Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Installation Procedure

Policy Management
Cloud Installation Guide for Release 12.6.1

F45856-01

April 2022

Oracle ® Communications Policy Management Cloud Installation Guide

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF PROCEDURES

1. INTRODUCTION

1.1 Purpose and Scope

This document describes the process for installation of the virtualized PCRF in various hypervisors. The focus is on the creation and configuration of individual or multiple VM components for deployment in an NFV-I environment. This document does not cover standard product installation and topology configuration, reference other documentation for those purposes.

At the completion of this guide, and assuming that is configured, it is possible to:

- Access the Management interfaces for the Policy System.
- Proceed with topology configuration of the Policy System.

1.2 References

[1] F46327-02—Oracle® Communications Policy Management, Release Notes, Release 12.6.1
[2] F55873-01—Oracle® Communications Policy Management, Network Function Virtualization Update, Release 12.6.1

1.3 Acronyms

An alphabetized list of acronyms used in the document.

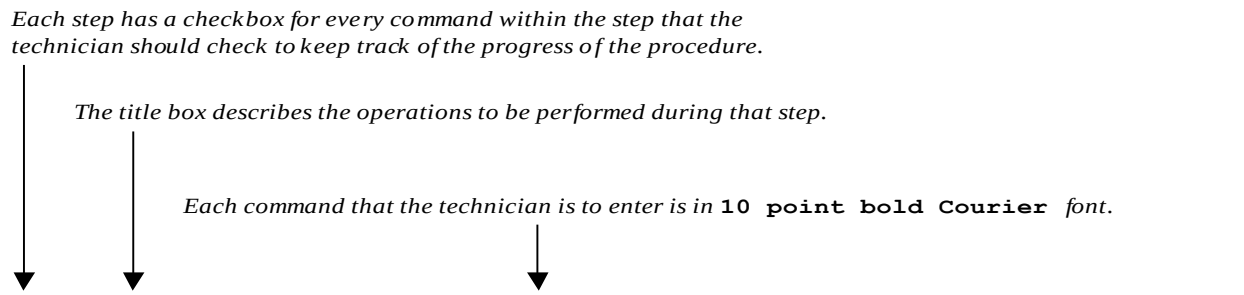
Table 1—Acronyms

Acronym	Definition
CMP	Configuration Management Platform
HOT	Heat Orchestration Template
KVM	Kernel-based Virtual Machine
LVM	Logical Volume Manager
MPE	Multimedia Policy Engine
MRA	Multi-Protocol Routing Agent, also known as the Policy Front End (PFE)
OAM	Operations, Administration and Management
PCRF	Policy and Charging Rules Function—Tekelec MPE
PFE	Policy Front End, also known as the Multi-Protocol Routing Agent (MRA)
NFV	Network Function Virtualization—Using IT virtualization related technologies to virtualize entire classes of network node functions.
NFV-I	NFV-Infrastructure—infrastructure/environment where VNFs are deployed. (including managers OpenStack, Oracle VM-M, vCloud Director)
VIM	Virtual Infrustructure Manager—It is a software is responsible for ensuring that physical and virtual resources work smoothly.
VM	Virtual Machine
VNF	Virtual Network Function—takes on the responsibility of handling specific network functions that run on one or more virtual machines (PCRF)
VNFC	Virtual Network Function Component (CMP, MPE, MRA/PFE VMs)

Acronym	Definition
vNIC	Virtual Network Interface Controller
NAPD	Network Architecture Planning Document.

1.4 Terminology

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



1. ☐	**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`

Figure 1—Instructions Example

Table 2—Terminology

Term	Definition
Configuration Management Platform (CMP)	(CMP) A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.
Guest	The VM running on the host server.
Host	The server where the VM (Guest) is running.
Host Server	The host server is the baremetal server that runs the hypervisor. The host server, via the deployed hypervisor, contains the various virtual machines (VMs) that realize the Policy System. The host server may contain other virtual machines unrelated to the Policy System, however this is outside of the scope of this document.
KVM	A virtualization infrastructure for the Linux kernel that turns it into a hypervisor.
Multimedia Policy Engine (MPE)	A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization
OpenStack	A set of open source software tools for building and managing cloud computing platforms for public and private clouds.

Term	Definition
platcfg	The platform configuration utility used in TPD to configure IP and host values for a server.
Policy Front End (PFE) Also known as the Multi-Protocol Routing Agent (MRA)	Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server (MPE) devices
qcow2	qcow2 is an updated version of the qcow format
vCenter	The VIM product from VMware which is used to create and manage the virtual machines.
vSphere	The hypervisor product from VMware run as a headless operating system which supports virtual machines

2. GENERAL DESCRIPTION

This document defines the steps to perform the initial installation of the Policy Management 12.6.1 application on a supported Cloud platform. For more information see *Network Function Virtualization Update*.

3. INSTALL OVERVIEW

This section provides a brief overview of the recommended method for installing the source release software on a Cloud.

Host hardware, installed hypervisor, and VM management software is understood before starting the install process.

3.1 Required Materials

The image files listed in Table 3 are required for installation of all the Policy Management components. OVA files are required for vShpere/Oracle VM manager installation. QCOW2 files are required for KVM/OpenStack installation. Table 3 represents the complete list of image files for the release.

Table 3—Image Filelist

Planning	
Mapping of virtual machines to host servers	
Mapping of virtual machine vNICs to host networking	
Virtual machine configuration details	
Usernames and passwords for Hypervisors/NFV managers	
Access Permissions for host servers/control nodes	
Software	
Policy Management CMP image	cmp-*xxx*-x86_64.ova cmp-xxx-x86_64.qcow2.tar.bzip2
Policy Management MRA image	mra-*xxx*-x86_64.ova mra-xxx-x86_64.qcow2.tar.bzip2
Policy Management MPE image	mpe-*xxx*-x86_64.ova mpe-xxx-x86_64.qcow2.tar.bzip2
Policy Management MPE-LI image	mpe-li-*xxx*-x86_64.ova mpe-li-xxx-x86_64.qcow2.tar.bzip2

Note: *xxx* in the image file description is the release level information for the image file

3.2 Installation Strategy

Installation of cloud deployable Policy Management requires careful planning and assessment of all configuration materials and installation variables. Among the data that is collected are:

- The mapping of virtual machines to host servers
- The mapping of virtual machine vNIC to host networking
- NAPD containing virtual machine details (VM guest names, IP addresses, and so on)
- The location of the image files that are used to create the virtual machines

3.3 Preparation Checklist

It is important to have all the resources necessary and to have planned as much as possible before beginning the installation process.

Collect the common items regardless of the installation method. Refer to the subsections for specific preparation items that depend on the method of install.

Table 4—Installation Preparation Checklist: Common Items

Check	Item Description
	Mapping of virtual machines to host servers
	Mapping of virtual machine vNIC to host networking
	Policy Management NAPD containing VM guest names, IP address assignments, and so on.
	Username and passwords for each Policy System component
	All necessary software image files

3.3.1 vSphere Checklist

Table 5—Installation Preparation Checklist: vSphere Specific Items

Check	Item Description
	VMware client installed on local machine (for example, a laptop).
	Host username and passwords for access to hypervisor

3.3.2 KVM Checklist

Table 6—Installation Preparation Checklist: KVM Specific Items

Check	Item Description
	KVM host server access (username and password)
	KVM host server file transfer privileges (for example, SSH)
	KVM host server LVM availability and privileges
	Ability to export display (if using virt-manager)

3.3.3 OpenStack Checklist

Table 7—Installation Preparation Checklist: OpenStack Specific Items

Check	Item Description
	OpenStack control node console access (username and password)
	OpenStack control node File transfer privileges (for example, SSH)
	OpenStack control node privileges to upload qcow2 image files
	OpenStack modules available: • Glance • Keystone • Neutron • Nova • Heat
	Horizon GUI tenant username/password
	Heat Template
	The version of Openstack is Liberty or higher

3.3.4 Oracle VM Manager Checklist

Table 8—Installation Preparation Checklist: Oracle VM Manager Specific Items

Check	Item Description
	Oracle VM manager web interface username and password
	OVA files available and accessible to the Oracle VM manager via URL

4. INSTALLATION PRODEDURES

Installation procedures are divided into the following sections:

- VMware specific procedures

  Used when the hypervisor that hosts the Policy Management VMs is VMware vSphere version 6.5 or greater.

- KVM specific procedures

  Used when the hypervisor that hosts the Policy Management VMs is KVM version 1.5.3 or greater.

- OpenStack specific procedures

  Used when OpenStack is used to install Policy Management VMs on different computer nodes (hosts).

- Oracle VM server specific procedures

  Used when Oracle VM-M is used to install Policy Management VMs on different Oracle VM-S servers.

- Common procedures

  Used regardless of the hypervisor that hosts the Policy Management VMs.

Figure 2 represents the expected flow of installation processes.

