# Cisco Prime Network Registrar Virtual Appliance

The Cisco Prime Network Registrar virtual appliance includes all the functionality available in a version of Cisco Prime Network Registrar 10.0 installed on any Linux operating system.

This chapter describes how to install Cisco Prime Network Registrar virtual appliance and includes the following sections:



## System Requirements

There are three kits that can be used to install the virtual appliance:

- An OVA which runs on VMware ESXi 5.5 or later
- A KVM kit which runs on a KVM hypervisor running on CentOS 7.x or Red Hat (RHEL)
- A cloud image which can be deployed to Openstack

These kits are effectively identical, and in this guide, when the OVA is discussed, the discussion applies to all three kits unless otherwise noted.

Each of these kits were created to require limited resources: 1 virtual CPU, 8 GB main memory, 6 GB swap partition, and a 7.5 GB system partition with 5.4 GB available (free). The total disk storage required is 14 GB. You will almost certainly want to increase the size of the system disk, and giving the virtual appliance additional virtual CPU's can increase the performance considerably. You should ensure that sufficient resources are available on the host that you are targeting for the deployment to meet these requirements.

You must increase the resources used by the virtual appliance or it will not function successfully. There are two different regimes: running a local cluster, or running a regional cluster and local cluster on the same machine. The recommendations below are for running the virtual appliance(s) on a Jumpstart, but these are also useful starting points for any local or regional cluster deployment. For a local cluster:

- CPU: 1 socket, 8 CPUs
- Memory: 12 GB
- Disk: 100 GB or greater

For a regional cluster running on the same Jumpstart as a local cluster:

- CPU: 1 socket, 7 CPUs
- Memory: Minimum 8 GB
- Disk: 35 GB

You may need substantially more disk space than listed above based on the size of your deployment. You can increase the disk space by resizing the allocated disk and rebooting the appliance.

# Installing and Upgrading Cisco Prime Network Registrar Virtual Appliance

You can deploy the virtual appliance in any of three environments, VMware ESXi 5.5 or later, CentOS/RHEL 7.5 KVM hypervisor, or OpenStack. After discussing the information that you will need to determine for any deployment, the individual environments are discussed in detail.

## Preparing to Deploy the Cisco Prime Network Registrar Virtual Appliance

In order to deploy the Cisco Prime Network Registrar virtual appliance and configure its network connection, you have to answer several questions. Some of these questions concern the networking environment in which the virtual appliance is being deployed, and some of them concern values which are unique to the particular virtual appliance being deployed.

The questions that are unique to the installation of this particular virtual appliance are listed below. You must decide on answers to these questions before you deploy the virtual appliance.

- A virtual machine name for the deployed virtual appliance.
- A root password for the underlying Linux CentOS operating system.
- An IPv4 address for the virtual appliance.
- A DNS name associated with the IPv4 address of the virtual appliance.
- A username and password for the initial administrator account for the Cisco Prime Network Registrar application.

**Note** From CPNR 9.1 and later you can copy an existing VM to create a new local cluster (snapshot), you must generate a new UUID and re-register it with the regional cluster to avoid duplication of UUID, see the “Generating new UUID” section of Cisco Prime Network Registrar 10.0 Admin Guide.

The questions concerning the networking environment are as follows. The answers to these questions are not unique to the virtual appliance, but are instead values that are determined by the environment in which you will deploy the virtual appliance:

- The network mask associated with the IP address of the virtual appliance itself.
- The default gateway address for the virtual appliance.

- The IP address of at least one DNS server that can be accessed by the virtual appliance, although it is best if you have the IP addresses of two DNS servers to provide additional availability.
- Any proxy values necessary for the virtual appliance to access the Internet (if you want the virtual appliance to have access to the Internet).
- If this is a local cluster installation, you will need to determine the IP address of the Cisco Prime Network Registrar regional cluster to which this local cluster will connect in order to receive its license information. If this is a regional cluster installation, you can ignore this requirement.

# Deploying the Regional Cluster OVA or Local Cluster OVA on VMware

The Cisco Prime Network Registrar virtual appliance is supported for production use on VMware ESXi 5.5 or later and can be accessed or managed using the VMware vSphere client. The Cisco Prime Network Registrar virtual appliance is made available in an Open Virtual Appliance (OVA) package.

