



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 8.3 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, page 1](#)
- [Installing and Upgrading Cisco Prime Network Registrar Virtual Appliance, page 2](#)
- [Upgrading the Cisco Prime Network Registrar Virtual Appliance, page 5](#)
- [Next Steps: Cisco Prime Network Registrar Virtual Appliance, page 8](#)

System Requirements

The memory and storage parameters are specified in the OVA file. However, you should ensure that sufficient resources are available on the host that you are targeting for the deployment to meet these requirements.

The OVA deployment allocates 2 GB of RAM to the virtual appliance. In addition, you will almost certainly find that you also will need disk space beyond the 16 GB minimum allocation provided when the virtual appliance is installed. It is possible to expand the disk usage after the virtual appliance is installed.



Note

It is worth some effort to determine the likely amount of disk storage that you need at the time you first install the virtual appliance. If you increase the size of the disk space after you have configured and used the product, you must back up all the work that you have done prior to increasing the disk storage. However, if you increase the disk storage when you first install the product, no backup is necessary, since in the unlikely event something goes wrong while expanding the disk storage, nothing valuable would be lost. At worst, you would simply have to reinstall the virtual appliance.

The Cisco Prime Network Registrar virtual appliance is supported on VMware ESXi 5.0 or later systems that are themselves supported ESXi 5.0 or later systems. VMware provides a bootable program which helps you identify whether the hardware on which it is run supports ESXi 5.0 and later. In some cases, the capabilities that are not available from ESXi 5.0 or later are capabilities that are required to run the Cisco Prime Network Registrar virtual appliance. For example, ESXi 5.0 or later will run on some hardware on which it is not officially supported, and will run only 32 bit operating systems on that hardware. The Cisco Prime Network

Registrar virtual appliance consists of a 64 bit Linux operating system running a 32 bit version of the Cisco Prime Network Registrar application. Thus, the 64 bit OS included with the virtual appliance will not run on the ESXi 5.0 or later platform described above. The hardware platforms on which ESXi 5.0 or later runs in this degraded and unsupported mode are becoming less common over time.

Installing and Upgrading Cisco Prime Network Registrar Virtual Appliance

The Cisco Prime Network Registrar virtual appliance is supported for production use on VMware ESXi 5.0 or later and can be accessed or managed using vSphere client of VMware. 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.

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.

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 IP address or DNS name of the ESXi installation on which you intend to deploy the virtual appliance.
- The IP address or DNS name of any vCenter server associated with the ESXi installation, above.
- 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 address 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

**Note**

Before deploying the virtual appliance, verify that your VMware server is running on VMware supported hardware. If you are not sure whether your environment can support a 64-bit guest operating system, you can verify by downloading and running the VMware "CPU Identification Utility" which indicates 64-bit VMware support. This utility can be found on the VMware site at: http://www.vmware.com/download/shared_utilities.html

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 zip file.

The names are:

- cpnr_8_3_local.ova for the local virtual appliance
- cpnr_8_3_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.
The Thick provisioned format is selected by default.
- 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. 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 8.3 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, enter the following command:
`configurenetwork`

Step 5 You should configure the following:

- **IPv4** - To change the IPv4 address.
- **IPv6** - To change the IPv6 address (optional unless you are supporting DHCPv6 with this server).
- **Hostname** - To change the hostname of the virtual appliance.
- **DNS 1** - To change DNS Server 1 details.
- **DNS 2** - To change DNS Server 2 details (optional).

Step 6 To save the settings, enter y (Yes) when prompted.

Note To view the current network configuration, type **View**.

Step 7 Enter **Exit** to complete the network configuration. The changes are saved and the Virtual Appliance restarts along with the Cisco Prime Network Registrar Application.

Note The operating system does not restart at this point.

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 6.5 using the data from an existing virtual appliance.

Related Topics

[Upgrading the Cisco Prime Network Registrar Installation to run on a Cisco Prime Network Registrar Virtual Appliance, on page 5](#)

[Upgrading the Cisco Prime Network Registrar Virtual Appliance , on page 7](#)

Upgrading the 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](#).

To do this follow the steps:

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:
`/etc/init.d/nwreglocal stop`

Step 3 Copy the file `cnr_prepareforupgrade` from `/opt/nwreg2/{local | regional}/usrbin` from the virtual appliance system to the Cisco Prime Network Registrar installation being upgraded.

