CHAPTER 2

Installing and Upgrading Cisco Prime Network Registrar

This chapter describes how to install Cisco Prime Network Registrar 8.1 on Windows, Solaris, or Linux systems. It includes the following sections:

Checklist

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

- Does my operating system meet the minimum requirements to support Cisco Prime Network Registrar 8.1? (See the "System Requirements" section on page 1-2.)
- Does my hardware meet the minimum requirements? (See the "System Requirements" section on page 1-2.)
- If necessary, have I excluded Cisco Prime Network Registrar directories and subdirectories from virus scanning? (See the "Backup Software and Virus Scanning Guidelines" section on page 1-5.)
- On Windows, are other applications closed, including any virus-scanning or automatic-backup software programs? Is the Debugger Users group included in the Local Users and Groups?
- Do I have the proper software license? (See the "License Files" section on page 1-4.)
- 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?
- Is the cluster mode of operation regional or local?

- Is this a full or client-only installation?
- Is the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK), installed on the system? If so, where?
- Should the web UI use an HTTP or HTTPS connection, or both?
- 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?
  - Is my Cisco Prime Network Registrar task list empty?
  - Am I upgrading from a supported version (Cisco Prime Network Registrar 6.3 and later)?
  - Do I have the correct cnr_mcdexport tool? Note that the mcd_export tool is required only if you are upgrading from versions earlier to 7.2.

Before You Begin

Verify that you are running a supported operating system and that your environment meets all other current system requirements (see the "System Requirements" section on page 1-2).

If you are running an unsupported operating system, back up your Cisco Prime Network Registrar data and upgrade your operating system before installing this latest release.

To upgrade the operating system:

Step 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.

Step 2 Ensure that no pending database tasks result from recent edits. You can confirm that the task lists are empty by viewing the CCM and MCD Tasks pages under the Administration menu in the web UI. Wait until both lists are empty before proceeding with the update.

Step 3 Back up your database. The installation program tries to detect configuration data from an earlier installation and will upgrade the data.

Step 4 Upgrade your operating system.

Obtaining Cisco Prime Network Registrar License Files

When you purchase Cisco Prime Network Registrar 8.1, 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:

Step 1 Read the Software License Claim Certificate document packaged with the software.

Step 2 Note the Product Authorization Key (PAK) number printed on the certificate.

Step 3 Log into one of the Web sites 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 8.0 permanent uncounted \
    VENDOR_STRING=<Count>1</Count> HOSTID=ANY \
    NOTICE="<LicFileID>20110919130037832</LicFileID><LicLineID>4</LicLineID> \
    <PAK></PAK><CompanyName></CompanyName>" SIGN=521EA9F0925C
```

Installation and Upgrade Procedure

The procedure is essentially the same for a new installation or upgrade; except that the upgrade requires a few additional steps. See:

- Installing Cisco Prime Network Registrar 8.1, page 2-3
- Upgrade Considerations, page 2-9
- Reverting to Earlier Product Version, page 2-11

Installing Cisco Prime Network Registrar 8.1

To install Cisco Prime Network Registrar 8.1:

Step 1 Log into the target machine using an account that has administrative privileges:

- Windows—Account in the Administrators group
- Solaris and Linux—**su** (superuser) or root account

Windows—Close all open applications, including any antivirus software.

Step 2 Download and install the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK), if you have not already done so. These are available from the Oracle website.

Note On Windows, add the full path of the bin subdirectory of your Java installation folder to your PATH environment variable; for example, C:\Program Files (x86)\Java\jdk1.5.0_06\bin.

Step 3 If you are not configuring secure login to the web UI, skip to Step 4. If you are configuring secure login, you must create a keystore file by using the Java **keytool** utility, which is located in the bin subdirectory of the Java installation (see Step 2). Use the utility to define a self-signed certificate, or to request and later import a certificate from an external signing authority:

a. To create a keystore file containing a self-signed certificate, run this command and respond to the prompts:

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore k-file
    Enter keystore password: password
    What is your first and last name? [Unknown]: name
    What is the name of your organizational unit? [Unknown]: org-unit
    What is the name of your organization? [Unknown]: org-name
    What is the name of your City or Locality? [Unknown]: local
```

```
What is the name of your State or Province? [Unknown]: state
What is the two-letter country code for this unit? [Unknown]: cc
Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc correct? [no]: yes
Enter key password for <tomcat> (RETURN if same as keystore password):
```

The keystore filename (*k-file*) is its fully qualified path. You will be entering the keystore path and password in Step 15.

Note You must use 128-bit SSL to disable weak ciphers in the web UI. For more information, see Appendix D, "Enhancing Security for Web UI".

b. To create a Certificate Signing Request (CSR) that you will submit to the Certificate Authority (CA) when you request a certificate, create the keystore file as in the previous substep, then execute this command:

```
> keytool -certreq -keyalg RSA -alias tomcat -file certreq.cer -keystore k-file
  ...
```

Submit the resulting certreq.cer file to the CA. Once you receive the certificate from the CA, first download the Chain Certificate from the CA, then import the Chain Certificate and your new Certificate into the keystore file, as follows:

```
> keytool -import -alias root -keystore k-file -trustcacerts -file chain-cert-file
> keytool -import -alias tomcat -keystore k-file -trustcacerts -file new-cert-file
```

For details on the **keytool** utility, see the documentation at the Java website of Oracle. For details on the **keystore** file and Tomcat, see the documentation at the website of the Apache Software Foundation.

