Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Installation Procedure

Oracle ® Communications Policy Management Cloud Installation Guide 12.3

E85332-01

July 2017

Oracle ® Communications Policy Management Cloud Installation Guide

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1 Purpose and Scope

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

At the completion of this guide, and assuming that the customer networking has been correctly configured, it should be possible to:

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

1.2 References

[1] E85328-01 – Oracle® Communications Policy Management, Release Notes, Release 12.3
[2] E85331-01 White Paper—Oracle® Communications Policy Management, Virtual Network Function Overview and Direction, Release 12.3

1.3 Acronyms

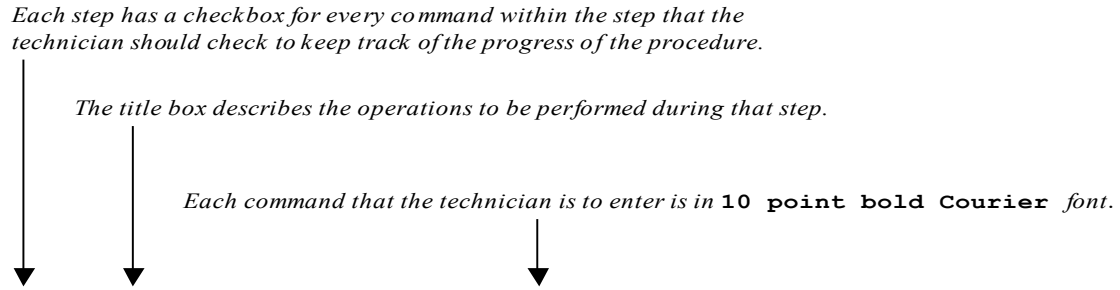
An alphabetized list of acronyms used in the document.

Table 1—Acronyms

Acronym	Definition
CMP	Configuration Management Platform
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 VNF(s) 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)
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 on which 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.
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
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

Term	Definition
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 12.3 application on a supported Cloud platform. For more information see *Virtual Network Function Overview and Direction* [2].

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 should be understood by the operator before starting the install process.

3.1 Required Materials

The OVA files listed in Table 3 are required for installation of all the Policy Management components. Not all OVA files are required for each installation. Table 3 represents the complete list of OVA files for the release.

Table 3—OVA Filelist

Planning	
Mapping of Virtual Machines to Host Servers	
Mapping of Virtual Machine vNICs to Host Networking	
Virtual Machine Configuration Details	
Usernames/passwords for Hypervisors/NFV Managers	
Access Permissions for Host Servers/Control Nodes	
Software	
Policy Management CMP OVA	cmp-*xxx*-x86_64.ova
Policy Management MRA OVA	mra-*xxx*-x86_64.ova
Policy Management MPE OVA	mpe-*xxx*-x86_64.ova
Policy Management MEDIATION OVA	mediation-*xxx*-x86_64.ova
Policy Management MPE-LI OVA	mpe-li-*xxx*-x86_64.ova

NOTE: *xxx* in the OVA file description is the release level information for the OVA 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 should be 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 OVA 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.

Below are the common items to be collected regardless of the installation method. Refer to the subsections for specific preparation items that depend upon 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/passwords for each Policy System component to be installed
	All necessary software OVA 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/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/password)
	KVM Host Server File transfer privileges (for example, SSH)
	KVM Host Server qemu-img 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/password)
	Openstack control node File transfer privileges (for example, SSH)
	Openstack control node privileges to unpack OVA files
	Openstack modules available: • Glance • Keystone • Neutron • Nova
	Horizon GUI tenant username/password

3.3.4 OVM Checklist

Table 8—Installation Preparation Checklist: OVM Specific Items

Check	Item Description
	OVM Web Interface username/password
	OVA files available and accessible to the OVM 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 5.5 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.

The below figure represents the expected flow of installation processes.

