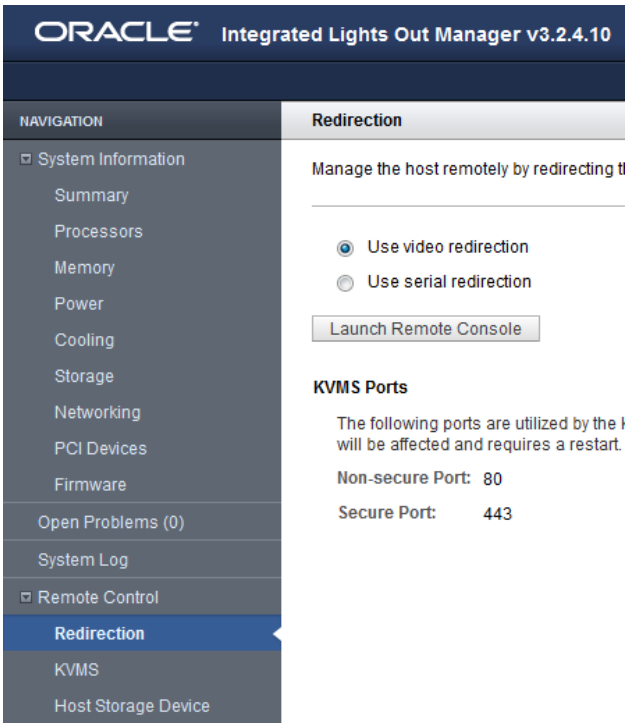
Step	Procedure	Results
9. ☐	**iLO3/iLO4 Web GUI**: Open virtual image	Navigate to **Virtual Drives -> CD/DVD -> Virtual Image**.  Navigate to the location of the ISO image file specified by the procedure referenced in this appendix.  Select the desired file and click **Open**.
10. ☐	**iLO3/iLO4 Web GUI**: 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.  Return to procedure that referenced this appendix.

Appendix F.2 Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

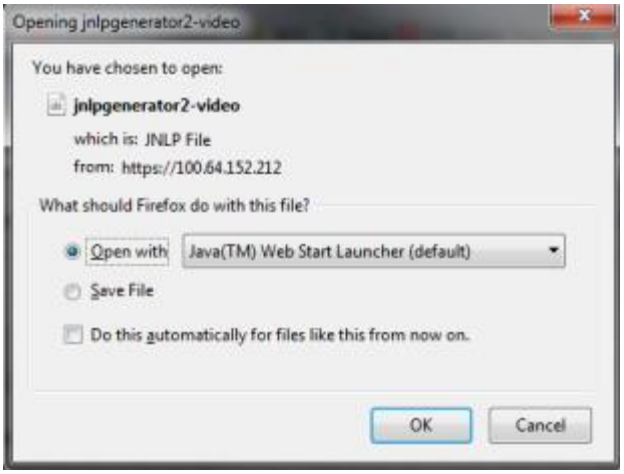
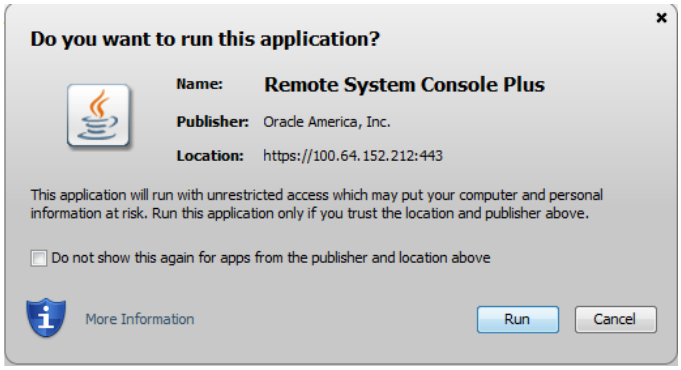
This procedure attaches an ISO image to an Oracle rack mount server.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

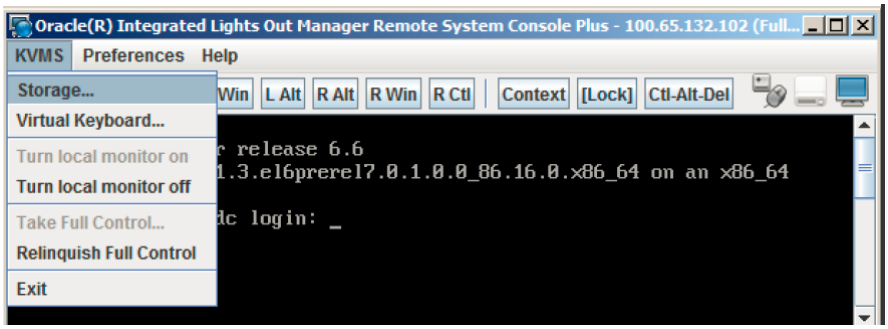
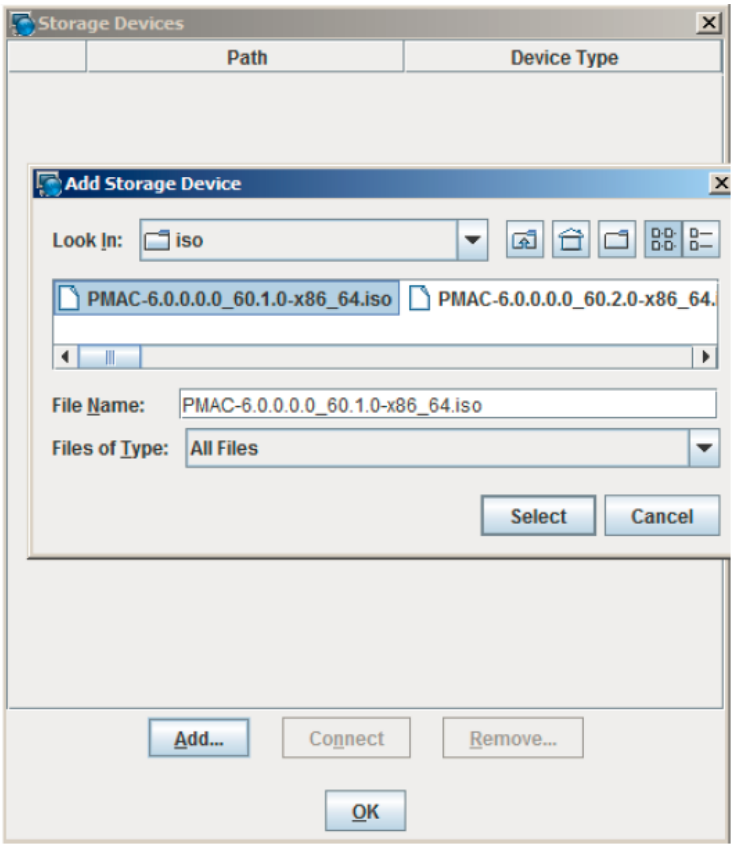
Procedure 115. Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

Step	Procedure	Results
1. ☐	**Local Workstation**: Access the ILOM Web GUI and login	From: `https://<ilom_IP>/` Log into the Oracle rack mount server ILOM. 
2. ☐	**ILOM Web GUI**: Access the remote console	Navigate to **Remote Control -> Redirection**. Click **Launch Remote Console**. 

Procedure 115. Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

Step	Procedure	Results
3. ☐	**ILOM Web GUI**: Access the remote console	Click **OK** and open with **Java Web Start Launcher**.  Select **Continue** and **Run** for any security warning prompts.  