Note You have to choose either local or regional from {local | regional} based on the upgrade that you are doing, that is, local upgrade or regional upgrade.

You can do it using sftp, for example:

```
[root@cnr-machine-being-upgraded usrbin]# sftp 10.10.10.12
Connecting to 10.10.10.12...
Warning: Permanently added '10.10.10.12' (RSA) to the list of known hosts.
root@10.10.10.12's password:
sftp> cd /opt/nwreg2/local/usrbin
sftp> get cnr_prepareforupgrade
Fetching /opt/nwreg2/local/usrbin/cnr_prepareforupgrade to cnr_prepareforupgrade
/opt/nwreg2/local/usrbin/cnr_prepareforupgrad 100% 3265    3.2KB/s   00:00
```

Step 4 Execute `cnr_prepareforupgrade` on the system being upgraded.

Step 5 If the version of Cisco Prime Network Registrar which you are moving to the virtual appliance is a version earlier than Cisco 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 6 Tar the existing `install-path/local/data` directory using the command:

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

- Step 7** Copy the tar file created to the new virtual appliance.
- Step 8** Shut down Cisco Prime Network Registrar on the new virtual appliance using the command:
`/etc/init.d/nwreglocal stop`
- Step 9** Rename the existing database to **.orig** using the command:
`mv /var/nwreg2/local/data /var/nwreg2/local/data.orig`
- Step 10** Untar the latest database, transferred in **Step 4**, using **tar xvf tarfile.tar**.
- Step 11** Reboot the Cisco Prime Network Registrar virtual appliance using VMware vSphere.
-

Upgrading the Cisco Prime Network Registrar Virtual Appliance

To upgrade an existing Cisco 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:

-
- Step 1** Deploy the latest Cisco Prime Network Registrar virtual appliance (with the new OS version) on the ESXi machine where the existing Cisco Prime Network Registrar virtual appliance resides.
- Step 2** Shut down Cisco Prime Network Registrar on the existing virtual appliance. Use either `/etc/init.d/nwreglocal stop` or `/etc/init.d/nwregregion stop` to stop the application, depending on whether you are operating on a local or regional cluster.
- Step 3** Run **cnr_prepareforupgrade** on the existing appliance.
- Step 4** Shut down the virtual machine of the existing appliance.
- Step 5** The next few steps will guide you through the process of copying the data disk (which contains the Network Registrar databases) from the existing virtual appliance to the new virtual appliance. You will use vSphere to make the copy. Ensure that you have shut down both virtual appliances before copying.
- Step 6** Select the ESXi platform in vSphere. It is not a particular virtual machine that you have to select, but rather the container in which these virtual machines appear.
- Step 7** Select the **Configuration** tab and click the **Storage** link under Hardware area. You can now see the datastores in the right hand window. Determine the datastore in which the files for your virtual machines reside.
- Note** You should have selected the datastore when you deployed the virtual machines, if you have more than one datastore. If you have only one, no selection was required at the time of deployment.
- Step 8** Right-click the datastore that contains the existing virtual machine. Select **Browse Datastore...** A Datastore Browser is displayed which shows you the file structure of your ESXi datastore.
- Note** The directories which you see in the Datastore Browser use the names given to the virtual appliances when they were first deployed, which may or may not be the current names of the virtual appliances. If you changed the name of a virtual appliance after it was deployed, that name change will not be reflected in the file structure in the datastore.
- Step 9** Select the folder for the existing virtual appliance from the tree structure displayed at the left pane of the Database Browser window. You can see the files which are associated with the existing virtual appliance in the right pane of the

Database Browser window. Find the existing data disk from the list of files displayed in the right pane. The name of the file of the existing data disk ends with **_1.vmdk** and is the largest file in the virtual machine.