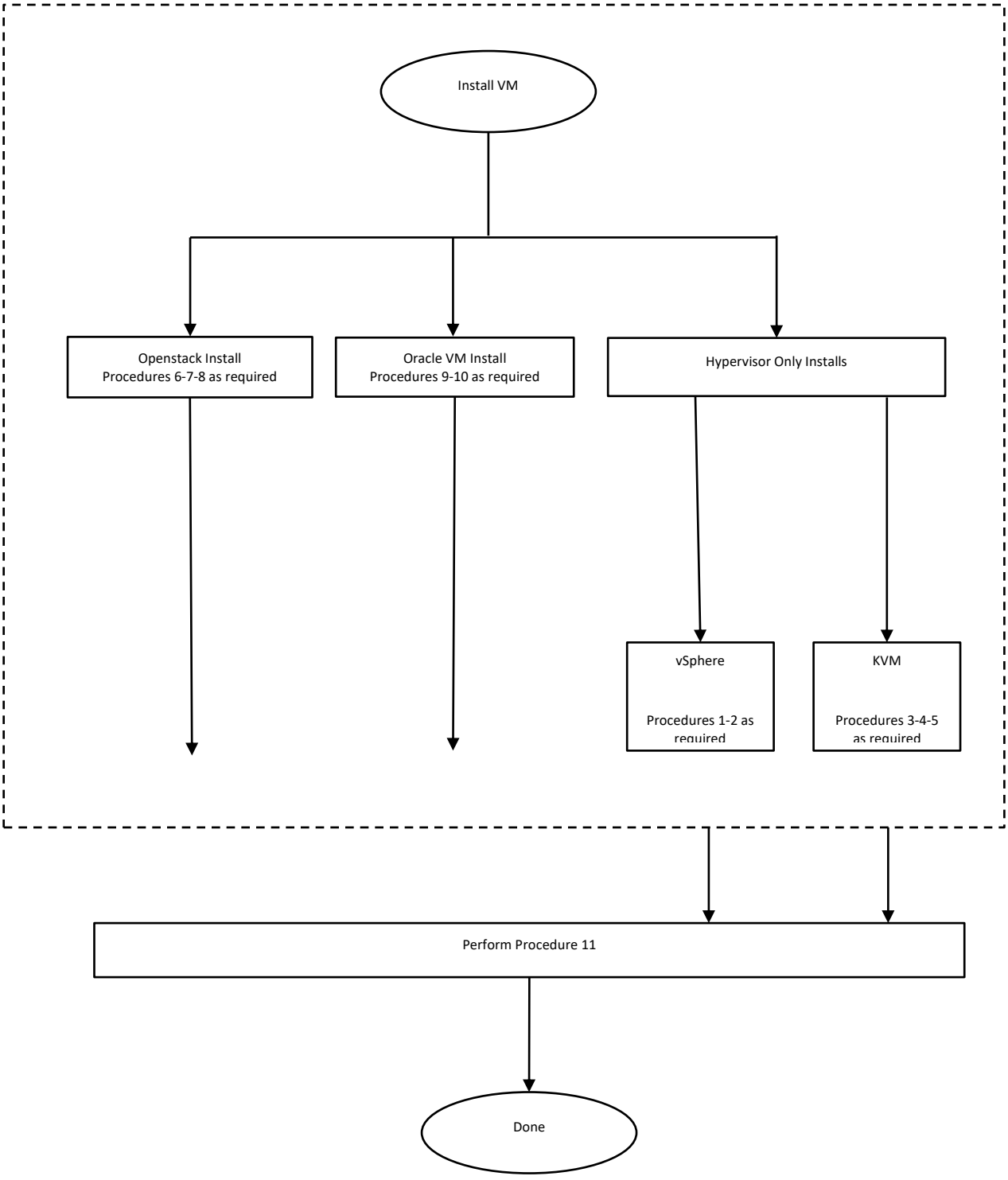


Figure 2—Policy Management VM Installation Process

4.1 vSphere Installation Procedures

vSphere installation procedures are tailored to work with VMware vSphere. The procedures that are used depend upon the unique characteristics of the install that is being performed. Figure 3 shows the order and the dependencies for each host server that contains at least one Policy Management VM.

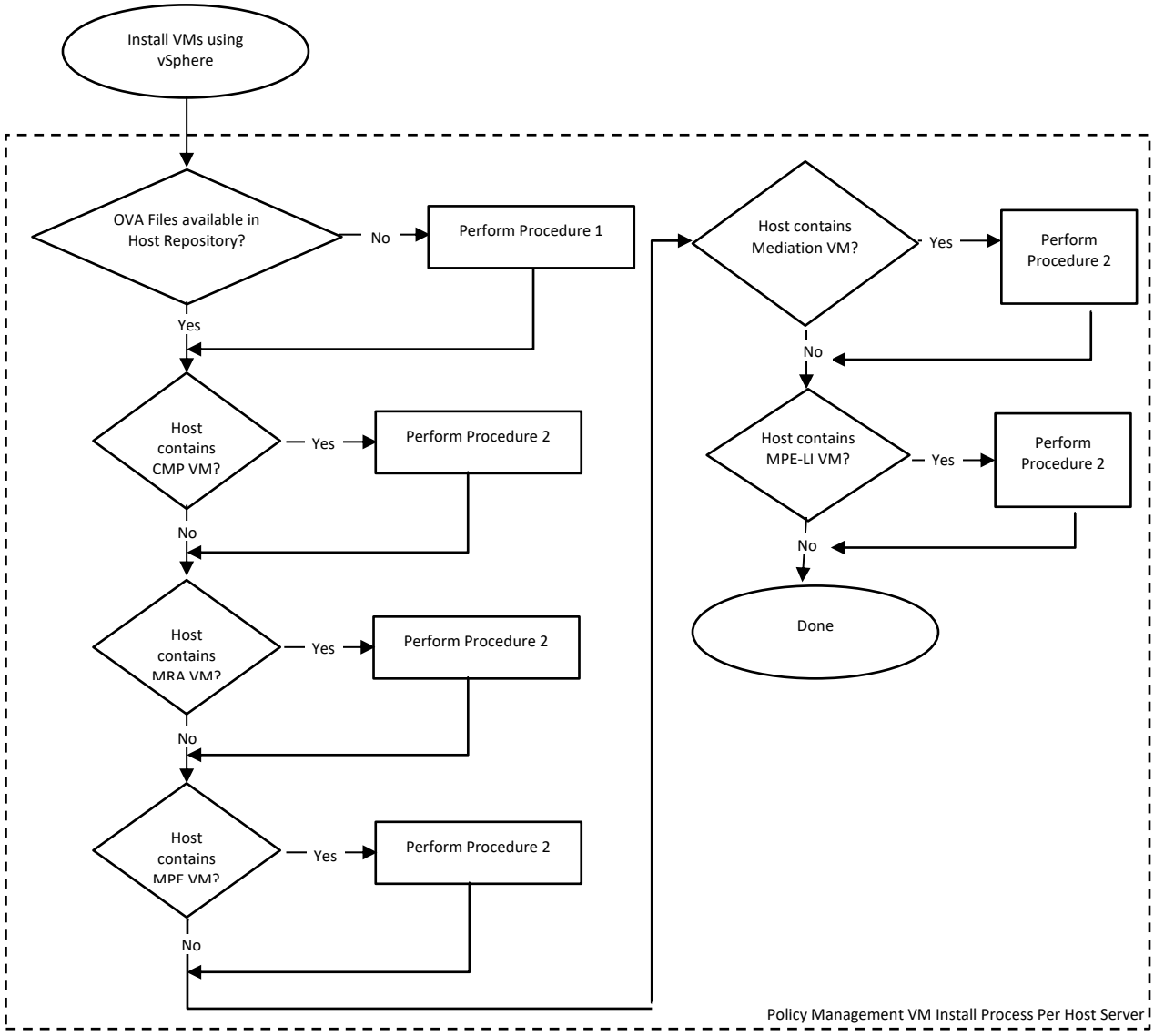


Figure 3—VMware vSphere Installation Process

4.1.1 Procedure 1—Import Policy Management OVA

This procedure adds the necessary Policy Management OVA files to the VMware catalog or repository. The procedure requires that Policy Management OVA files is placed into the catalog for the host or repository.

- If host servers use a shared repository for hosting OVA images, then it is likely that all Policy Management OVA files are hosted in that repository.
- If host servers have private repositories, then this procedure requires only that Policy Management OVA files that are associated with the Policy Management VM created on the particular host server are added to the private repository.

At the end of this procedure, all host servers that host a Policy Management VM have access to the Policy Management OVA files necessary to create Policy Management VMs.

Required materials:

- VMware vSphere client
- VMWare vSphere host server username snd password
- Mapping of Policy Management components to host servers
- Policy Management OVA files

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 1 Import Policy Management OVA

Step	Procedure	Details
1. ☐	Add Policy Management OVA files to host server	1. Launch the VMware vSphere client of your choice 2. Connect to the target VMware vSphere host via the VMware vSphere client. 3. Add each Policy Management OVA image to the VMware vSphere catalog or repository if the host server is to deploy an instance of the Policy Management OVA image
2. ☐	Repeat for all host servers	Repeat Step 1 for each VMware vSphere host server that hosts a Policy Management VM. **NOTE:** If a common repository is used, then tdo not repeat this procedure for each VMware host server.
---End of Procedure---		

4.1.2 Procedure 2—Create and Configure Policy Management VM

This procedure creates an instance of the Policy Management VM based on the Policy Management OVA file and configured with the resource profile described in Appendix A.