Procedure 115. Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

Step	Procedure	Results
4. ☐	**iLOM Remote Console**: Mount the ISO from the remote console	Navigate to **KVMS** -> **Storage**.  Click **Add** and browse to the ISO located on the local machine.  Click **Select**. Once the ISO image is selected, click **Connect**. 

Appendix G. Upgrade Cisco 4948 PROM

This procedure upgrade the Cisco 4948 PROM.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 116. Upgrade Cisco 4948 PROM

Step	Procedure	Results

1. ☐	**Virtual PMAC/ Management Server**: Verify 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 PMAC system:
		`$ ls /var/TKLC/smac/image/<PROM_image_file>`
		For a NON-PMAC 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 [2] HP Solutions Firmware Upgrade Pack.

2. ☐	**Virtual PMAC/ Management Server**: Attach to switch console	If upgrading the firmware on switch1A, 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` If upgrading the firmware on switch1B, connect serially to switch1B by issuing the following command as admusr on the PMAC 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`

Procedure 116.Upgrade Cisco 4948 PROM

Step	Procedure	Results

3. ☐	**Virtual PMAC/ 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`
		Issue **ping** command:
		Note: The IP address <pmac_mgmt_ip_address> is 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, make sure the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, then contact My Oracle Support (MOS).

Procedure 116.Upgrade Cisco 4948 PROM

Step	Procedure	Results

4. ☐	**Virtual PMAC/ 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)`

5. ☐	**Virtual PMAC/ Management Server (Switch Console Session)**: Reload 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** message displays.

6. ☐	**Virtual PMAC/ 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 PMAC/ Management Server (Switch Console Session)**: Verify upgrade	The switch reboots when the firmware upgrade completes. Allow it to boot. 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 the version is the desired new version.
		If the switch does not boot properly, or has the wrong ROM version, contact My Oracle Support (MOS).

8. ☐	**Virtual PMAC/ Management Server**: Reset switch to factory defaults	Connect serially to the switch as outlined in step 4. , and reload by performing the following commands:
		`Switch# write erase`
		`Switch# reload`
		Wait until the switch reloads, then exit from console, enter **Ctrl-e + c + .** and you are returned to the server prompt.
		Note: There may be messages from the switch, if asked to confirm, press **Enter**. If asked yes or no, type **No** and press **Enter**.

Appendix H. Operational Dependencies on Platform Account Passwords

This appendix describes the operational dependencies on platform account passwords 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.

Before modifying the passwords stored on PMAC, perform a backup of PMAC databases in case you need to return to default passwords. To accomplish this, execute steps 6. through 8. in 9.5 Configure PMAC Application. To restore the passwords stored in the backup file, you can refer to steps 4 through 9 (inclusive), in Procedure 1 of the *PMAC Disaster Recovery*, latest release.

Appendix H.1 PMAC Credentials for Communication with Other System Components

This section covers the credentials that can be changed using the PMAC updateCredentials utility and the Platform dependencies users must be aware of to keep PMAC fully functional. Only the credentials the PMAC considers user accessible are listed here.

oaUSer

PMAC 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 PMAC uses. Lastly, all enclosures already provisioned in the PMAC must be rediscovered.

- 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 **Update User**.
- To update the credentials on the PMAC, execute the following on the UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=oaUser
  ```
- To rediscover an enclosure already provisioned in the PMAC inventory, log into the PMAC GUI and navigate to **Hardware > System Inventory > Cabinet XXX > Enclosure XXXXX** and click **Rediscover Enclosure**.

msa

All SAN controllers PMAC is expected to communicate with must be updated to have the new credentials and then the updateCredentials should be used to match credentials PMAC uses.

- To update the credentials, log into Fibre Channel Disk Controller via ssh as a manage user. Then execute:

  ```
  # set password manage
  ```
- To update the credentials on the PMAC, execute the following in the UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=msa
  ```

tpdPlatCfg

- To update the tpdPlatcfg credentials on the PMAC, log into the PMAC server shell with the root credentials and execute:

  ```
  $ passwd platcfg
  ```
- The Storage Configuration functionality on the PMAC uses the TPD platcfg credentials when communicating with its TVOE host. If the tpdPlatcfg credentials are changed on the PMAC TPD OS, it must also be changed on the PMAC application using this command.

  To update the credentials on the PMAC, execute the following in the UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=tpdPlatCfg
```

tvoeUser

TVOE administrator passwords need to be changed for all TVOE hosts PMAC is expected to communicate with and then the updateCredentials should be used to match the credentials PMAC uses. Note each time a new TVOE is installed its default password has to be updated to match.

- To update the credentials, log into the TVOE UI with the admusr credentials and execute:

  ```
  $ passwd
  ```

- To update the credentials on the PMAC, execute the following on the UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=tvoeUser
  ```

backupPassword

PMAC 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.

- To update the passphrase on a PMAC, execute the following in the UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=backupPassword
  ```

remoteBackupUser

If pmacop credentials are changed on a redundant PMAC, the updateCredentials should be used to match credentials the primary PMAC uses.

- To update the credentials on a redundant PMAC, log into the redundant PMAC UI with the pmacop credentials and execute:

  ```
  $ passwd
  ```

- To update the credentials on the primary PMAC, execute the following in primary PMAC UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=remoteBackupUser
  ```

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 PMAC. 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.

- 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.
- To modify the default oobUser credentials on the PMAC, execute the following in the UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=oobUser
  ```

- To add a RMS to PMAC system inventory with its unique iLO password, refer to 9.15 Add Rack Mount Server to the PMAC System Inventory.
- To edit iLO password of a specific RMS already in PMAC system inventory, refer to 9.16 Edit Rack Mount Server in the PMAC System Inventory.

tpdProvd

The tpdProvd credentials are used to allow tpdProvd communication between the PMAC and servers on its control network. The procedure for updating the tpdProvd password has changed as of PMAC 66.5.0. The user can now enter multiple passwords which can be matched to one or more individual servers. The update of the password on the PMAC does not use the updateCredentials script in this case. It uses two new commands under the pmacadm cli interface: addProvdCredentials and deleteProvdCredentials.

Expected Behaviors

1. If a tpdProvd password is changed on a non-discovered provisioned server (seen in the Main Menu->Software=>Software Inventory page but no data is associated to it) on both the server side and the **PMAC** side, after a few minutes, the IPv6 address will appear in the “Address” field and the server will self discover. The server can also be fully discovered if that server is selected in the grid and the **Rediscover** button is selected.
2. If a tpdProvd password is changed on an existing discovered server but not updated on the **PMAC side**, that server will remain discovered in the Main Menu->Software->Software Inventory page until a **sentry restart** is performed. Once performed, the server will no longer show as discovered in the Software Inventory page. Once the tpdProvd password has been updated on the **PMAC**, the behavior in number 1 will occur.

Procedure

a. Update the password on a given server or group of servers (assuming all passwords are the same for the group) either using the linux **passwd** command on the server(s) or by some other means.

b. From a PMAC shell, use the following command to add the password(s) to the PMAC database and update the PMAC messaging interface. This command will prompt the user for the password and echo asterisks as characters are entered.

   Note: --flushBAs can be set to "no" if entering multiple passwords and set to "yes" on the last password add. If --flushBAs is not set to "yes" on the last password entry, a **sentry restart** must be performed on the PMAC to flush out all the Broker Agents (server interfaces) in the PMAC messaging system and rebuild them using the new passwords.

   ```
   /usr/bin/sudo /usr/TKLC/smac/bin/pmacadm addProvdCredentials --
   flushBAs=yes
   ```

c. The new password can be verified using the following command (this should return a valid response with a password. If it fails, there may be a tpdProvd password mismatch issue between the PMAC and the server):

   ```
   /usr/bin/sudo /usr/TKLC/smac/bin/pmaccli getHostCommStr --
   ip=<ipv4 address of the server> --accessType=ro
   ```

d. If a password must be removed (and the exact spelling of the password is known), it can be deleted from the PMAC database and messaging system using the following command (again note that the user is prompted for the password):

   ```
   /usr/bin/sudo /usr/TKLC/smac/bin/pmacadm deleteProvdCredentials -
   -flushBAs=yes
   ```

Appendix H.2 PMAC GUI Account Credentials

Modification of any of the PMAC GUI accounts has no system impact. The PMAC GUI users can be updated by logging into the PMAC GUI as pmacadmin, and navigating to **Administration** > **Users**. Select the user from the first **Username** list and click **Set Password**. Enter the new password twice and click **Continue**.

Appendix H.3 PMAC Linux User Account Credentials

Modification of any PMAC 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 PMAC, use the updateCredentials to match the credentials the primary PMAC uses. If admusr credentials are changed after configuration of the netconfig repository, then delete netconfig services and re-add using the new credentials.

- To update the pmacop credentials on a redundant PMAC, log into the redundant PMAC UI with the pmacop credentials and execute:

  ```
  $ passwd
  ```

- To update the pmacop credentials the primary PMAC uses to communicate with the redundant PMAC, execute the following in primary PMAC UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=pmacop
  ```

Appendix H.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
```

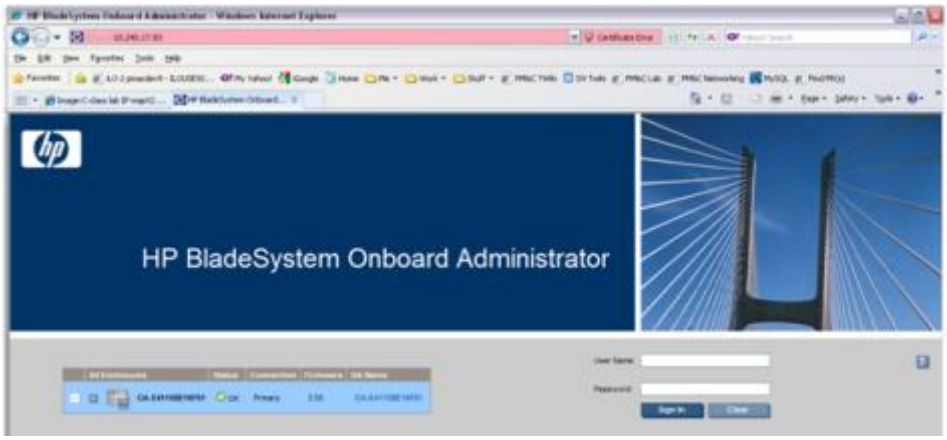
The preceding command prompts for a new pass phrase. It re-encrypts the credentials and stores the pass phrase to a file for use by netConfig.

Appendix I. Disable SNMP on the OA

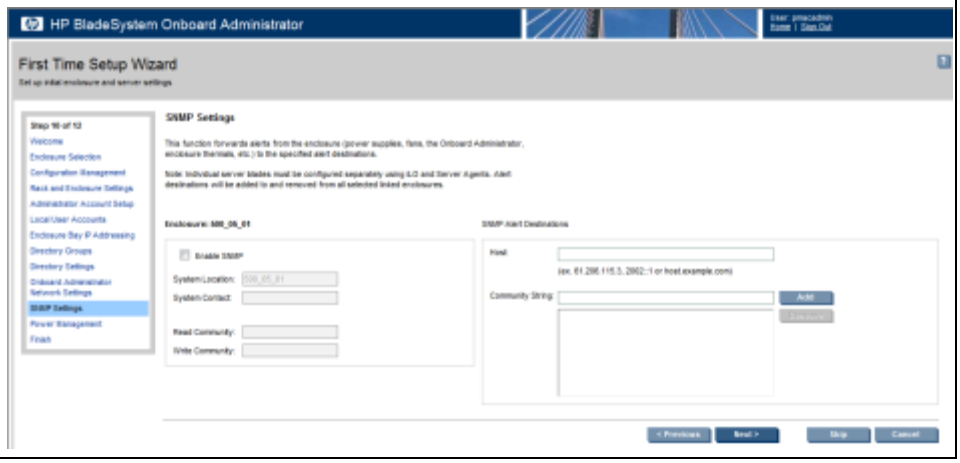
This procedure disables SNMP on the OA.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 117.Disable SNMP on the OA

Step	Procedure	Results
1. ☐	**OA GUI**: Login	From a web browser, navigate to the OA Bay1 IP address assigned in 7.1 Configure Initial OA IP. `http://<OA_IP>` Login as an administrative user. The original password is on a paper card attached to each OA. 
2. ☐	**OA GUI**: SNMP Settings	Use either the **First Time Setup Wizard SNMP Settings** menu or the **Enclosure Information > Enclosure Settings > SNMP Settings** menu.

Procedure 117.Disable SNMP on the OA

Step	Procedure	Results
3. ☐	**OA GUI**: SNMP Settings	Unmark the **Enable SNMP** checkbox. 

Appendix J. Downgrade Firmware on a 6125G Switch

This procedure downgrades firmware on 6125G enclosure switches when they are found to contain firmware newer than the qualified baseline. See [2] HP Solutions Firmware Upgrade Pack for the target firmware version.

Prerequisite: This procedure assumes the netConfig repository data fill is complete including copying the target firmware to the netConfig server (PMAC).

Note: Do not use this procedure for 6125XLG switches. See Appendix K for the correct procedure for that switch.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 118.Downgrade Firmware on a 6125G Switch

Step	Procedure	Results

1. ☐	**Active OA**: Login	SSH into the active OA and login as the administrative user.
		`login as: <oa_user>`
		`<oa_user>@<oa_ip>'s password: <oa_password>`

2. ☐	**Active OA**: Access serial console	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]`

Procedure 118.Downgrade Firmware on a 6125G Switch

3. ☐	**Switch**: Determine firmware	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`
		If the firmware is found to be newer than the target firmware, then proceed with the rest of this procedure; otherwise, gracefully exit the switch and PMAC.

4. ☐	**Virtual PMAC**: Login	SSH into the PMAC and login as **admusr**.
		`login as: admusr`
		`Password: <admusr_password>`
		`Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61`
		`[admusr@<pmac> ~]$`

5. ☐	**Virtual PMAC**: Copy firmware	Copy the firmware file to the switch.
		`$ sudo /usr/bin/scp 6125-cmw520-r2105.bin <switch_user>@<switch_ip>:/6125-cmw520-r2105.bin`
		`<switch_user>@<switch_ip>'s password: <switch_platform_password>`
		`100% 16MB 766.3KB/s 00:21`

6. ☐	**Virtual PMAC**: Exit	Gracefully exit from the PMAC SSH session. `$ logout`

7. ☐	**Active OA**: Login	If not already connected, ssh into the active OA and login as the administrative user.
		`login as: <oa_user>`
		`<oa_user>@<oa_ip>'s password: <oa_password>`

8. ☐	**Active OA**: Access serial console	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]`

Procedure 118.Downgrade Firmware on a 6125G Switch

9. ☐	**Switch**: Reboot 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`
		`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`
		`This command will reboot the device. Continue? [Y/N]: Y`
		`#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 ]`

Procedure 118.Downgrade Firmware on a 6125G Switch

10. ☐	**Switch**: Access File Control menu	Select **4** to access the file control 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

Procedure 118.Downgrade Firmware on a 6125G Switch

11. ☐	**Switch**: Identify target firmware	Select **1** from the file control menu to list all files 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
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 ]
```

