Next Steps

This chapter contains the following sections:

Configuring Cisco Prime Network Registrar

After installing Cisco Prime Network Registrar, you can perform the following tasks:

- Get started with Cisco Prime Network Registrar—See Cisco Prime Network Registrar 10.1 Quick Start Guide.
- Set up DHCP addresses, DHCP failover, and DNS update—See Cisco Prime Network Registrar 10.1 DHCP User Guide.
- Set up Authoritative and Caching DNS services—See Cisco Prime Network Registrar 10.1 Caching and Authoritative DNS User Guide.
- Perform administrative tasks, such as local and regional administration, set up Cisco Prime Network Registrar virtual appliance, and so on—See Cisco Prime Network Registrar 10.1 Administration Guide.
- Configure and manage Cisco Prime Network Registrar via CLI—See Cisco Prime Network Registrar 10.1 CLI Reference Guide.
- Configure and manage Cisco Prime Network Registrar via REST API—See Cisco Prime Network Registrar 10.1 REST APIs Reference Guide.

Starting Cisco Prime Network Registrar

To administer the local and regional clusters that you have installed, you must enter the appropriate license file (web UI) or the filename (CLI).

To enter license information in web UI or CLI:

Step 1 Start the Cisco Prime Network Registrar web UI or CLI:

- To access the web UI, open the web browser and use the HTTP (non-secure login) or HTTPS (secure login) website:

  `http://hostname:http-port`

  `https://hostname:https-port`

  where:

  - *hostname* is the actual name of the target host.
  - *http-port* and *https-port* are the default HTTP or HTTPS port that are specified during installation. (See Installing and Upgrading Cisco Prime Network Registrar).

  On Windows, you can access the web UI from the Start menu from the local host:

  - On a local cluster—Choose **Start** > **Programs** > **Network Registrar 10.1** > **Network Registrar 10.1 local Web UI** (or **Network Registrar 10.1 local Web UI (secure)** if you enabled secure login).
  - On a regional cluster—Choose **Start** > **Programs** > **Network Registrar 10.1** > **Network Registrar 10.1 regional Web UI** (or **Network Registrar 10.1 regional Web UI (secure)** if you enabled secure login).

- To start the CLI:
  - Windows—Navigate to the *install-path*\bin directory and enter this command:

    nrcmd -C *cluster-ipaddress* **-N** *username* **-P** *password*
  - Linux—Navigate to the *install-path*\usrbin directory and enter this command

    install-path/usrbin/**nrcmd -C** *clustername* **-N** *username* **-P** *password*

Step 2 If you did not enter license information during the installation procedure, you must do so now:

Note You must add the licenses in the Regional cluster which means the Regional should be installed first. The local cluster has to be registered with the regional cluster at the time of installation or at the time of your first login. You can choose the services (dhcp, dns, cdns) for the local based on the licenses added in the Regional cluster.

- Web UI—Click **Browse** to navigate to the license file.
- CLI—Enter an absolute or relative path for the license filename, as follows:

  nrcmd> **license create** *filename*

Step 3 Enter the username and password, that was created during the installation procedure.

Starting and Stopping Servers

In Windows, you can stop and start the Cisco Prime Network Registrar server agent from the Services feature of the Windows Control Panel. If the installation completed successfully and you enabled the servers, the Cisco Prime Network Registrar DNS and DHCP servers start automatically each time you reboot the machine.

For the TFTP server, you must use the following Cisco Prime Network Registrar CLI command to enable it to restart on bootup:

```
nrcmd> tftp enable start-on-reboot
```

All servers in the cluster are controlled by the Cisco Prime Network Registrar regional or local server agent. You can stop or start the servers by stopping or starting the server agent.

For details on stopping and starting servers, see the *Cisco Prime Network Registrar 10.1 Administration Guide*.

Starting and Stopping Servers on Windows

To start and stop servers on Windows:

Step 1 Choose **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 From the Service list, choose **Network Registrar Local Server Agent** or **Network Registrar Regional Server Agent**.

Step 3 Click **Restart** or **Stop**, as required, and then click **Close**.