At the end of this procedure, all Policy Management VMs have been:

- Created based on the Policy Management OVA file
- Configured with the resource profile
- Mapped to the network resource for the host based on the Policy Management NAPD
- Powered on

Required materials:

- VMware vSphere client
- VMWare vSphere host server username and password
- Mapping of Policy Management components to host servers
- Mapping of virtual machine vNICs to host networking
- Policy Management NAPD

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 2 Create and Configure Policy Management VM

Step	Procedure	Details
1. ☐	Login to VMware host	1. Launch the VMware vSphere client of your choice 2. Connect to the target VMware vSphere host via the VMware vSphere client
2. ☐	Create the Policy Management VM	1. Browse the catalog or repository where the Policy Management OVA image is located and select the Policy Management OVA image a. The Policy Management OVA image varies depending on the Policy Management component being installed. 2. Create the Policy Management VM using the Policy Management OVA image a. Name the Policy Management VM instance based upon the agreed upon VM name for the Policy Management component as defined by the Policy Management NAPD. b. Select the datastore where the VM image is stored.
3. ☐	Configure the resources for the Policy Management VM	1. Configure the Policy Management VM according to the resource profile defined in Appendix A for the Policy Management component. 2. Map the vNICs for the VM to host networking. Use the Policy Management NAPD to determine the mapping between the Policy Management VM instance and the Network resource for the host.
4. ☐	Power on the Policy Management VM	1. Use the VMware vSphere client to Power On the Policy Management VM. 2. Verify the Policy Management VM powered on
5. ☐	Repeat For Each Policy Management VM	Repeat steps 1 through 4 for each Policy Management VM
---End of Procedure---		

4.2 KVM Installation Procedures

KVM installation procedures are tailored to work with the KVM hypervisor running on Linux. The procedures that are used depend upon the unique characteristics of the install that is being performed. Figure 4 shows the order and the dependencies for each host server that contains at least one Policy Management VM.

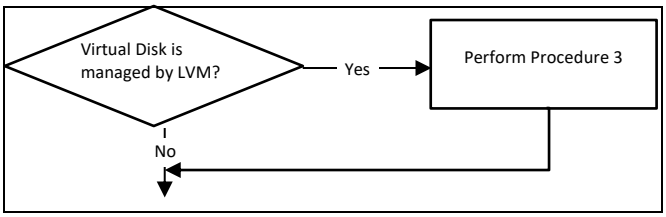


Figure 4—KVM Installation Process

4.2.1 Procedure 3—Configure LVM Disk Storage For KVM VMs

This procedure describes how to use LVM to manage disk storage for the KVM VM.

At the end of this procedure, you will have:

- Created LVM disk storage for each KVM VM
- Mounted LVM to storage directory for the VM.

Required materials:

- Linux host server username and password
- Capability to create directory on host servers
- Capability to create physical volume(pv), volume group(vg), and logical volume(lv) on host servers
- Capability to format file system
- Capability to mount LVM device

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 3 Configure LVM disk storage for KVM VMs

Step	Procedure	Details
1. ☐	Create physical Volume	Create physical volume on the suitable disk partition of host server. **Example** `$ pvcreate /dev/sda3` Where `/dev/sda3` is an example of disk partition.
2. ☐	Create Volume Group	Create Volume group on the physical volume **Example** `$ vgcreate vgguests /dev/sda3` Where: • `vgguests` is the volume group name • `/dev/sda3` is the physical volume created in step 1.

Step	Procedure	Details
3. ☐	Create Logical Volume for KVM VM	Create LVM partition and add it to a volume group. **Example** `$ lvcreate -n mpe9 -L 108G vgguests` Where: • `mpe9` is name of the VM • `108G` is the disk storage size for the VM • `vgguests` is the vg created in step2. **NOTE:** For PCRF product, the disk storage must be 108G.
4. ☐	Format LV to ext4	**Example** `$ mkfs.ext4 /dev/vgguests/mpe9`
5. ☐	Create mont point of LVM	Create a directoy to store data for the VM. **Example** `$ mkdir /home/VM-hosts/mpe9`

6. ☐	Get the UUID of LV	**Example**
		`$ blkid /dev/vgguests/mpe9`
		You receive a response result similar to:
		`/dev/vgguests/mpe9: UUID="8babcea9-36b3-4fee-838a-3f0aa2312997" TYPE="ext4"`

7. ☐	Add the LVM file system info to /etc/fstab	**Example**
		`$ vi /etc/fstab`
		Add this line to the end of the file:
		`UUID=8babcea9-36b3-4fee-838a-3f0aa2312997 /home/VM-hosts/mpe9 ext4 defaults 0 0`

8. ☐	Mount the LV device to the designated directory	**Example**
		`$ mount -a`
		Or
		`$ mount`
		You receive a response result similar to:
		`/dev/mapper/vgguests-mpe9 on /home/VM-hosts/mpe9 type ext4 (rw,relatime,seclabel,stripe=128,data=ordered)`

9. ☐	Repeat for all host servers	Repeat steps 1 through 8 for each KVM host server that hosts a Policy Management VM.
---End of Procedure---		

4.2.2 Procedure 4—Upload Policy Management QCOW2 Image

This procedure adds the necessary Policy Management QCOW2.tar.bzip2 files to the host running the KVM hypervisor, and then decompress to the QCOW2 format required by KVM.

- If the host server is using a shared repository, then the location of the directory referencing the connected network storage must be known as well as the location where source QCOW2 files are to stored.
- If the host server is using a local repository, then the local directory where KVM hosts VMs must be known as well as the location where source QCOW2 files are stored.

At the end of this procedure, all host servers that hosts a Policy Management VM has access to the Policy Management QCOW2 files necessary to create Policy Management VMs.

Required materials:

- Linux host server username and password
- Capability to transfer files to the host server or Shared Repository
- Capability to decompress (unpack) tar.bzip2 file
- Mapping of Policy Management components to host servers
- Policy Management CMP QCOW2.tar.bzip2 file
- Policy Management MRA QCOW2.tar.bzip2 file
- Policy Management MPE QCOW2.tar.bzip2 file
- Policy Management MPE-LI QCOW2.tar.bzip2 file

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 4 Upload Policy Management QCOW2 Image

Step	Procedure	Details
1. ☐	Add Policy Management qcow2.tar.bzip2 files to host server	For each Policy Management VM component type that the host server is to deploy, SCP (or otherwise transfer) the corresponding Policy Management qcow2.tar.bzip2 image to the identified directory on the host server where images are stored.
2. ☐	Extract QCOW2 files from qcow2.tar.bzip2 files	1. Login (SSH) to the host server 2. For each Policy Management VM component type that the host server is to deploy: a. Navigate to the directory where the Policy Management qcow2.tar.bzip2 file was transferred b. Uncompress the image template using tar. **Example** `$ tar -jxvf <filename>.qcow2.tar.bzip2`
3. ☐	Repeat for all host servers	Repeat steps 1 through 2 for each KVM host server that hosts a Policy Management VM. **NOTE:** If a common repository is used, do not repeat this procedure for each KVM host server.
---End of Procedure---		

4.2.3 Procedure 5—Create and Configure Policy Management VM

This procedure creates an instance of the Policy Management VM based on the corresponding Policy Management QCOW2 file and configured with the resource profile described in Appendix A.

At the end of this procedure, all Policy Management VMs have been:

- Created based on the corresponding Policy Management QCOW2 file
- Configured with the resource profile
- Mapped to the network resource for the host based on the Policy Management NAPD
- Powered on

Required materials:

- Linux host server username and password
- Ability to export the host server display (XHost)
- Capability to run virt-manager
- Mapping of Policy Management components to host servers
- Mapping of virtual machine vNICs to host networking
- Policy Management NAPD

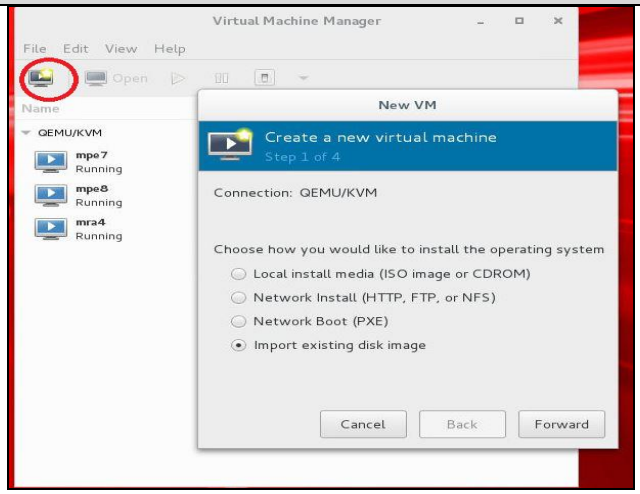
Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

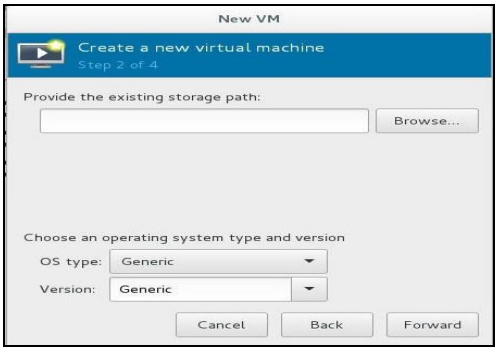
Procedure 5 Create and Configure Policy Management VM

Step	Procedure	Details
1. ☐	Login to KVM host	1. Login (SSH) to the host server 2. Launch the virt-manager GUI interface. `$ virt-manager` **NOTE:** Because this is a graphical user interface, the display must be exported to the client machine that is accessing the server. In addition, the username that is provided to access the KVM host must also be a member of the libvirt group.
2. ☐	Create the Policy Management VM	1. Create the Policy Management VM using the corresponding Policy Management QCOW2 image 2. Name the Policy Management VM instance based upon the agreed upon VM name as defined by the Policy Management NAPD. 3. Select the existing disk image as the <*qcow2 filename*>.qcow2 image. The detailed steps: 1. Click the Create icon to create a virtual machine or navigate to **File → New Virtual Machine** 2. Check Import existing disk image then click **Forward**.

