



Oracle® Communications

Installation Procedure

Policy Management Cloud Installation Guide for Release 15.0

F87583-09

November 2024

Oracle® Communications Policy Management Cloud Installation Guide

Copyright © 2018, 2024 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

TABLE OF CONTENTS

1. INTRODUCTION..... 6

1.1 Purpose and Scope 6

1.2 References..... 6

1.3 Acronyms 6

1.4 Terminology..... 7

2. GENERAL DESCRIPTION..... 9

3. INSTALL OVERVIEW 10

3.1 Required Materials..... 10

3.2 Installation Strategy 10

3.3 Preparation Checklist..... 11

3.3.1 vSphere Checklist..... 11

3.3.2 KVM Checklist..... 11

3.3.3 OpenStack Checklist 12

3.3.4 Oracle VM Manager Checklist 12

4. INSTALLATION PRODEDURES 13

4.1 vSphere Installation Procedures 15

4.1.1 Procedure 1—Import Policy Management OVA..... 16

4.1.2 Procedure 2—Create and Configure Policy Management VM 16

4.2 KVM Installation Procedures 18

4.2.1 Procedure 3—Configure LVM Disk Storage For KVM VMs..... 18

4.2.2 Procedure 4—Upload Policy Management QCOW2 Image 20

4.2.3 Procedure 5—Create and Configure Policy Management VM 22

4.2.4 CPU Pinning Configuration on KVM hosts (X9-2 servers)..... 27

4.3 OpenStack Installation Procedures 33

4.3.1 Procedure 6—Create flavor/image/network/availability_zone In OpenStack 34

4.3.2 Procedure 7—Create and Configure Policy Management VM using Heat Template 37

4.3.3 Procedure 8—Create and Configure Policy Management VM 40

4.4 Oracle Linux Virtualization Manager Installation Procedures 42

4.4.1 Procedure 9—Upload Policy Management OVA Files 43

4.4.2 Procedure 10—Create and Configure Policy Management VM 44

4.5 Common Installation Procedures 45

4.5.1 Procedure 11—Configure VM Policy Mode 45

- 5. CONFIGURE POLICY APPLICATION SERVERS IN WIRELESS MODE..... 50**
 - 5.1 Perform Initial Server Configuration of Policy Servers—platcfg 50
 - 5.2 Perform Initial Configuration of the Policy Servers—CMP GUI 56
 - 5.3 Performing SSH Key Exchanges 61
 - 5.4 Configure Routing on Your Servers 64
 - 5.5 Configure Policy Components 65
 - 5.5.1 Adding MPE and MRA to CMP Menu..... 65
 - 5.5.2 Configure MPE Pool on MRA (Policy Front End)..... 71
 - 5.5.3 Define and Add Network Elements 74
 - 5.6 Load Policies and Related Policy Data..... 78
 - 5.7 Add a Data Source..... 79
 - 5.8 Perform Test Call..... 80
 - 5.9 Pre-Production Configurations..... 81
- APPENDIX A. RESOURCE PROFILES..... 82**
- APPENDIX B. RESOURCE PROFILES..... 83**
- APPENDIX C. VM NETWORKING LAYOUT 85**
- APPENDIX D. X9-2 SERVER BIOS SETTINGS AND RECOMMENDED CONFIGURATIONS FOR OS INSTALLATION..... 86**
- APPENDIX E. PORT USAGE AND RECOMMENDED ENABLING FOR FIREWALL ACCESS 89**

TABLE OF FIGURES

Figure 1—Instructions Example	7
Figure 2—Policy Management VM Installation Process.....	14
Figure 3—VMware vSphere Installation Process	15
Figure 4—KVM Installation Process	18
Figure 5—OpenStack Policy Management VM Install Process	33
Figure 6—Oracle Linux Virtualization Manager Policy Management VM Install Process	42

TABLE OF TABLES

Table 1—Acronyms	6
Table 2—Terminology	7
Table 3—Image Filelist	10
Table 4—Installation Preparation Checklist: Common Items.....	11
Table 5—Installation Preparation Checklist: vSphere Specific Items.....	11
Table 6—Installation Preparation Checklist: KVM Specific Items	11
Table 7—Installation Preparation Checklist: OpenStack Specific Items.....	12
Table 8—Installation Preparation Checklist: Oracle VM Manager Specific Items	12
Table 9—Policy Management VM Resource Profiles Component.....	82
Table 10—Policy Management VM Resource Profiles Component	83
Table 11—Policy Management VM Network Layout	85

TABLE OF PROCEDURES

Procedure 1 Import Policy Management OVA.....	16
Procedure 2 Create and Configure Policy Management VM	17
Procedure 3 Configure LVM disk storage for KVM VMs.....	18
Procedure 4 Upload Policy Management QCOW2 Image	20
Procedure 5 Create and Configure Policy Management VM	22
Procedure 6 Create flavor/image/network/availability_zone In OpenStack.....	34
Procedure 7 Create and Configure Policy Management VM using Heat Template	37
Procedure 8 Create and Configure Policy Management VM	40
Procedure 9 Upload Policy Management OVA Files	43
Procedure 10 Create and Configure Policy Management VM	44
Procedure 11 Configure VM Policy Mode	45

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, refer 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] Oracle® Communications Policy Management, Release Notes, Release 15.0
- [2] Oracle® Communications Policy Management, Network Function Virtualization Update, Release 15.0

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 Infrastructure 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:

Each step has a checkbox for every command within the step that the technician should check to keep track of the progress of the procedure.

The title box describes the operations to be performed during that step.

Each command that the technician is to enter is in 10 point bold Courier font.

1.	☐	ServerX: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. <code>\$ cu -l /dev/ttyS7</code>
----	--------------------------	---	---

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 15.0 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 vSphere/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.

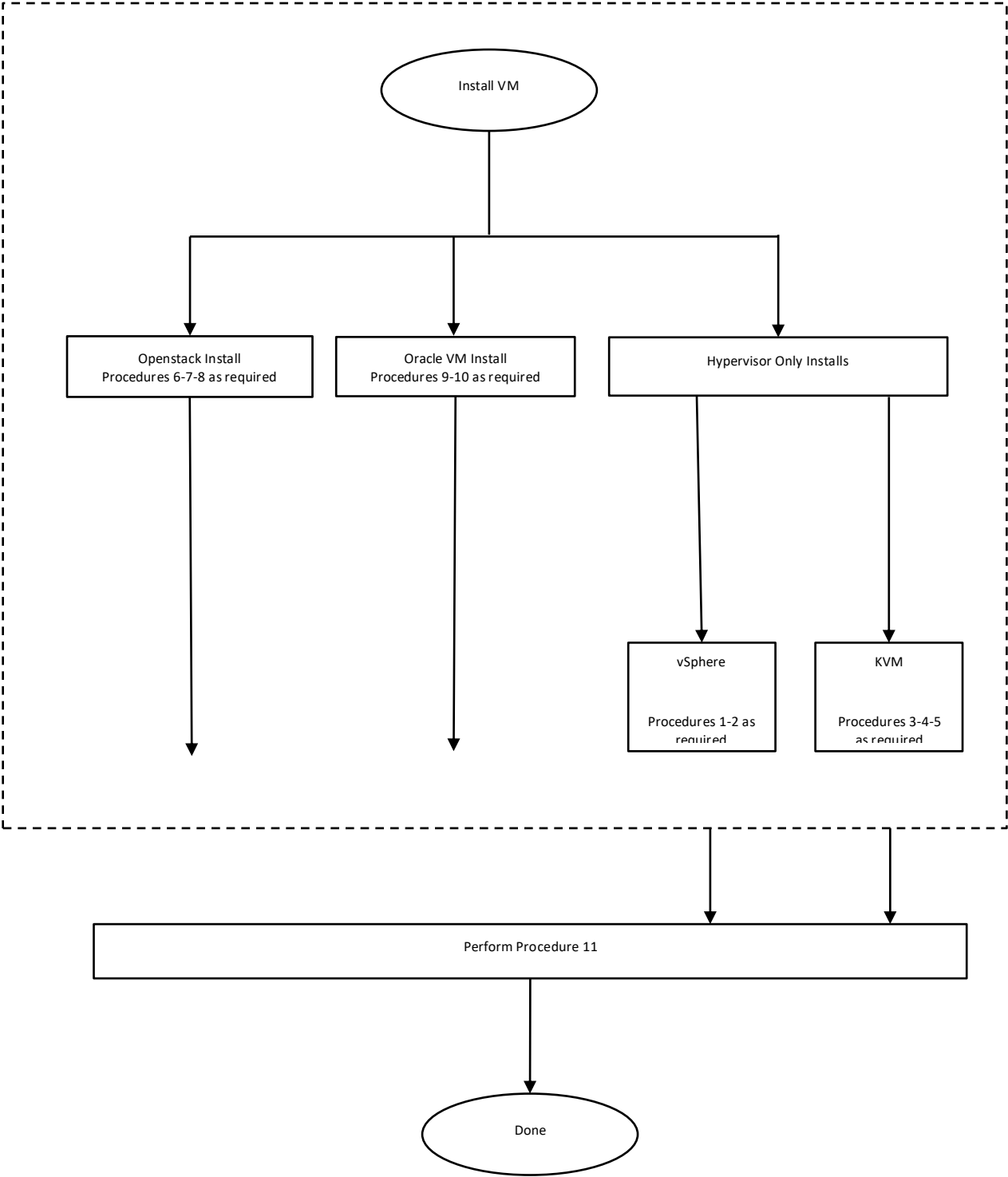


Figure 2—Policy Management VM Installation Process

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.

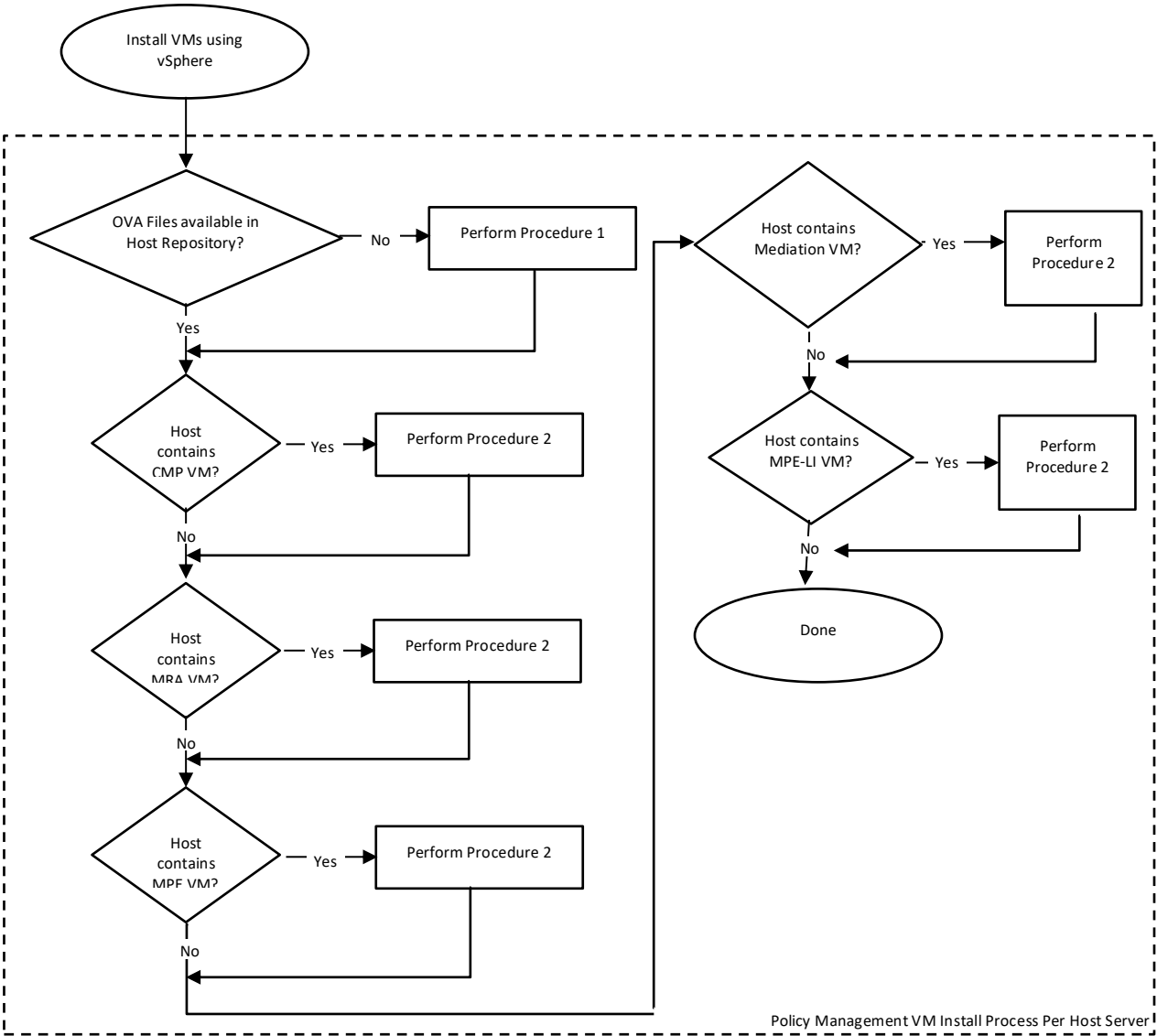


Figure 3—VMware vSphere Installation Process

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 and 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 do 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 [5](#).

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 5 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.

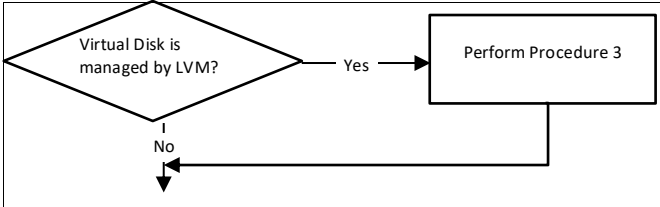


Figure 4—KVM Installation Process

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.

Note: For X9-2 KVM configuration and volume requirements, refer [Appendix D](#).

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 <code>\$ pvcreate /dev/sda3</code> Where <code>/dev/sda3</code> is an example of disk partition.

Step	Procedure	Details
2. ☐	Create Volume Group	Create Volume group on the physical volume Example <pre>\$ vgcreate vgguests /dev/sda3</pre> Where: • <code>vgguests</code> is the volume group name • <code>/dev/sda3</code> is the physical volume created in step 1.
3. ☐	Create Logical Volume for KVM VM	Create LVM partition and add it to a volume group. Example <pre>\$ lvcreate -n mpe9 -L 108G vgguests</pre> Where: • <code>mpe9</code> is name of the VM • <code>108G</code> is the disk storage size for the VM • <code>vgguests</code> is the vg created in step2. NOTE: For PCRf product, the disk storage must be 108G.
4. ☐	Format LV to ext4	Example <pre>\$ mkfs.ext4 /dev/vgguests/mpe9</pre>
5. ☐	Create mount point of LVM	Create a directory to store data for the VM. Example <pre>\$ mkdir /home/VM-hosts/mpe9</pre>
6. ☐	Get the UUID of LV	Example <pre>\$ blkid /dev/vgguests/mpe9</pre> You receive a response result similar to: <pre>/dev/vgguests/mpe9: UUID="8babcea9-36b3-4fee-838a-3f0aa2312997" TYPE="ext4"</pre>
7. ☐	Add the LVM file system info to <code>/etc/fstab</code>	Example <pre>\$ vi /etc/fstab</pre> Add this line to the end of the file: <pre>UUID=8babcea9-36b3-4fee-838a-3f0aa2312997 /home/VM-hosts/mpe9 ext4 defaults 0 0</pre>
8. ☐	Mount the LV device to the designated directory	Example <pre>\$ mount -a</pre> Or <pre>\$ mount</pre> You receive a response result similar to: <pre>/dev/mapper/vgguests-mpe9 on /home/VM-hosts/mpe9 type ext4 (rw,relatime,seclabel,stripe=128,data=ordered)</pre>
9. ☐	Repeat for all host servers	Repeat steps 1 through 8 for each KVM host server that hosts a Policy Management VM.

Step	Procedure	Details
---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 <pre>\$ tar -jxvf <filename>.qcow2.tar.bzip2</pre>
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.

Step	Procedure	Details
---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 [5](#).

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

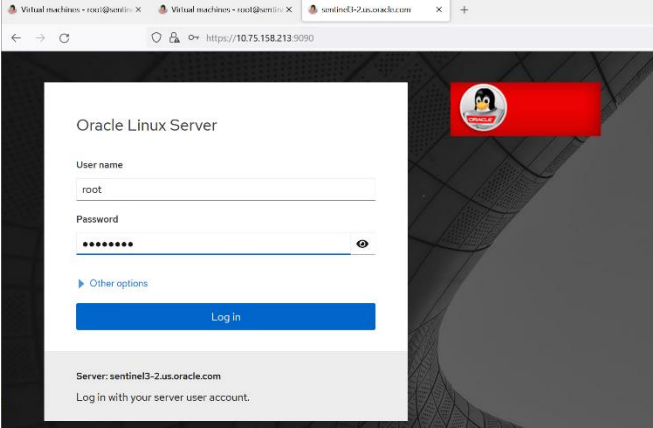
- Created based on the corresponding Policy Management QCOW2 file
- Configured with the resource profile
- Mapped to the network resource for the host based on the Policy Management NAPD
- Powered on
- For X9-2 hosts and 46 vCPU profile, it is recommended NOT to have two Active MRA nodes in the same KVM. You can have CMP + MPE, CMP + MRA, CMP + CMP, MPE + MPE, MPE + MRA as preferable pairs of servers in a single KVM host.