The VMware vSphere client can be connected directly to your ESXi installation, or it can be connected to a vCenter server which in turn is connected to your vSphere installation. Connecting through vCenter provides a number of capabilities that connecting directly to ESXi does not. If a vCenter server is available and associated with the ESXi installation, it should be used.

To install the Cisco Prime Network Registrar virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a .ova file.

The names are:

- *cpnr_10_0_local.ova* for the local virtual appliance
- *cpnr_10_0_regional.ova* for the regional virtual appliance

Download the virtual appliance of your choice. Every Cisco Prime Network Registrar local cluster installation must connect to a Cisco Prime Network Registrar regional cluster in order to receive the necessary license information required to operate. Thus, before you install a Cisco Prime Network Registrar local virtual appliance you must identify the IP address of the regional cluster to which it will connect to receive the license information.

Using vSphere, connect directly to the ESXi installation or the vCenter server, and select the ESXi installation where the OVA is to be deployed.

If you have a vCenter server available, you can connect the ESXi hypervisor to your existing vCenter server and manage it through that vCenter server. Managing all your VMware hypervisors through a common vCenter server provides many benefits.

The screens that you see while managing the ESXi hypervisor with a vSphere client through a vCenter server are different from the screens that you see while connecting the vSphere client directly to the ESXi hypervisor. You can see additional screens if connected through vCenter server. These screens do not actually provide any benefit for the operations in which you will engage to deploy the Cisco Prime Network Registrar virtual appliance. The benefits to using the vCenter server approach come after the initial deployment of the virtual appliance.

To deploy a Regional Cluster OVA or Local Cluster OVA:

**Step 1** From vSphere menu, choose **File > Deploy OVF Template**.

The Deploy OVF Template Source window appears.

**Step 2** To deploy the OVA file, click **Browse** and navigate to select the OVA file (.ova) available on the local machine where vSphere is running.

**Note** You cannot browse for URLs and you must enter the full path to the file.

**Step 3** Click **Next**.

The OVF Template Details window appears. It displays the product name, the size of the OVA file, and the amount of disk space that needs to be available for the virtual appliance.

**Step 4** Verify the OVA template details and click **Next**.

**Step 5** Provide a name to the new virtual appliance and click **Next**.

**Note** You must enter the same name while configuring the virtual appliance, so make sure you remember this name.

The **Disk Format** window appears on versions prior to ESXi 6.5 and the **Deployment Options** window appears for ESXi 6.5 or later versions.

The **Thick** provisioned format is selected by default for versions prior to ESXi 6.5 and the **Thin** provisioned format is selected by default for ESXi 6.5 and later versions. You should select the **Thick** regardless of the default value.

**Step 6** Click **Next** to continue.

**Note** The virtual appliance is only supported when deployed with thick provisioning.

**Step 7** To map the networks used in this OVA template to the networks in your inventory, select the current destination network and choose the destination network from the Destination Networks drop-down list. Click **Next**.

The Ready to Complete window appears.

**Step 8** Click **Finish** to begin deployment of the OVF Template.

# Booting and Configuring Cisco Prime Network Registrar Virtual Appliance

To boot and then configure the Cisco Prime Network Registrar virtual appliance:

**Note**

You must set the memory and CPUs based on the requirements prior to clicking the **Power on** button ( ). Once you start the VM you cannot change the memory or CPU settings until you shut down.

**Step 1** After deploying the Virtual Appliance OVA, select the virtual machine name in vSphere, right-click on it and select **Open Console**.

**Step 2** Click the **Power on** button ( ) on the console and click in the window after clicking the Power on button.

During the initial boot of the newly deployed machine, you will be prompted to enter a root (system) password, which is not the Cisco Prime Network Registrar application password.

**Note** This is the root password for the underlying Linux operating system on which the Cisco Prime Network Registrar 10.0 application is installed. You will be asked to enter this password twice. You will need root access to the underlying Linux operating system at various times in the future, so make sure that you remember this password.

The boot process can take a while, both before you are asked for a root password, as well as after you enter the root password.

The End User License Agreement window appears on the first boot. Read the license agreement in its entirety, and only if you understand and accept the license terms, enter y (Yes).

**Step 3** Log into the server as the root user.

**Step 4** To configure the network for the Virtual Appliance, see the Appendix F "Configuring Network Access on RHEL/CentOS 7.x Using nmcli" on page 67.