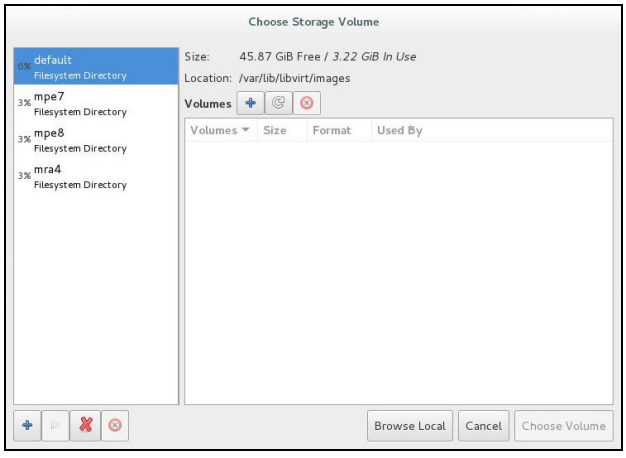
Step	Procedure	Details



3. Click **Browse** to select volume storage and then click **Forward**.



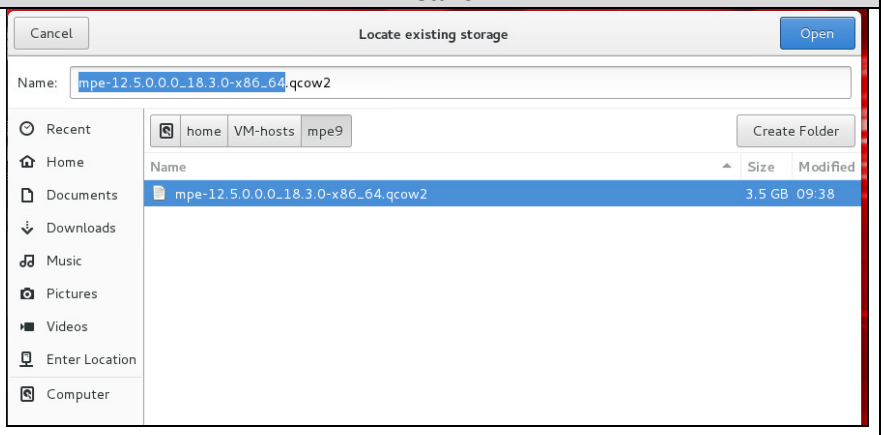
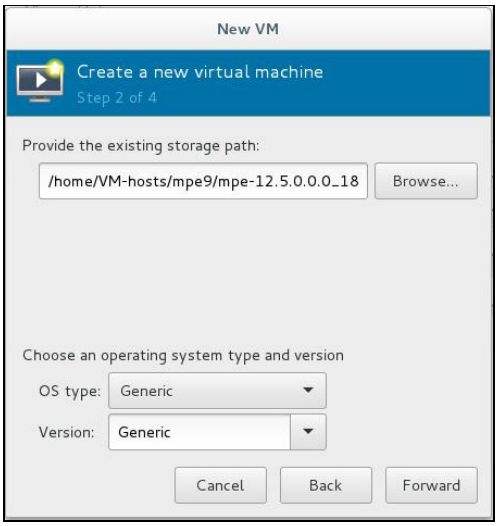
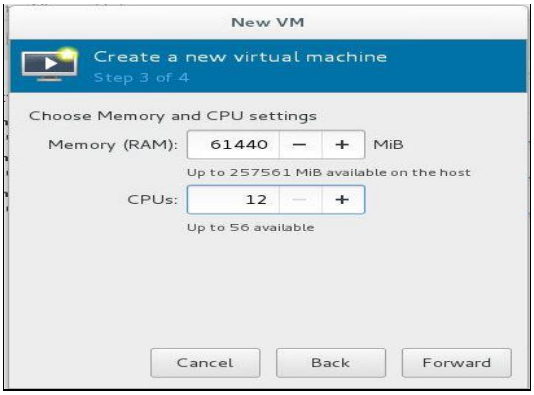
4. Click **Browse Local**.



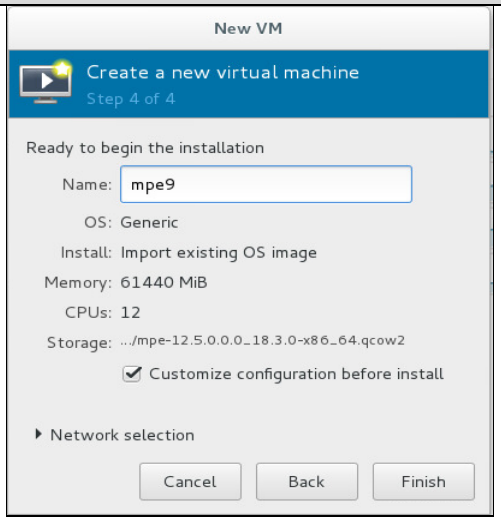
5. Navigate to where the qcow2 file is located.

   NOTE: Before this step, The qcow2 file must be copied to the directory where the VM files are stored, for example, `/home/VM-hosts/mpe9`

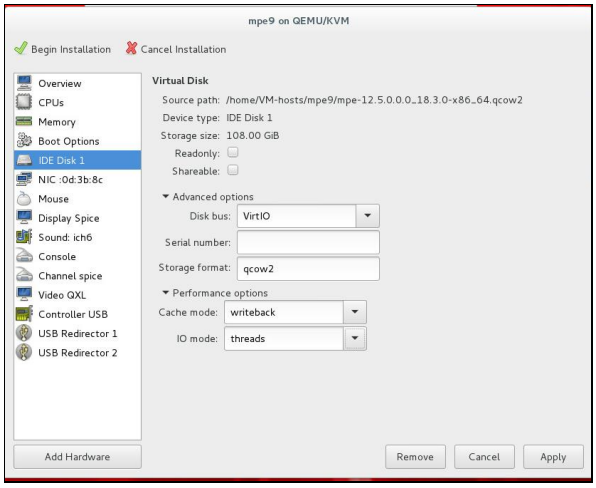
6. Click **Open** to return to previous page.

Step	Procedure	Details
		 7. Click **Forward** to configure the VM 
3. ☐	Configure the resources for the Policy Management VM	1. Configure the Policy Management VM according to the resource profile defined in Appendix A for the Policy Management component type. 2. Set RAM and CPUs according to the resources profile.  3. Enter the name of the VM and select **Customize configuration before install.** 4. Click **Finish**.

Step	Procedure	Details

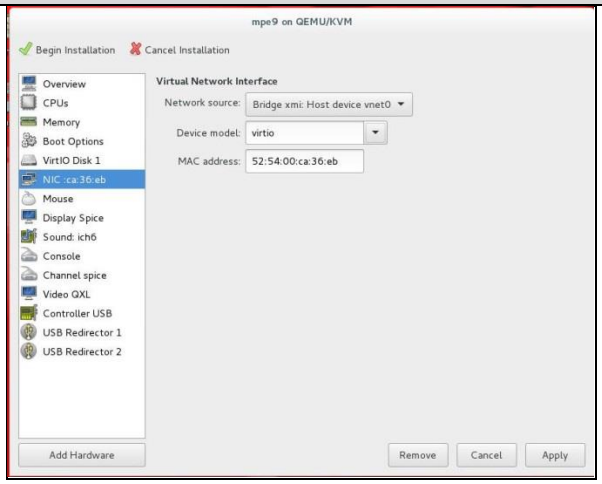


5. Select **IDE Disk 1** and change:
   - Disk bus to **VirtIO**
   - Cache mode to **writeback**
   - IO mode to **threads**
6. Click **Apply**.



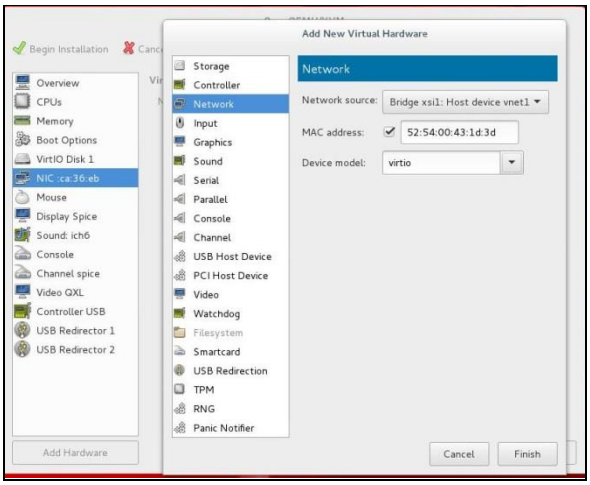
7. Map the vNICs for the VM to host networking. Use the Policy Management NAPD to determine the mapping between the Policy Management VM instance and the Network resource for the host.
8. Change the default virtual network interface Device model to **virtio**
9. Click **Apply**.