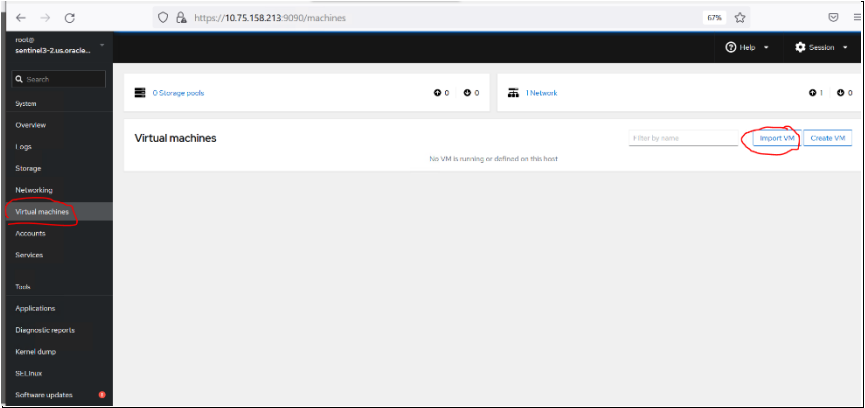
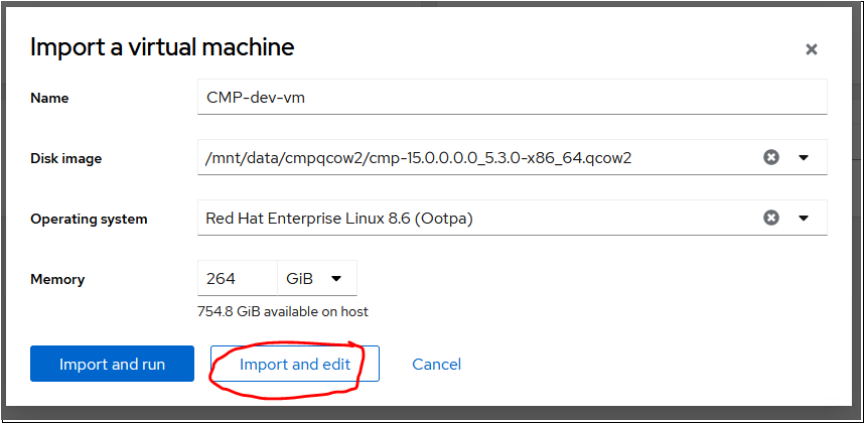
Required materials:

- Linux host server username and password
- Ability to export the host server display (XHost)
- 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. Log in (SSH) to the host server. 2. If cockpit is installed follow the next steps, else refer to the "Alternate Procedure" available at the end of the procedure. 3. Log in to cockpit GUI using url. The supported browser version is Firefox 115.2.1esr. For example, https://kvmhostip:port/  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.

Step	Procedure	Details
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 Virtual Machines tab and, click Import VM.  2. Provide all details in Import VM screen as below and click Import and Edit option. 
3. ☐	Configure the resources for the Policy Management VM	1. Configure the Policy Management VM according to the resource profile defined in Appendix B for the Policy Management component type. 2. Navigate to the Virtual Machines tab. Select the VM name and click Edit. 3. Update the vCPUs and Memory according to the VM profile.

Step	Procedure	Details																											
		Virtual machines > CMP-dev-vm CMP-dev-vm Run : Overview General Connection System State Shut off Memory 264.0 GiB edit vCPUs 46 edit CPU type host edit Boot order disk edit Autostart ☐ Run when host boots Watchdog none add Hypervisor details Emulated machine pc-q35-rhel8.6.0 Firmware BIOS Console Please start the virtual machine to access its console. 4. Navigate to the Networking tab under the selected VM. Remove default bridge network and add virtual network interfaces (number of interfaces depends on the requirement). NOTE: Bridge adding configuration: Add the bridge with OAM (eth0) network first and then add the second bridge (eth1) for SigA. Usage Memory CPU Disks <table><tr><th>Device</th><th>Used</th><th>Capacity</th></tr><tr><td>disk</td><td>12.3 GiB</td><td>255 GiB</td></tr></table> Network interfaces No network interfaces defined for this VM Host devices No host devices assigned to this VM Shared directories Add virtual network interface Interface type Bridge to LAN Source bridge1 Model virtio (Linux, perf) MAC address ☒ Generate automatically ☐ Set manually Add Cancel Network interfaces <table><tr><th>Type</th><th>Model type</th><th>MAC address</th><th>IP address</th><th>Source</th><th>State</th><th></th></tr><tr><td>bridge</td><td>virtio</td><td>52:54:00:77:a3:b4</td><td></td><td>bridge0</td><td>up</td><td> Remove Unplug Edit </td></tr><tr><td>bridge</td><td>virtio</td><td>52:54:00:7b:b4:ca</td><td></td><td>bridge1</td><td>up</td><td> Remove Unplug Edit </td></tr></table> NOTE: Adding number of interfaces is based on the requirement (In this screenshot, new network interfaces (OAM and SIGA) has been added. However, you can also add other interfaces SIGB, SIC, BACKUP, and REP.	Device	Used	Capacity	disk	12.3 GiB	255 GiB	Type	Model type	MAC address	IP address	Source	State		bridge	virtio	52:54:00:77:a3:b4		bridge0	up	Remove Unplug Edit	bridge	virtio	52:54:00:7b:b4:ca		bridge1	up	Remove Unplug Edit
Device	Used	Capacity																											
disk	12.3 GiB	255 GiB																											
Type	Model type	MAC address	IP address	Source	State																								
bridge	virtio	52:54:00:77:a3:b4		bridge0	up	Remove Unplug Edit																							
bridge	virtio	52:54:00:7b:b4:ca		bridge1	up	Remove Unplug Edit																							
4. ☐	Power on the Policy Management VM	1. Navigate to the Virtual Machines tab. Select the VM name and click Run. You can check ongoing activities on the Console.																											

Step	Procedure	Details
		Virtual machines > CMP-dev-vm CMP-dev-vm Run Overview General ConnectionSystem StateShut off Memory264.0 GB edit vCPUs46 edit CPU typehost edit Boot orderdisk edit AutostartRun when host boots Watchdognone add Hypervisor details Emulated machinepc-q35-rhel8.6.0 FirmwareBIOS Usage Memory0 / 264 GB 70% of 48.0 GB Console VNC console Send key Disconnect Starting Resets System Activity Logs... [OK] Started E-Bus System Message Bus. [OK] Started snd_mixer_ossd --timer. Starting OpenSSH ecdda Server Key Generation... [OK] Started Generate summary of yesterday's process accounting. [OK] Reached target Timers. [OK] Started Restore /run/inittabfs on shutdown. [OK] Started Resets System Activity Logs. Starting update of the root trust anchor DNSEC validation in unbound... [OK] Started pid_conf startup script.. [OK] Started OpenSSH ed25519 Server Key Generation. [OK] Started OpenSSH ecdda Server Key Generation. [OK] Starting TMLibnet startup script... [3.933725] snd_hda_codec_generic hdaudioC0D0: autoconfig for Generic: line_outs=1 (0x3/0x0/0x0/0x0/0x0) type:line [3.936590] snd_hda_codec_generic hdaudioC0D0: speaker_outs=0 (0x0/0x0/0x0/0x0/0x0) [3.938903] snd_hda_codec_generic hdaudioC0D0: hp_outs=0 (0x0/0x0/0x0/0x0/0x0) [3.940594] snd_hda_codec_generic hdaudioC0D0: mono mono_out=0x0 [3.942611] snd_hda_codec_generic hdaudioC0D0: inputs: [3.944852] snd_hda_codec_generic hdaudioC0D0: Line=0x5 [OK] Started Login Service. [OK] Reached target Sound Card. [OK] Started OpenSSH rsa Server Key Generation. [OK] Reached target sshd-keygen.target. [OK] Started IP6 firewall with iptables. [OK] Started IP4 firewall with iptables. [OK] Reached target Network (Pre). Mounting RPC Pipe File System... Mounting /var/TLG... Mounting /var/constant... [OK] Mounted RPC Pipe File System. [4.583251] EXT4-fs (da-2): mounted filesystem with ordered data mode. Opts: (null) [4.585463] EXT4-fs (da-3): mounted filesystem with ordered data mode. Opts: (null) [OK] Reached target rpc_pipefs.target. [OK] Mounted /var/TLG. [OK] Mounted /var/constant. Mounting /var/constant/upgrade... 2. Wait for few minutes to install the VM. Once VM installation is done, the VM Console is displayed as below:

Step	Procedure	Details
		Console Expand VNC console Send key Disconnect NOTICE - PROPRIETARY SYSTEM This system is intended to be used solely by authorized users in the course of legitimate corporate business. Users are monitored to the extent necessary to properly administer the system, to identify unauthorized users or users operating beyond their proper authority, and to investigate improper access or use. By accessing this system, you are consenting to this monitoring. montnamec5301ff4632 login: _ 71°F Clear 3:04 AM 3. Log in with root/NextGen and run appRev and syscheck and verify build details.
5. ☐	Repeat For Each Policy Management VM	Repeat steps 1 through 4 for each Policy Management VM.
---End of Procedure---		

ALTERNATE PROCEDURE:

If customer is not having cockpit installed, then use the following *virt-install* command for installing VM:

```
virt-install --name={ VM_NAME } --ram { RAM } --vcpus { vCPUs } --network bridge:bridge0,model=virtio --network bridge:bridge1,model=virtio --network bridge:bridge2,model=virtio --graphics none --connect qemu:///system --disk=/mnt/data/{ VM_NAME }.qcow2,format=qcow2,bus=virtio --noautoconsole --import
```

Here, the VM_NAME, RAM, and vCPUs need to be provided and can be used as a variable. The networks are assumed to be bridge0, bridge1, and bridge2 for OAM, SIG A and SIG B respectively. The qcow2 to be used is provided with the absolute path in the --disk parameter.

Note: For running virt-install the following libraries need to be present in KVM:

- virt-install
- libguestfs
- qemu-kvm
- python3
- libvirt

Note: CPU pinning should be configured on all VMs installed on KVM host.

4.2.4 CPU Pinning Configuration on KVM hosts (X9-2 servers)

CPU pinning can be performed through VM definition XML.

CPU pinning is like pinning a particular physical CPU to each Virtual CPU.

In order to pin all vCPUs (0 to 12) and (0-45) based on VM profile, you need to run *virsh edit VMname* and add all vCPUs with corresponding cpuset manually and save it. Then, restart the VM to apply the changes.

For example:

X9-2 servers with 96cpus have two Numa nodes:

- NUMA node0 CPU(s): 0-23, 48-71
- NUMA node1 CPU(s): 24-47, 72-95

Here 0,48,24,72 can be reserved for host and remaining cpus can be configured for cpu pinning for VMs.

TO RESERVE CPUs for HOST USE CPUAffinity, manually edit */etc/systemd/system.conf* file on KVM host

CPUAffinity for HOST: (edit */etc/systemd/system.conf* file and enable CPUAffinity and add respective CPU's) example:CPUAffinity=0 32 64 96

TO MAKE SURE HOST IS NOT USING PINNED CPUS

Run the following command for CPU isolation on KVM host:

```
#grubby --update-kernel=ALL --args="isolcpus=1-23,25-47,49-71,73-95"
```

After the above steps, reboot the host.

After configuring CPU isolation using the above command, verify isolated CPUs using below command.

cat /sys/devices/system/cpu/isolated on KVM host

sample output : 1-23,25-47,49-71,73-95

For 12 vcpus, you can configure CPU pinning as below:

1. Shutdown the VM.
2. *virsh edit VM1*
3. Add cputune configuration as below

VM1:

```
<vcpu placement='static'>12</vcpu>
```

```
<cputune>
```

```
<vcpupin vcpu='0' cpuset='1'/>
```

```
<vcpupin vcpu='1' cpuset='2'/>
```

```
<vcpupin vcpu='2' cpuset='3'/>
```

```
<vcpupin vcpu='3' cpuset='4'/>
```

VM3:

```
<vcpu placement='static'>12</vcpu>
```

```
<cputune>
```

```
<vcpupin vcpu='0' cpuset='25'/>
```

```
<vcpupin vcpu='1' cpuset='26'/>
```

```
<vcpupin vcpu='2' cpuset='27'/>
```

```
<vcpupin vcpu='3' cpuset='28'/>
```

```

<vcpupin vcpu='4' cpuset='5'/>
<vcpupin vcpu='5' cpuset='6'/>
<vcpupin vcpu='6' cpuset='7'/>
<vcpupin vcpu='7' cpuset='8'/>
<vcpupin vcpu='8' cpuset='9'/>
<vcpupin vcpu='9' cpuset='10'/>
<vcpupin vcpu='10' cpuset='11'/>
<vcpupin vcpu='11' cpuset='12'/>
</cputune>

```

VM2:

```

<vcpu placement='static'>12</vcpu>
<cputune>
  <vcpupin vcpu='0' cpuset='49'/>
  cpuset='73'/>
  <vcpupin vcpu='1' cpuset='50'/>
  <vcpupin vcpu='2' cpuset='51'/>
  <vcpupin vcpu='3' cpuset='52'/>
  <vcpupin vcpu='4' cpuset='53'/>
  <vcpupin vcpu='5' cpuset='54'/>
  <vcpupin vcpu='6' cpuset='55'/>
  <vcpupin vcpu='7' cpuset='56'/>
  <vcpupin vcpu='8' cpuset='57'/>
  cpuset='81'/>
  <vcpupin vcpu='9' cpuset='58'/>
  <vcpupin vcpu='10' cpuset='59'/>
  <vcpupin vcpu='11' cpuset='60'/>

```

For 46vpcu, CPU pinning need to configure as below:

VM1 ;

```

<vcpu placement='static'>46</vcpu>
<cputune>
  <vcpupin vcpu='0' cpuset='1'/>

```

```

<vcpupin vcpu='4' cpuset='29'/>
<vcpupin vcpu='5' cpuset='30'/>
<vcpupin vcpu='6' cpuset='31'/>
<vcpupin vcpu='7' cpuset='32'/>
<vcpupin vcpu='8' cpuset='33'/>
<vcpupin vcpu='9' cpuset='34'/>
<vcpupin vcpu='10' cpuset='35'/>
<vcpupin vcpu='11' cpuset='36'/>
</cputune>

```

VM4:

```

<vcpu placement='static'>12</vcpu>
<cputune>
  <vcpupin vcpu='0'
  <vcpupin vcpu='1' cpuset='74'/>
  <vcpupin vcpu='2' cpuset='75'/>
  <vcpupin vcpu='3' cpuset='76'/>
  <vcpupin vcpu='4' cpuset='77'/>
  <vcpupin vcpu='5' cpuset='78'/>
  <vcpupin vcpu='6' cpuset='79'/>
  <vcpupin vcpu='7' cpuset='80'/>
  <vcpupin vcpu='8'
  <vcpupin vcpu='9' cpuset='82'/>
  <vcpupin vcpu='10' cpuset='83'/>
  <vcpupin vcpu='11' cpuset='84'/>

```

```
<vcupin vcpu='1' cpuset='2'/>
<vcupin vcpu='2' cpuset='3'/>
<vcupin vcpu='3' cpuset='4'/>
<vcupin vcpu='4' cpuset='5'/>
<vcupin vcpu='5' cpuset='6'/>
<vcupin vcpu='6' cpuset='7'/>
<vcupin vcpu='7' cpuset='8'/>
<vcupin vcpu='8' cpuset='9'/>
<vcupin vcpu='9' cpuset='10'/>
<vcupin vcpu='10' cpuset='11'/>
<vcupin vcpu='11' cpuset='12'/>
<vcupin vcpu='12' cpuset='13'/>
<vcupin vcpu='13' cpuset='14'/>
<vcupin vcpu='14' cpuset='15'/>
<vcupin vcpu='15' cpuset='16'/>
<vcupin vcpu='16' cpuset='17'/>
<vcupin vcpu='17' cpuset='18'/>
<vcupin vcpu='18' cpuset='19'/>
<vcupin vcpu='19' cpuset='20'/>
<vcupin vcpu='20' cpuset='21'/>
<vcupin vcpu='21' cpuset='22'/>
<vcupin vcpu='22' cpuset='23'/>
<vcupin vcpu='23' cpuset='49'/>
<vcupin vcpu='24' cpuset='50'/>
<vcupin vcpu='25' cpuset='51'/>
<vcupin vcpu='26' cpuset='52'/>
<vcupin vcpu='27' cpuset='53'/>
<vcupin vcpu='28' cpuset='54'/>
<vcupin vcpu='29' cpuset='55'/>
<vcupin vcpu='30' cpuset='56'/>
<vcupin vcpu='31' cpuset='57'/>
```

```
<vcpupin vcpu='32' cpuset='58' />
<vcpupin vcpu='33' cpuset='59' />
<vcpupin vcpu='34' cpuset='60' />
<vcpupin vcpu='35' cpuset='61' />
<vcpupin vcpu='36' cpuset='62' />
<vcpupin vcpu='37' cpuset='63' />
<vcpupin vcpu='38' cpuset='64' />
<vcpupin vcpu='39' cpuset='65' />
<vcpupin vcpu='40' cpuset='66' />
<vcpupin vcpu='41' cpuset='67' />
<vcpupin vcpu='42' cpuset='68' />
<vcpupin vcpu='43' cpuset='69' />
<vcpupin vcpu='44' cpuset='70' />
<vcpupin vcpu='45' cpuset='71' />
</cputune>
```

VM2:

```
<vcpu placement='static'>46</vcpu>
<cputune>
  <vcpupin vcpu='0' cpuset='25' />
  <vcpupin vcpu='1' cpuset='26' />
  <vcpupin vcpu='2' cpuset='27' />
  <vcpupin vcpu='3' cpuset='28' />
  <vcpupin vcpu='4' cpuset='29' />
  <vcpupin vcpu='5' cpuset='30' />
  <vcpupin vcpu='6' cpuset='31' />
  <vcpupin vcpu='7' cpuset='32' />
  <vcpupin vcpu='8' cpuset='33' />
  <vcpupin vcpu='9' cpuset='34' />
  <vcpupin vcpu='10' cpuset='35' />
  <vcpupin vcpu='11' cpuset='36' />
  <vcpupin vcpu='12' cpuset='37' />
```