# Deploying the Regional Cluster or Local Cluster on a KVM Hypervisor

To install the Cisco Prime Network Registrar virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a .bz2 file.

The names are:

- *cpnr_10_0_local.kvm.tar.bz2* for the local virtual appliance
- *cpnr_10_0_regional.kvm.tar.bz2* for the regional virtual appliance

Download the virtual appliance of your choice. Every Cisco Prime Network Registrar local cluster installation must connect to a Cisco Prime Network Registrar regional cluster in order to receive the necessary license information required to operate. Thus, before you install a Cisco Prime Network Registrar local virtual appliance you must identify the IP address of the regional cluster to which it will connect to receive the license information.

To install Cisco Prime Network Registrar on a KVM Hypervisor, extract the distribution tar archive (**cpnr_10_0_local.kvm.tar.bz2** or **cpnr_10_0_regional.kvm.tar.bz2**) using the following command:

```
root$ tar xvjf cpnr_10_0_local.kvm.tar.bz2
```

If you are unpacking both the local and the regional KVM kits, you must untar them in separate directories to avoid filename conflicts.

**Note** The extraction takes a few minutes and it requires a minimum of 14 GB free disk space. You should see the following files:

- cpnr_10_0_local-disk1.raw—contains the disk for the virtual machine
- installonkvm—installs the virtual machine
- readme.kvm.txt—contains the installation instructions

The first file (-disk1.raw) is the actual file that will be used as the disk file for the resulting CPNR KVM virtual machine. This file should be placed in the directory where you want it to reside long-term as the "source

path" for the virtual disk in the CPNR KVM virtual machine. While you can move it even after the virtual machine is installed, it is easier to start with it in the correct location. You should move the `installonkvm` script along with it. The `installonkvm` script needs to be executable in order to operate correctly.

To proceed with the installation, follow the instructions as specified in the `readme.kvm.txt` file.

Once the installation is complete, see the Appendix F "Configuring Network Access on RHEL/CentOS 7.x Using nmcli" on page 67.

# Deploying the Regional Cluster or Local Cluster on OpenStack

To install the Cisco Prime Network Registrar virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a .ova file.

The names are as follows:

- *cpnr_10_0_local.qcow2* for the local virtual appliance
- *cpnr_10_0_regional.qcow2* for the regional virtual appliance

Download the virtual appliance of your choice. Every Cisco Prime Network Registrar local cluster installation must connect to a Cisco Prime Network Registrar regional cluster in order to receive the necessary license information required to operate. Thus, before you install a Cisco Prime Network Registrar local virtual appliance you must identify the IP address of the regional cluster to which it will connect to receive the license information.

To run the local cluster or regional cluster on OpenStack, you must first create a local or regional image out using the **.qcow2** distribution kit.

After this image exists, you may launch an instance of the local or regional cluster. The Flavor you associate with the instance needs at least 1 VCPU, 8GB of RAM, and at least 14 GB of root disk storage. In order to have an operational instance of CPNR, you must allocate more than the absolute minimum of 14 GB of root disk storage. See the System Requirements, on page 1 section for the amount of disk space needed for a local or regional cluster.

An instance of Cisco Prime Network Registrar will be created with a fixed IP address. Cisco Prime Network Registrar will automatically use any IP addresses associated with interfaces that it can detect when it is started. If the interface available to Cisco Prime Network Registrar has an IP address allocated to it from a provider network (i.e., it is accessible to the clients that need the DHCP or DNS capabilities provided by Cisco Prime Network Registrar), then you can configure Cisco Prime Network Registrar normally.

You have two options when creating an OpenStack instance with respect to root login. When you install a Cisco Prime Network Registrar virtual appliance on VMware or using the KVM kit, you configure the root password for the underlying Linux system on the system console when the virtual machine is first booted. However, usually OpenStack instances are created and deployed in such a way as to only allow logins with SSH using an SSH key-pair that is configured as part of the OpenStack instance. Many OpenStack instances do not allow root password login at all, and only allow login using SSH with an SSH key-pair.

A Cisco Prime Network Registrar OpenStack instance can be configured to operate in either of these two regimes:

Option 1: require root password configuration and allow root login using a password.

Option 2: disable the root password configuration and login, an **SSH** key-pair is required to login.