Step	Procedure	Details

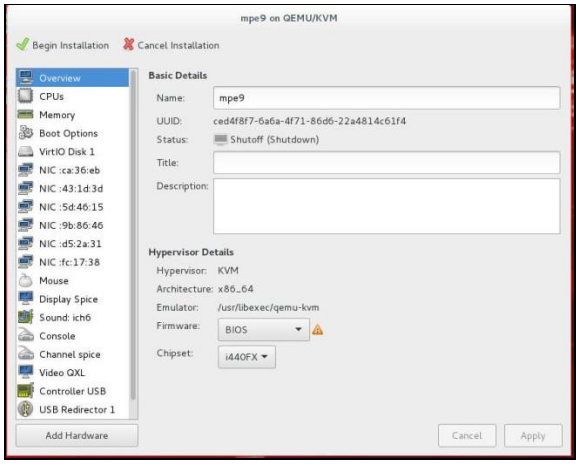


10. Click **Add Hardware** and add 5 more network interfaces.
11. Click **Finish**.

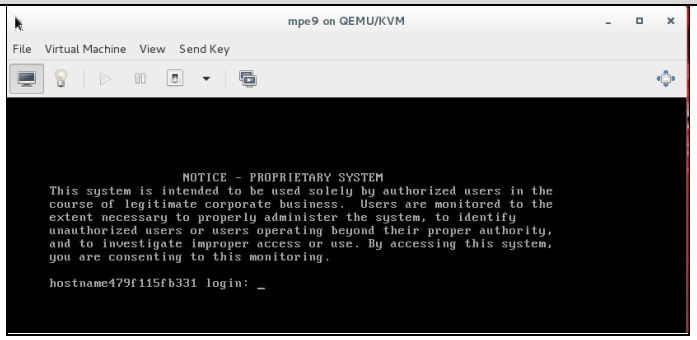
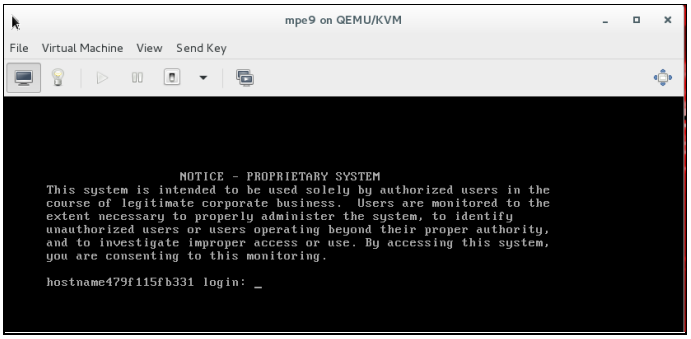
NOTE: The device Model is virtio.



12. Verify that six vNICs are added and click **Begin Installation** to launch VM.



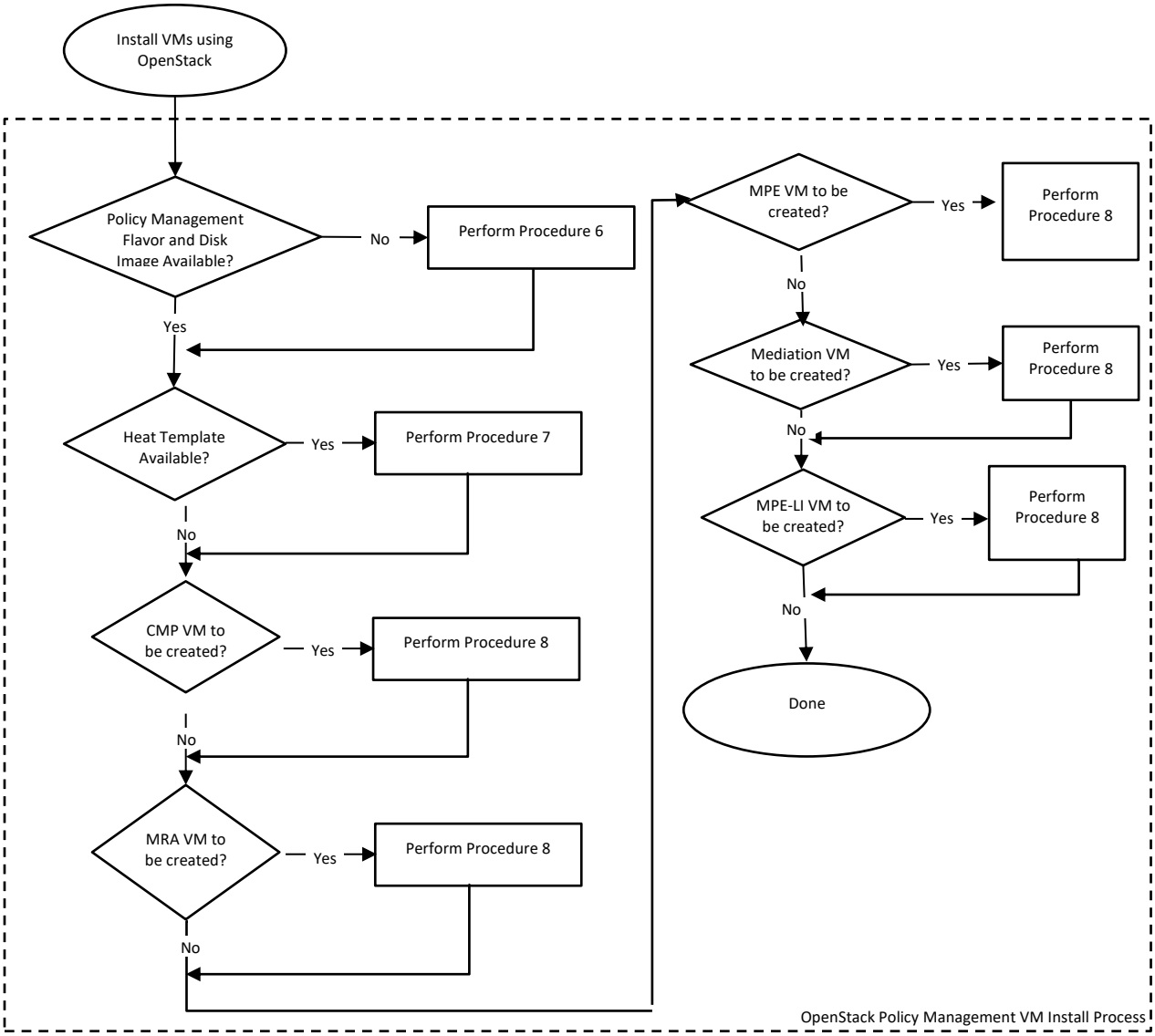
VM installation finishes.

Step	Procedure	Details
		
4. 6	Power on the Policy Management VM	1. Use the virt-manager client to Power On the Policy Management VM. 2. Verify the Policy Management VM is powered on. After the VM is powered, the VM is listed. 
5. ☐	Repeat For Each Policy Management VM	Repeat steps 1 through 4 for each Policy Management VM
---End of Procedure---		

4.3 OpenStack Installation Procedures

OpenStack installation procedures are tailored to work with OpenStack. Procedures are performed on the OpenStack control node. Since OpenStack installations may vary, this procedure assumes that the OpenStack installation has these core services available:

- Glance
- Keystone
- Neutron
- Nova
- Heat



In addition, the Horizon GUI is used for certain VM instance and profile configuration items.

Figure 5—OpenStack Policy Management VM Install Process

4.3.1 Procedure 6—Create flavor/image/network/availability_zone In OpenStack

This procedure describes how to create flavor/image/network/availability_zone for OCPM VM creation.

At the end of this procedure, the necessary Policy Management qcow2 files are imported to the Glance image catalog for the OpenStack control node. And the flavor/image/network/availability_zone are ready for VM creation.

Required materials:

- OpenStack control node administration username and password
- Horizon GUI Policy Management tenant username and password
- Capability to transfer files to the OpenStack control node
- Capability to unpack qcow2.tar.bzip2 files on the OpenStack control node
- Capability to create flavor/image/network/availability_zone on the OpenStack control node
- Policy Management CMP, MRA, MPE, and MPE-LI qcow2.tar.bzip2 files

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 6 Create flavor/image/network/availability_zone In OpenStack

Step	Procedure	Details
1. ☐	Create Policy Management VM Instance Flavors	Create instance flavors Use the resource profile information in Appendix A to create flavors for each type of VM. Flavors are created with the Horizon GUI in the Admin section, or with the **`nova flavor-create`** command line tool. Make the flavor names as informative as possible. **Example** `$ nova flavor-create pcrf auto 61440 108 12` Where: • `pcrf` is the flavor name. • vCPU is `12` • RAM is `60G` • Storage is `108G`

2. ☐	Copy qcow2.tar.bzip2 files to OpenStack Control Node	Copy the qcow2.tar.bzip2 file to the OpenStack Control Node
		
		Example
		
		`$ scp cmp-xxx-x86_64.qcow2.tar.bzip2 admusr@controller:~`
		`$ scp mra-xxx-x86_64.qcow2.tar.bzip2 admusr@controller:~`
		`$ scp mpe-xxx-x86_64.qcow2.tar.bzip2 admusr@controller:~`
		`$ scp mpe-li-xxx-x86_64.qcow2.tar.bzip2 admusr@controller:~`
		
		Where *xxx* is the release level information for the qcow2.tar.bzip2 file.