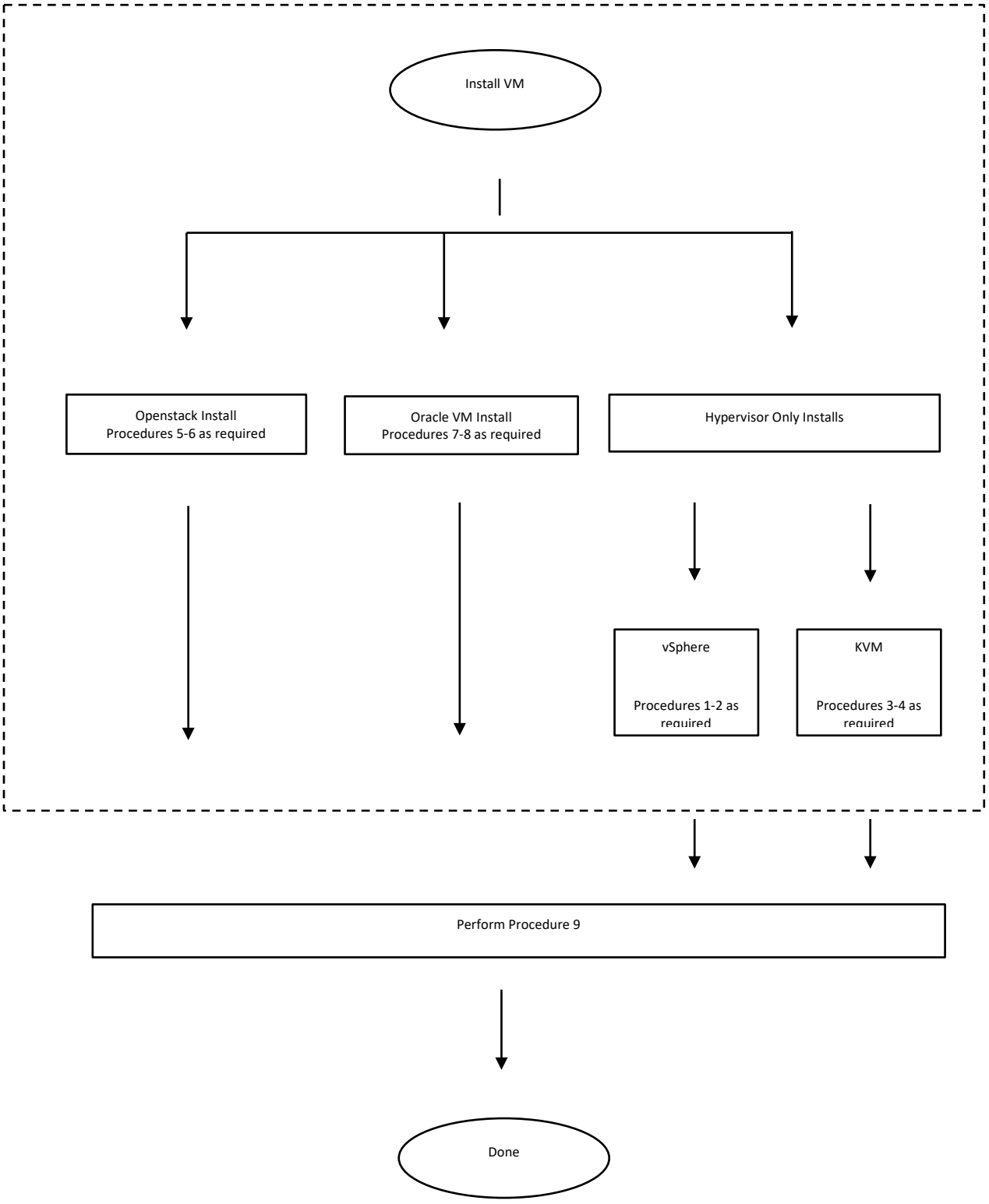


Figure 2—Policy Management VM Installation Process

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. The following flow chart shows the order and the dependencies for each Host Server that contains at least one Policy Management VM.