**Option 1**

This is the default approach for all Cisco Prime Network Registrar virtual appliance kits, and requires no additional actions. You will launch an instance from the Cisco Prime Network Registrar virtual appliance image, and on first boot you will have to bring up a console window for the Cisco Prime Network Registrar instance, and enter a root password for the Linux system, and accept the End User License Agreement. After the first boot, you will not need to access the console. You can also access this instance with an **SSH** key-pair.

**Option 2**

If you wish to deploy the Cisco Prime Network Registrar virtual appliance instance in a way that is more in accordance with the usual practice for OpenStack instance deployment, you can configure the Cisco Prime Network Registrar OpenStack instance to not allow root logins with a password, and require an **SSH** key-pair to login. If you also wish to allow a password based login for a user other than root with root permissions, instructions on how to configure are listed below.

When you launch an OpenStack instance from WebUI, to prevent root password login you will have to perform specific configuration in the Configuration section of the Launch instance dialog. You will need to provide a Customization Script -- which is analogous to User Data in other systems. You will need to configure a script (provided below) which will make the OpenStack instance disable the root password based login. After you deploy an instance configured with this Customization script, the only way to gain the access to the Linux operating system on the instance is to login via **ssh** using the **ssh key pair** associated with the instance at the time of launch.

For example, you might login with: "ssh -i keypairname.pem root@a.b.c.d". If you did not associate a key pair with the instance, or have lost access to the key pair, you will not be able to login to the instance. There is no default root password when the instance is created in this way, and the root password login is disabled.

To configure option 2, enter the following in the "Customization Script" text box:

**#cloud-boothook**

**#!/bin/bash**

**if [ ! -f /etc/cloud/cloud.cfg.orig ]; then**

**cp /etc/cloud/cloud.cfg /etc/cloud/cloud.cfg.orig**

**cp /etc/cloud/cloud.cfg.norootpasswd /etc/cloud/cloud.cfg**

**fi**

**Note** If you choose option 2 and once you gained access to the instance using the **ssh key pair**, if you would like to login with a password as well, you can create a new Linux user using the **useradd** command and make that user a member of the group wheel. You must also give that user a secure password using the **passwd** command. Then you can always login with **ssh** or to the console as that user and have root privileges.

To create a user to allow password login, use the following command:

```
useradd safeuser -g wheel
```

```
passwd safeuser
```

Then, if you need root access, login as **safeuser** and use the following command:

```
sudo su
```

enter the password for **safeuser**, and you will become a root user.

If the IP addresses that are associated with the available interfaces are fixed addresses (i.e., they are only accessible to other instances in OpenStack), then you will need to associate a floating address with Cisco Prime Network Registrar instance. This floating address must then be accessible to the clients of the DHCP or DNS service to be provided by the Cisco Prime Network Registrar instance. You will have to configure the DHCP server provided by Cisco Prime Network Registrar to return the IP address of the floating address as its server-id, instead of the fixed IP address that Cisco Prime Network Registrar can detect that is associated with the interface built into the instance. In order to configure DHCP for this situation, you will need to be in expert mode, and configure the DHCP Policy attribute "dhcp-server-identifier-address" with the floating address allocated to this instance. Then the DHCP server will return the configured IP address (which will be the externally visible IP address of this instance) instead of the IP address that the DHCP server can detect from examining the interface that it is using for communications with clients (which is the fixed IP address).

A local cluster needs to be registered with a regional cluster. After this registration, the regional cluster needs to be able to connect to the local cluster. When the local cluster initially registers with the regional cluster, it sends its IP address to the regional cluster. If the regional cluster can contact the local cluster by using the IP address that the local cluster sees is configured to its network interface, then no action need be taken. This would be the case if the local cluster has a fixed IP address that is only visible within the OpenStack cloud, but the regional cluster was also in the same cloud. If the regional cluster can ping the IP address that the local cluster sees as the IP address on its network interface, then no additional steps are necessary. However, in the event that the regional cluster is not local to the OpenStack cloud on which the local cluster is running, and the local cluster has a floating address in addition to a fixed address, then the regional cluster's configuration for the local cluster needs to have its IP address updated to be that of the floating address (and not the fixed address, which is what it will have from the initial registration).

When allocating a local cluster, you should consider allocating 4 or even 8 VCPUs and at least 12 GB of RAM, with more for large systems. Local clusters will absolutely need more than the 7+ GB free space available in the minimal installation. Regional clusters will probably need additional disk space, but 2 to 4 VCPUs and 8 to 12GB of RAM will suffice for many installations.