Procedure 118.Downgrade Firmware on a 6125G Switch

12. ☐	**Switch**: Set application file type	Select **2** from the file control menu to set the application file type.
		`======================<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`

13. ☐	**Switch**: Select file	Select the firmware file identified in step 11. **Error! Reference source not found.**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>`

14. ☐	**Switch**: Modify file attribute	Select **1** from the file attributes menu to modify the file attribute to **+Main**.
		`Modify the file attribute:`
		`============================================================`
		`|<1> +Main |`
		`|<2> -Main |`
		`|<3> +Backup |`
		`|<4> -Backup |`
		`|<0> Exit |`
		`============================================================`
		`Enter your choice(0-4): 1`
		`This operation may take several minutes. Please wait....`
		`Set the file attribute success!`

Procedure 118.Downgrade Firmware on a 6125G Switch

15. ☐	**Switch**: Verify change	Select **1** from the file control menu to 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
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              |
============================================================
```

Procedure 118.Downgrade Firmware on a 6125G Switch

16. ☐	**Switch**: Exit	Select **0** from the file control menu to Exit to the main 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`

Procedure 118.Downgrade Firmware on a 6125G Switch

17. ☐	**Switch**: Boot the system	Select **1** from the extend-bootware menu to Boot the system. ***Note***: Do NOT select reboot by choosing **0**! ***Note***: During this process you may be asked 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 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:

Procedure 118.Downgrade Firmware on a 6125G Switch

18. ☐	**Switch**: Login	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`
		`Password: password`
		`#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`
		`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 ]`

19. ☐	**Switch**: Disconnect from the switch	Gracefully disconnect from the switch serial console by pressing **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`

20. ☐	**Active OA**: Logout	Log out of the OA. `> logout`

Appendix K. Downgrade Firmware on a 6125XLG Switch

This procedure downgrades the 6125XLG enclosure switches when they are found to contain firmware newer than the qualified baseline. See [2] HP Solutions Firmware Upgrade Pack for the target firmware version.

Prerequisite: This procedure assumes the netConfig repository data fill is complete including copying the target firmware to the netConfig server (PMAC).

Note: Do not use this procedure for 6125 switches. See Appendix J for the correct procedure for that switch.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 119. Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results

1. ☐	**Active OA**: Login	SSH into the active OA and login as the administrative user:
		`login as: <oa_user>`
		`<oa_user>@<oa_ip>'s password: <oa_password>`

2. ☐	**Active OA**: Access serial console	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>`
		`Username: <switch_user>`
		`Password: <switch_password>`

3. ☐	**Switch**: Determine firmware	Execute the **display version** command to determine if a downgrade of the firmware needs to be performed.
		`> 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`
		If the firmware is found to be newer than the target firmware, then proceed with the rest of this procedure; otherwise, gracefully exit the switch and PMAC.

4. ☐	**Virtual PMAC**: Login	SSH into the PMAC and login as **admusr**.
		`login as: admusr`
		`Password: <admusr_password>`
		`Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61`
		`[admusr@<pmac> ~]$`

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results

5. ☐	**Virtual PMAC**: Copy firmware	Copy the firmware file to the switch.
		`$ sudo /usr/bin/scp 6125XLG-CMW710-R2403.ipe <switch_user>@<switch_ip>:/6125XLG-CMW710-R2403.ipe`
		`<switch_user>@<switch_ip>'s password: <switch_platform_password>`
		`100% 16MB 766.3KB/s 00:21`

6. ☐	**Virtual PMAC**: Exit	Gracefully exit from the PMAC SSH session. `$ logout`

7. ☐	**Active OA**: Login	If not already connected, ssh into the active OA and login as the administrative user.
		`login as: <oa_user>`
		`<oa_user>@<oa_ip>'s password: <oa_password>`

8. ☐	**Active OA**: Access serial console	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>`
		`Username: <switch_user>`
		`Password: <switch_password>`

9. ☐	**Switch**: Reboot 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`
		`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`
		`This command will reboot the device. Continue? [Y/N]: Y`
		`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 ]`

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results
10. ☐	**Switch**: Access File Control menu	Select **4** to access the file control 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
11. ☐	**Switch**: Identify target firmware	Select **1** from the file control menu to list all files and identify the target firmware from the list. ***Note***: Two files are identified: A system file and 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 Display all file(s) in flash: 'M' = MAIN 'B' = BACKUP 'S' = SECURE '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.ipe |

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results
		|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.dat
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_2011		0101000725.did
27 796 Jan/01/2011 00:00:14 N/A flash:/license/history/DeviceID_2011		0101000014.did
28 805 Jan/01/2011 00:00:18 N/A flash:/license/history/DeviceID_2011		0101000018.did
29 54222848 Aug/19/2015 16:57:16 N/A flash:/6125xlg-cmw710-system-r2406p0		3.bin
30 8331264 Aug/19/2015 16:57:06 N/A flash:/6125xlg-cmw710-boot-r2406p03.		bin
31 9345024 Aug/19/2015 17:11:38 M flash:/6125xlg-cmw710-boot-r2403.bin	 ========== [OUTPUT REMOVED]

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results
12. ☐	**Switch**: Set bin file type	Select **2** from the file control menu to set the bin file type. ==========<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
13. ☐	**Switch**: Select file	Select the firmware file identified in step 11. and enter the corresponding line number. '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-r2403. | |bin | |2 54222848 Aug/19/2015 16:57:16 N/A flash:/6125xlg-cmw710-system-r2406p | |03.bin | |3 8331264 Aug/19/2015 16:57:06 N/A flash:/6125xlg-cmw710-boot-r2406p03 | |03.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 another file No.(0-Finish choice): 4 Enter another file No.(0-Finish choice):0 You have selected: flash:/6125xlg-cmw710-system-r2403.bin flash:/6125xlg-cmw710-boot-r2403.bin

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results
14. ☐	**Switch**: Modify file attribute	Select **1** from the file attributes menu to modify the file attribute to **+Main**. Modify the file attribute: ========== |<1> +Main | |<2> -Main | |<3> +Backup | |<4> -Backup | |<0> Exit | ========== Enter your choice(0-4): 1 This operation may take several minutes. Please wait.... Set the file attribute success!
15. ☐	**Switch**: Verify change	Select **1** from the file control menu to 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 Bin File type | |<3> Delete File | |<0> Exit To Main Menu | ========== Enter your choice(0-3): 1 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.ipe| |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.dat |

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results
		|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-r2403.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_20110101000		725.did
27 796 Jan/01/2011 00:00:14 N/A flash:/license/history/DeviceID_20110101000		014.did
28 805 Jan/01/2011 00:00:18 N/A flash:/license/history/DeviceID_20110101000		018.did
29 54222848 Aug/19/2015 16:57:16 N/A flash:/6125xlg-cmw710-system-r2406p03		.bin
30 8331264 Aug/19/2015 16:57:06 N/A flash:/6125xlg-cmw710-boot-r2406p03.bin
31 9345024 Aug/19/2015 17:11:38 M flash:/6125xlg-cmw710-boot-r2403.bin| ========== 16. ☐	**Switch**: Exit	Select **0** from the file control menu to Exit to the main 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

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results
17. ☐	**Switch**: Boot the system	Select **1** from the extend-bootware menu to Boot the system. ***Note***: Do NOT select reboot by choosing **0**! ***Note***: During this process you may be asked 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 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:

Procedure 119.Downgrade Firmware on a 6125XLG Switch

Step	Procedure	Results

18. ☐	**Switch**: Login	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] [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 ]`

19. ☐	**Switch**: Disconnect from the switch	Gracefully disconnect from the switch serial console by pressing **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]`

20. ☐	**Active OA**: Logout	Log out of the OA. `> logout`

Appendix L. Change Switch Passwords (netConfig)

This procedure changes switch passwords using netConfig. This updates the passwords in both the repository and on the devices.

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: This operation should be scheduled with the customer. Executing these commands as stated does not cause a service interruption. The switches are not rebooted or initialized; however, as with all in-service operations, caution should be taken.

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 --repolistDevices`

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. 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 PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments allow for future simplification of network configuration procedures.

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

Variable	Value
<netConfig_server_mgmt_IP_address>	
<switch_hostname> From NAPD or output from `listDevices` command	
<cleartext_password>	

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 120.Change Switch Passwords (netConfig)

Step	Procedure	Results

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` Take note of the target device name. This is referred to as the variable <switch_hostname> in subsequent steps.

Procedure 120.Change Switch Passwords (netConfig)

Step	Procedure	Results

3. ☐	**netConfig Server**: Change password	For device types 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)`
		For device types 6120, 6125G, or 6125XLG:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> setPassword password=<cleartext_password>; history -d $(history 1)`
		Note: The appended part of the command, `; history -d $(history 1)`, deletes the history so 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**: Logout	Gracefully exit from the netConfig server SSH session: `$ logout`

Appendix M.Uninstall Symantec NetBackup Client

This procedure uninstalls 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 may not 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.