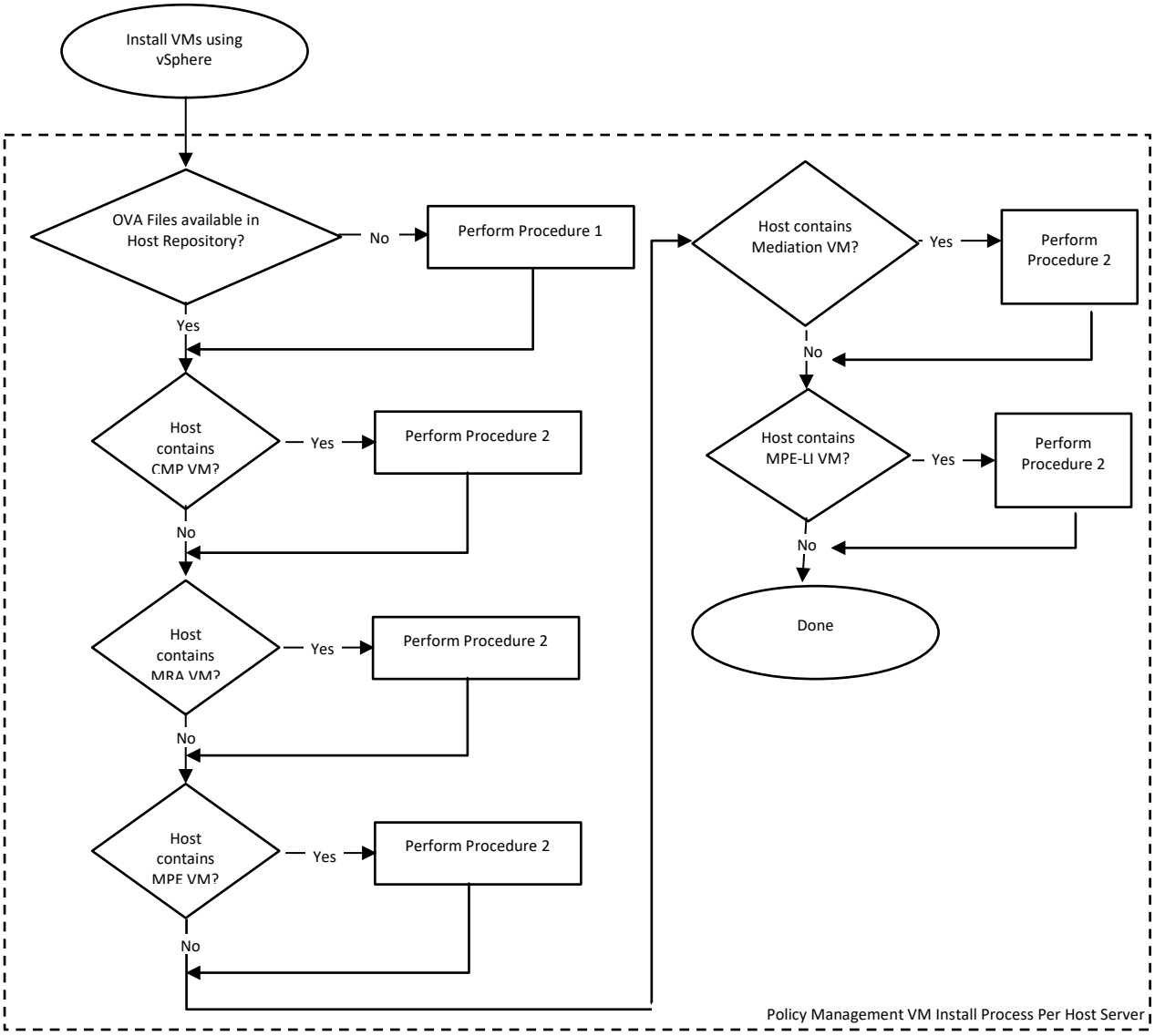


Figure 3—VMware vSphere Installation Process

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 Policy Management OVA files to be 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 within that repository.
- If Host Servers have private repositories, then this procedure requires only those Policy Management OVA files that are associated with the Policy Management VM to be created on the particular Host Server, to be 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/password
- Mapping of Policy Management components to Host Servers
- Policy Management OVA files

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

Step	Procedure	Details
2. ☐	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
3. ☐	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 4.5.1Appendix 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/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. Boxes have been provided for this purpose under each step number.

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

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 4.5.1Appendix 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 1through 4 for each Policy Management VM to be created
---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. The following flow chart describes the order and the dependencies for each Host Server that contains at least one Policy Management VM.