- Step 10** Right-click the file you found in **Step 9** and select **Copy**.
- Step 11** Select the folder of the new virtual appliance in the left pane of the Datastore Browser window. You can see the files currently associated with the new virtual appliance in the right pane of the window. Right-click in the right pane, and not on a particular file, and select **Paste**. Since the file you are copying may be rather large, you can see a progress popup which shows the copy progress. Close the Datastore Browser window when the copy is complete.
- Step 12** Select the new virtual appliance in the left pane of the vSphere client window and select **Edit virtual machine settings**. The Virtual Machine Properties window is displayed. The Hardware tab is selected by default. If it is not, then select it.
- Step 13** Select Hard disk 2 and click **Remove**. Accept the default **Removal Option** of **Remove from virtual machine** which does not delete the virtual disk file itself, but rather just removes it from the virtual machine.
- Step 14** Select the new virtual appliance again in the left pane of the vSphere client window and select **Edit virtual machine settings** again. Click **Add** in the Virtual Machine Properties window to add the hard disk you copied from the existing virtual machine.
The **Add Hardware** window is displayed.
- Step 15** Choose **Hard Disk** from the list of device types and click **Next**.
- Step 16** Check the **Use an existing virtual disk** check box to allow you to use the virtual disk that you just copied from the existing virtual appliance and click **Next**.
- Step 17** Click **Browse** to locate the disk file path. Select the datastore where you placed the copy of the virtual disk in the Browse Datastore window. Click **Open** and you can see the list of virtual machines on this datastore. Select the directory of the new virtual appliance from the list and click **Open**. You can see the list of virtual disks in the directory for that virtual machine. Probably two of them will be named the same as the new virtual machine, and one of them will be named based on the existing virtual machine. Select the one named for the existing virtual machine and click **OK**. Click **Next**.
- Step 18** Click **Next** again to accept the **Advanced Options** unchanged.
- Step 19** Click **Finish** to complete the operation.
This takes you back to the Virtual Machine Properties window, and the list of hardware in the virtual machine now has the **New Hard Disk (adding)** in the list. Click **OK** to finish.
You can now start the new virtual machine. It will have the entire data disk of the existing virtual machine.
- Note** The 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.
- Step 20** Run the file and press return on the console to complete the boot process.
- Step 21** 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.

Next Steps: Cisco Prime Network Registrar Virtual Appliance

Configuring Cisco Prime Network Registrar

To access the Cisco Prime Network Registrar Application use the following URLs:

- Regional:
 - http://<ipv4-address-you-assigned>:8090
 - https://<ipv4-address-you-assigned>:8453
- Local:
 - http://<ipv4-address-you-assigned>:8080
 - https://<ipv4-address-you-assigned>:8443

The URLs to manage Cisco Prime Network Registrar are the URLs displayed on the Console screen under **manage the Cisco Prime Network Registrar 8.3 application**.

Both the insecure as well as the secure access links are provided on the Configuration Window after successfully entering the network configuration.



Note The local server and regional server use different ports for both standard and secure access.

To manage the Cisco Prime Network Registrar 8.3 application:

-
- Step 1** Browse to any URL displayed under **manage the Cisco Prime Network Registrar 8.3 application** (either secure or standard access).
- Note** If you are using secure access for login, choose **I understand the risks** when you get the warning 'This Connection is Untrusted' and click **Add Exception** and **Confirm Security Exception** for this page. The Cisco Prime Network Registrar New Product Installation page is displayed.
- Step 2** Enter the Name and Password for the superuser administrator in the New Product Installation > Add Superuser Administrator page.
- Note** This account is different from the root password which you entered earlier. This is an account in the Cisco Prime Network Registrar product for the most privileged Cisco Prime Network Registrar administrator, who will have permission to create additional administrator accounts in the Cisco Prime Network Registrar product.
- Step 3** Enter the IP address of a CCM regional cluster and the SCP port in use on that cluster. There is no default for the port number, but port number 1244 is often used for the regional cluster. You must register with a regional cluster in order to operate the product.
- Step 4** Check the services which you wish to use on this virtual appliance.
- Note** You must check the boxes for the services you intend to use on this virtual appliance, or you will not be able to see the user interface for these services in the Web UI. You may select DHCP and select either DNS or CDNS. It is possible to run both DNS and CDNS servers on the same machine at the same time in export mode configuration, but we do not recommend that.
- Step 5** Click **Register**.
The Configuration Summary page is displayed. It will not have any DHCP or DNS boxes checked, because you do not have any configuration for any of these services yet. If you checked DHCP on the previous page, you can see **DHCP services configured for start on reboot**, and similarly for DNS.
You can now proceed to configure DHCP, DNS, or CDNS servers on this virtual machine.
-

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 You must manually power up the virtual machine.

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 6.5, 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.

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.