<vcpupin vcpu='13' cpuset='38' />
<vcpupin vcpu='14' cpuset='39' />
<vcpupin vcpu='15' cpuset='40' />
<vcpupin vcpu='16' cpuset='41' />
<vcpupin vcpu='17' cpuset='42' />
<vcpupin vcpu='18' cpuset='43' />
<vcpupin vcpu='19' cpuset='44' />
<vcpupin vcpu='20' cpuset='45' />
<vcpupin vcpu='21' cpuset='46' />
<vcpupin vcpu='22' cpuset='47' />
<vcpupin vcpu='23' cpuset='73' />
<vcpupin vcpu='24' cpuset='74' />
<vcpupin vcpu='25' cpuset='75' />
<vcpupin vcpu='26' cpuset='76' />
<vcpupin vcpu='27' cpuset='77' />
<vcpupin vcpu='28' cpuset='78' />
<vcpupin vcpu='29' cpuset='79' />
<vcpupin vcpu='30' cpuset='80' />
<vcpupin vcpu='31' cpuset='81' />
<vcpupin vcpu='32' cpuset='82' />
<vcpupin vcpu='33' cpuset='83' />
<vcpupin vcpu='34' cpuset='84' />
<vcpupin vcpu='35' cpuset='85' />
<vcpupin vcpu='36' cpuset='86' />
<vcpupin vcpu='37' cpuset='87' />
<vcpupin vcpu='38' cpuset='88' />
<vcpupin vcpu='39' cpuset='89' />
<vcpupin vcpu='40' cpuset='90' />
<vcpupin vcpu='41' cpuset='91' />
<vcpupin vcpu='42' cpuset='92' />
<vcpupin vcpu='43' cpuset='93' />

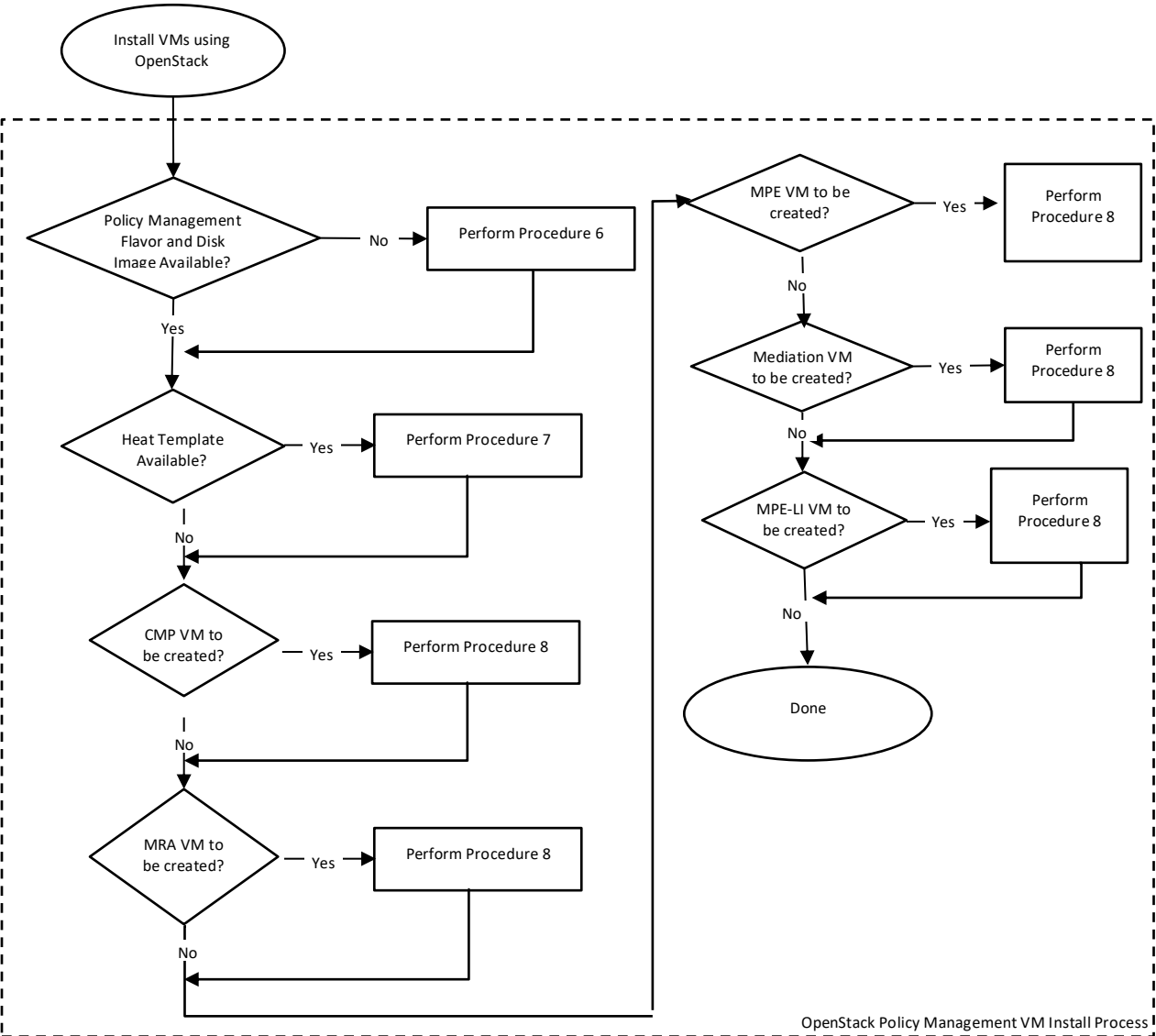
```
<vcpupin vcpu='44' cpuset='94' />  
<vcpupin vcpu='45' cpuset='95' />  
</cputune>
```

After restarting VM just check *virsh vcpuinfo VMname* to verify CPU pinning.

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 5 to create flavors for each type of VM. Flavors are created with the Horizon GUI in the Admin section, or with the <code>nova flavor-create</code> command line tool. Make the flavor names as informative as possible. Example <pre>\$ nova flavor-create pcrf auto 61440 108 12</pre> Where: • <code>pcrf</code> is the flavor name. • vCPU is <code>12</code> • RAM is <code>60G</code> • Storage is <code>256G</code>
2. ☐	Copy qcow2.tar.bzip2 files to OpenStack Control Node	Copy the qcow2.tar.bzip2 file to the OpenStack Control Node Example <pre>\$ 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:~</pre> 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 <pre>\$ ssh admusr@controller</pre> 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 <pre>\$ 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</pre> 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: <pre>\$. keystone_admin</pre> 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 <pre>\$ glance image-create --name cmp-xxx-x86_64 --disk-format qcow2 -- container-format bare --visibility public --file /image_directory/cmp-xxx-x86_64.qcow2</pre>

Step	Procedure	Details
5. ☐	Create Network for Policy Management VM Instance	Create an instance for the networks. Use the network information in 5 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 <pre>\$ 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 [<i>CIDR</i>]</pre> Notes: • <i><segmentation_id></i> is VLAN ID for VLAN networks or tunnel-id for GRE/VXLAN networks. • <i><network_type></i> is the physical mechanism by which the virtual network is implemented. • <i><physical_network_name></i> is Name of the physical network over which the virtual network is implemented. • <i>NAME</i> is the name of the network or subnet. • <i>GATEWAY_IP</i> is the Gateway IP of this subnet. • <i>NETWORK</i> is the Network ID or name this subnet belongs to. • <i>CIDR</i> 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 <pre>\$ openstack aggregate create --zone <availability-zone> <name> \$ openstack aggregate add host <aggregate> <host></pre> The first command is to create an availability zone • where <i><availability-zone></i> is availability zone name and <i><name></i> is the aggregate name. The second command is to adding one host server to the zone • where <i><aggregate></i> is Aggregate (name or ID) and <i><host></i> is the host to add to <i><aggregate></i>.
---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:
 - o The Policy Management flavor for the Policy Management component type
 - o 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.
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 <code>heat stack create</code> command line tool. Make the stack name as informative as possible. 1. Source the OpenStack admin user credentials: <pre>\$. keystone_admin</pre>

Confidential - Oracle Restricted

Step	Procedure	Details																				
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.																				
5. ☐	Configure Topology	Refer to step 3 for IP addresses. for example: <table><thead><tr><th>Key name</th><th>Description</th></tr></thead><tbody><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></tbody></table>	Key name	Description	CMPSITE1_OAM_IP	CMP OAM VIP	CMPSITE1_SERVERA_OAM_IP	CMP Server A OAM IP	CMPSITE1_SERVERB_OAM_IP	CMP Server B OAM IP	MPE1-1-1_SERVERA_OAM_IP	MPE1-1, Server A OAM IP	MPE1-1-1_SERVERB_OAM_IP	MPE1-1,Server B OAM IP	MPE1-1-1_SIGA_IP	MPE 1-1, SIGA VIP	MRA1-1_SERVERA_OAM_IP	MRA 1-1, Server A OAM IP	MRA1-1_SERVERB_OAM_IP	MRA 1-1, Server B OAM IP	MRA1-1_SIGA_IP	MRA 1-1, SIGA VIP
Key name	Description																					
CMPSITE1_OAM_IP	CMP OAM VIP																					
CMPSITE1_SERVERA_OAM_IP	CMP Server A OAM IP																					
CMPSITE1_SERVERB_OAM_IP	CMP Server B OAM IP																					
MPE1-1-1_SERVERA_OAM_IP	MPE1-1, Server A OAM IP																					
MPE1-1-1_SERVERB_OAM_IP	MPE1-1,Server B OAM IP																					
MPE1-1-1_SIGA_IP	MPE 1-1, SIGA VIP																					
MRA1-1_SERVERA_OAM_IP	MRA 1-1, Server A OAM IP																					
MRA1-1_SERVERB_OAM_IP	MRA 1-1, Server B OAM IP																					
MRA1-1_SIGA_IP	MRA 1-1, SIGA VIP																					
6. ☐	(Optional) Update Network Resource, such as IPs	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 heat stack-update CLI command.																				
---End of Procedure---																						

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 5, and the imported Policy Management qcow2 file.

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

- Created based on:
 - o The Policy Management flavor for the Policy Management component type
 - o 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 <pre>\$. /root/keystonerc_admin</pre> 2. Get the configuration values for the Policy Management component type a. The image ID <pre>\$ glance image-list</pre> b. The flavor ID <pre>\$ nova flavor-list</pre> c. The network IDs <pre>\$ neutron net-list</pre> d. The availability zone to use (identifying the zone to use for the Policy Management VM) <pre>\$ openstack availability zone list</pre> 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. <pre>\$ nova hypervisor-list</pre> f. An informative name for the instance (from the Policy Management NAPD). The instance name selected is also the hostname of the Policy Management VM. 3. Create and boot the VM instance

Step	Procedure	Details
		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. <pre>\$ 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></pre> 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 5 are included in the nova boot command with a nic option. 4. View the instance using the nova tool <pre>\$ nova list --all-tenants</pre> 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 <pre>\$ neutron port-list</pre> 2. Add the VIP address to the address pairs list of the interface port for the Policy Management VM instance. <pre>\$ neutron port-update <port ID> --allowed-address-pairs list=true type=dict ip_address=<VIP address ></pre>
3. ☐	Repeat For Each Policy Management VM	Repeat steps 1 and 2 for each Policy Management VM.
---End of Procedure---		

4.4 Oracle Linux Virtualization Manager Installation Procedures

Oracle Linux Virtualization Manager (OLVM) procedures are tailored to work with OLVM. Procedures are performed using the OLVM web interface. Figure 6 shows the order and the dependencies of performing the install using OLVM.

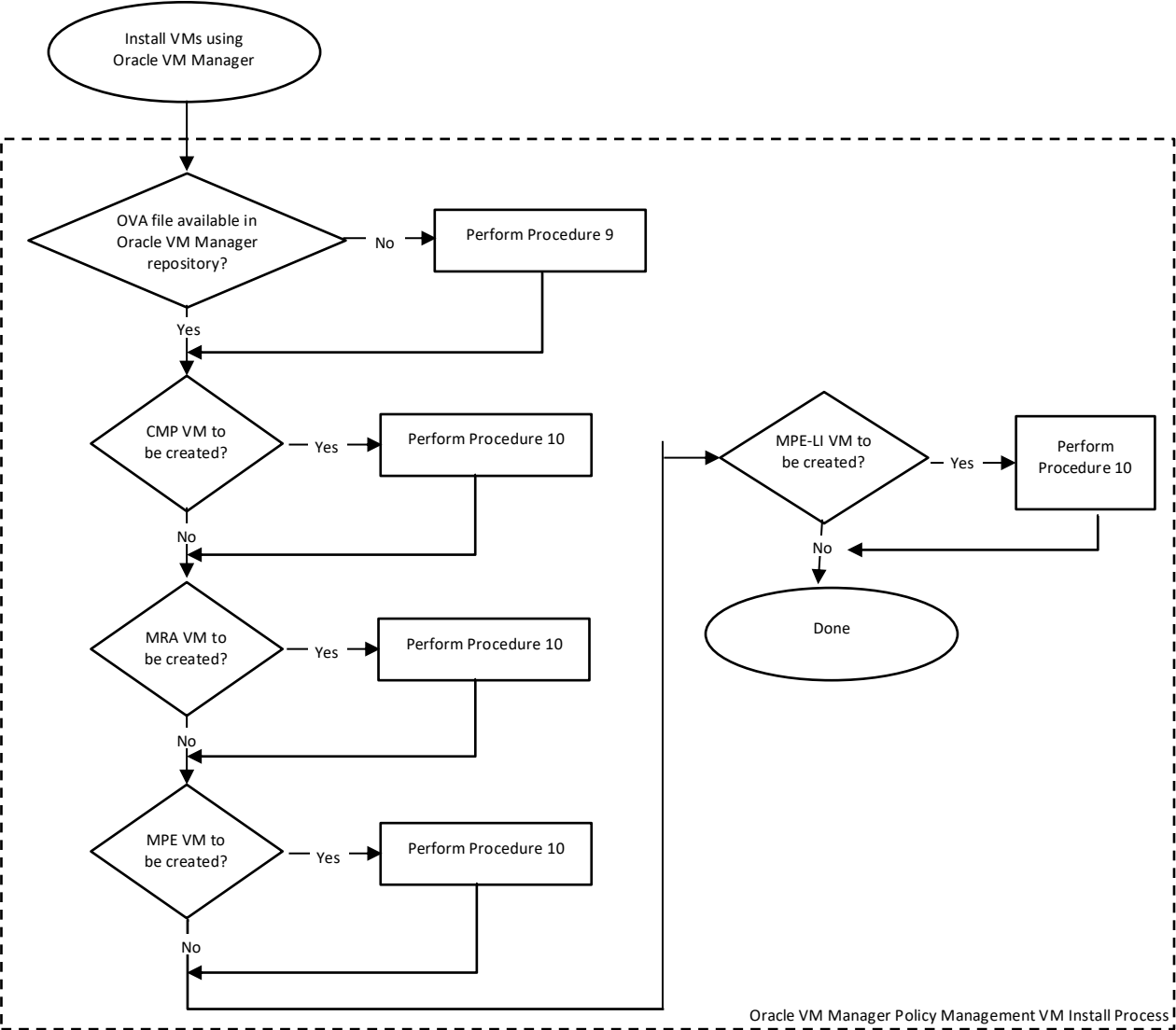


Figure 6—Oracle Linux Virtualization Manager Policy Management VM Install Process

4.4.1 Procedure 9—Upload Policy Management OVA Files

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

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

Required materials:

- OLVM web interface username and password
- OVA Files available and accessible to the OLVM 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 OLVM Web interface	Login to the OLVM web interface
2. ☐	Add Policy Management OVA files to OLVM	Transfer each applicable Policy Management OVA file to the OLVM. 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 [5](#).

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 OLVM web interface	Login to the OLVM web interface
2. ☐	Create the Policy Management VM	Create the Policy Management VM using the corresponding Policy Management qcow2 or OVA image that was uploaded to the OLVM 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 OLVM networking. Use the Policy Management NAPD to determine the mapping between the Policy Management VM instance and the OLVM network resource.
4. ☐	Power on the Policy Management VM	1. Use the OLVM 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:

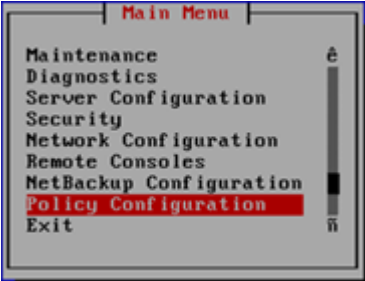
- Configured with the Policy Mode
- Initial configuration is complete.