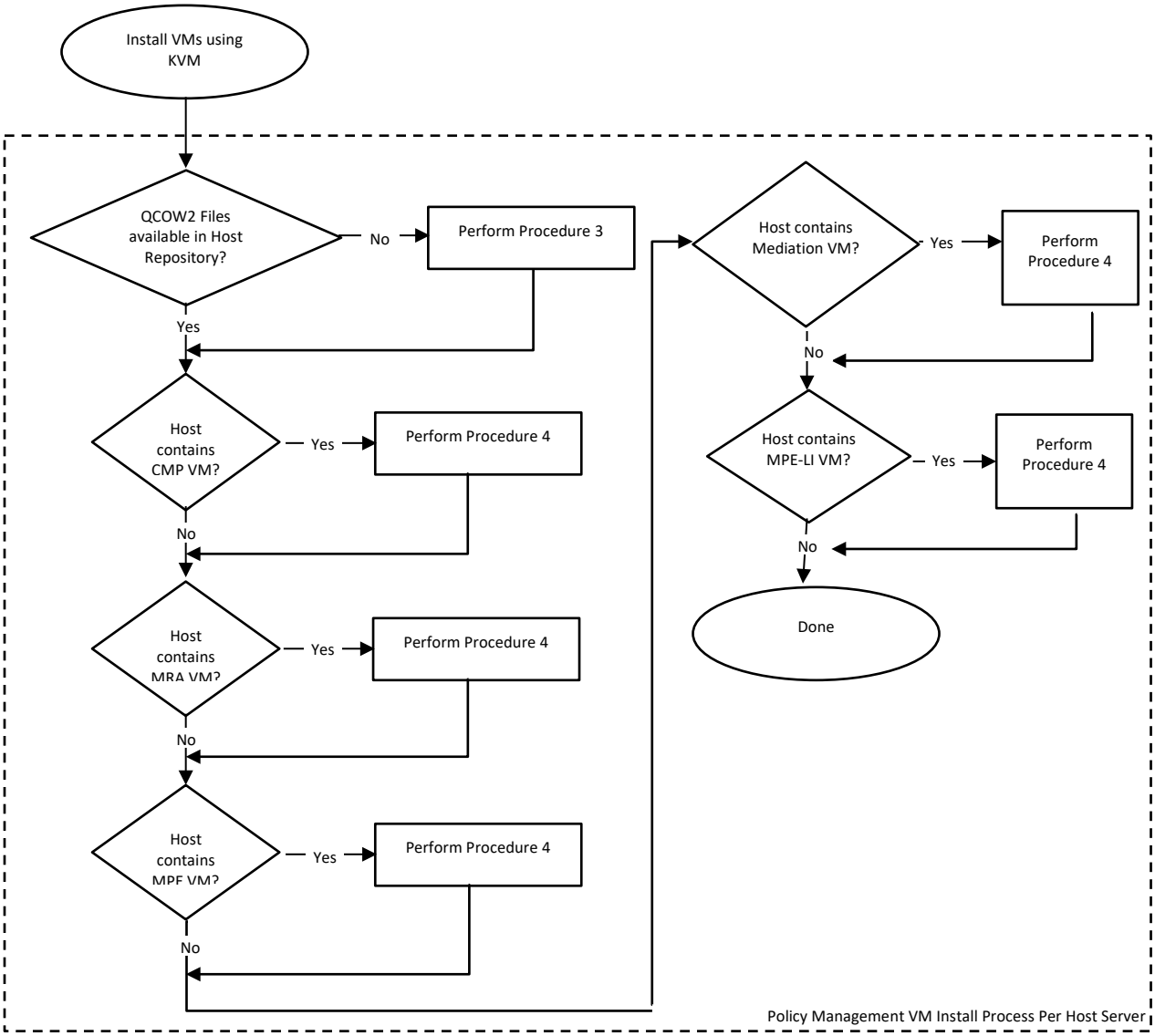


Figure 4—KVM Installation Process

4.2.1 Procedure 3—Upload Policy Management OVA and Convert to QCOW2

This procedure adds the necessary Policy Management OVA files to the host running the KVM hypervisor, and then converts the OVA format 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 be 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 to be 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/password
- Capability to transfer files to the Host Server or Shared Repository
- Capability to run qemu-img on Host Server or Shared Repository
- Mapping of Policy Management components to Host Servers
- Policy Management CMP OVA file
- Policy Management ORA OVA file
- Policy Management MPE OVA file

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

Step	Procedure	Details
1. ☐	Add Policy Management OVA 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 OVA image to the identified directory on the Host Server where OVA images can be stored.
2. ☐	Extract OVF files from OVA 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 OVA file was transferred b. Uncompress the image template using tar. For example: **Example** `$ tar –xvf <ova_filename>.ova`

Step	Procedure	Details
3. ☐	Convert VMDK image to QCOW2 format	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 OVA file was uncompressed b. Convert the vmdk image to qcow2 format: **Example** `$ qemu-img convert -O qcow2 cmp-xxx-x86_64.vmdk cmp-xxx-x86_64.qcow2` Where *xxx* is the release level information for the vmdk file.
4. ☐	Repeat for all Host Servers	Repeat steps 1 through 3 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---		

4.2.2 Procedure 4—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 4.5.1Appendix 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/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. Boxes have been provided for this purpose under each step number.

