Preparing for the Installation

This chapter covers any tasks that you have to perform before installing Cisco Prime Network Registrar.

Installation Checklist

This section explains the procedures you must follow to install Cisco Prime Network Registrar.

Before you perform the installation or upgrade, ensure that you are prepared by reviewing this checklist:

Table 1: Installation Checklist

Task	Checkoff
Does my operating system meet the minimum requirements to support Cisco Prime Network Registrar 11.0? (See System Requirements)	☐
Does my hardware meet the minimum requirements? (See System Requirements)	☐
If necessary, have I excluded Cisco Prime Network Registrar directories and subdirectories from virus scanning? (See Backup Software and Virus Scanning Guidelines, on page 4)	☐
Do I have the proper software license? (See License Files)	☐
Am I authorized for the administrative privileges needed to install the software?	☐
Does the target installation server have enough disk space?	☐
Is this a new installation or an upgrade?	☐
Which type of installation is this - regional cluster, local cluster, or client-only?	☐
Is the 64-bit JRE/JDK installed on the system? If so, where?	☐

Task	Checkoff
Am I upgrading from an earlier version of Cisco Prime Network Registrar? If so:	☐
• Are there any active user interface sessions?	☐
• Is my database backed up?	☐
• Am I upgrading from a supported version (Cisco Prime Network Registrar 8.3 and later)?	☐
Are the required packages for Linux installed? (See System Requirements for Linux OS)	☐
Is the signature for the Cisco Prime Network Registrar image verified? (see Image Signing, on page 3)	☐

Before You Begin

Verify that you are running a supported operating system and that your environment meets all other current system requirements (see System Requirements).

To upgrade the operating system:

1. Use the currently installed Cisco Prime Network Registrar release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.
2. Back up your database. The installation program tries to detect configuration data from an earlier installation and will upgrade the data.
3. Upgrade your operating system and install the prerequisite software.

Note In this document, when *install-path* is used, it refers to the path where Cisco Prime Network Registrar is installed (that is, /opt/nwreg2/{local | regional}.

Obtaining Cisco Prime Network Registrar License Files

Cisco Prime Network Registrar 11.0 supports both Smart Licensing and traditional licensing. However, it does not support the hybrid model, that is, you can use any one of the license types at a time. Smart Licensing is enabled by default in Cisco Prime Network Registrar. If you want to use traditional licenses, you must first disable Smart Licensing (see the *"Disabling Smart Licensing" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

Smart Licensing:

When you purchase Cisco Prime Network Registrar 11.0 with Smart License, the licenses get deposited to your Smart Account in the CSSM (or Satellite). You must register Cisco Prime Network Registrar with the CSSM (or Satellite) using web UI or CLI to use these licenses. See the *"Registering Cisco Prime Network Registrar with the CSSM" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Traditional Licensing:

When you purchase Cisco Prime Network Registrar 11.0, you receive a FLEXlm license file in an e-mail attachment from Cisco, after you register the software.

You must copy the license file to a location which will be accessible during the regional cluster installation before you attempt to install the software. The installation process will ask you for the location of the license file.

To obtain a license file:

1. Read the Software License Claim Certificate document packaged with the software.
2. Note the Product Authorization Key (PAK) number printed on the certificate.
3. Log in to one of the websites described on the certificate, and follow the registration instructions. The PAK number is required for the registration process.

   You should receive the license file through e-mail within one hour of registration.

A typical license file might look like:

```
INCREMENT base-system cisco 11.0 permanent uncounted \

 VENDOR_STRING=<Count>1</Count> HOSTID=ANY \

 NOTICE="<LicFileID>20110919130037832</LicFileID><LicLineID>4</LicLineID> \

 <PAK></PAK><CompanyName></CompanyName>" SIGN=521EA9F0925C
```

Image Signing

Starting from Cisco Prime Network Registrar 11.0, all the Cisco Prime Network Registrar images are signed. The RPM images have implicit signature, whereas the non-RPM images have a separate corresponding signature file. It is recommended that you verify the signature before installing Cisco Prime Network Registrar.

To verify the signature for the RPM images, do the following:

1. Import the GPG public key (**CPNR11-rel.gpg**) into the RPM using the following command. If you do not import the GPG public key into the RPM, then while installing, you will get a warning message.

   ```
   # rpm --import CPNR11-rel.gpg
   ```

2. Run the following command:

   ```
   # rpm -K file.rpm
   file.rpm: rsa sha1 (md5) pgp md5 OK
   ```

   Meaning: Package is signed, correct GPG key is imported

   Output from the above command shows that there are actually three distinct features of the package file that are checked by the -K option (use the -Kv option for verbose):

   - Size message indicates that the size of the packaged files has not changed.
   - PGP message indicates that the digital signature contained in the package file is a valid signature of the package file contents, and was produced by the organization that originally signed the package.
   - MD5 message indicates that a checksum contained in the package file and calculated when the package was built, matches a checksum calculated by RPM during verification. Because the two checksums match, it is unlikely that the package has been modified.

OK means that each of these tests was successful.

Other possible outputs of **rpm –K** command are as follows:

- # **rpm –K** *file.rpm*
  file.rpm: size md5 OK

  Meaning: Package not signed.

- # **rpm –K** *file.rpm*
  file.rpm: size (PGP) md5 OK (MISSING KEYS)

  Meaning: Wrong public key.

- # **rpm –K** *file.rpm*
  file.rpm: size PGP MD5 NOT OK

  Meaning: The RPM file has been changed or tampered with.

- # **rpm –K** *file.rpm*
  file.rpm: RSA sha1 ((MD5) PGP) md5 NOT OK (MISSING KEY)

  Meaning: Package is signed, but GPG keys are not imported.

To run the signature verification program for the non-RPM images, do the following:

1. Download the verification file (**cpnr_image_verification.gtar.gz**) from the same location as the images. This file contains the public certificate, signature verification script, and the README file.
2. Run the signature verification script using the following command:

   ./cisco_x509_verify_release.py3 -e CNR_REL_KEY-CCO_RELEASE.pem -i *image* **-s** *signature* **-v dgst -sha512**

   For example:

   ```
   # ./cisco_x509_verify_release.py3 -e CNR_REL_KEY-CCO_RELEASE.pem -i
   cpnr-local-11.0-1.el8.x86_64_rhel_docker.tar.gz -s
   cpnr-local-11.0-1.el8.x86_64_rhel_docker.tar.gz.signature -v dgst -sha512
   ```

Running Other Protocol Servers

You cannot run the Cisco Prime Network Registrar DNS, CDNS, DHCP, or TFTP servers concurrently with any other DNS, DHCP, or TFTP servers. If there are port conflicts when a server starts, the server will log issues and not function correctly.

If you want to disable a protocol server and prevent the Cisco Prime Network Registrar server from starting automatically after a system reboot, use the **server** {**dns** | **cdns** | **dhcp** | **tftp**} **disable start-on-reboot** command in the CLI.

Backup Software and Virus Scanning Guidelines

If you have automatic backup or virus scanning software enabled on your system, exclude the Cisco Prime Network Registrar directories and their subdirectories from being scanned. If they are not excluded, file locking issues can corrupt the databases or make them unavailable to the Cisco Prime Network Registrar processes. If you are installing in the default locations, exclude the /var/nwreg2 directories and their subdirectories.