# Upgrading the Cisco Prime Network Registrar Virtual Appliance

This section describes the procedure for upgrading Cisco Prime Network Registrar to Cisco Prime Network Registrar virtual appliance and upgrading the operating system to CentOS 7.5 using the data from an existing virtual appliance.

## Upgrading a Cisco Prime Network Registrar Installation to run on a Cisco Prime Network Registrar Virtual Appliance

This section describes how to upgrade an existing installation of Cisco Prime Network Registrar to become a Cisco Prime Network Registrar virtual appliance.

**Note** This procedure upgrades a current version of Cisco Prime Network Registrar running on a Linux operating system to a current version of the Cisco Prime Network Registrar virtual appliance. If you need to move from a different platform, you have to first convert to the Linux platform prior to upgrading to a virtual appliance. If you need to move from a different version of Cisco Prime Network Registrar to the current version of the virtual appliance, you have to first upgrade to the current version of Cisco Prime Network Registrar on an external Linux system before upgrading to the virtual appliance. See Installing and Upgrading Cisco Prime Network Registrar.

**Step 1** Install the Cisco Prime Network Registrar virtual appliance.

**Step 2** Shut down the Cisco Prime Network Registrar application being upgraded using the following command: **systemctl stop nwreglocal**

**Step 3** If the version of Cisco Prime Network Registrar which you are moving to the virtual appliance is a version earlier than Cisco Prime Network Registrar 7.2, then perform the following steps:

**Note** If you are upgrading from 7.2, you do not require the cnr_mcdexport kit because 7.2 clusters do not use the MCD DB database technology and you can skip this step.

a) Download the upgrade preparation kit, cnr_mcdexport_linux5.tar, from Cisco.com.
b) Untar the downloaded archive and run the script cnr_mcdexport.

**Step 4** Tar the existing ***install-path*/local/data** directory using the command:

```
tar cvf tarfile.tar data
```

**Step 5** Copy the tar file created to the new virtual appliance.

**Step 6** Shut down Cisco Prime Network Registrar on the new virtual appliance using the command:

```
systemctl stop nwreglocal
```

**Step 7** Rename the existing database to **.orig** using the command:

```
mv /var/nwreg2/local/data /var/nwreg2/local/data.orig
```

**Step 8** Untar the latest database, transferred in **Step 4**, using **tar xvf tarfile.tar**.

**Step 9** Copy any existing extensions from the system being upgraded to the correct directories on the new virtual appliance.

**Step 10** Reboot the Cisco Prime Network Registrar virtual appliance using VMware vSphere.

# Upgrading to a new Version of the Virtual Appliance Operating System

To upgrade and to use a new version of the Cisco Prime Network Registrar virtual appliance, install a new virtual appliance which has the new operating system version on it, and then move the data and configuration from the existing virtual appliance to the new virtual appliance.

To do this follow the steps in the section : Upgrading the Cisco Prime Network Registrar Virtual Appliance, on page 8

You can now start the new virtual machine. It will have the entire data directory of the existing virtual machine.

**Note** The new virtual machine with the upgraded operating system will pause during the boot process and instruct you to upgrade the Cisco Prime Network Registrar database to match the database version of the Cisco Prime Network Registrar application that resides on the new virtual machine. Whenever this pause during the boot process and message appears, CPNR will not be able to start until after the script /opt/nwreg2/local/usrbin/upgrade_cnr (or /opt/nwreg2/regional/usrbin/upgrade_cnr for a regional cluster) has been run. Cisco Prime Network Registrar has been masked using systemctl, and the upgrade_cnr script will unmask it before performing the upgrade.

**Step 1** Press return on the console to complete the boot process.

**Step 2** Log in as root and run the displayed command.
After boot completion, you should see your existing configuration running with the new version of Cisco Prime Network Registrar on the new virtual machine.

## Upgrading the Cisco Prime Network Registrar Application

If you want to upgrade the installation of Cisco Prime Network Registrar that currently exists on the virtual appliance to a new version of Cisco Prime Network Registrar, follow the procedure in this document to perform a straightforward software product upgrade. The installation of Cisco Prime Network Registrar delivered on the virtual appliance is a regular installation of the Cisco Prime Network Registrar software product.