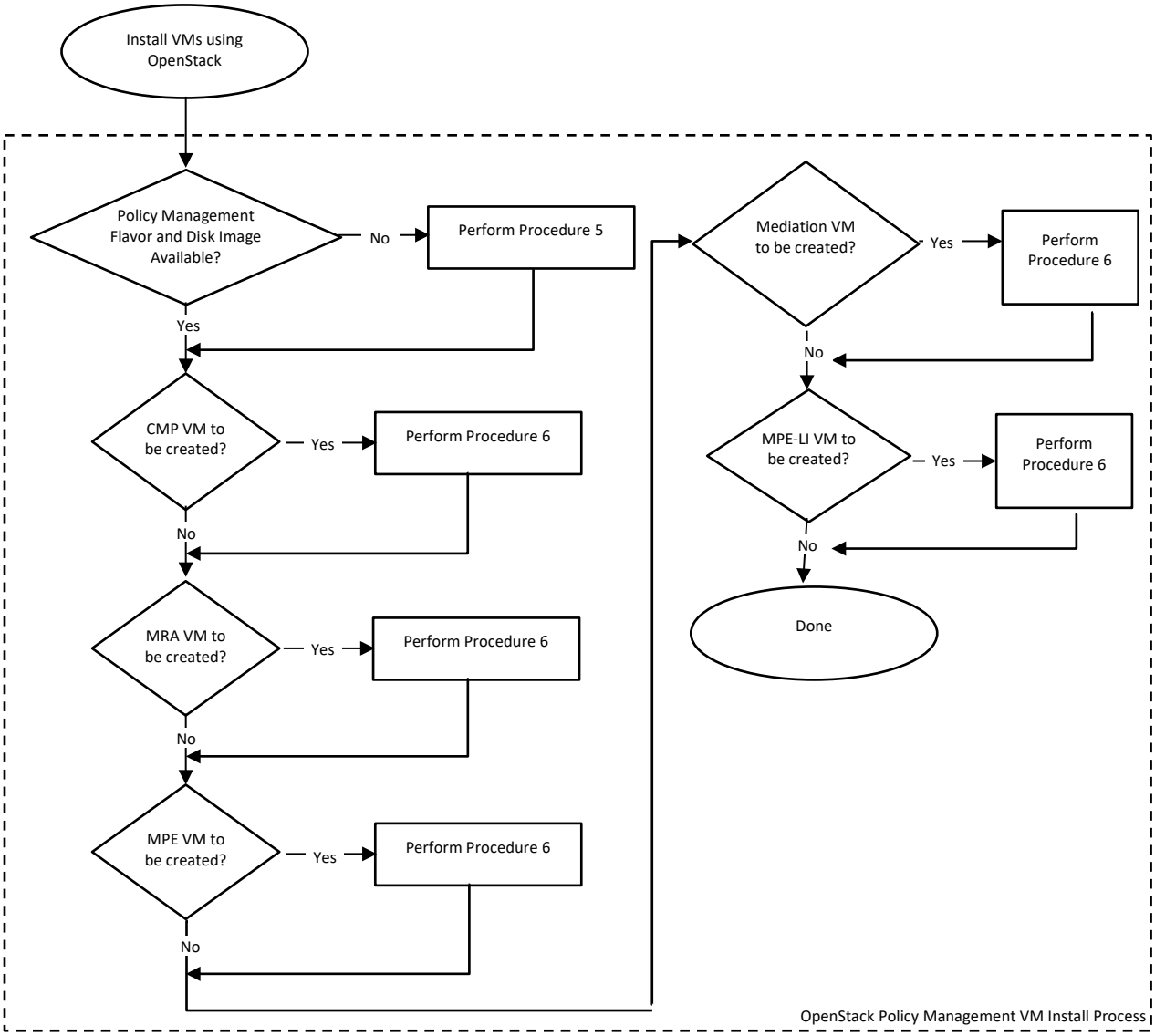
If this procedure fails, contact Oracle Technical Services and ask for assistance.

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:** Since 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.
3. ☐	Configure the resources for the Policy Management VM	1. Configure the Policy Management VM according to the Resource Profile defined in 4.5.1Appendix A for the Policy Management component type. 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 virt-manager client to Power On the Policy Management VM. 2. Verify the Policy Management VM powered on
5. ☐	Repeat For Each CMP	Repeat steps 1 through 4 for each Policy Management VM to be created
---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 the following core services available:

- Glance
- Keystone
- Neutron
- Nova



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 5—Import OVA Files

This procedure imports the necessary Policy Management OVA files to the Glance image catalog for the Openstack control node.

At the end of this procedure, all Policy Management VM OVA files are available for VM creation.

Required materials:

- Openstack control node administration username/password
- Horizon GUI Policy Management tenant username/password
- Capability to transfer files to the Openstack control node
- Capability to unpack OVA files on the Openstack control node
- Policy Management OVA files

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

Step	Procedure	Details
1. ☐	Create Policy Management VM Instance Flavors	Create instance flavors Use the resource profile information in 4.5.1Appendix A to create flavors for each type of VM. Flavors can be 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.

2. ☐	Copy OVA files to Openstack Control Node	Copy the OVA file to the Openstack Control Node
		
		Example
		
		`$ scp cmp-xxx-x86_64.ova admusr@node:~`
		`$ scp mra-xxx-x86_64.ova admusr@node:~`
		`$ scp mpe-xxx-x86_64.ova admusr@node:~`
		`$ scp mediation-xxx-x86_64.ova admusr@node:~`
		`$ scp mpe-li-xxx-x86_64.ova admusr@node:~`
		
		Where *xxx* is the release level information for the ova file.