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 121.Uninstall Symantec NetBackup Client

Step	Procedure	Results
1. ☐	Back up application	Back up your application as described in your application documentation. Take care not to use NetBackup since the NetBackup client is being removed from the server.

Procedure 121.Uninstall Symantec NetBackup Client

<table>
<tr><th>Step</th><th>Procedure</th><th>Results</th></tr>
<tr><td>2. ☐</td><td>Target Server: Login</td><td>SSH into the server and login as admusr.
<pre>login as: admusr
Password: <admusr_password>
Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61
[admusr@<target_server> ~]$</pre></td></tr>
<tr><td>3. ☐</td><td>Target Server: Determine the NetBackup client version</td><td>Determine the NetBackup client version by inspecting the version file:
<pre>[admusr@<target_server> ~]$ sudo /bin/cat
/usr/openv/netbackup/bin/version
NetBackup-RedHat2.6.18 7.6.0.1
[admusr@<target_server> ~]$</pre></td></tr>
<tr><td>4. ☐</td><td>Target Server: Determine packages installed and services configured</td><td>Determine the NetBackup client packages installed and services configured on the server by inspecting the client profile configuration file. For some versions of NetBackup, a configuration file is not used and does not exist. If your installation does not use a client profile file, refer to Table 2 for your specific release.
Table 2. Installed Packages and Services for NetBackup Client 7.0, 7.1, 7.5, and 7.7
<table>
<tr><th>NetBackup Client Version</th><th>Packages (RPMs)</th><th>Services</th></tr>
<tr><td>NB 7.0</td><td>VRTS pbx</td><td>RC: netbackup</td></tr>
<tr><td>NB 7.1</td><td>SYMCpdddea
SYMCnbjre
SYMCnbjava
SYMCnbclt
VRTS pbx</td><td>RC: netbackup</td></tr>
<tr><td>NB 7.5 and NB 7.7</td><td>SYMCpdddea
SYMCnbjre
SYMCnbjava
SYMCnbclt
VRTS pbx</td><td>RC: netbackup
RC: vxpbx_exchanged</td></tr>
</table>
Note: The client profile configuration file includes the client version in the name. For example, NB7601.conf where 7601 represents the client version number with the periods removed. In this example, version 7.6.0.1 is used.
Inspect the client profile configuration file.
<pre>[admusr@<target_server> ~]$ sudo /bin/cat
/usr/TKLC/plat/etc/netbackup/profiles/NB7601.conf
VERSION=7.6.0.1
RPMS="SYMCpddea,SYMCnbjre,SYMCnbjava,SYMCnbclt,VRTSpbx"
RC_SERVICES="netbackup,vxpbx_exchanged"</pre></td></tr>
</table>

Procedure 121.Uninstall Symantec NetBackup Client

Step	Procedure	Results

5. ☐	**Target Server**: Stop all NetBackup processes	Stop the Symantec NetBackup client services identified in step 4. This example stops the services for NetBackup version 7.6.0.1.
		`[admusr@<target_server> ~]$ sudo service netbackup stop`
		`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`
		`Stopped Symantec Private Brach Exchange`

6. ☐	**Target Server**: Verify the processes stopped	Verify all NetBackup processes are stopped. No output is expected. `[admusr@<target_server> ~]$ sudo /usr/openv/netbackup/bin/bpps`
7. ☐	**Target Server**: Ensure directory is not already in use	Ensure the directory to which the NetBackup LV is mounted is not already in use. This is a precautionary step. `[admusr@<target_server> ~]$ cd ~`

8. ☐	**Target Server**: Delete services	Delete the NetBackup services identified in the client profile from step 4. In this example, the NetBackup client services are netbackup and vxpbx_exchanged.
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf del netbackup`
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf del vxpbx_exchanged`

9. ☐	**Target Server**: Reconfigure services	Reconfigure the server services after the deletion: `[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf reconfig`

10. ☐	**Target Server**: xxx	Uninstall the NetBackup client packages identified in the client profile from step 4. 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`
		`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!`

Procedure 121.Uninstall Symantec NetBackup Client

Step	Procedure	Results
11. ☐	**Target Server**: Verify removal of client RPMs	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"`

12. ☐	**Target Server**: Clean up directory	Clean up the **/etc/rc.d/init.d** directory.
		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`
		`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`
		The output of this example shows the netbackup service file was not removed. Delete the service file:
		`[admusr@<target_server> ~]$ sudo rm -f /etc/rc.d/init.d/netbackup`

13. ☐	**Target Server**: Identify volume and volume group	Identify the NetBackup logical volume (LV) and volume group (VG). The LV and VG are referenced in later steps.
		`[admusr@<target_server> ~]$ sudo lvs`
		`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`
		The output shows the NetBackup LV is named **netbackup_lv** and the VG is **vgroot**.

14. ☐	**Target Server**: Identify processes using volume	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`
15. ☐	**Target Server**: Unmount device	Unmount **/usr/openv** device from the NetBackup LV: `[admusr@<target_server> ~]$ sudo /bin/umount -l /usr/openv`
16. ☐	**Target Server**: Remove LV entry	Remove the NetBackup LV entry from **/etc/fstab** file. `[admusr@<target_server> ~]$ sudo /bin/sed -i.bak '/netbackup_lv/d' /etc/fstab`
17. ☐	**Target Server**: Check in file	Check the **/etc/fstab** file into the RCS. `[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/rcscheck /etc/fstab`

Procedure 121.Uninstall Symantec NetBackup Client

Step	Procedure	Results

18. ☐	**Target Server**: Verify removal of file	Verify the removal of the entry from the **/etc/fstab** file.
		Compare the **/etc/fstab** file to the **/etc/fstab.bak** backup file.
		`[admusr@<target_server> ~]$ sudo /usr/bin/diff /etc/fstab.bak /etc/fstab`
		`19d18`
		`< /dev/vgroot/netbackup_lv /usr/openv ext4 defaults 1 2`

19. ☐	**Target Server**: Remove backup file	Remove the **/etc/fstab.bak** file. `[admusr@<target_server> ~]$ sudo rm -f /etc/fstab.bak`
20. ☐	**Target Server**: Remove volume	Remove the NetBackup LV identified in step step 13. Take care to use the correct volume group. `[admusr@<target_server> ~]$ sudo /sbin/lvremove -f /dev/vgroot/netbackup_lv`
21. ☐	**Target Server**: Remove client package entries	Execute the command in this step to remove the NetBackup client package entries from the **pkgKeep.conf** file. The NetBackup client packages were identified in step 4. If **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`

22. ☐	**Target Server**: Verify removal of packages	Verify the removal of the NetBackup client package entries from the **pkgKeep.conf** file by comparing the pkgKeep.conf to the **pkgKeep.conf.bak** backup file.
		`[admusr@<target_server> ~]$ sudo /usr/bin/diff /usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak /usr/TKLC/plat/etc/upgrade/pkgKeep.conf`
		`1,5d0`
		`< SYMCnbclt`
		`< SYMCnbjava`
		`< SYMCnbjre`
		`< SYMCpddea`
		`< VRTSpbx`

23. ☐	**Target Server**: Remove backup file	Remove the pkgKeep.conf.bak file. `[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak`
24. ☐	**Target Server**: Remove configuration file	Remove the client profile configuration file, if one exists. The existence of this file is determined in step step 4. ***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`

Procedure 121.Uninstall Symantec NetBackup Client

Step	Procedure	Results
25. ☐	**Target Server**: Remove script file	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 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/scripts/NB7601`

26. ☐	**Target Server**: Remove firewall rules	Remove the firewall rules related to NetBackup.
		Note: This step varies depending on how the application implemented the firewall rules. The example in this step illustrates 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.
		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`
		`[admusr@<target_server> ~]$ sudo /sbin/service iptables restart`
		`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`
		`[admusr@<target_server> ~]$ sudo /sbin/service ip6tables restart`
		`ip6tables: Setting chains to policy ACCEPT: filter [ OK ]`
		`ip6tables: Flushing firewall rules: [ OK ]`
		`ip6tables: Applying firewall rules: [ OK ]`

27. ☐	**Target Server**: Remove firewall configuration files	Remove firewall configuration files related to NetBackup.
		Note: This step varies depending on how the application implemented the firewall rules. The example in this step illustrates 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.
		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`

Procedure 121. Uninstall Symantec NetBackup Client

Step	Procedure	Results
28. ☐	**Target Server**: Update hosts file	Update the /etc/hosts file to remove the NetBackup server host using the platcfg utility. ***Note***: If the NetBackup entry in the **/etc/hosts** file is an alias and you do not want to delete the host, select **Delete Alias** instead of **Delete Host**. The rest of the steps remain the same. 1. As admusr, execute the **sudo su - platcfg** command 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 deletion. 8. Exit out of the platcfg utility.

29. ☐	**Target Server**: Verify server health	No unexpected alarms should display and no missing package files should exist.
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/alarmMgr -alarmStatus`
		`[admusr@<target_server> ~]$ sudo rpm -Va`

Appendix N. Configuring NUMA on pmac-deploy

This appendix explains the new NUMA tuning options added to the pmac-deploy command.

Prerequisites:

- No other manual activity is currently in progress on the TVOE host.
- **syscheck** and **alarmMgr** on the TVOE host show no outstanding issues.
- There is adequate resources to properly deploy the PMAC on the TVOE host.

Assumptions/Limitations:

- Users of these new options must fully understand the use and setting of the numa/vcpu assignments and the affects this can have on the overall performance of the TVOE host, the PMAC, and any VMs that may reside on the same TVOE host.
- When --numa is not entered on the command line, the PMAC will use the numa that the TVOE has reserved CPU(s) on. That is usually 0 but it can be something else. This value is defined in file **/usr/TKLC/tvoe/etc/host_resources.cfg** as a comma separated string with a label called **RESERVED_CPUS**.
- NUMA boundaries cannot be crossed when defining the cpuset.
- If more reserved CPUs are configured in the **/usr/TKLC/tvoe/etc/host_resources.cfg** file than are available on a given NUMA when using the new options on deploy, the configuration will fail.

New Options:

The new options include the following:

--cpuset

This option is a CSV string but can include ranges separated by a dash. It can be optionaly combined with the --numa option but is mutually exclusive with the --restrictCPus and --startCpu options given below. It attempts to associate the provided cpuset to the PMAC on the given NUMA. Any duplicate CPUs identified in the cpuset will be removed during the configuration process. The number of CPUs in the cpuset must be equal to or greater than the number of vcpus defined (--vcpus defaults to 1).

Example:

```
--cpuset=1,2,3-5
```

```
--numa=0 --cpuset=1,2,3-5
```

```
--numa=0 --vcpus=4 --cpuset=1,2,3-5
```

--restrictCpus

This option is a simple Boolean. The presents of this option indicates TRUE. It can be combined optionally with the --numa and --vcpus options. It instructs the pmac-deploy to find CPUs on the given NUMA (first available first served) based on the number of VCPUs defined by the --vcpus option (which is optional and defaults to 1). It then associates them to the PMAC guest on deploy. This option is mutually exclusive with the --cpuset option.

Example:

```
--restrictCpus
```

```
--numa=0 --restrictCpus
```

```
--numa=0 --vcpus=4 --restrictCpus
```

--startCpu

This option is paired with the --restrictCpus option to instruct the deploy to start its CPU search at the given CPU number on the given NUMA (they are in a sorted list). It is mutually exclusive with all other options in the deploy command.

Example:

```
--restrictCpus --startCpu=2
```

```
--numa=0 --vcpus=3 --restrictCpus --startCpu=2
```

Appendix O. Update the PMAC GSOAP Cipher List

This procedure defines the method required to update the PMAC **GSOAP** cipher list and how to verify the update was successful.

Prerequisites:

- The file /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg is present on the system.
- No other PMAC manual activity is currently in progress on the PMAC (for example, IPM, Guest creations, etc.).
- syscheck and alarmMgr on the PMAC show no outstanding issues.

Assumptions/Limitations:

- On upgrades, this file will always be overwritten with the contents of the new file version from the new PMAC release. The old file will be copied into the same directory as pmacgsoap.cfg.rpmnew. If the file ciphers have previously been changed and the user wishes to maintain that change, the user

must manually update/merge the previous contents of the file into the new version created by the upgrade.

Step	Procedure	Results
1. ☐	PMAC Login	Connect to the PMAC shell and log into the PMAC as admusr.
2. ☐	Change to root user	If not logged in as the root user, sudo to the root user. `[admusr@p3Pmac1 ~]# sudo su -`
3. ☐	Make Backup copy of Pmac GSOP config file	Make a backup copy of the **/usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg** file and preserve the current permissions and ownership. `cp -p /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg.backup`

4. ☐	Run syscheck and alarmMgr	Make sure syscheck and alarmMgr show no outstanding issues.
		`[root@p3Pmac1 ~]# syscheck`
		`[root@p3Pmac1 ~]# alarmMgr --alarmStatus`

5. ☐	Edit the PMAC GSOAP config file	Edit the /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg file:
		`[root@p3Pmac1 ~]# cd /usr/TKLC/smac/etc/gsoap`
		`[root@p3Pmac1 ~]# vim pmacgsoap.cfg`

6. ☐	Update the cipher list	Change/update the line **ssl_ciphers=....** using vim or vi commands. Add appropriate ciphers to this list. Make sure the format is followed exactly. All ciphers must be separated by a single ":". All protocols which are to be excluded should be prefixed with the "!" character. Note: Currently there is no check for inadvertent special characters as the format for a cipher may change in future releases of openssl. In some cases adding special characters can cause the addition to fail and generate a fatal error in smacTalk. Note: In some cases an invalid cipher may simply get ignored by **openssl**. Before editing this list make sure the ciphers that are being added are valid and known to **openssl**. The **openssl ciphers -v 'cipher list'** command (and other variations) can be used to verify the cipher(s) being added. Details of **openssl** can be found in numerous places on the Web. One good source is at https://wiki.openssl.org/index.php/Command_Line_Utilities
7. ☐	Save pmacgsoap.cfg file	Save the changes made to the **pmacgsoap.cfg** file.

Step	Procedure	Results

8. ☐	Check status of sentry	On the PMAC shell the sentryd smacTalk process must be restarted. This action will take down the smacTalk process (and others) and restart them. This restart re-creates the smacTalk process and (among other actions) binds in the **GSOAP** context, reads the **pmacgsoap.cfg** file cipher list and binds that into the **GSOAP openssl** port.
		First check the status of sentryd. This should show the smacTalk and smacMon processes as **"running"** with a valid **PID** number. If the **sentry restart** command is successful the **PID** number will change as well as the **StartTS**.
		`[root@p3Pmac1 ~]# sentry status`
		`sending status command...`
		`PMAC Sentry Status`
		`------------------`
		`sentryd started: Wed Apr 25 13:56:30 2018`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`----------------- ------ ----------- -------------------------`
		`smacTalk 23115 running Wed Apr 25 13:56:30 2018 1`
		`smacMon 23143 running Wed Apr 25 13:56:30 2018 1`
		`hpiPortAudit 23178 running Wed Apr 25 13:56:30 2018 1`
		`snmpEventHandler 23216 running Wed Apr 25 13:56:30 2018 1`
		`Thu Apr 26 07:55:12 2018`
		`Command Complete.`

9. ☐	Perform sentry restart	Perform a sentry restart.
		`[root@p3Pmac1 ~]# sentry restart`
		`sending restart command...`
		`sentryd is shutting down all application software, please wait...`
		`sentryd is restarting...`
		`Thu Apr 26 07:56:52 2018`
		`Command Complete.`

Step	Procedure	Results

10. ☐	Check status of sentry	Immediately issue a **sentry status** command. If the results of this command is “no response from sentryd” on the first try, this is normal as sentryd has not come back up yet. Issue the command again until either all processes are at the **“running state”** or smacTalk fails to recover.
		`[root@p3Pmac1 ~]# sentry status`
		`sending status command...`
		`no response from sentryd (Timer expired), try command again`
		`Thu Apr 26 07:56:04 2018`
		`Command Complete.`
		The smacTalk and smacMon processes status may show as **"in recovery"**. If this is present issue the sentry status command again a few times until all processes have recovered as **"running"**.
		`[root@p3Pmac1 ~]# sentry status`
		`sending status command...`
		`PMAC Sentry Status`
		`------------------`
		`sentryd started: Thu Apr 26 07:56:58 2018`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`---------- ------ ---------- ---------- -`
		`smacTalk --- in recovery Thu Apr 26 07:56:58 2018 1`
		`smacMon --- not running --- 0`
		`hpiPortAudit --- not running --- 0`
		`snmpEventHandler --- not running --- 0`
		`[root@p3Pmac1 ~]# sentry status`
		`sending status command...`
		`PMAC Sentry Status`
		`------------------`
		`sentryd started: Thu Apr 26 07:56:58 2018`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`---------- ------ ---------- ---------- -`
		`smacTalk 8544 running Thu Apr 26 07:56:58 2018 1`
		`smacMon 8573 running Thu Apr 26 07:56:58 2018 1`
		`hpiPortAudit 8595 running Thu Apr 26 07:56:58 2018 1`
		`snmpEventHandler 8618 running Thu Apr 26 07:56:58 2018 1`
		`Thu Apr 26 07:57:06 2018`
		`Command Complete.`
		If the smacTalk process fails to return to a “running” state, proceed to step 12 and come back to 11 when the issues have been resolved.

Step	Procedure	Results
11. ☐	Remove the backup PMAC GSOAP config file	Remove the backup file if desired at /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg.backup.

Step	Procedure	Results

12. ☐	**sentry restart failure**	If smacTalk encounters a fatal error due to an invalid or unacceptable cipher list, the **sentry restart** and **sentry status** output will look like the following:
		`[root@p3Pmac1 ~]# sentry status`
		`sending status command...`
		`PMAC Sentry Status`
		`------------------`
		`sentryd started: Wed Apr 25 12:42:30 2018`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`--- --- --- --- --`
		`smacTalk --- not running --- 2`
		`smacMon 8350 running Wed Apr 25 12:42:30 2018 1`
		`hpiPortAudit 8373 running Wed Apr 25 12:42:30 2018 1`
		`snmpEventHandler 8402 running Wed Apr 25 12:42:30 2018 1`
		If this problem occurs, look at the **smacTalkDbug.log** file for some idea as to why it failed. There should be logs based on the following error conditions:
		1. If the **openssl** function call **SSL_CTX_set_cipher_list** returns 0 meaning it could not interpret the provided cipher list.
		Log:
		"Unable to add GSOAP SSL cipher list - rc: 0"
		2. If the cipher list contained in the **pmacgsoap.cfg** file is an empty string.
		Log:
		"Unable to add GSOAP SSL cipher list - list empty - check file: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg"
		3. If the **openssl** function **SSL_CTX_set_cipher_list** returns something other than 0 or 1 (new version and not expected to occur).
		Log:
		"Unable to add GSOAP SSL cipher list - unknown rc: <unknown rc> - check file: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg"