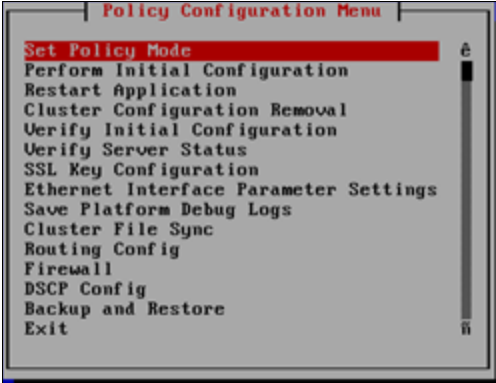
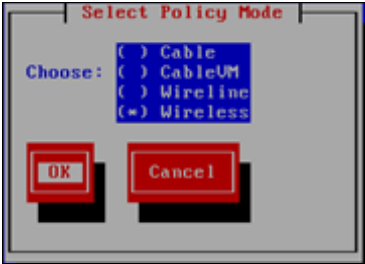
Required materials:

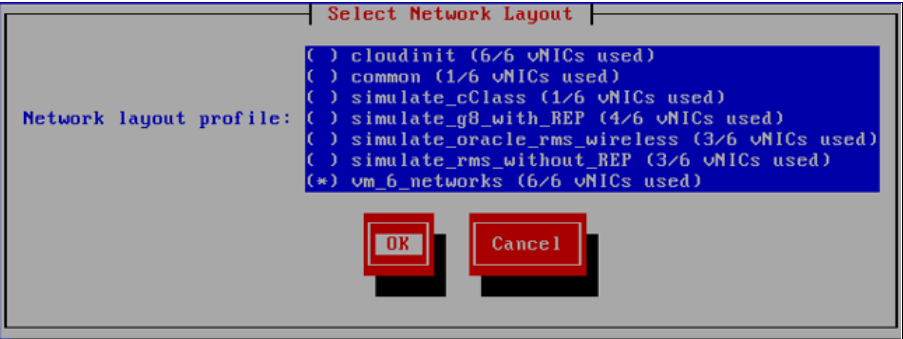
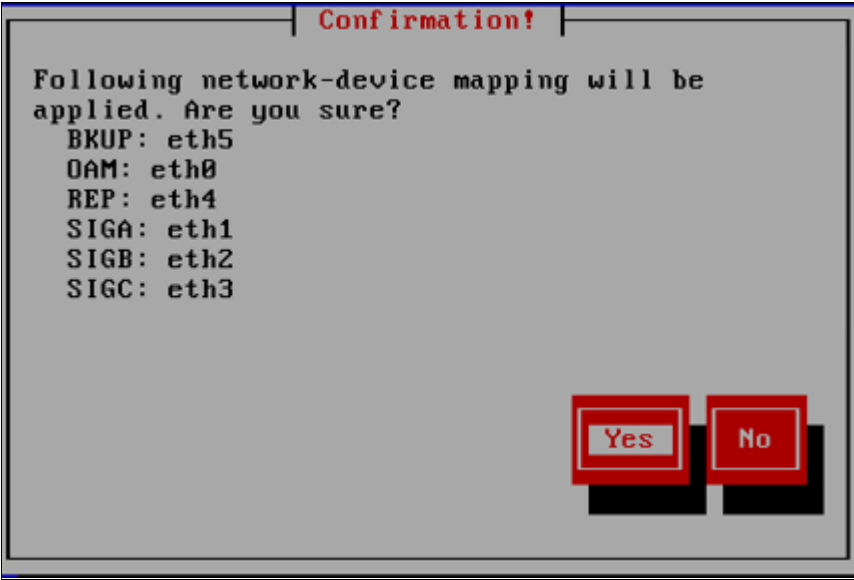
- Access to the powered on Policy Management VM guests

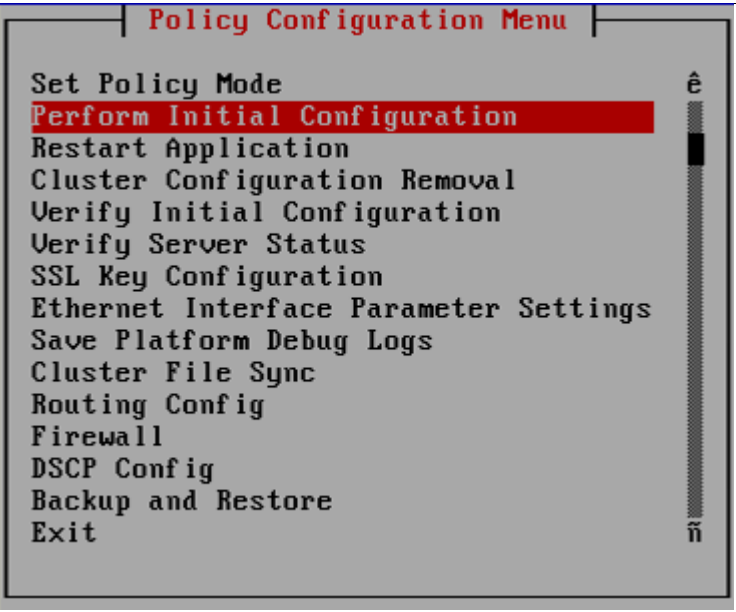
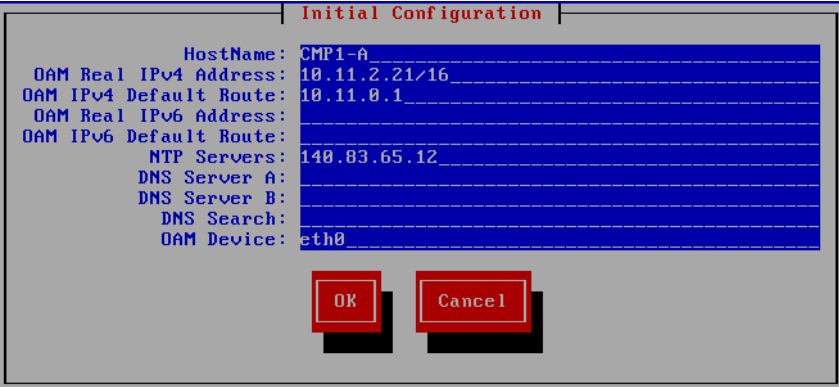
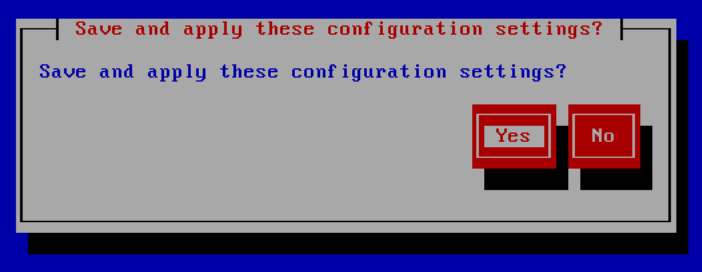
Check off (✓) each step as it is completed. Check boxes are beside each step for this purpose.
If this procedure fails, contact Oracle Technical Services and ask for assistance.

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 <pre>\$ su - platcfg</pre>
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.  <tr><td>10. ☐</td><td>Repeat For Each Policy Management VM</td><td> 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 </td></tr>	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
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---		

5. CONFIGURE POLICY APPLICATION SERVERS IN WIRELESS MODE

The following procedures configure the Policy Management Application and establish the network relationships, to a level that allows a basic test call through the system.

It is assumed that the Installation tasks associated with preparing the appropriate Installation Environment in Section 4 are completed before proceeding with the following tasks.

The post-installation tasks consist of the following:

1. Establishing network addresses and connections for every Policy Management server
2. Configuring the first CMP server
3. Configuring the CMP Site 1 cluster to manage the Policy Management network
4. Configuring a CMP Site 2 cluster for Geo-Redundancy (optional)
5. Configuring Policy Management clusters
6. Exchanging SSH keys between Policy Management servers
7. Configuring routing on servers

[Configuration Management Platform Wireless User's Guide](#)

[Platform Configuration User's Guide](#)

Note:

By default, network architecture with 6 VLANs is available in PCRF. It is not necessary to use 6 network architecture, OAM and SIGA being the minimal requirements.

Customers can use any network for Replication and Heartbeat / Backup Heartbeat. The customer can select any network for replication and define the static IP on path configuration for each server in the cluster.

By default, map the 'eth' networks are mapped to SIG-A/B/C/REP/BKUP as per convention but they can be used by configuring the option.

5.1 Perform Initial Server Configuration of Policy Servers—platcfg

You must configure the operation, administration, and management (OAM) network address of the server, as well as related networking. Perform the referenced procedure on every server in the Policy Management network.

Prerequisites:

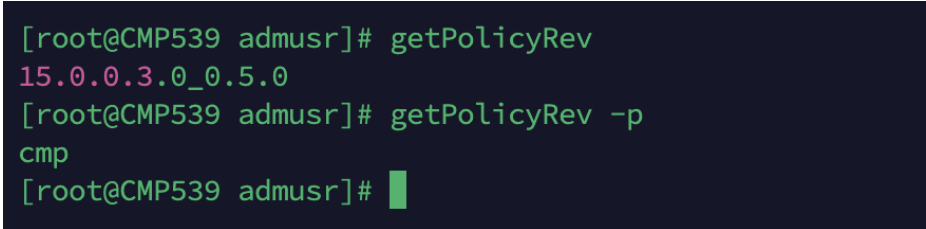
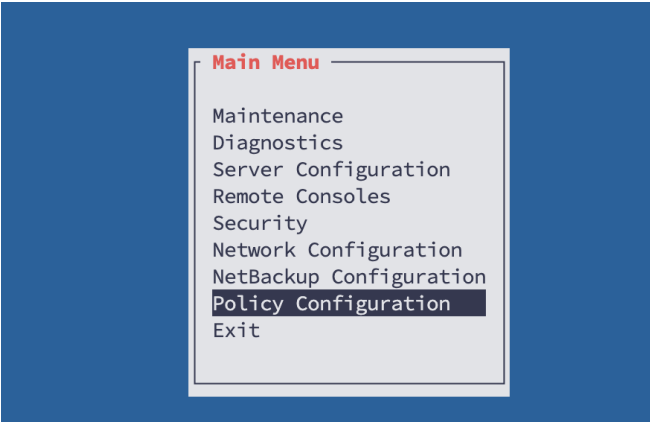
To complete this procedure, you need the following information:

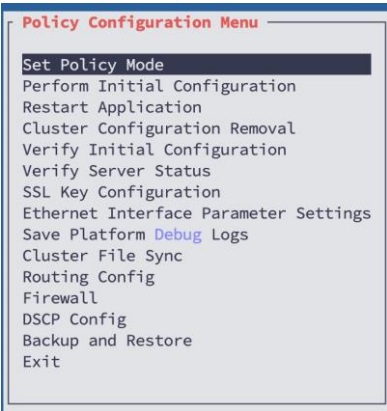
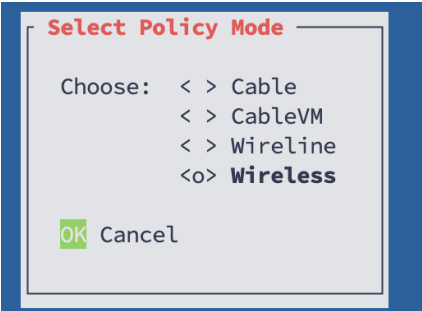
- This procedure assumes that you are using Policy Management in a Wireless.
- Hostname—The unique hostname for the device being configured.
- OAM Real IP IPv4 Address—The IP address that is permanently assigned to this device.
- OAM Default IPv4 Route—The default route of the OAM network. The MPE and MRA system may move the default route to the SIG-A interface after the topology configuration is complete. The default route remains on the OAM interface for the CMP system.
- OAM Real IP IPv6 Address (optional)—The IP address that is permanently assigned to this device.

- OAM Default IPv6 Route (optional)—The default route of the OAM network. Note the MPE and MRA system may move the default route to the SIG-A interface after the topology configuration is complete. The default route remains on the OAM interface for the CMP system.
- NTP Servers—Reachable NTP server) (ntp_address).
- DNS Server A (optional)—A reachable DNS server.
- DNS Server B (optional)—A reachable DNS server.
- DNS Search—The domain name appended to a DNS query.
- Device—The bond interface of the OAM device. Use the default value, as changing this value is not supported.
- OAM VLAN ID—The OAM network VLAN ID.
- SIG A VLAN ID—The Signaling-A network VLAN ID.

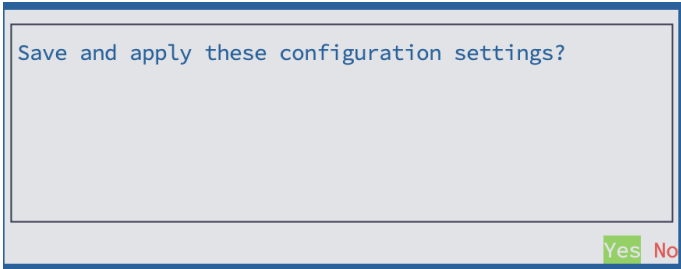
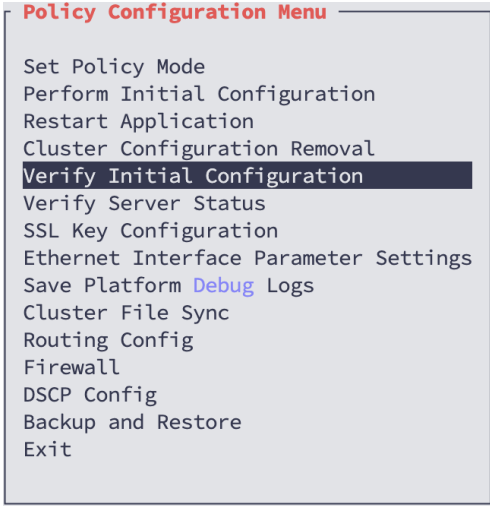
Check off (✓) each step as it is completed. Check boxes are provided next to each step number.
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 12 - Perform Initial Server Configuration of Policy Servers—platcfg

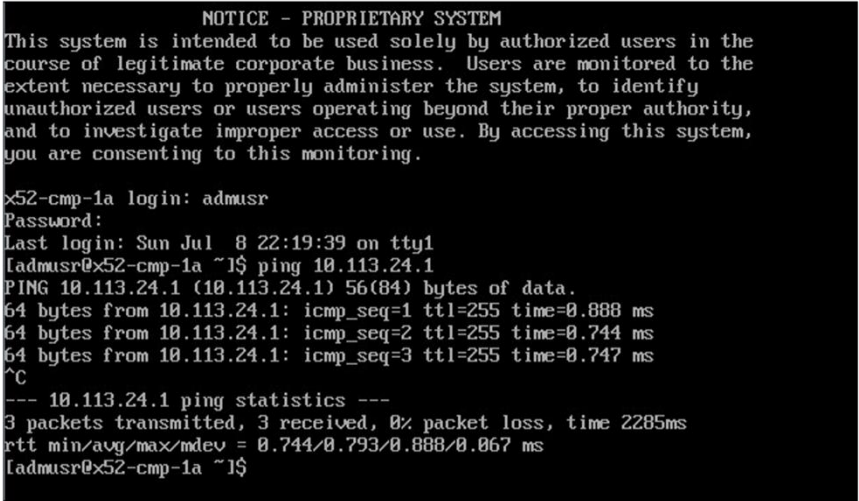
Step	Procedure	Details
1.	Log in to the server and verify the server type	Log in as root, via the Remote Console, and confirm the installed Policy Management software version and server profile # getPolicyRev # getPolicyRev -p  The server profile is either cmp, mpe, mra.
2.	Log in to platcfg	1. Open the platcfg utility by running the following command: # su – platcfg  The platcfg tool opens. 2. Select Policy Configuration.

		3. The policy configuration menu Opens. 
3.	Set Policy Mode	1. Go to the Select Policy Mode menu Select Wireless from the options.  2. Click OK. Wireless is the default configuration. If the current policy mode is Wireless, this prompt is not displayed, and Wireless mode is set. Click Yes. Depending on the hardware configuration, a Select Network Layout screen may open. Refer to Configuration Management Platform Wireless User's Guide (Setting Policy Management Mode) for further detail. If the Select Network Layout screen does not display, you are returned to the Policy Configuration Menu.
4.	Perform Initial Configuration	From the policy Configuration Menu, select Perform Initial Configuration.

		Policy Configuration Menu Set Policy Mode Perform Initial Configuration Restart Application Cluster Configuration Removal Verify Initial Configuration Verify Server Status SSL Key Configuration Ethernet Interface Parameter Settings Save Platform Debug Logs Cluster File Sync Routing Config Firewall DSCP Config Backup and Restore Exit The initial configuration form opens: Initial Configuration HostName: CMP539 OAM Real IPv4 Address: 192.168.5.39/24 OAM IPv4 Default Route: 192.168.5.1 OAM Real IPv6 Address: OAM IPv6 Default Route: NTP Servers: 10.250.32.10 DNS Server A: DNS Server B: DNS Search: OAM Device: eth0 OK Cancel
5.	Perform Initial Configuration	Enter the configuration values and then click OK, where: HostName—The unique name of the host for the device being configured. OAM Real IPv4 Address—The IPv4 address that is permanently assigned to this device. OAM IPv4 Default Route—The IPv4 default route of the OAM network. OAM Real IPv6 Address—The IPv6 address that is permanently assigned to this device. OAM IPv6 Default Route—The IPv6 default route of the OAM network. NTP Server (required)—A reachable NTP server on the OAM network. DNS Server A (optional)—A reachable DNS server on the OAM network. DNS Server B (optional)—A second reachable DNS server on the OAM network. DNS Search—the domain name appended to a DNS query OAM Device—The bond interface of the OAM device. Note that the default value must be used because changing this value is not supported. OAM VLAN—The OAM network VLAN ID (only applies to c-Class servers; field does not display otherwise). NOTE: All the fields listed above are required, except for fields DNS Server and DNS Search, which are optional but recommended. NOTE: Every network service and IP flow that is supported by IPv4 is supported by IPv6. Either interface or a combination of the two is configured. 1. Enter the configuration information.

		2. Click OK to save and apply the configuration. At this point the screen pauses for approximately a minute. This is normal behavior. 3. A confirmation message displays, click YES to save and apply the configurations.  The platcfg form processes the configuration of the server, and then it returns to the platcfg menu.
6.	Verify Initial Configuration	From the policy Configuration Menu, select Verify Initial Configuration. 