Step	Procedure	Details

3. ☐	Unpack the OVA files	1. Login (SSH) to the OpenStack Control Node
		Example
		`$ ssh admusr@node`
		2. In an empty directory unpack the OVA files using the **`tar`** command.
		a. Navigate to the directory where the Policy Management CMP OVA file was uploaded
		b. Uncompress/unpack the OCMP OVA files
		Example
		`$ tar -xvf cmp-xxx-x86_64.ova`
		`$ tar -xvf mra-xxx-x86_64.ova`
		`$ tar -xvf mpe-xxx-x86_64.ova`
		`$ tar -xvf mediation-xxx-x86_64.ova`
		`$ tar -xvf mpe-li-xxx-x86_64.ova`
		Where *xxx* is the release level information for the ova file.
		3. One of the unpacked files for each OVA file has a vmdk extension. This is the VM image file that must be imported.
		For example: cmp-*xxx*-x86_64.vmdk
		Where *xxx* is the release level information for the vmdk file.

4. ☐	Import the VMDK images into Glance	1. Source the Openstack admin user credentials, as below:
		`$ . keystonerc_admin`
		2. Import each Policy Management disk image (vmdk) using the **`glance`** utility from the command line.
		NOTE: The name attribute sets the name to be used in the glance repository. In the example, the same name was selected as the vmdk name, without the vmdk extension.
		This process takes approximately 5 minutes, depending on the underlying infrastructure
		Example
		`$ glance image-create --name cmp-xxx-x86_64 --is-public true --is-protected false --progress --container-format bare --disk-format vmdk --file cmp-xxx-x86_64.vmdk`

---End of Procedure---		

4.3.2 Procedure 6—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 4.5.1Appendix A, and the imported Policy Management vmdk 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 vmdk file for the Policy Management component type or 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/password
- Horizon GUI Policy Management tenant username/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. Boxes have been provided for this purpose under each step number.

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

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 following configuration values for the Policy Management component type
		a. The image ID
		`$ glance image-list`
		c. The flavor ID
		`$ nova flavor-list`
		d. The network ID(s)
		`$ neutron net-list`
		e. The availability zone to use (identifying the ZONE to use for the Policy Management VM)
		`$ openstack availability zone list`
		f. The hypervisor list (identifying the compute NODE to use for the Policy Management VM). This is optional only if the compute NODE is to be statically used for the instance.
		`$ nova hypervisor-list`
		g. An informative name for the instance (from the Policy Management

Step	Procedure	Details

		NAPD). The instance name selected is also the hostname of the Policy Management VM.
		3. Create and boot the VM instance
		The instance must be 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 that IPv6 addresses should 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 to be specifically assigned the instance
		- [,v4-fixed-ip….] is optional and only necessary if assigning an IP to the interface
		- All interfaces listed in 4.5.1Appendix A are to be 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 may be 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 to be added>`

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

4.4 Oracle VM Manager (OVM) Installation Procedures

Oracle VM Manager (OVM) procedures are tailored to work with Oracle VM Manager. Procedures are performed using the OVM web interface. The following flow chart describes the order and the dependencies of performing the install using OVM.