# Next Steps: Cisco Prime Network Registrar Virtual Appliance

## Configuring Cisco Prime Network Registrar with the CLI on Virtual Appliance

The Cisco Prime Network Registrar command line interpreter (CLI) can be used to configure the virtual appliance in two ways:

- You can use the nrcmd CLI on the virtual appliance directly by first using SSH to connect into the underlying Linux operating system on the virtual appliance. You can use any username and password which you have created on the virtual appliance for the SSH login, and you must use an administrator username and password for the Cisco Prime Network Registrar to use the nrcmd CLI to configure Cisco Prime Network Registrar.

  

  **Note** As distributed, there is only one valid user for the Linux operating system—root. While you can login as root to use the Cisco Prime Network Registrar CLI, you might want to add additional users to the system. Use the useradd program to add additional users. You can type **man useradd** for more information on how to add additional users.

- Alternatively, you can use the nrcmd CLI on some other system in the network to configure and manage Cisco Prime Network Registrar on the virtual appliance the same way that you would use it to manage any remote installation of Cisco Prime Network Registrar. This requires installing Cisco Prime Network Registrar (typically only the client-only installation) on the other system.

## Configuring the Virtual Appliance to Automatically Power Up

You can configure the ESXi hypervisor to automatically power up the Cisco Prime Network Registrar virtual appliance when power is restored to the ESXi hypervisor layer.

**Note** The KVM kit is installed with automatic power up enabled.

To configure automatic power up:

**Step 1** In the vSphere client, select the ESXi machine to which you are connected. It is not a specific virtual machine that you have to select but the ESXi hypervisor on which they reside.

**Step 2** Select the **Configuration** tab.

**Step 3** Click the **Virtual Machine Startup/Shutdown** link under the **Software** area. You should see the virtual machine in the list shown in window.

**Step 4** Click the **Properties...** link present at the top right corner of the page. If you do not see that, resize the window until you do.

The Virtual Machine Startup and Shutdown page is displayed.

**Step 5** Check the **Allow virtual machines to start and stop automatically with the system** check box.

**Step 6** Select the virtual machine running the Cisco Prime Network Registrar virtual appliance and use the **Move Up** button on the right to move it up into the group labelled **Automatic Startup**.

**Step 7** Click **OK** .

This ensures that whenever power is restored to the ESXi hypervisor the Cisco Prime Network Registrar appliance powers up automatically.

# Managing the Cisco Prime Network Registrar Virtual Appliance

You can manage the underlying Linux operating system, which is based on CentOS 7.5, by logging in as the root user. You may use SSH to log into the virtual appliance with the username root and the root password you specified when you first booted the virtual appliance. On Openstack you may use the key pair created when you launched the instance.

You will probably want to create additional users on the Linux system so that people can access the Linux system with a username other than root.

The Linux system which is included on the virtual appliance is stripped down to a considerable degree and thus does not include things that are not required to run or manage the Cisco Prime Network Registrar application, such as a window system manager and its associated GUI user interface. However, all the tools necessary to support and manage the Cisco Prime Network Registrar application are included on the Linux operating system used inside of the virtual appliance.

You may also want to take additional steps to secure the SSH connection. For instance, configuring it to prevent logging on as root, and requiring a user to **su** to gain root privileges after logging on as another user.

You may wish to perform other configuration changes on the underlying Linux operating system in order to lock it down in ways appropriate to your environment.

**Note** Cisco Prime Network Registrar customers are solely responsible for keeping their OS up to date regarding patches that they desire to apply and Cisco is not responsible for the same.

## Post OVA Installation

Follow the below steps to get the latest CentOS updates, latest version of installed packages and security updates before configuring the CPNR.

**Note** The command "yum update" will update the running system with new and changed software that in most cases did not exist when the CPNR application was tested with the operating system shipped on the virtual appliance. The updates that are installed as part of the "yum update" command do not cause any problems for the CPNR application. However, Cisco cannot guarantee that the CPNR application will perform without any problems when interfacing with software that wasn't available when our testing was performed. You should perform your own testing to ensure that everything is operating correctly in your environment after a "yum update" command has been executed prior to placing the updated virtual appliance into production.

**Step 1** Login as root.

**Step 2** Configure networking.

**Step 3** Go to the root prompt and do “#yum update ”.

**Step 4** Reboot the system and then configure the CPNR.