		Platform Configuration Utility Copyright (C) 2003, 2024, Oracle and/or its affiliates. All rights reserved. Hostname: CHPS39 Index Table of Contents Date/Time: 08/30/2024 14:07:02 Hardware Type: KVM BRIUPDevice="eth0" DNSSearch="" DNSServerAs="" DNSServerB="" DefaultGw="192.168.5.1" DefaultIPv6Gw="" Device="eth0" HostName="CHPS39" LayoutProfile="cloudinit" NtpServIPAddr="10.250.32.10" OAMDevice="eth0" OAMMTU="1450" REFDevice="eth4" SIGADevice="eth1" SIGAMTU="1450" SIGBDDevice="eth2" SIGBMTU="1450" SIGGDevice="eth3" ServIPAddr="192.168.5.39/24" ServIPv6Addr="" NTP Status: Name/IP Address NP NR Span Frequency Freq Skew Offset Std Dev ===== ntpserver1 6 3 77m -0.065 0.571 -11us 250us Forward Backward Top Bottom Exit
7.	Verify Server Status	Exit from this screen and select Verify Server Status: Policy Configuration Menu Set Policy Mode Perform Initial Configuration Restart Application Cluster Configuration Removal Verify Initial Configuration Verify Server Status SSL Key Configuration Ethernet Interface Parameter Settings Save Platform Debug Logs Cluster File Sync Routing Config Firewall DSCP Config Backup and Restore Exit Index Table of Contents Policy Process Management Status: Running Server Role: Unknown NOTES: At this point in the installation procedure, the Server Role is Unknown. Unknown is a valid state during initial configuration because the cluster is not formed. If the product is MPE the Policy Process Management Status is Not Running. Not Running is a valid state for MPE in this step. Click Exit until you exit the platcfg utility. You are returned to Linux prompt screen.

8.	Ping the OAM default gateway to verify server is available on the network	From the Linux command prompt ping the OAM gateway (default Gateway from the initial config procedure) to verify that the gateway is reachable. Ping the OAM gateway to verify that it is reachable:  <pre> NOTICE - PROPRIETARY SYSTEM This system is intended to be used solely by authorized users in the course of legitimate corporate business. Users are monitored to the extent necessary to properly administer the system, to identify unauthorized users or users operating beyond their proper authority, and to investigate improper access or use. By accessing this system, you are consenting to this monitoring. x52-cmp-1a login: admusr Password: Last login: Sun Jul 8 22:19:39 on tty1 [admusr@x52-cmp-1a ~]\$ ping 10.113.24.1 PING 10.113.24.1 (10.113.24.1) 56(84) bytes of data. 64 bytes from 10.113.24.1: icmp_seq=1 ttl=255 time=0.888 ms 64 bytes from 10.113.24.1: icmp_seq=2 ttl=255 time=0.744 ms 64 bytes from 10.113.24.1: icmp_seq=3 ttl=255 time=0.747 ms ^C --- 10.113.24.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2285ms rtt min/avg/max/mdev = 0.744/0.793/0.888/0.067 ms [admusr@x52-cmp-1a ~]\$ </pre> If the gateway is reachable it is possible to SSH to the server IP and login as admusr If you cannot SSH to the configured server or cannot reach the OAM gateway, review the initial configurations and review the network setup to ensure there are not any connectivity issues. Run <code>ip -4 addr</code> (IPv4) or <code>ip -6 addr</code> (IPv6) to confirm the IP addresses configured during the initialization are present.

5.2 Perform Initial Configuration of the Policy Servers—CMP GUI

This procedure performs initial configuration of the CMP GUI on the installed environment.

Note: In a deployment that has Geo-Redundant CMP servers (that is, CMP servers at two different sites), the other pair of CMP servers are added to the network topology using the CMP server at Site 1. The CMP Site 1 cluster pushes the configuration to the Site 2 (Geo-Redundant) CMP servers later.

This procedure configures the CMP at the active site (CMP Site 1).

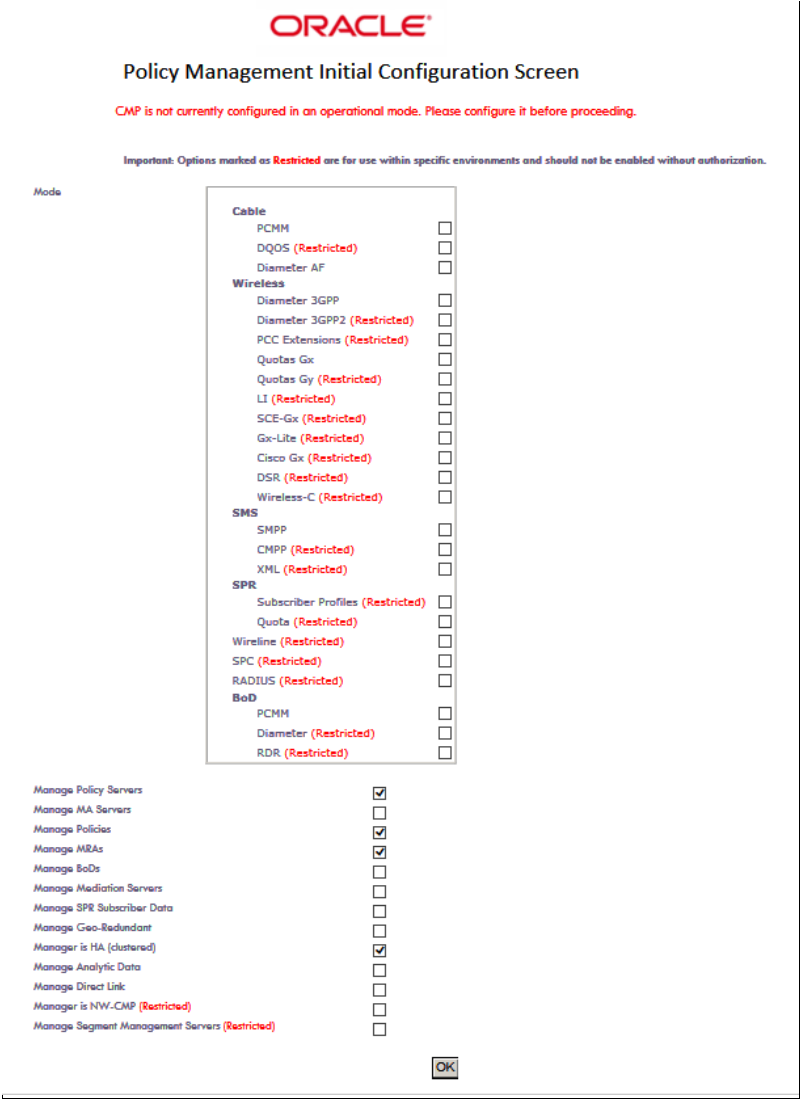
Prerequisites:

- Network access to the CMP OAM REAL IP address, to open a web browser (HTTP)
- If network access to the CMP is not available and the installation has an Aggregation switch, then a laptop is configured to use a port on the Aggregation switch to access the CMP GUI. If an Aggregation switch is not available, a temporary switch may be used to provide network access to the CMP GUI.

Check off (✓) each step as it is completed. Check boxes are provided next to each step number.
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 13 - Perform Initial Configuration of the Policy Servers—CMP GUI

Step	Procedure	Details
1. ☐	CMP GUI	Open CMP GUI for the first time by opening the CMP OAM IP address in a supported browser: <code>http://<cmp_real_OAM_ip></code> NOTE: The initial GUI configuration is performed on either CMP that is located at Site1. If this is not a geo-redundant solution, there is not a Site 2 location. If Network access is not enabled and the Installation has an Aggregation switch, then a laptop is configured to use a port on the Aggregation switch to access the CMP GUI. Alternately, if an Aggregation switch is not available, a temporary Aggregation switch may be needed during installation.

Step	Procedure	Details
2. ☐	CMP GUI: Set CMP Mode in 1 st selected CMP	After you are connected to the CMP GUI for the first time, you are prompted to configure operation mode settings for the system, which define what functionality is configurable from the CMP GUI. The selection depends on the deployment. The Policy Management Initial Configuration Screen presents as follows:  NOTE: Modes are changed at a later time if needed, but the method to access to this mode selection is not documented.] Contact Oracle Support if Mode selection is changed after the initial configuration.
3. ☐	CMP GUI: Set CMP Mode in 1 st selected CMP	This configuration example provides basic functionality for a Policy Wireless solution. The wireless mode of operation was confirmed in earlier procedures. (Selections are for example only). For more detail, refer to the CMP Modes section of the Configuration Management Platform Wireless User's Guide

NOTE: Restricted mode options are only selected with the advice of an Oracle Support representative.

The following examples are for reference only. The particular requirements for any given configuration may be specific a customer.

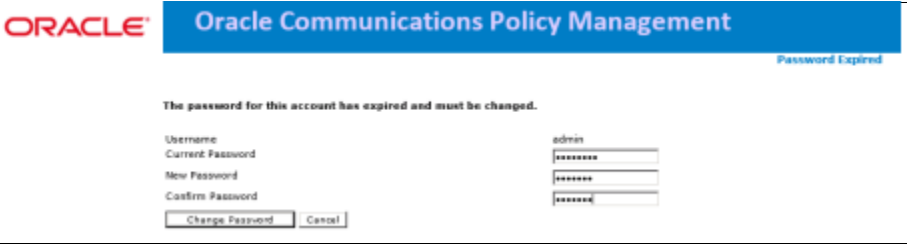
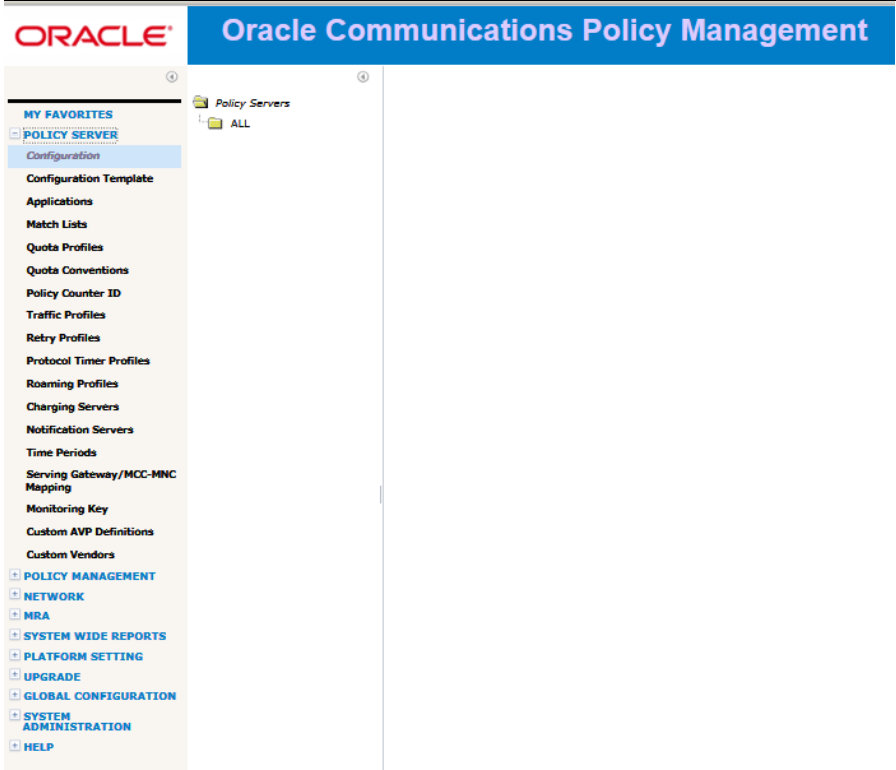
For a Wireless network:

- Wireless: Diameter 3GPP
- Quotas Gx
- Manage Policy Servers
- Manage Policies
- Manage MRAs
- Manage Geo-Redundant
- Manager is HA (clustered)

For a Wireless-C network:

- Wireless: Diameter 3GPP, Quotas Gx, DSR, Wireless-C; SMS: CMPP
- Manage Policy Servers
- Manage Policies
- Manage MRAs
- Manage SPR Subscriber Data

Step	Procedure	Details
		Manager is HA (clustered) About using Wireless-C Mode: Wireless-C supports a wireless system supporting SMS Notification Statistics and SCTP counters Additional Information: Diameter 3GPP, 3GPP2(Restricted) and Gx-Lite (Restricted) enable the functionality required to support these protocols in a Policy Management solution LI (Restricted) is used if the MPE installation uses LI (Lawful Intercept) functions. To use this option, the LI version of the MPE ISO image must be installed on the MPEs in the Policy Management solution. Contact Oracle Support for additional Information. Manage Policy Servers and Manage Policies are basic functions of the Policy Management solution Manage MRAs is only needed if MRAs, which are optional, are planned in the deployment Manager is HA (clustered) provides High Availability functionality for a clustered pair of servers. Manager is NW CMP and Manager is S-CMP are specific to a Tiered CMP System deployment. Refer to Configuration Management Platform Wireless User's Guide for the procedure to deploy a Tiered CMP System. NOTE: The mode selections on this form depend on the deployment. Conform the selections with the engineering team responsible for the planned Policy Management solution deployment.
4. ☐	CMP GUI: Login to CMP GUI	After finishing the policy mode selection and clicking OK, login screen displays. 

Step	Procedure	Details
5. ☐	CMP GUI: Set admin password	Initial, default login is admin/policies After login, the system prompts you to change the admin password.  Enter the default password then the new password twice and click Change Password.
6. ☐	CMP GUI: Verify that the CMP GUI is displayed, with expected menus.	
—End of Procedure—		

5.3 Performing SSH Key Exchanges

You must exchange SSH keys between the CMP, MPE, MRA servers. Perform this procedure whenever you add additional servers to the Policy Management topology. You can run the command multiple times, even if keys were exchanged

Note: After the topology is set up and SSH keys are exchanged, it is possible that a server in the topology changes its keys. This happens when:

- A server is added to the topology

- A server is re-installed
- A server is replaced by another server
- A server has its SSH keys recreated manually

In any of the above scenarios, rerun this procedure. The SSH provisioning utility rechecks the existing SSH key exchanges in the topology and provisions any key exchanges not performed. You can run the command multiple times, even if keys were exchanged.

Prerequisite:

- CMP Site 1 cluster is configured and GUI available
- Before beginning this procedure, the systems that are exchanging keys must be configured and reachable.

Check off (✓) each step as it is completed. Check boxes are provided next to each step number.
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 14 - Performing SSH Key Exchanges

Step	Procedure	Details
1. ☐	Ssh to CMP Site 1 active server: Run Key Exchanges on all servers	1. Use SSH to connect to the active server at the CMP Site 1 cluster as the admusr user. 2. Enter the command <code>sudo ha.mystate</code> to confirm that the server is the active server in the HA cluster. The following example shows an active server: <pre>login as: admusr Using keyboard-interactive authentication. Password: [admusr@cmp236 ~]\$ sudo ha.mystate resourceId role node subResources lastUpdate DbReplication Active A0582.070 0 0425:164256.062 VIP Active A0582.070 0 0425:164256.064 QP Active A0582.070 0 0425:164256.104 DbReplication cld OOS A0582.070 0 0425:164245.744 [admusr@cmp236 ~]\$</pre>
2. ☐	Ssh to CMP Site 1 active server: Run Key Exchanges on all servers	1. Enter the following command: <pre>\$ sudo qpSSHKeyProv.pl-prov (double dash)</pre> You are prompted: The password of admusr in topology 2. Enter the admusr password (<i>admusr_password</i>). The procedure exchanges keys with the rest of the servers in the Policy Management topology. If the key exchange is successful, the procedure displays the message SSH keys are OK. The following example shows a successful key exchange:

		<pre>C[admusr@x52cmp-1a ~]\$ sudo qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@x52mpe-1b ... Connecting to admusr@x52mra-1b ... Connecting to admusr@x52mpe-1a ... Connecting to admusr@x52mra-1a ... Connecting to admusr@x52cmp-1a ... Connecting to admusr@x52cmp-1b ... [1/6] Provisioning SSH keys on x52mpe-1b ... [2/6] Provisioning SSH keys on x52mra-1b ... [3/6] Provisioning SSH keys on x52mra-1a ... [4/6] Provisioning SSH keys on x52mpe-1a ... [5/6] Provisioning SSH keys on x52cmp-1a ... [6/6] Provisioning SSH keys on x52cmp-1b ... SSH keys are OK.</pre>
3. ☐	SSH to CMP Site 1 active server: Verify Key Exchanges on all servers	1. Enter the following command to verify that the keys are successfully exchanged: <pre>\$sudo qpSSHKeyProv.pl-check-verbose</pre> You are prompted for the password of admusr in topology. 2. Enter the admusr password (admusr_password). The procedure verifies keys with the rest of the servers in the Policy Management topology and displays the results of each exchange. The following example shows all keys are checked and exchanged successfully:

		<pre>[admusr@x52cmp-1a ~]\$ sudo qpSSHKeyProv.pl --check --verbose The password of admusr in topology: Connecting to admusr@x52mpe-1b ... Connecting to admusr@x52mra-1b ... Connecting to admusr@x52mpe-1a ... Connecting to admusr@x52mra-1a ... Connecting to admusr@x52cmp-1a ... Connecting to admusr@x52cmp-1b ... [1/6] Checking SSH keys on x52mpe-1b ... [2/6] Checking SSH keys on x52mra-1b ... [3/6] Checking SSH keys on x52mra-1a ... [4/6] Checking SSH keys on x52mpe-1a ... [5/6] Checking SSH keys on x52cmp-1a ... [6/6] Checking SSH keys on x52cmp-1b ... From root@x52cmp-1b (10.240.220.230): to root@x52cmp-1b (10.240.220.230): OK to root@x52mra-1a (10.240.220.232): OK to root@x52cmp-1a (10.240.220.229): OK to root@x52mpe-1b (10.240.220.236): OK to root@x52mpe-1a (10.240.220.235): OK to root@x52mra-1b (10.240.220.233): OK From root@x52mra-1a (10.240.220.232): to root@x52mra-1b (10.240.220.233): OK From root@x52cmp-1a (10.240.220.229): to root@x52cmp-1b (10.240.220.230): OK to root@x52mra-1a (10.240.220.232): OK to root@x52cmp-1a (10.240.220.229): OK to root@x52mpe-1b (10.240.220.236): OK to root@x52mpe-1a (10.240.220.235): OK to root@x52mra-1b (10.240.220.233): OK From root@x52mpe-1b (10.240.220.236): to root@x52mpe-1a (10.240.220.235): OK From root@x52mpe-1a (10.240.220.235): to root@x52mpe-1b (10.240.220.236): OK From root@x52mra-1b (10.240.220.233): to root@x52mra-1a (10.240.220.232): OK SSH keys are OK. [admusr@x52cmp-1a ~]\$</pre>
—End of Procedure—		

5.4 Configure Routing on Your Servers

On the MPE and MRA servers, the default route is initially configured to route all traffic via the OAM interface for remote servers. This facilitates clustering and topology configurations. However, in many networking environments, it is desirable to route signaling traffic (that is, Diameter messages) using the Signaling interfaces of the servers and switches, and OAM traffic (that is, replication, configuration, alarms, and reports) using the OAM interface. This requires configuring routing on the servers.