Step	Procedure	Details

3. ☐	Unpack the qcow2.tar.bzip2 files	1. Login (SSH) to the OpenStack Control Node
		Example
		`$ ssh admusr@controller`
		2. In an empty directory unpack the qcow2.tar.bzip2 files using the **`tar`** command.
		a. Navigate to the directory where the Policy Management CMP, MPE, MRA, or MPE-LI qcow2.tar.bzip2 file was uploaded
		b. Uncompress (unpack) the OCPM qcow2.tar.bzip2 files
		Example
		`$ tar -jxvf cmp-xxx-x86_64.qcow2.tar.bzip2`
		`$ tar -jxvf mra-xxx-x86_64.qcow2.tar.bzip2`
		`$ tar -jxvf mpe-xxx-x86_64.qcow2.tar.bzip2`
		`$ tar -jxvf mpe-li-xxx-x86_64.qcow2.tar.bzip2`
		Where *xxx* is the release level information for the ova file.
		3. One of the unpacked files for each tar.bzip2 file has a qcow2 extension. This is the VM image file that is imported to openstack.
		For example: cmp-*xxx*-x86_64.qcow2
		Where *xxx* is the release level information for the qcow2 file.

4. ☐	Import the qcow2 images into Glance	Create instance images.
		Image is created with the Horizon GUI in the Admin section, or with the **`glance image-create`** command line tool. Make the image names as informative as possible.
		1. Source the OpenStack admin user credentials:
		`$ . keystonerc_admin`
		2. Import each Policy Management disk image (qcow2) using the **`glance`** utility from the command line.
		NOTE: The name attribute sets the name in the glance repository. In the example, the same name was selected as the qcow2 image name, without the qcow2 extension.
		This process takes several mins, depending on the underlying infrastructure.
		Example
		`$ glance image-create -name cmp-xxx-x86_64 --disk-format qcow2 --container-format bare --visibility public --file /image_directory/cmp-xxx-x86_64.qcow2`

Step	Procedure	Details

5. ☐	Create Network for Policy Management VM Instance	Create an instance for the networks.
		
		Use the network information in Appendix A to create OAM/SIGA/SIGB/SIGC/REP/BKUP network for OCPM VM. Network is created with the Horizon GUI in the Admin section, or with the **`neutron net-create and neutron subnet-create`** command line tool. Make the network names as informative as possible.
		
		Example
		
		`$ neutron net-create --provider:segmentation_id <segmentation_id> --provider:network_type <network_type> --provider:physical_network <physical_network_name> NAME`
		
		`$ neutron subnet-create --gateway GATEWAY_IP --name NAME NETWORK [CIDR]`
		
		Notes:
		
		• *<segmentation_id>* is VLAN ID for VLAN networks or tunnel-id for GRE/VXLAN networks.
		• *<network_type>* is the physical mechanism by which the virtual network is implemented.
		• *<physical_network_name>* is Name of the physical network over which the virtual network is implemented.
		• *NAME* is the name of the network or subnet.
		• *GATEWAY_IP* is the Gateway IP of this subnet.
		• *NETWORK* is the Network ID or name this subnet belongs to.
		• *CIDR* is the CIDR of subnet to create.
		
		Repeat step 5 for all other networks

6. ☐	Create availability zone for Policy Management VM Instance	Create availability zone for instances
		
		Availability zone is created with the Horizon GUI in the Admin section, or with the **`openstack aggregate create`** and **`openstack aggregate add host`** commands. Make the availability zone name as informative as possible.
		
		Example
		
		`$ openstack aggregate create --zone <availability-zone> <name>`
		
		`$ openstack aggregate add host <aggregate> <host>`
		
		The first command is to create an availability zone
		
		• where *<availability-zone>* is availability zone name and *<name>* is the aggregate name.
		
		The second command is to adding one host server to the zone
		
		• where *<aggregate>* is Aggregate (name or ID) and *<host>* is the host to add to *<aggregate>*.

---End of Procedure---		

4.3.2 Procedure 7—Create and Configure Policy Management VM using Heat Template

This procedure creates all the Policy Management VMs based on a heat template.

At the end of this procedure, all Policy Management VMs have been:

- Created based on:
  - The Policy Management flavor for the Policy Management component type
  - The Policy Management qcow2 file for the Policy Management component type
- Mapped to the network resource for the host based on the Policy Management NAPD
- Powered on
- Policy Mode and virtual machine are complete

Required materials:

- OpenStack control node administration username and password
- Horizon GUI Policy Management tenant username and password
- Mapping of Policy Management components to host servers
- Mapping of virtual machine vNICs to host networking
- Policy Management NAPD

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

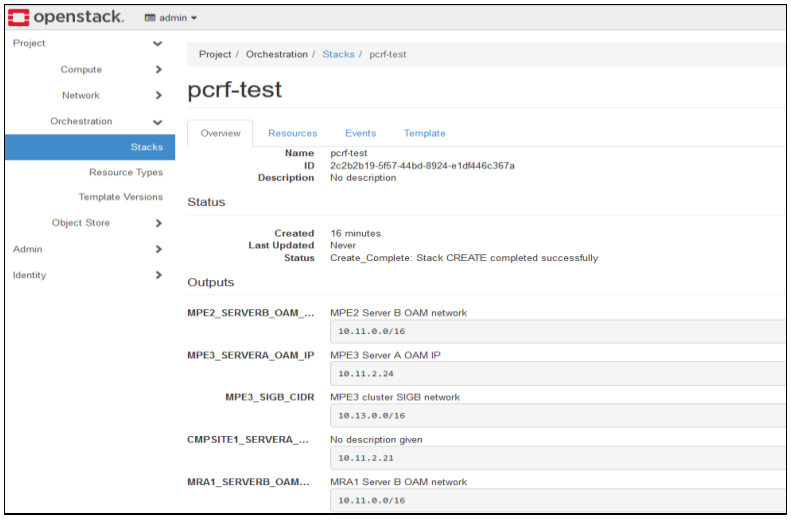
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 7 Create and Configure Policy Management VM using Heat Template

Step	Procedure	Details
1. ☐	Prepare Heat Template	Collect information for the heat template. - Mapping of network, for example network names for OAM, SIGA, SIGB, SIGC, REP and BKUP. - Whether we can use DHCP for all IPs? - Whether we need to use fixed IP for MRAs? - Whether prevent_arp_spoofing is True? If so, we must use VRRP (allowed address pair) in heat for VIPs. - If the user_data and cloudinit for initial-config is used? - Image/availability zone/flavor/ntp/mimode? **Example** Download the example from the Oracle Help Center (yaml example) In the template, it describes 1 CMP cluster, 3 MPE clusters and 2 MRA clusters, there are 2 VMs in each cluster named with xxx_SERVERA and xxx_SERVERB. Modify the example heat template based on your openstack configuration.

Step	Procedure	Details

2. ☐	Create Stack	Create stack for all Policy Management VMs
		
		Heat stack is created with the Horizon GUI in the **Project->Orchestration->Stacks** section, or with the **`heat stack create`** command line tool. Make the stack name as informative as possible.
		
		1. Source the OpenStack admin user credentials:
		`$ . keystonerc_admin`
		
		2. Create stack using the **`heat`** utility from the command line.
		
		This process takes several mins, depending on the underlying infrastructure.
		
		Example
		`$ heat stack-create pcrf-test -f pcrf-heat-example.yaml`

Step	Procedure	Details
3. ☐	Check Stack Information	Create stack Information. After creation, run the **`heat stack-show`** command to get the IP addresses allocated from OpenStack. **NOTE:** IP addresses are used in topology configuration. **Example** `$ heat stack-show pcrf-test`  The heat stack is also created from OpenStack dashboard web UI. In that case, the output is viewed in the Overview page: 
4. ☐	Set Policy Mode and Perform Initial Config	The policy mode and initial configuration is automatically performed for every VM if configuring user data in a heat template. Section 4.5 describes how to manual configure or use CLI mode to double check the configuration.

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>5. ☐</td><td>Configure Topology</td><td>Refer to step 3 for IP addresses. for example:
<table>
<tr><th>Key name</th><th>Description</th></tr>
<tr><td>CMPSITE1_OAM_IP</td><td>CMP OAM VIP</td></tr>
<tr><td>CMPSITE1_SERVERA_OAM_IP</td><td>CMP Server A OAM IP</td></tr>
<tr><td>CMPSITE1_SERVERB_OAM_IP</td><td>CMP Server B OAM IP</td></tr>
<tr><td>MPE1-1-1_SERVERA_OAM_IP</td><td>MPE1-1, Server A OAM IP</td></tr>
<tr><td>MPE1-1-1_SERVERB_OAM_IP</td><td>MPE1-1,Server B OAM IP</td></tr>
<tr><td>MPE1-1-1_SIGA_IP</td><td>MPE 1-1, SIGA VIP</td></tr>
<tr><td>MRA1-1_SERVERA_OAM_IP</td><td>MRA 1-1, Server A OAM IP</td></tr>
<tr><td>MRA1-1_SERVERB_OAM_IP</td><td>MRA 1-1, Server B OAM IP</td></tr>
<tr><td>MRA1-1_SIGA_IP</td><td>MRA 1-1, SIGA VIP</td></tr>
</table>
</td></tr>
<tr><td>6. ☐</td><td>(Optional) Update Network Resource, such as IPs</td><td>If there is an IP change or VM change, you must update the heat template.

It is not necessary to rebuild everything, the heat stack is updated either from the OpenStack dashboard or using the <code>heat stack-update</code> CLI command.</td></tr>
<tr><td colspan="3">---End of Procedure---</td></tr>
</table>

4.3.3 Procedure 8—Create and Configure Policy Management VM

This procedure creates an instance of a Policy Management VM based on the Policy Management flavor that was based on the resource profile described in Appendix A, and the imported Policy Management qcow2 file.