		4. If the **pmacgsoap.cfg** file is successfully opened but the proper cipher list search string "ssl_ciphers" cannot be found. This string should always be on a separate line beginning at column 0.
		Log:
		"Unable to add GSOAP SSL cipher list - unable to find ssl_ciphers - check file: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg"
		5. If the **pmacgsoap.cfg** file is missing or cannot be opened due to inadvertent permission changes.
		Log:
		"Unable to open: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg"

13. ☐	Go to PMAC Logs directory	Change directories to the PMAC log directory: `[root@p3Pmac1 ~]# cd /var/TKLC/smac/logs)`

Step	Procedure	Results
14. ☐	Examine logs or contact next level of support	Edit the **smactalkDbug.log file**. Go to the bottom of the file (if using **vim** use **shift G**). Search up for "cipher" (if using vim enter **Esc ?cipher**). Span up or down in the logs to follow the flow of the cipher list settings. The first log to look for should contain the text: **"Returning cipher list"** with the cipher list as given in the **/usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg** file. If these logs do not fully explain the failure (as in it failed with a return code of 0), The cipher list changes made will have to be validated to make sure what was added is in the correct format and is a valid cipher. If unable to resolve the issue please contact the next level of support.

Appendix P. Increase the PMAC NetBackup Filesystem Size

This procedure increases the PMAC NetBackup file system to accommodate upgrading to NetBackup 7.7 or greater. Currently, the recommended filesystem size for NetBackup 7.7 is 5GB. 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` and set to 2GB.
- There is a filesystem on the PMAC guest at `/dev/<device_name>` mounted to `/usr/openv`' and sized to 2GB.
- The NetBackup filesystem on the PMAC 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 can differ from `/dev/vdd`. This can be determined by issuing the `df -h` command on the PMAC before starting this procedure and searching for the `/usr/openv` NetBackup filesystem. Once NetBackup has been enabled and configured on a PMAC, 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 PMAC shell or from a TVOE shell.
- Performing this procedure increases the size of the NetBackup filesystem to 5GB. You can use this procedure to increase the NetBackup volume to any size that can be accommodated by the TVOE host. 5GB is the required size for NetBackup 7.7.
- Each step in this procedure begins 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 PMAC.

Procedure 122.Increase the PMAC NetBackup Files System Size

Step	Procedure	Results
1. ☐	**TVOE Host**: Login	Connect to the management server's TVOE host shell and log into the PMAC shell as **admusr** using ssh.

Procedure 122.Increase the PMAC NetBackup Files System Size

Step	Procedure	Results

2. ☐	**TVOE Host**: Verify existing volume	Verify the existing TVOE NetBackup volume is set to 2GB.
		6. Display the logical volume sizes.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvs`
		`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`
		Display the logical volume details.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvdisplay /dev/vgguests/<pmac_guest>_netbackup.img`
		`--- 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`

3. ☐	**PMAC**: Verify filesystem	Verify the NetBackup filesystem is set to 2GB.
		`[admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv`
		`Filesystem Size Used Avail Use% Mounted on`
		`/dev/vdd 2.0G 69M 2.3G 1% /usr/openv`

Procedure 122.Increase the PMAC NetBackup Files System Size

Step	Procedure	Results

4. ☐	**TVOE Host**: Resize volume	Resize the NetBackup volume from 2GB to 5GB.
		`[admusr@<tvoe_host> ~]$ usr/bin/sudo /sbin/lvextend --size 5G /dev/vgguests/<pmac_guest>_netbackup.img`
		`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`

5. ☐	**TVOE Host**: Verify increase	Verify the size of the volume has increased to 5GB.
		7. Display the logical volume sizes.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvs`
		`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`
		`plat_var vgroot -wi-ao---- 1.00g`
		8. Display the logical volume details.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvdisplay /dev/vgguests/<pmac_guest>_netbackup.img`
		`--- 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`

Procedure 122.Increase the PMAC NetBackup Files System Size

Step	Procedure	Results

6. ☐	**PMAC**: Verify filesystem	Verify the space on the PMAC NetBackup filesystem has not changed.
		`[admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv`
		`Filesystem Size Used Avail Use% Mounted on`
		`/dev/vdd 2.0G 69M 2.3G 1% /usr/openv`

7. ☐	**TVOE Host**: Verify PMAC is aware of volume size increase	1. Ensure the PMAC is made aware of the volume size increase.
		2. Identify the PMAC guest using the **virsh** command.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh list --all`
		`Id Name State`
		`86 <pmac_guest> running`
		Shut down the PMAC guest.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh shutdown <pmac_guest>`
		`Domain <pmac_guest> is being shutdown`
		3. Wait for the PMAC shutdown to complete. 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`
		`Id Name State`
		`86 <pmac_guest> shut off`
		4. Once shutdown is complete, restart the PMAC.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh start <pmac_guest>`
		`Domain <pmac_guest> started`
		5. Verify the PMAC has completed the restart. This can be checked by executing the command **sudo virsh console <pmac_guest>** and checking for the PMAC guest login prompt.
		Once the escape character is displayed, press **Enter** once more to reach the login prompt.
		Afterwards, press **Ctrl-]** to exit the PMAC login prompt and return to the TVOE host prompt.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh console <pmac_guest>`
		`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`

Procedure 122.Increase the PMAC NetBackup Files System Size

Step	Procedure	Results

8. ☐	**PMAC**: Verify volume size	Verify the volume size increase is 5GB as seen from the PMAC.
		`[admusr@<pmac_guest> ~]$ /usr/bin/sudo admusr /sbin/fdisk -l /dev/netbackup`
		`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`

9. ☐	**PMAC**: Resize filesystem	Resize the PMAC NetBackup filesystem to 5GB.
		1. 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`
		`/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)`
		2. Unmount 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.

Procedure 122.Increase the PMAC NetBackup Files System Size

Step	Procedure	Results

		Note: There **umount** command does not generate output upon success.
		`[admusr@<pmac_guest> ~]$ /usr/bin/sudo /bin/umount /usr/openv`
		3. Execute the **e2fsck** command to make sure the NetBackup filesystem is clean.
		`[admusr@<pmac_guest> ~]$ /usr/bin/sudo /sbin/e2fsck /dev/netbackup`
		`e2fsck 1.43-WIP (20-Jun-2013)`
		`/dev/netbackup: clean, 11/327680 files, 37999/1310720 blocks`
		4. Execute the **resize2fs** command to resize the filesystem and map it to the 5GB size of the disk volume on the TVOE host. If the size attribute is not included in the command, the NetBackup filesystem resizes to the total free space on the TVOE host volume. This should be 5GB since 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`
		`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.`
		5. Re-mount the **/usr/openv** NetBackup filesystem with the **mount -a** command.
		`[admusr@<pmac_guest> ~]$ mount -a`
		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).
		6. 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 5GB instead of 2GB.
		`[admusr@<pmac_guest> ~]$ /bin/mount`
		`/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)`

Procedure 122.Increase the PMAC NetBackup Files System Size

Step	Procedure	Results
		/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) The second command in this sub-step shows the NetBackup filesystem using 5GB instead of 2GB. [admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv Filesystem Size Used Avail Use% Mounted on /dev/vdd 5.0G 69M 4.3G 1% /usr/openv 7. Change the directory to the **/usr/openv** directory and verify any files contained on the original 2GB NetBackup filesystem are still available on the new 5GB NetBackup filesystem. [admusr@<pmac_guest> ~]$ /bin/ls -l /usr/openv 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

Appendix Q. netConfig backupConfiguration/ restoreConfiguration/upgradeFirmware with TPD Cipher Change

Beginning with TPD 7.6.0.0.0_88.50.0, the cipher list is restricted to allow only a limited number of ciphers for ssh access to the servers. As a result, netConfig backup and restore operations are not functional with Cisco switches (3020, 4948s) since these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown here:

```
[admusr@p5-pmac ~]$ sudo netConfig --device=3020_ip backupConfiguration
service=ssh_ip filename=backup
Command failed: backupConfiguration
Error saving to SSH service
[admusr@p5-pmac ~]$
```

To avoid this issue while maintaining a focus on improved security, the Procedure 123 must be executed before and after netConfig backup and restore operations.

Procedure 123. Turn Off Cipher List Before backupConfiguation/restoreConfiguration/upgradeFirmware Command

STEP #	This procedure prepares the PMAC to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup or restore operations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Error! Reference source not found.** and ask for assistance.	

1. ☐	Turn off cipher list	From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		Add # in the beginning of the following three lines to comment them out, the result is:
		`#Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`#MaxAuthTries 4`
		`#LoginGraceTime 1m`

2. ☐	Restart sshd	`sudo service sshd restart`

3. ☐	Run the netConfig backupConfiguation/restoreConfiguration/upgradeFirmware command	For a backup operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig backupConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a restore operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig restoreConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a upgrade operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig upgradeFirmware --device=<switch_name> service=<ssh_service> filename=<Cisco IOS>`

Procedure 124. Resume Cipher List After backupConfiguation/restoreConfiguration/upgradeFirmware Command

STEP #	This procedure restores the PMAC restricted cipher list after perform the netConfig backup and restore operations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Error! Reference source not found.** and ask for assistance.	

1. ☐	Resume the cipher list	From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		Uncomment the three lines:
		`Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`MaxAuthTries 4`
		`LoginGraceTime 1m`

2. ☐	Restart sshd	`sudo service sshd restart`

Appendix R. 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 are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the 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 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.

Locate Product Documentation on the Oracle Help Center

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 display under the headings N**etwork 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 displays. 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.