If you are using the Signaling interfaces, you must configure the required static routes on the MPE and MRA servers to separate OAM and Signaling traffic. The recommended method to provide separation is:

- Add static routes on the OAM network to management servers (CMP, NTP, SNMP, PM&C).
Note: Administration of the MPE and MRA servers that require SSH access may be impacted by moving the default gateway and may need static routes as well.
- Change the default route on the servers to the Sig-A network.

In this way, traffic to other signaling points in the network follows the default route over the Sig-A network.

Other routing configurations may be required, depending on your needs.

Prerequisite:

Before beginning this procedure, verify that you have SSH access to the MPE and MRA servers.

You need the following information to complete this procedure:

- The root account password (root_password)
- At a minimum, the following static routes:
 - o Site 1 and 2 CMP OAM network (if not co-located)
 - o Server C for georedundant MPE and MRA clusters
 - o NTP server
 - o DNS server
 - o snmp_trap_destination (SNMP trap destination)
 - o Remote backup archives
 - o External syslog servers
 - o Any host you wish the MPE or MRA server to access over the OAM network (that is, routes to mates in georedundant networks)

The procedure for configuring routing on your servers is described in the [Platform Configuration User's Guide](#)

Tip: During this procedure, ensure that access to the server ILOM or iLO remote console is always available if a route change impacts remote access to get back into the server. Using SSH from the CMP system to connect to the MRA or MPE servers is recommended to minimize such impacts.

Note: You must perform this procedure for every MPE and MRA server. Perform this procedure only for the MPE and MRA servers, as the CMP system retains the default route on the OAM interface.

5.5 Configure Policy Components

This section covers procedures to configure the Policy Servers to a minimum level to perform a test call.

5.5.1 Adding MPE and MRA to CMP Menu

This procedure configures the Policy Server (MPE) and MRA applications.

Prerequisite:

- Network access to the CMP OAM IP address, to open a web browser (HTTP)
- MRA and MPE clusters are added to the CMP Topology

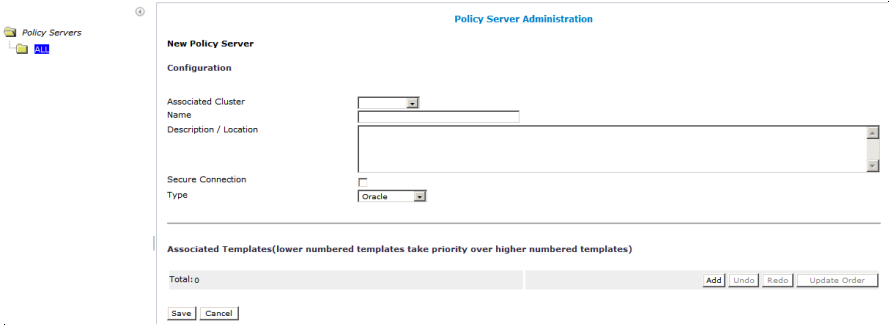
NOTE: Only the following Web Browsers are supported in OCPM 12.6.1

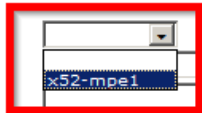
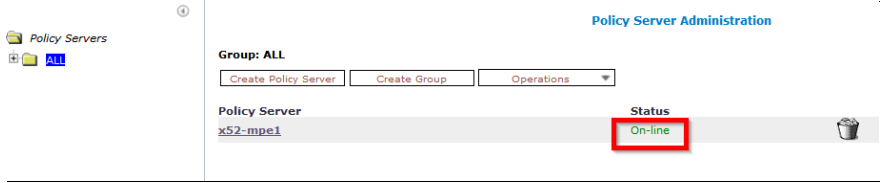
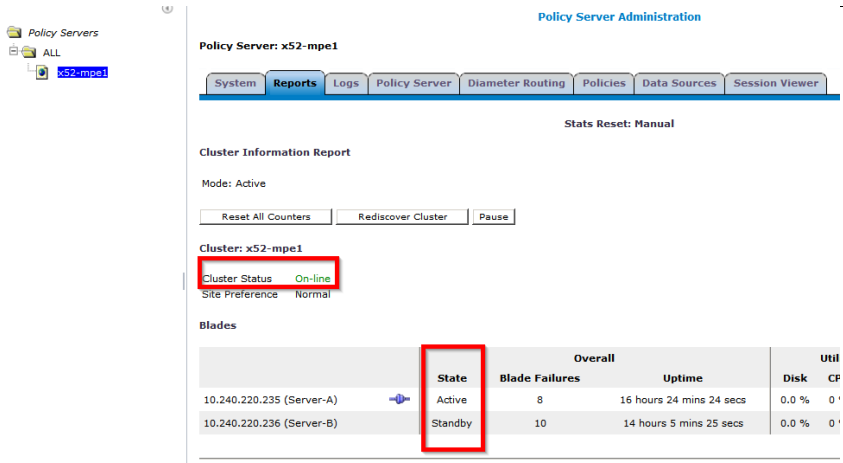
- o Mozilla Firefox® release 81.0 or later
- o Google Chrome version 86.0 or later

*Internet Explorer is not supported for this procedure

Check off (✓) each step as it is completed. Check boxes are provided next to each step number.
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 15 - Adding MPE and MRA to the CMP Menu

Step	Procedure	Details
1. ☐	Create Policy Server in CMP GUI	1. Navigate to Policy Server→ Configuration→ Policy Servers  2. Click Create Policy Server in the Policy Server Administration screen:  3. Enter values for the configuration attributes: a. Associated Cluster (required)—Select the cluster with which to associate this MPE device. MPE clusters configured in Topology Settings are listed. b. Name—Name of this MPE device. The default is the associated cluster name. c. Description/Location (optional)—Information that defines the function or location of this MPE device. d. Secure Connection—Designates whether or not to use the HTTPS protocol for communication (certificates must be configured to use this option) between Policy Management devices. If selected, devices communicate over port 8443. e. Type—Defines the policy server type: ☐ Oracle (default)—The policy server is an MPE device and is managed by the CMP. ☐ Unmanaged—The policy server is not an MPE device and therefore cannot be actively managed by the CMP. This selection is useful when an MPE device is routing traffic to a non-Oracle policy server. NOTE: When configuring an associated cluster, the menu is populated with MPE clusters that are configured in the CMP Topology from previous steps.

Step	Procedure	Details
		New Policy Server Configuration Associated Cluster Name Description / Location  4. Click Save and confirm Configured Policy Server status is On-line. 
2. ☐	Check MPE cluster in Reports tab	1. Navigate to Policy Server→Configuration→ <MPE>→ Reports tab  2. Validate that MPE cluster status is On-line and that both active and standby servers displayed correctly.
3. ☐	Diameter configuration of MPE	1. Nvaigate to Policy Server→ Configuration→ <MPE>→Policy Server tab There are many configurations on Policy Server tab for an associated MPE. The most important configurations to define is Diameter Realm and identity to enable Diameter connections.

Step

Procedure

Details

Policy Servers

ALL

MPE01

Cache Quota Usage

true

false

undefined

Cache Entity State

true

false

undefined

Subscribe Quota Usage

true

false

undefined

Subscribe Entity State

true

false

undefined

Diameter

Diameter Realm

oracle.com

Diameter Identity

pcrf.oracle.com

Default Resource Id

Correlate PCEF sessions

true

false

undefined

Validate user

true

false

undefined

Diameter PCEF Default Profile

N/A

Use Synchronous Sd

true

false

undefined

Identify Duplicate sessions based on APN

true

false

undefined

Subscriber ID to detect duplicate sessions

Protocol Timer Profile

Prevent Overlapping Rule Names

true

false

undefined

S9:

Initiate S9 Requests

true

false

undefined

Accept S9 Requests

true

false

undefined

Primary DEA

<None>

Secondary DEA

<None>

2. To define these Diameter parameters, click **Modify**.

3. Enter the Diameter Realm and Identity for your network

4. Click **Save**

Attribute	Description
Diameter Realm	The domain of responsibility (for example, galactel.com) for the MPE device.
Diameter Identity	The fully qualified domain name (FQDN) of the MPE device (for example, mpe3.galactel.com).

For example:

Diameter

Diameter Realm

oracle.com

Diameter Identity

pcrf.oracle.com

Default Resource Id

<None>

Correlate PCEF sessions

Yes

Validate user

No

Diameter PCEF Default Profile

<None>

Use Synchronous Sd

No

Identify Duplicate sessions based on APN

No

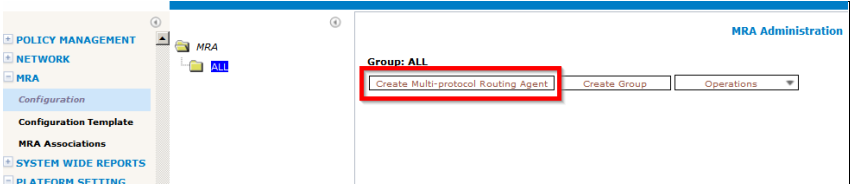
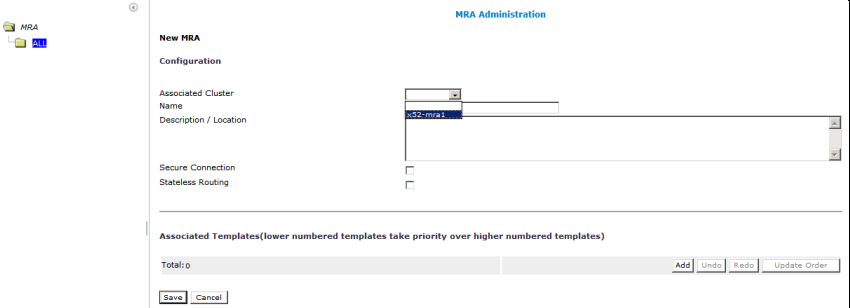
Subscriber ID to detect duplicate sessions

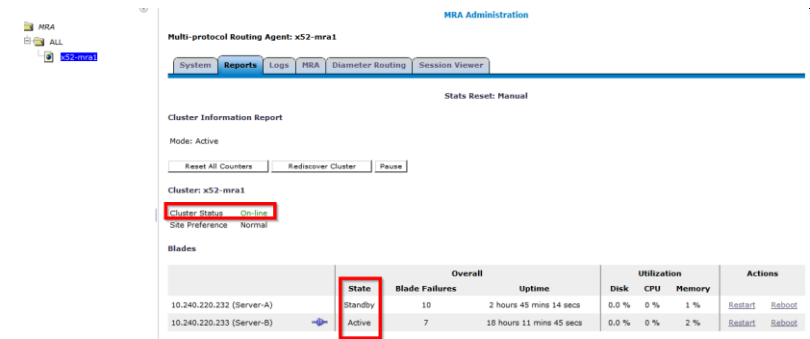
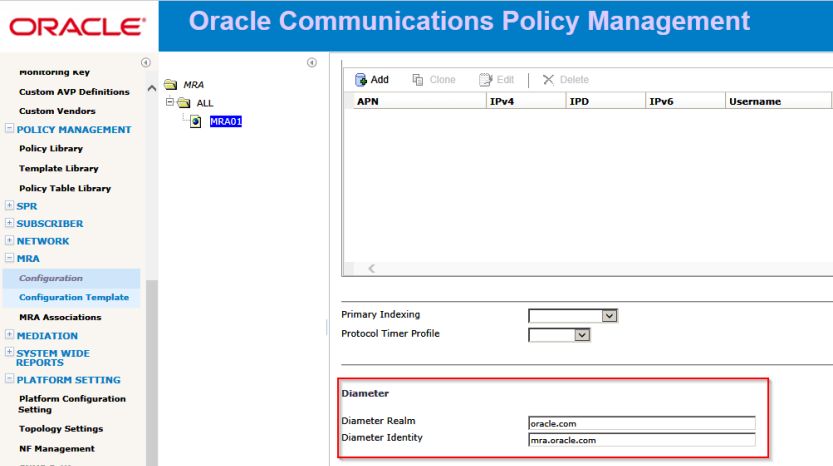
Prevent Overlapping Rule Names

false

Protocol Timer Profile

undefined

Step	Procedure	Details
4. ☐	Create MRA in CMP GUI	1. Navigate to MRA → Configuration → ALL  2. Click Create Multi-protocol Routing Agent in the MRA Administration screen:  3. Enter information as appropriate for the MRA cluster: - Associated Cluster (required)—Select the MRA cluster from the list. - Name (required)—Enter a name for the MRA cluster. - Description/Location (optional)—Free-form text. Enter up to 250 characters. - Secure Connection—Select to enable a secure HTTP connection (HTTPS) instead of a normal connection (HTTP). The default is a non-secure (HTTP) connection. - Stateless Routing—Select to enable stateless routing. In stateless routing, the MRA cluster only routes traffic; it does not process traffic. The default is stateful routing. 4. Click Save and confirm that the configured MRA status is On-line. 

Step	Procedure	Details
5. ☐	Check MRA cluster in Reports tab	5. Navigate to MRA → Configuration → MRA → Reports tab  6. Validate that MPE cluster status is On-line and that both active and standby servers display correctly.
6. ☐	Diameter configuration for MRA	1. Navigate to MRA → Configuration → MRA → MRA tab It is important to define Diameter Realm and identity to enable Diameter messaging to function:  2. To define these Diameter parameters, click Modify 3. Enter the Diameter Realm and Identity that your network uses. 4. Click Save. Diameter Diameter Realm Diameter Identity oracle.com mra.oracle.com
—End of Procedure—		

5.5.2 Configure MPE Pool on MRA (Policy Front End)

If MRAs (Policy Front End) are used in the Policy Management System, the MPEs for which the MRA acts as the Policy Front End, must be added to the MPE Pool on the MRA. If MPEs are not used in the Policy solution, skip this procedure.

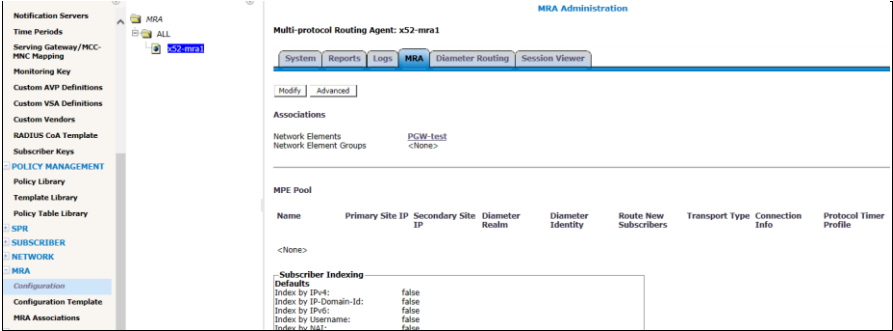
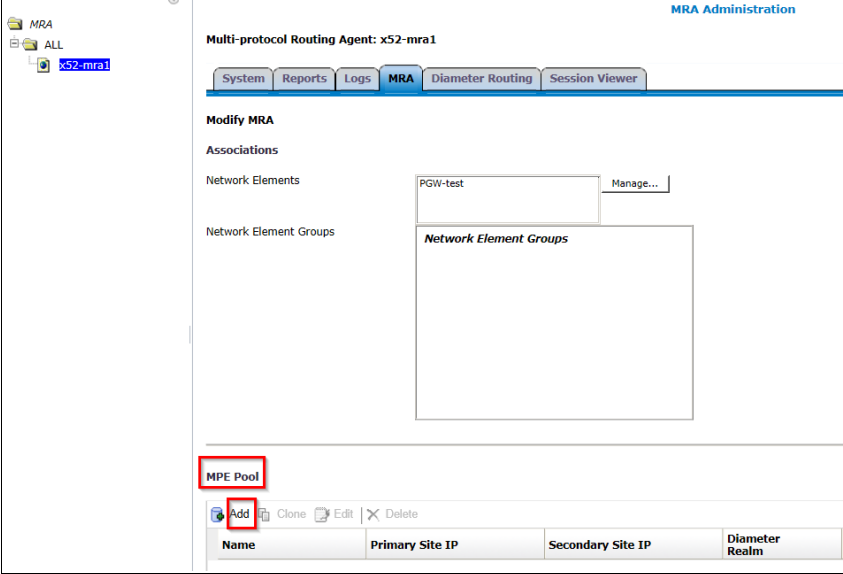
This procedure adds the MPE clusters to the MPE Pool of the MRA (Policy Front End)

Prerequisite:

- Network access to the CMP OAM IP address, to open a web browser (HTTP)
- MRA and MPE clusters are added to the CMP Menu

Check off (✓) each step as it is completed. Check boxes are provided next to each step number.
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 16 - Configure MPE Pool on MRA (Policy Front End)

Step	Procedure	Details
1. ☐	Configure MPE Pool on MRA	1. Navigate to MRA → Configuration → <MRA> → MRA tab  2. Click Modify in the MRA Administration screen: The MPE Pool configuration form opens.  3. Click Add under MPE Pool. The Add Diameter MPE Peer form opens.