At the end of this procedure, all Policy Management VMs have been:

- Created based on:
  - The Policy Management flavor for the Policy Management component type
  - The Policy Management qcow2 file for the Policy Management component type
- Mapped to the network resource for the host based on the Policy Management NAPD
- Powered on

Required materials:

- OpenStack control node administration username and password
- Horizon GUI Policy Management tenant username and password
- Mapping of Policy Management components to host servers
- Mapping of virtual machine vNICs to host networking
- Policy Management NAPD

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 8 Create and Configure Policy Management VM

Step	Procedure	Details

1. ☐	Create and boot the Policy Management VM Instance from the glance image	1. Source the admin user credentials
		`$ . /root/keystonerc_admin`
		2. Get the configuration values for the Policy Management component type
		a. The image ID
		`$ glance image-list`
		b. The flavor ID
		`$ nova flavor-list`
		c. The network IDs
		`$ neutron net-list`
		d. The availability zone to use (identifying the zone to use for the Policy Management VM)
		`$ openstack availability zone list`
		e. The hypervisor list (identifying the compute node to use for the Policy Management VM). This is optional only if the compute node is static for the instance.
		`$ nova hypervisor-list`
		f. An informative name for the instance (from the Policy Management NAPD). The instance name selected is also the hostname of the Policy

Step	Procedure	Details

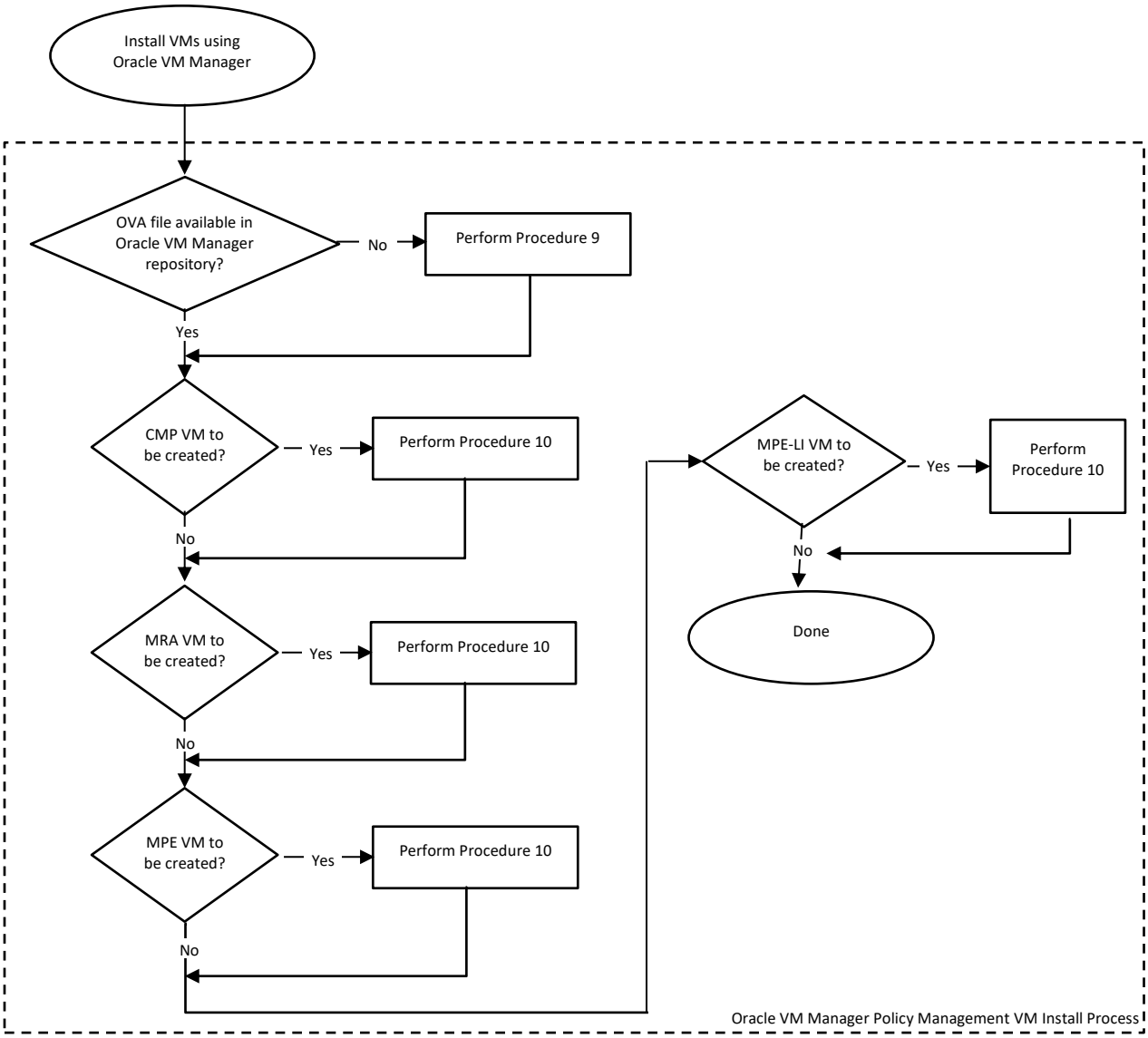
		Management VM.
		3. Create and boot the VM instance
		The instance is owned by the Policy Management tenant user, not the admin user. Source the credentials of the Policy Management tenant user and issue the following command. Use one nic argument for each IP/interface.
		NOTE: IPv6 addresses use the v6-fixed-ip argument instead of the v4-fixed-ip argument.
		`$ nova boot --image <image ID> --flavor <flavor ID> --availability-zone <ZONE[:NODE]> --nic net-id=<first network ID>[,v4-fixed-ip=<first ip address>] --nic net-id=<second network id>[,v4-fixed-ip=<second ip address>] <instance name>`
		NOTE:
		- the <*instance name*> is the hostname of the VM
		- [:NODE] is optional and used if the host server is specifically assigned to the instance
		- [,v4-fixed-ip….] is optional and only necessary if assigning an IP to the interface
		- All interfaces listed in Appendix A are included in the **`nova boot`** command with a nic option.
		4. View the instance using the **`nova`** tool
		`$ nova list --all-tenants`
		The VM takes approximately 5 minutes to boot and is accessed through both network interfaces and the Horizon console tool.

2. ☐	Configure VIP (optional)	If a VIP is required on an interface, then perform the following steps.
		1. Find the port ID associated with the interface for the VM instance that is requires a VIP
		`$ neutron port-list`
		2. Add the VIP address to the address pairs list of the interface port for the Policy Management VM instance.
		`$ neutron port-update <port ID> --allowed-address-pairs list=true type=dict ip_address=<VIP address >`

3. ☐	Repeat For Each Policy Management VM	Repeat steps 1 and 2 for each Policy Management VM.
---End of Procedure---		

4.4 Oracle VM Manager Installation Procedures

Oracle VM manager procedures are tailored to work with Oracle VM manager. Procedures are performed using the Oracle VM manager web interface. Figure 6 shows the order and the dependencies of



performing the install using Oracle VM manager.

Figure 6—Oracle VM Manager Policy Management VM Install Process

4.4.1 Procedure 9—Upload Policy Management OVA Files

This procedure adds the necessary Policy Management OVA files to Oracle VM manager.

At the end of this procedure, the Policy Management OVA files are stored and available in the Oracle VM manager repository.

Required materials:

- Oracle VM manager web interface username and password
- OVA Files available and accessible to the Oracle VM manager via URL.

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 9 Upload Policy Management OVA Files

Step	Procedure	Details
1. ☐	Login to Oracle VM manager Web interfacw	Login to the Oracle VM manager web interface
2. ☐	Add Policy Management OVA files to Oracle VM manager	Transfer each applicable Policy Management OVA file to the Oracle VM manager. **NOTE:** Do not create the VM as part of the transfer. VM instances are created in subsequent procedures.
---End of Procedure---		

4.4.2 Procedure 10—Create and Configure Policy Management VM

This procedure creates an instance of the Policy Management VM based on the Policy Management OVA file and configured with the resource profile described in Appendix A.

At the end of this procedure, all Policy Management VMs have been:

- Created based on the Policy Management OVA file
- Configured with the resource profile
- Mapped to the network resource for the host based on the Policy Management NAPD
- Each Policy Management VM has been powered on

Required materials:

- Oracle VM manager web interface username and password
- OVA file available in the Oracle VM manager Repository
- Mapping of Policy Management components to host servers
- Mapping of virtual machine vNICs to Networking
- Policy Management NAPD

Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 10 Create and Configure Policy Management VM

Step	Procedure	Details
1. ☐	Login to Oracle VM manager web interface	Login to the Oracle VM manager web interface
2. ☐	Create the Policy Management VM	Create the the Policy Management VM using the corresponding Policy Management qcow2 or OVA image that was uploaded to the Oracle VM manager repository. **NOTE:** The VM instance is created with the resource profile that is contained as part of the OVA definition.
3. ☐	Edit the Policy Management VM	1. After created, edit the Policy Management VM 2. Change the VM name to the name defined in the Policy Management NAPD 3. Map the vNICs to the VM to Oracle VM manager networking. Use the Policy Management NAPD to determine the mapping between the Policy Management VM instance and the Oracle VM manager network resource.
4. ☐	Power on the Policy Management VM	1. Use the Oracle VM manager web interface to start the VM instance running. 2. Verify the Policy Management VM is running.
5. ☐	Repeat For Each Policy Management VM	Repeat Steps 1 through 4 for each Policy Management VM.
---End of Procedure---		

4.5 Common Installation Procedures

Regardless of the hypervisor used to manage on Policy Management VM, there are common procedures that are performed. Primarily, each installed Policy Management VM must have an initial configuration set before to proceeding with initial configuration of the Policy Management component (CMP, MRA, MPE, MPE-LI).