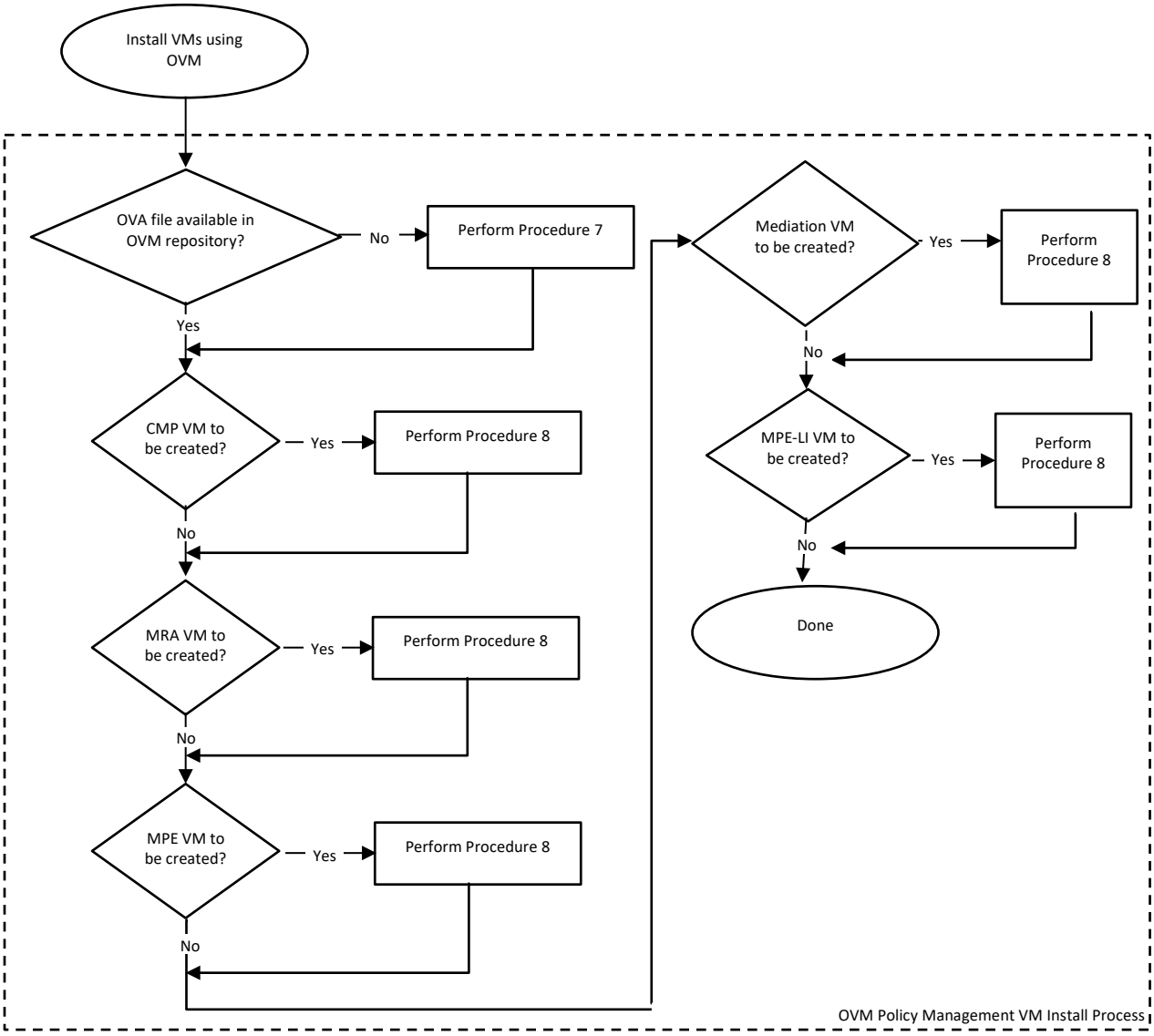


Figure 6—OVM Policy Management VM Install Process

4.4.1 Procedure 7—Upload Policy Management OVA Files

This procedure adds the necessary Policy Management OVA files to OVM.

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

Required materials:

- OVM web interface username/password
- OVA Files available and accessible to the OVM via URL.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

Step	Procedure	Details
1. ☐	Login to OVM Web Interface	Login to the OVM web interface
2. ☐	Add Policy Management OVA files to OVM	Transfer each applicable Policy Management OVA file to the OVM. **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 8—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 4.5.1Appendix 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:

- OVM web interface username/password
- OVA file available in the OVM 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. Boxes have been provided for this purpose under each step number.

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

Step	Procedure	Details
1. ☐	Login to OVM Web Interface	Login to the OVM 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 OVM 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. Once 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 OVM Networking. Use the Policy Management NAPD to determine the mapping between the Policy Management VM instance and the OVM Network resource.
4. ☐	Power on the Policy Management VM	1. Use the OVM 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 to be created.
---End of Procedure---		

4.5 Common Installation Procedures

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

4.5.1 Procedure 9—Configure VM Policy Mode

This procedure configures an installed Policy Management VM with the Policy Mode the VM is to expect. This must be done for each VM after VM creation and power on, and prior to Initial Configuration of the component (CMP, MRA, MPE).