Add Diameter MPE Peer

MPE TypeInternal

Associated MPEx52-mpe1

Namex52-mpe1

Primary Site IP10.196.239.38

Secondary Site IP

Diameter Realmoracle.com

Diameter Identityx52-mpe1.oracle.com

Protocol Timer Profileundefined

Route New Subscribers☒

Transport

☒ TCP

Connections1

☐ SCTP

Max Incoming Streams8

Max Outgoing Streams8

Save

Cancel

4. On the Add Diameter MPE Peer form, select an MPE cluster in the Associated MPE list.

The Associated MPE list, shows the MPE clusters configured in the CMP topology.

Add Diameter MPE Peer

MPE Type

Internal

Associated MPE

x52-mpe1

Name

Primary Site IP

Secondary Site IP

Diameter Realm

Diameter Identity

Protocol Timer Profile

undefined

Route New Subscribers

☒

Transport

☒ TCP

Connections

1

☐ SCTP

Max Incoming Streams

8

Max Outgoing Streams

8

Save

Cancel

Add Diameter MPE Peer

MPE TypeInternal

Associated MPEx52-mpe1

Namex52-mpe1

Primary Site IP10.196.239.38

Secondary Site IP

Diameter Realmoracle.com

Diameter Identityx52-mpe1.oracle.com

Protocol Timer Profileundefined

Route New Subscribers☒

Transport

☒ TCP

Connections1

☐ SCTP

Max Incoming Streams8

Max Outgoing Streams8

Save

Cancel

The required fields auto-populate.

5. Click **Save**

NOTE: The Diameter Realm and Diameter Identity must be configured on the MPE.

The MPE cluster is listed in the MPE Pool.

MPE Pool

 Add	 Clone	 Edit	 Delete	
Name	Primary Site IP	Secondary Site IP	Diameter Realm	Diameter Identity
x52-mpe1	10.196.239.38		oracle.com	x52-mpe1.oracle.com

6. Navigate to the bottom of the form and click **Save** again.

Diameter Identitynetramra.oracle.com

S9

Primary DEA<None>

Secondary DEA<None>

Save

Cancel

The MPE cluster is listed in the MPE Pool.

MPE Pool

Name	Primary Site IP	Secondary Site IP	Diameter Realm	Diameter Identity	Route New Subscribers	Transport Type	Connection Info
x52-mpe1	10.196.239.38		oracle.com	x52-mpe1.oracle.com	true	TCP	Connections : 1

7. Confirm the Diameter connection to the MPE from the MRA on the MRA Reports tab

Navigate to **MRA → Configuration → <MRA> → Reports** tab

MRA

ALL

x52-mra1

Multi-protocol Routing Agent: x52-mra1

SystemReportsLogsMRADiameter RoutingSession Viewer

Stats Reset: Manual

Cluster Information Report

Mode: Active

Reset All CountersRediscover ClusterPause

Cluster: x52-mra1

Cluster Status On-line

Blades

	State	Blade Failures	Overall Uptime
10.240.220.232 (Server-A)	Standby	10	1 day 5 hours 30 mins 33 secs
10.240.220.233 (Server-B)	Active	7	1 day 20 hours 57 mins 5 secs

Protocol Statistics

Name	Connections	Total client messages in / out	Total messages timeout
Diameter			
Diameter AF Statistics	1	0 / 0	0
Diameter PCEF Statistics	1	0 / 0	0
Diameter CTF Statistics	1	0 / 0	N/A
Diameter BBREF Statistics	1	0 / 0	0
Diameter S9 Statistics	1	0 / 0	0
Diameter TDF Statistics	1	0 / 0	0
Diameter DRMA Statistics	1	14 / 14	0

A 1401 Log is noted in the MPE Trace Log that the Diameter connection between the MRA and the MPE is established.

1401 Warning Diameter:Transport connection opened with peer 10.196.68.10:34824

—End of Procedure—

5.5.3 Define and Add Network Elements

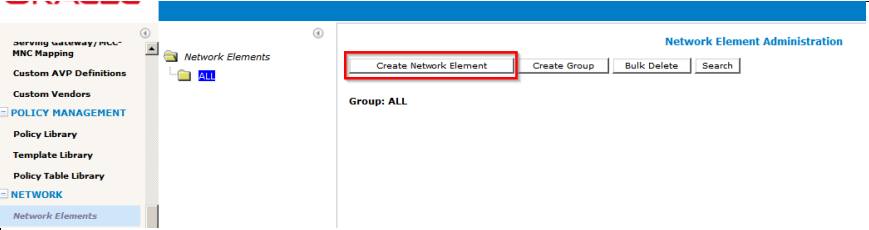
Network elements are configured in the CMP to define the external systems that the Policy Server communicates.

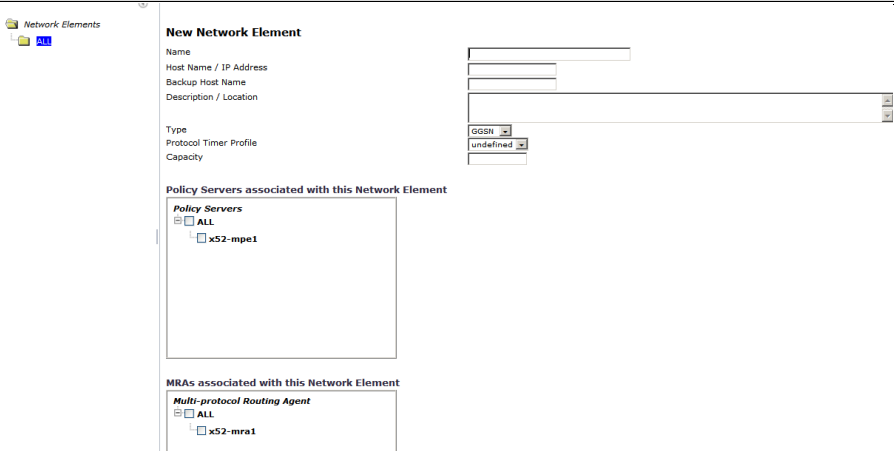
Prerequisite:

- Network access to the CMP OAM IP address, to open a web browser (HTTP)
- MRA and MPE clusters are added to the CMP Menu

Check off (✓) each step as it is completed. Check boxes are provided next to each step number.
If this procedure fails, contact Oracle Technical Services and ask for assistance.

Procedure 17 - Define and Add Network Elements

Step	Procedure	Details
1. ☐	Create Network Element in CMP GUI	1. Navigate to Network→Network Elements→All  2. Click Create Network Element on the Network Element Administration screen:

Step	Procedure	Details
		
		3. Enter information for the network element: Name (required)—The name of the network element. Host Name/IP Address (required)—Registered domain name, or IP address in IPv4 or IPv6 format, of the network element. Backup Host Name (optional)—Alternate address that is used if communication between the MPE device and the primary address for the network element fails. Description/Location (optional)—Free-form text. Enter up to 250 characters. Type (required)—Select the type of network element. The supported types are: NOTE: This list varies depending on the configuration of the CMP system. ? PDSN—Packet Data Serving Node (with the sub-types Generic PDSN or Starent) ? HomeAgent—Customer equipment Home Agent ? GGSN (default)—Gateway GPRS Support Node ? HSGW—HRPD Serving Gateway ? PGW—Packet Data Network Gateway ? SGW—Serving Gateway ? DPI—Deep Packet Inspection device ? DSR—Diameter Signaling Router device ? NAS—Network Access Server device Protocol Timer Profile—select a protocol timer profile. For information on creating protocol timers, see Managing Protocol Timer Profiles in the Configuration Management Platform Wireless User’s Guide Capacity—Not applicable. - When you finish, click Save. - For this example a PGW Network Element is defined.

Step	Procedure	Details
		New Network Element Name Host Name / IP Address Backup Host Name Description / Location Type Protocol Timer Profile Capability Capacity PGW undefined Usage-Report-26

4. After completing the form, click **Save**.

Network Elements

ALL

Network Element Administration

Create Network Element>Create Group>Bulk Delete>Search

Group: ALL

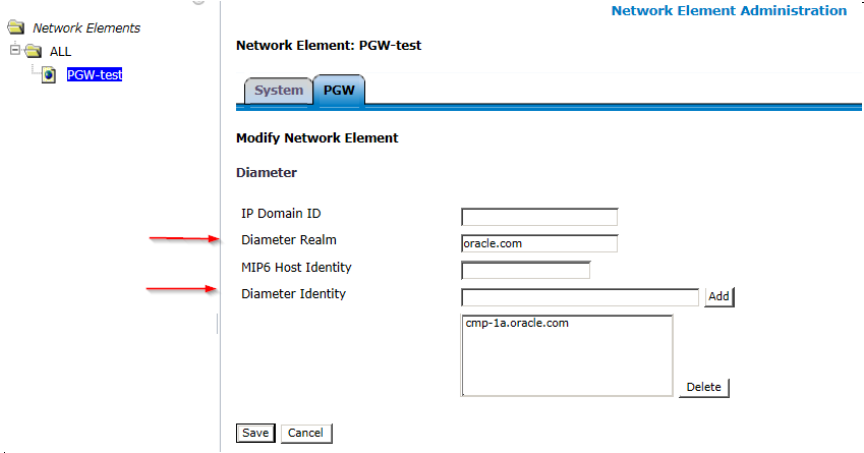
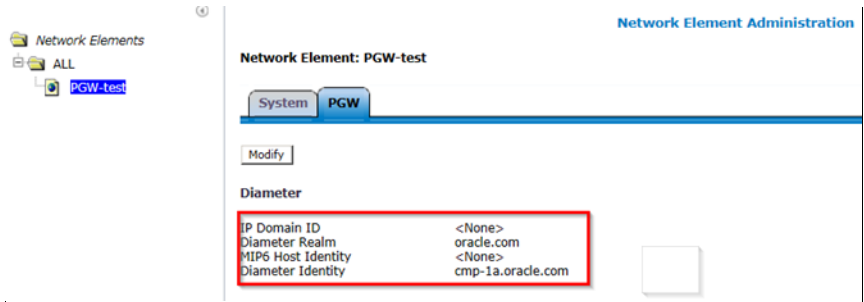
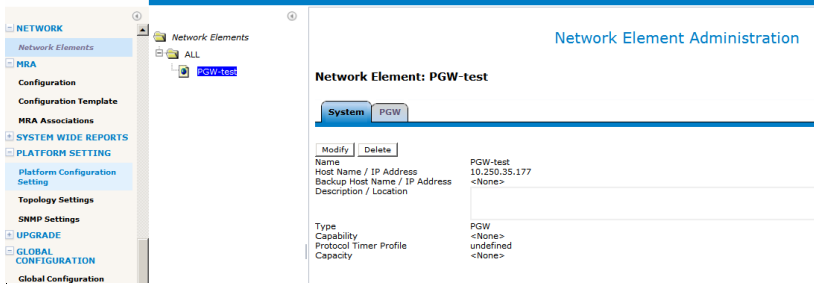
Name

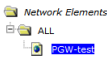
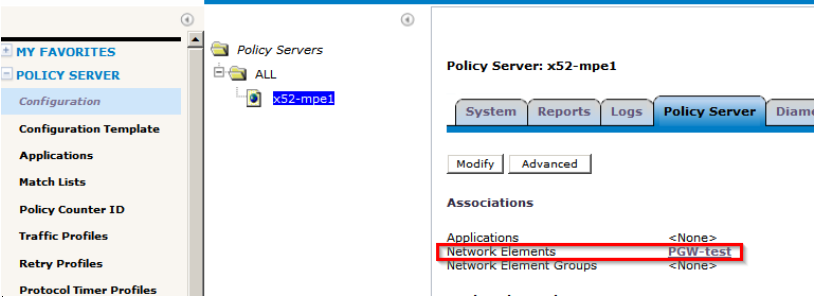
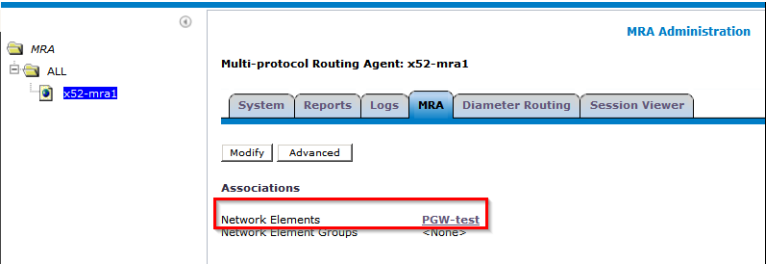
Host Name / IP Address

PGW-test

10.250.35.177

The Network Element is created.

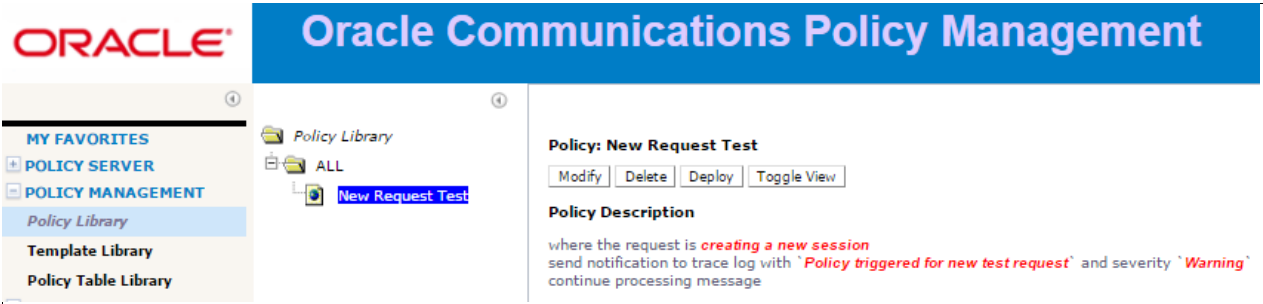
Step	Procedure	Details
		 NOTE: This tab is dependent on the Network Element type that was configured during the previous step. In this example the Network Element type used is a PGW (Packet Gateway) which is used to establish a Diameter connection to the Policy Management System. 4. When you finish, click Save. 
3.	☐ Deploy Network Element in CMP GUI	1. Navigate to Network→Network Elements→<Network Element entity>  2. Click Modify in the Network Element Administration screen and select the options to deploy the network element to the MPE and MRA (if present).

Step	Procedure	Details			
		 Network Elements - ALL - x52-mpe1 Capacity Policy Servers associated with this Network Element Policy Servers - ALL - x52-mpe1 MRAs associated with this Network Element Multi-protocol Routing Agent - ALL - x52-mra1			
		3. Click Save. 4. Navigate to Policy Server → Configuration → <MPE> → Policy Server tab  5. Confirm the deployed Network Element is associated with the MPE. 6. Navigate to MRA → Configuration → <MRA> → MRA tab  7. Confirm the deployed Network Element is associated with the MRA. <tr><td colspan="3">—End of Procedure—</td></tr>	—End of Procedure—		
—End of Procedure—					

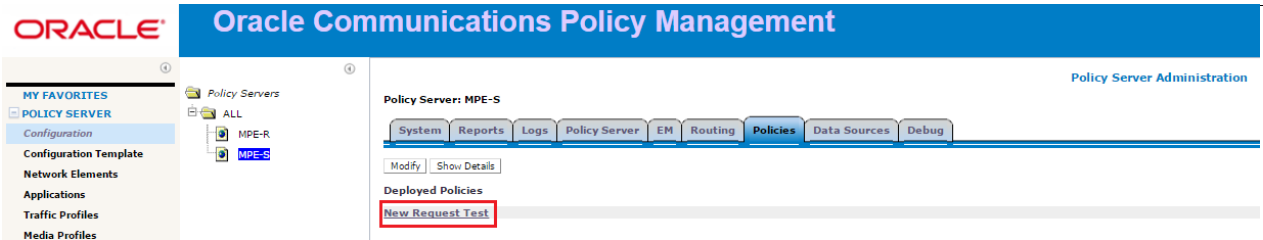
5.6Load Policies and Related Policy Data

This step is optional. Policies are not required to process a test call but for the purpose of verification, a basic policy is installed manually, or using an import action and an xml file. The policy must be deployed to the MPE which processes the test call.

Here is an example of a very simple policy that is used to confirm session creation for a test call by viewing the trace logs on the MPE that processes the test call.



Note: This policy must be deployed to the MPE that processes Diameter session requests. Deployed policies are verified using the Policies tab for the MPE that processes the test request:



5.7 Add a Data Source

This step is optional. When the test call is received by the MPE, the MPE is configured to perform a Subscriber lookup to an appropriately configured Subscriber Database. Refer to [Configuration Management Platform Wireless User’s Guide](#) for more information.

The screenshot shows the 'Add Data Source' configuration form. It has tabs for 'Server Info', 'Search Criteria', 'Search Filters', and 'Associated Data Sources'. The 'Common' section includes fields for 'Admin State' (checked), 'Realm', 'Unique Name', 'Sh Profile' (set to 'ProfileV1'), and 'Protocol Timer Profile' (set to 'undefined'). There are checkboxes for 'Enable Subscription' and 'Use Notif-Eff' (checked). The 'Transport' section has radio buttons for 'TCP' (selected) and 'SCTP', with 'Connections' set to '1'. The 'Primary Servers' section includes fields for 'Primary Identity', 'Primary Address', 'Primary Port' (3868), 'OAM IP', 'Secondary Identity', 'Secondary Address', and 'Secondary Port' (3868). 'Save' and 'Cancel' buttons are at the bottom right.

Here is a sample configuration. This form is specific to the site.

Edit Data Source

Server Info

Search Criteria

Search Filters

Associated Data Sources

Common

Admin State☒

Realmoracle.com

Unique NameMPBay10

Sh ProfileProfileV4

Protocol Timer Profileundefined

Enable Subscription☒

Use Notif-Eff☒

Transport

☒ TCP

☐ SCTP

Connections1

Max Incoming Streams8

Max Outgoing Streams8

Primary Servers

Primary Identitympbay10.oracle.com

Primary Address10.196.165.22

Primary Port3868

Secondary Identity

Secondary Address

Secondary Port3868

Save

Cancel

5.8Perform Test Call

A basic test call confirms that the system is ready for testing of call scenarios defined by the customer. The test call is initiated from the network element that was created. For example, a PGW (Packet Gateway) first establishes a Diameter connection with the PCRF and then initiate the test call by sending an Initial Diameter CCR-I message.