4.5.1 Procedure 11—Configure VM Policy Mode

This procedure configures an installed Policy Management VM with the Policy Mode the VM is to expect. This is required for each VM after VM creation and power on, and before to initial configuration of the component (CMP, MRA, MPE, MPE-LI).

At the end of this procedure, all Policy Management VMs have been:

- Configured with the Policy Mode
- Initial configuration is complete.

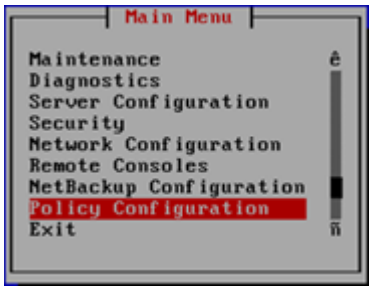
Required materials:

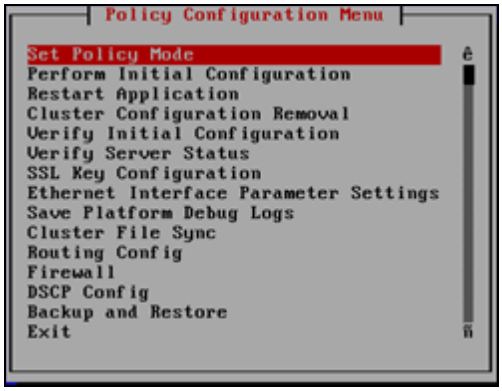
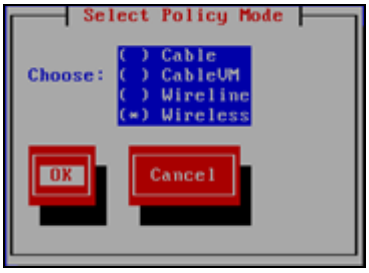
- Access to the powered on Policy Management VM guests

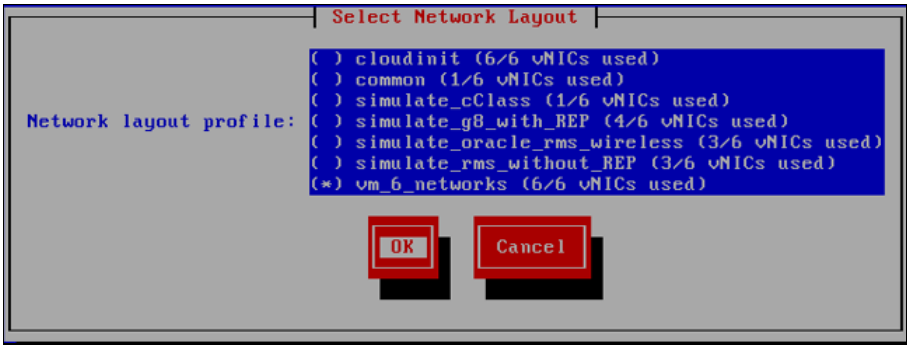
Check off (√) each step as it is completed. Check boxes are beside each step for this purpose.

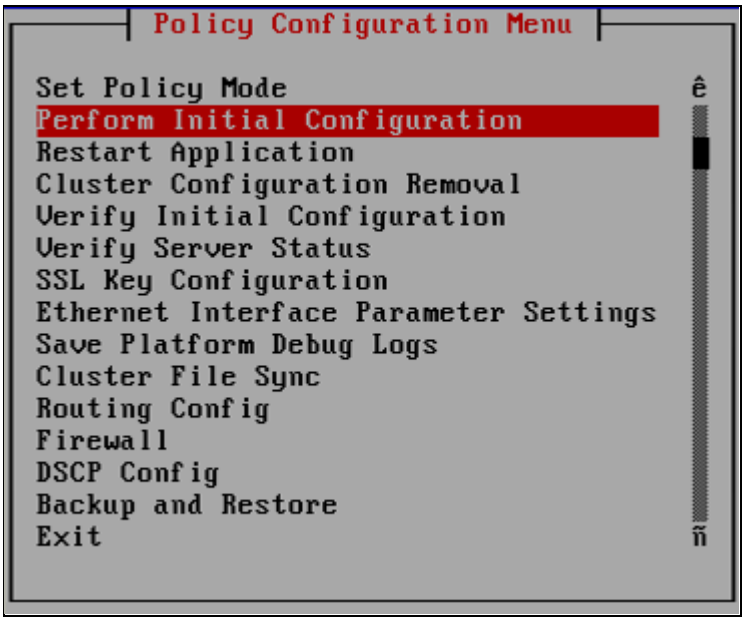
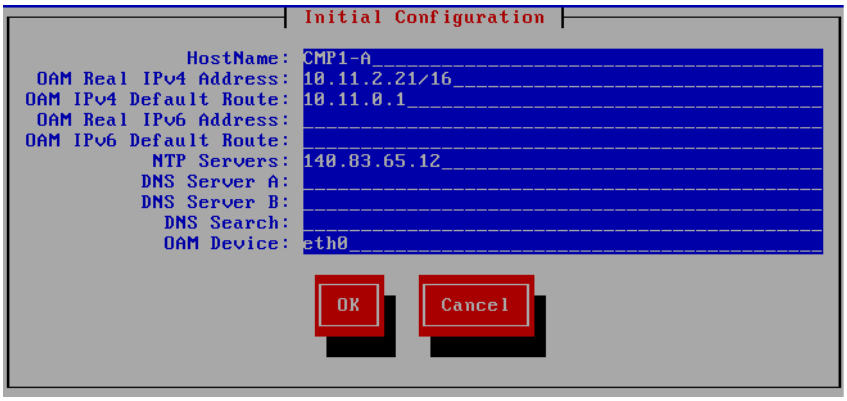
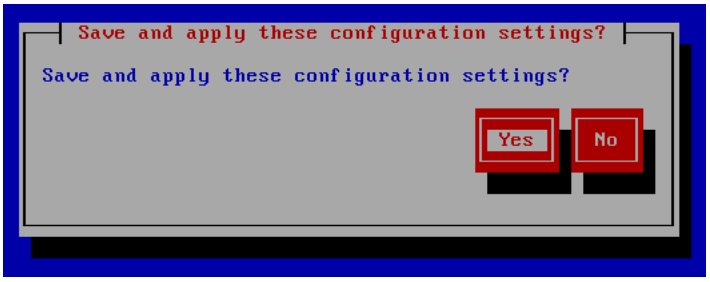
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 11 Configure VM Policy Mode

Step	Procedure	Details
1. ☐	Login to Policy Management VM	1. Login to the running instance of the Policy Management VM as root. 2. Launch platcfg `$ su - platcfg`
2. ☐	Select Policy Configuration	Select **Policy Configuration** from the platcfg Main Menu and press **Enter**. 

Step	Procedure	Details
3. ☐	Select Set Policy Mode	Select **Set Policy Mode** from the Policy Configuration Menu and press **Enter**. 
4. ☐	Select the appropriate Policy Mode	1. Select the policy mode associated with the deployment type:  **NOTE:** In the example, the Wireless mode is selected. 2. Click **OK** and press **Enter**.
5. ☐	Confirm the policy mode selection	Click **Yes** and press **Enter**.  **NOTE:** In the example, the Wireless mode was selected. The confirmation text differs depending on the policy mode selected.

Step	Procedure	Details
6. ☐	Select the Network Layout	1. Select the **vm_6_networks (6/6 vNICs used)** option from the Select Network Layout dialog.  2. Click **OK** and press **Enter**.
7. ☐	Confirm the Network Layout	1. Click **Yes** and press **Enter**. 
8. ☐	Exit platcfg	1. Exit platcfg 2. Logout of the Policy Management VM guest

Step	Procedure	Details
9. ☐	Perform Initial Config	1. Select Policy Configuration from the platcfg Main Menu and press Enter. 2. Select Perform Initial Configuration from the Policy Configuration Menu and press Enter.  3. Enter the host name, IPv4 address, route, NTP servers and so on  4. Click **OK**. 5. Click **Yes** to save and apply these configuration settings. 
10. ☐	Repeat For Each Policy Management VM	Repeat steps 1 through 9 for each Policy Management VM guest that was created. **NOTE:** MPE application comes up when MPE add into CMP TOPOLOGY

Step	Procedure	Details
---End of Procedure---		

APPENDIX A. RESOURCE PROFILES

Table 9—Policy Management VM Resource Profiles

Component	vCPU		RAM (GB)		Storage (GB)		vNIC	
	Suggestion	Minimum	Suggestion	Minimum	Suggestion	Minimum	Suggestion	Minimum
CMP	12	4	60	10	108		6	
MRA	12	10	60	32	108		6	
MPE	12	10	60	32	108		6	
MPE-LI	12	10	60	32	108		6	

APPENDIX B. VM NETWORKING LAYOUT

Table 10 represents the Policy Management network layout that is applied in each Policy Management VM.

Table 10—Policy Management VM Network Layout

Network Name/Function	Policy Management VM vNIC
OAM	eth0
SIGA	eth1
SIGB	eth2
SIGC	eth3
REP	eth4
BKUP	eth5