Starting and Stopping Servers on Linux

In Linux, the Cisco Prime Network Registrar servers automatically start up after a successful installation or upgrade. You do not need to reboot the system.

Note To start and stop Cisco Prime Network Registrar when running as **nradmin**, you must log into the server as a user in the nradmin group (or root). It is not possible to login as nradmin.

```
# /opt/nwreg2/local/bin/cnr_service start
```

```
# /opt/nwreg2/local/bin/cnr_service stop
```

To start and stop servers on Linux:

Step 1 Log in as superuser.

Step 2 Start the server agent by running the nwreglocal or nwregregion script with the *start* argument:

For the RHEL/CentOS 6.x local cluster:

```
# /etc/init.d/nwreglocal start
```

For the RHEL/CentOS 7.x local cluster:

```
# systemctl start nwreglocal
```

For the RHEL/CentOS 6.x regional cluster:

```
# /etc/init.d/nwregregion start
```

For the RHEL/CentOS 7.x regional cluster:

```
# systemctl start nwregregion
```

Step 3 Enter the **cnr_status** command to check that the servers are running:

```
# install-path/usrbin/cnr_status
```

Step 4 Stop the server agent by running the nwreglocal or nwregregion script with the stop argument:

For the RHEL/CentOS 6.x local cluster:

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

For the RHEL/CentOS 7.x local cluster:

```
# systemctl stop nwreglocal
```

For the RHEL/CentOS 6.x regional cluster:

```
# /etc/init.d/nwregregion stop
```

For the RHEL/CentOS 7.x regional cluster:

```
# systemctl stop nwregregion
```

Starting or Stopping Servers Using the Local Web UI

To start or stop servers in the local Web UI:

Step 1 From **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 To start or stop the DHCP, DNS, CDNS, TFTP, or SNMP servers, select the server in the Manage Servers pane and do any of the following:

- Click the **Start Server** button to start the server.
- Click the **Stop Server** button to stop the server.

Step 3 To reload the server, click the **Restart Server** button.

Starting and Stopping Servers Using the Regional Web UI

To start or stop servers in the regional Web UI:

Step 1 From **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 To start or stop the BYOD or SNMP servers, select the server in the Manage Servers pane and do any of the following:

- Click the **Start Server** button to start the server.
- Click the **Stop Server** button to stop the server.

Note The BYOD web server in the regional cluster will stop by default and must be manually restarted. To automatically restart the BYOD server, you must set autostart to true.

Step 3 To reload the server, click the **Restart Server** button.

Server Event Logging

System activity begins logging when you start Cisco Prime Network Registrar. The server maintains all the logs by default in the following directories:

- Windows:
  - Local cluster: C:\NetworkRegistrar\Local\logs
  - Regional cluster: C:\NetworkRegistrar\Regional\logs
- Linux:
  - Local cluster: /var/nwreg2/local/logs
  - Regional cluster: /var/nwreg2/regional/logs

To monitor the logs, use the **tail -f** command.

Caution In Windows, to avoid losing the most recent system Application Event Log entries if the Event Log fills up, use the Event Viewer system application and check the **Overwrite Events as Needed** check box in Event Log Settings for the Application Log. If the installation process detects that this option is not set properly, it displays a warning message advising corrective action.

Modifying ACLs in Windows Installations

The Cisco Prime Network Registrar installation program for Windows does not try to modify ACLs to restrict access to the installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities—**cacls** and **icacls**—to manually change file and directory permissions.

If you decide to manually change ACLs, we recommend that you control the settings so that the contents of the entire installation area are read-only to everyone except those in the Administrators system group.

The following files and sub directories contain data that you may want only the Administrators system group to access:

- *install-path***conf\cnr.conf**
- *install-path***tomcat\conf\server.xml**
- *install-path***conf\priv**
- *install-path***data**

Modifying the ACLs is strictly optional, and Cisco Prime Network Registrar will function normally without making any changes to them. See the documentation supplied by Microsoft for information about how to use the **cacls** and **icacls** utilities.