Note: Customer specific information such as Indexing and Diameter Realm and Diameter Identity may be required on the **MPE →Policy Server** tab for the test call. The following is a sample for reference only.

Policy Servers

ALL

MPE01

Policy Server: MPE01

System

Reports

Logs

Policy Server

Diam

Modify

Advanced

The configuration was applied successfully.

Associations

Applications<None>

Network ElementsPGW1

Network Element Groups<None>

Notification Servers<None>

Subscriber Indexing

Defaults

Index by IPv4:true

Index by IP-Domain-Id:false

Index by IPv6:false

Index by Username:false

Index by NAI:false

Index by E.164 (MSISDN):true

Index by IMSI:true

< No Overrides by APN >

Confidential - Oracle Restricted

5.9 Pre-Production Configurations

There are other steps required to verify the Operations configuration of the system. For example, to verify that the SNMP traps (Aarms) are being delivered to the Network Management centers. These are outside the scope of this document, but also need to be planned and performed.

Reference the following document for information on configuring SNMP:

[SNMP User's Guide 12.6](#)

Additional procedures are referenced from the following documents:

- [Platform Configuration User's Guide](#)
- [Configuration Management Platform, Wireless User's Guide](#)

Changes in the behavior of Release 12.6.1 are documented in the [Oracle® Communications Policy Management Release Notes Release 12.6.1](#)

Behavior Modifications

Firewall Enabled by Default—ER 22536198

Firewall functionality is enabled by default. The server firewall protects Policy Management against DDoS, flooding attacks, and unwanted connections. The settings are not altered during the upgrade.

APPENDIX A. RESOURCE PROFILES

Table 9—Policy Management VM Resource Profiles Component

Component	vCPU		RAM (GB)		Storage (GB)		vNIC	
	Suggestion	Minimum	Suggestion	Minimum	Suggestion	Minimum	Suggestion	Minimum
CMP	12	4	60	16	256		6	
MRA	12	10	60	32	256		6	
MPE	12	10	60	32	256		6	
MPE-LI	12	10	60	32	256		6	

APPENDIX B. RESOURCE PROFILES

Table 10—Policy Management VM Resource Profiles Component

Component	vCPU	RAM (GB)	Storage (GB)	vNIC
CMP	46	264	256	6
MRA	46	264	256	6
MPE	46	264	256	6
MPE-LI	46	264	256	6

Note: For large Profile MRA VM (46 vCPU Flavor), following settings need to be configured for optimal performance.

1. On KVM host (where the MRA VM is hosted): Check if the vhost queue size on KVM host is set to 8.

Following steps can be used to check/edit the same:

- a. Run the following command to shutdown the MRA VM:

```
virsh shutdown MRA <VM_NAME>
```

where, VM_NAME is the name of the VMs deployed on the KVM. Wait for the VMs to be properly shutdown.

- b. Run the command: `virsh edit <VM_NAME>`

- c. For each of the bridge add the below line of code:

```
<driver name='vhost' queues='8' />
```

Below is a screenshot to refer:

```
<interface type='bridge'>
  <mac address='52:54:00:62:45:f6' />
  <source bridge='bridge0' />
  <model type='virtio' />
  <driver name='vhost' queues='8' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0' />
</interface>
<interface type='bridge'>
  <mac address='52:54:00:ec:17:2b' />
  <source bridge='bridge1' />
  <model type='virtio' />
  <driver name='vhost' queues='8' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0' />
</interface>
<interface type='bridge'>
  <mac address='52:54:00:10:19:2b' />
  <source bridge='bridge2' />
  <model type='virtio' />
  <driver name='vhost' queues='8' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0' />
</interface>
```

- d. Save the file and start the MRA VM by running the following command: `virsh start <VM_NAME>`.

2. On CMP GUI (Configuring MRA advanced Settings):

- a. Login to CMP GUI.
- b. Navigate to MRA → Configuration → MRA tab for MRA Cluster → Advanced Settings.
- c. Add the following settings in Service Overrides along with the values mentioned:

DIAMETERDRA.NumberOfSchedulers = 4

DIAMETERDRA.ReadThreadCount =12

DIAMETERDRA.SchedulerInterQueueThreadCount =4

- d. Click **Save**.
- e. Navigate to MRA → Configuration → Reports tab for MRA Cluster and "Restart" the Active MRA to apply the values.

APPENDIX C. VM NETWORKING LAYOUT

This table represents the Policy Management network layout that is applied in each Policy Management VM.

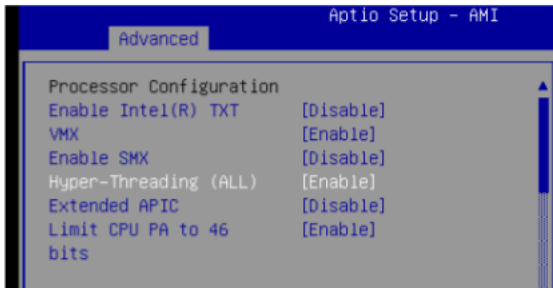
Table 11—Policy Management VM Network Layout

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

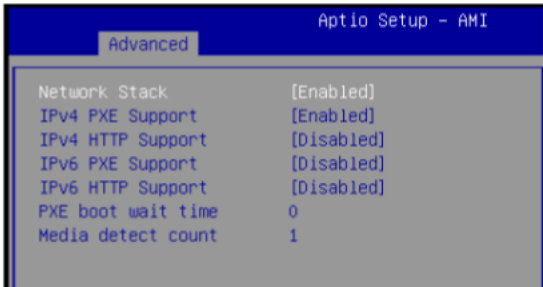
APPENDIX D. X9-2 SERVER BIOS SETTINGS AND RECOMMENDED CONFIGURATIONS FOR OS INSTALLATION

1. BIOS Settings Recommendations

- a. ILOM has the latest supported firmware.
- b. Hyper-Threading is enabled in BIOS. Refer the below screenshot.



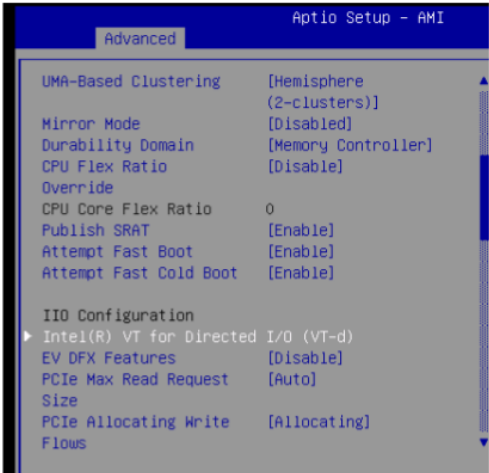
- c. Network Stack is enabled in BIOS. Refer the below screenshot.



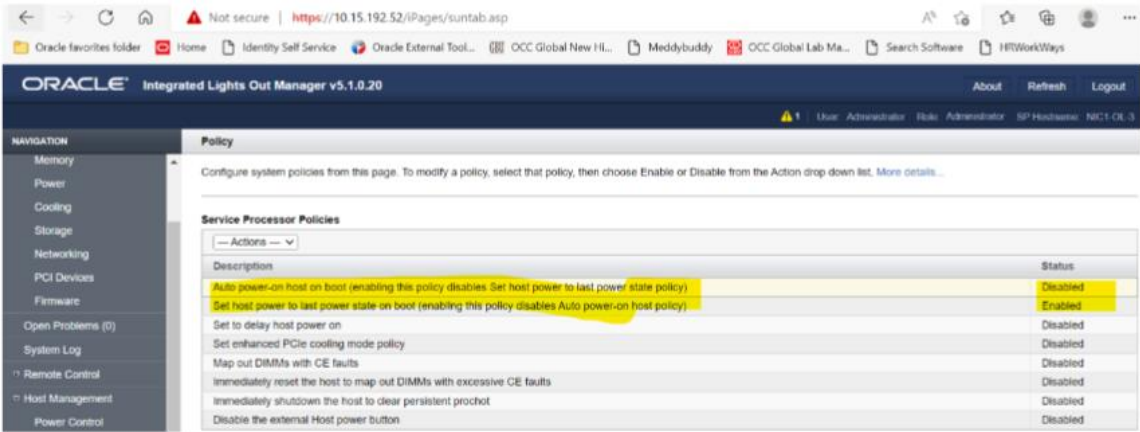
- d. PCI-E UEFI Driver is enabled in BIOS. Refer the below screenshot.



- e. VT-d is enabled in BIOS. Refer the below screenshot.



- f. Last Power State is enabled (ILOM GUI or CLI (e.g. set /SP/policy HOST_AUTO_POWER_ON=enabled HOST_LAST_POWER_STATE=enabled)). Refer the below screenshot.



- 2. **Firmware Version**
It is recommended to use the latest available firmware for Oracle X9-2 available on MOS portal.
- 3. **Raid or Not Raid Configurations?**
You can go with software Raid on X9-2 deployment.
- 4. **Partition layout (OS, Storage, Swap space, directories, and so on)**
For root file system partition, at least 50GB should be allotted (Mandatory) rest all the file systems may vary depends up on the disk capacity.

Engineering lab has the following Disk partition, but variation is allowed for customer as per need.

Filesystem	Size	Used	Avail	Use%	Mounted on
devtmpfs	378G	0	378G	0%	/dev
tmpfs	378G	0	378G	0%	/dev/shm
tmpfs	378G	4.0G	374G	2%	/run
tmpfs	378G	0	378G	0%	/sys/fs/cgroup
/dev/mapper/vg-root	550G	40G	511G	8%	/

<i>/dev/md3</i>	<i>3.5T</i>	<i>812G</i>	<i>2.7T</i>	<i>24%</i>	<i>/mnt/data</i>
<i>/dev/md1</i>	<i>1016M</i>	<i>460M</i>	<i>557M</i>	<i>46%</i>	<i>/boot</i>
<i>/dev/md0</i>	<i>200M</i>	<i>5.1M</i>	<i>195M</i>	<i>3%</i>	<i>/boot/efi</i>
<i>tmpfs</i>	<i>76G</i>	<i>0</i>	<i>76G</i>	<i>0%</i>	<i>/run/user/0</i>

5. Virtualization package release levels (KVM, OL, Hypervisor)

It is recommended to have the following versions:

- Oracle Linux 8.8 (Recommended to use latest OL8.x)
- KVM version 6.2.0

6. Installation Recommendation for Software

Software selection option "Virtualization Host".

In the additional software list: "Virtualization Platform", "Legacy UNIX Compatibility" and "Remote Management for Linux".

Additional Packages:

- virt-install - 3.2.0
- libguestfs-tools 1.44.0

Note:

For X9-2 KVM servers hosting 46 vCPU profile servers, it is recommended NOT to have 2 Active MRA nodes in the same KVM for optimal performance.

You can have CMP + MPE, CMP + MRA, CMP + CMP, MPE + MPE, MPE + MRA as preferable pairs of servers in single KVM host.

APPENDIX E. PORT USAGE AND RECOMMENDED ENABLING FOR FIREWALL ACCESS

<i>Interface (Default)</i>	<i>Protocol/Port</i>	<i>Source Device Name</i>	<i>Destination Device Name</i>	<i>Flow Description</i>
OAM/REPL	TCP/22	EDN Desktop and Employee VPN	vPCRF OAM/REPL and ILOM Interfaces	SSH/SFTP Administration
OAM	UDP/123	vPCRF OAM and ILOM Interfaces	NTP server	NTP/ Chrony
OAM	TCP/8080 TCP/8443	Desktops and Employee VPNs	Site 1&2 PCRF OAM and ILO EDN interfaces	HTTP Cache, XML files: Policies, Alerts, Counters
OAM	TCP/8080 TCP/8443	Site 1&2 PCRF Active CMP server's Real IP	Site 1&2 Active MRA's Real IP	
OAM	TCP/8080 TCP/8443	Site 1&2 PCRF Active CMP server's Real IP	Site 1&2 Active MPE's Real IP	
OAM	TCP/8080 TCP/8443	Site 1&2 PCRF Active MRA's server Real IP	Site 1&2 PCRF Active MPE's server Real IP	
OAM	TCP/8080 TCP/8443	Site 1&2 PCRF Active Primary CMP's Real IP	Site 1&2 PCRF Secondary CMP's Real IP	
OAM	UDP/80 TCP/80	EDN Desktops and Employee VPNs	Site 1&2 Active PCRF CMP	WEB Access GUI (HTTP)
OAM	TCP/443 UDP/443	EDN Desktops and Employee VPNs	Site 1&2 PCRF 1 & 2 OAM and ILO EDN interfaces	Secure Web Access to GUI (HTTPS)
OAM	UDP/53	Site 1&2 PCRF Active Primary CMP's Real IP	DNS server	A & AAAA queries for peer IPs (DNS)
OAM	UDP/69	EDN Desktop and Employee VPN	vPCRF OAM and ILOM Interfaces	Transfer Switch Configuration Files (TFTP)

OAM	UDP/161	Site 1&2 PCRF OAM and ILO interfaces	PCRF Site 1&2 OAM and any External Network Management System (NMS)	SNMP messages, PCRF app related
OAM	UDP/162	Site 1&2 PCRF OAM and ILO interfaces	PCRF Site 1&2 OAM and any External Network Management System (NMS)	SNMP traps
OAM	TCP/111	EDN Desktop and Employee VPN	Site 1&2 PCRF 1 & 2 OAM and ILO EDN interfaces	Software Upgrade Support - Rpc Bind
OAM	TCP/15360	Site 1&2 Active PCRF CMP	Site 1&2 PCRF MRA & MPE HA servers Real IP, PCRF MRA & MPE HA servers Real IP PCRF MRA & MPE server-C's Real IP PCRF DR-CMP's Real IP	Data Replication - COMCOL (SOAP) - cmSOAPA
OAM	TCP/16878/TCP41207/TCP16810	Site 1 & 2 PCRF local MRA & MPE HA servers Site 1&2 Active PCRF CMPs	Site 1&2 Active PCRF CMP's Real IP's	DB Replication - COMCOL (inetmerge). PCRF local MRA & MPE HA servers Alarms/Statistics updates to Active PCRF CMP
OAM/REPL	TCP/17398 TCP/17400 TCP/17401 TCP/17402 UDP/17401	Site-2 PCRF MRA HA servers	Site-1 PCRF mated MRA server-C's Real IP	DB Replication - COMCOL (inetrep)
OAM	TCP/20000	EDN Desktop and Employee VPN	vPCRF OAM and ILOM Interfaces	admin daemon port - tpdProvd
OAM	TCP/3002	EDN Desktop and Employee VPN	vPCRF OAM and ILOM Interfaces	Raw Serial Data
OAM	TCP/3389	EDN Desktop and Employee VPN	vPCRF OAM and ILOM Interfaces	Terminal Services
OAM	TCP/9300	EDN Desktop and Employee VPN	vPCRF OAM and ILOM Interfaces	Shared Remote Console
OAM	TCP/7710	Site 1&2 local PCRF MRA/MPE's Real IP	Site 1&2 PCRF mated MRA & MPE server-C's Real IP	PCRF server/server IPC (inter-process communication)

OAM	TCP/7710	Site 1&2 PCRF mated MRA & MPE server-C's Real IP	Site 1&2 local PCRF MRA/MPE's Real IP	PCRF server/server IPC (inter-process communication)
OAM	UDP/9663	PCRF CMP OAM IP's	PCRF CMP OAM IP's	Active to Standby/Spare MPE - Active MPE
OAM	TCP/3306	Site 1&2 PCRF CMP Cluster	Site 1&2 PCRF CMP's real IP	PCRF CMP MySQL Rep.
OAM	TCP/15616	Site 1&2 PCRF CMP HA servers	Site 1&2 PCRF CMP HA servers	lmysqld
OAM	UDP/514	Site 1&2 Active PCRF CMP, MPE, MRA	Syslog Server	Syslog/ Tracelog forwarding
Gx/SIGA	SCTP/3868 TCP/3868	PGWs	Site 1& 2 PCRF MRA VIPs	Gx Messaging to PCRF
Gx/SIGA	SCTP/3868 TCP/3868	Site 1& 2 PCRF MRA VIPs	PGWs	Gx Messaging from PCRF
Gx/SIGA	SCTP/3868 TCP/3868	HSGWs	PCRF MRA VIPs	Gx Messaging to PCRF
Gx-lite/SIGA	SCTP/3868 TCP/3868	Flash Networks Content Filtering	Site 1&2 PCRF MRA VIPs	Gx-Lite Messaging to PCRF
Sh/SIGA	SCTP/3868 TCP/3868	Site1&2 PCRF local MPE HA servers and mated MPE server-C	DRA	Sh PCRF Messaging with DRA/SPR
Sh/SIGA	SCTP/3868 TCP/3868	DRA	Site1&2 PCRF local MPE HA servers and mated MPE server-C	Sh PCRF Messaging with DRA
Sh/SIGA	SCTP/3868 TCP/3868	All PCRF MPES (IPv4)	All IMS HSS RAN IPv4 ingress groups	MPE Sh Messaging to HSS
SIGA	SCTP/3868 TCP/3868	All PCRF MRA (IPv6)	All PCRF MRA and MPE	PCRF site-to-site Diameter (MRA InterLink, MPE Backup Links)
Rx/SIGA	SCTP/3868 TCP/3868	All CSCF Rx hosts	PCRF MRA/MPE	CSCF Rx Messaging to PCRF
Li/SIGA	TCP/443	LiMF	PCRF MRA/MPE. PCRF local MPE HA server's VIP & mated MPE server-C's real IPs	X1 to MPES
Li/SIGA	TCP/51000	PCRF MRA/MPE. PCRF local MPE HA servers & mated MPE server-Cs	LiMF	MPE X2 to LiMF