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

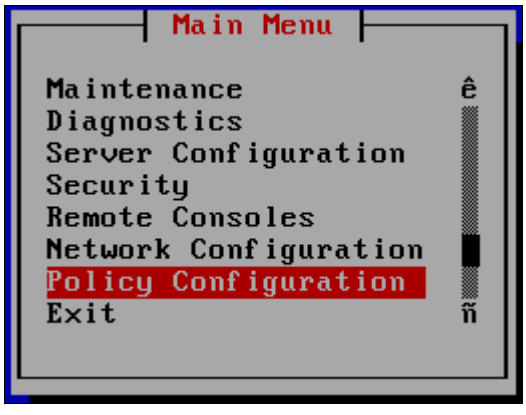
- Configured with the Policy Mode

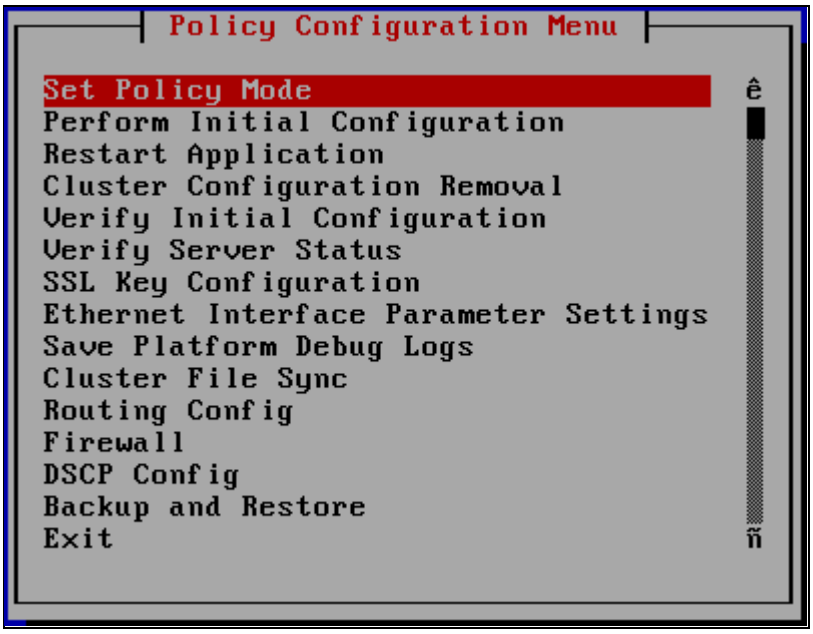
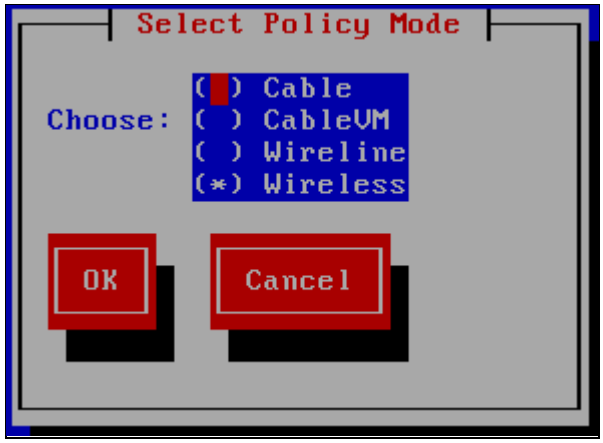
Required materials:

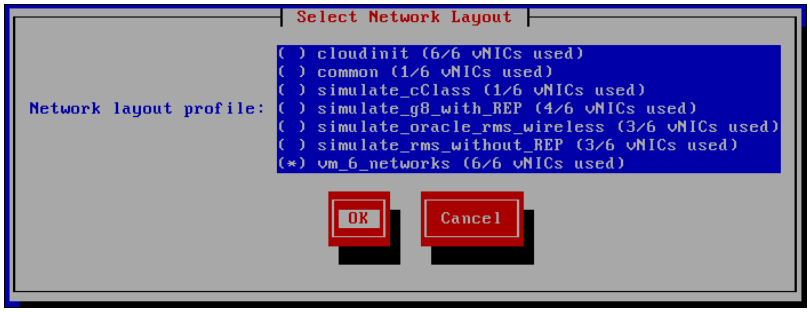
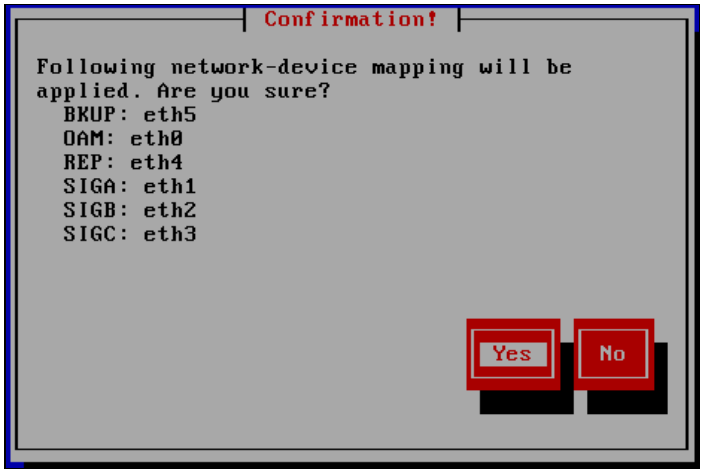
- Access to the powered on Policy Management VM guests

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

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**.

Step	Procedure	Details
5. ☐	Confirm the policy mode selection	Confirm the selected policy mode by clicking **Yes** and pressing **Enter**.  **NOTE:** In the example, the Wireless mode was selected. The confirmation text differs depending on the policy mode selected.
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	3. Confirm the network layout by clicking **Yes** and pressing **Enter**. 

Step	Procedure	Details
8. ☐	Exit platcfg	1. Exit platcfg 2. Logout of the Policy Management VM guest
9. ☐	Repeat For Each Policy Management VM	Repeat steps 1 through 8 for each Policy Management VM guest that was created
---End of Procedure---		

APPENDIX A. 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	
Mediation	12	10	60	32	108		6	
MPE-LI	12	10	60	32	108		6	

Table 9—Policy Management VM Resource Profiles

APPENDIX B. VM NETWORKING LAYOUT

The following represents the Policy Management network layout that is applied in each Policy Management VM.

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

Table 10—Policy Management VM Network Layout