Caution The Cisco Prime Network Registrar installation program for Windows does not try to modify ACLs to restrict access to installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities to manually change file and directory permissions. See the "Modifying ACLs in Windows Installations" section on page 1-6.

Step 4 Load the installation CD, or browse to the network resource where the Cisco Prime Network Registrar software is located. If you download a distribution file from the Cisco website, run it from a different directory than where you will install Cisco Prime Network Registrar.

- Windows—The cnr_8_0-windows.exe file is a self-extracting executable file that places the setup file and other files in the directory where you run it. (If you are not configured for Autostart, run the setup.exe file in that directory.) The Welcome to Cisco Prime Network Registrar window appears.

  Click **Next**. The second welcome window introduces the setup program and reminds you to exit all current programs, including virus scanning software. If any programs are running, click **Cancel**, close these programs, and return to the start of Step 4. If you already exited all programs, click **Next**.

- Solaris and Linux—Be sure that the **gzip** and **gtar** utilities are available to uncompress and unpack the Cisco Prime Network Registrar installation files. See the GNU organization website for information on these utilities. Do the following:

  1. Download the distribution file.
  2. Navigate to the directory in which you will uncompress and extract the installation files.
  3. Uncompress and unpack the .gtar.gz file. Use **gtar** with the **–z** option:

     ```
     gtar -zxpf cnr_8_0-linux5.gtar.gz
     ```
     or
     ```
     gtar -zxpf cnr_8_0-solaris.gtar.gz
     ```

To unpack the .gtar file that **gunzip** already uncompressed, omit the **–z** option:

```
gtar -xpf cnr_8_0-linux5.gtar
```

4. Run the following command or program:

   Solaris—Run the **pkgadd** command with the **–d** option that specifies the directory from which you are installing, with the **–a** option in case you want to upgrade from a previous release. The name of the Cisco Prime Network Registrar package is **nwreg2**:

   ```
   pkgadd -a pkgdir/solaris/nwreg2/install/cnradmin -d pkgdir/solaris nwreg2
   ```

   Linux—Run the install_cnr script from the directory containing the installation files:

   ```
   install-path # ./install_cnr
   ```

   The *install-path* is the CD-ROM directory that contains the installation files or the directory that contains the extracted Cisco Prime Network Registrar installation files, if they were downloaded electronically.

Step 5 Specify whether you want to install Cisco Prime Network Registrar in the local or regional cluster mode (see the "About Cisco Prime Network Registrar" section on page 1-1):

Note Since a Regional server is required for license management, install the Regional first so that you can register the local to the Regional. If you face any problem with synchronizing the regional cluster to the local cluster after registration, unset and set the password on the regional cluster, and sync again.

Tip Include a network time service in your configuration to avoid time differences between the local and regional clusters. This method ensures that the aggregated data at the regional server appears consistently. The maximum allowable time drift between the regional and local clusters is five minutes. If the time skew exceeds five minutes, then the installation process will not be able to correctly register the server with the regional. In this case, unset and set the password on the regional cluster, and sync again.

- Windows—Keep the default Cisco Prime Network Registrar Local or choose Cisco Prime Network Registrar Regional. Click **Next**. The Select Program Folder appears, where you determine the program folder in which to store the program shortcuts in the Start menu. Accept the default, enter another name, or choose a name from the Existing Folders list. Click **Next**.
- Solaris and Linux—Enter **1** for a local, or **2** for regional. The default mode is 1.

Note If you are upgrading, the upgrade process autodetects the installation directory from the previous release.

Step 6 Note these Cisco Prime Network Registrar installation default directories and make any appropriate changes to meet your needs:

Windows default locations:

Caution Do not specify the \Program Files (x86) or \Program Files or \ProgramData for the location of the Cisco Prime Network Registrar data, logs, and temporary files. If you do this, the behavior of Cisco Prime Network Registrar may be unpredictable because of Windows security.

- Local cluster
  - Program files (32-bit OS)—C:\Program Files\Network Registrar\Local
  - Program files (64-bit OS)—C:\Program Files (x86)\Network Registrar\Local
  - Data files—C:\NetworkRegistrar\Local\data
  - Log files—C:\NetworkRegistrar\Local\logs
  - Temporary files—C:\NetworkRegistrar\Local\temp
- Regional cluster
  - Program files (32-bit OS)—C:\Program Files\Network Registrar\Regional
  - Program files (64-bit OS)—C:\Program Files (x86)\Network Registrar\Regional
  - Data files—C:\NetworkRegistrar\Regional\data
  - Log files—C:\NetworkRegistrar\Regional\logs
  - Temporary files—C:\NetworkRegistrar\Regional\temp

Solaris and Linux default locations:

- Local cluster:
  - Program files—/opt/nwreg2/local
  - Data files—/var/nwreg2/local/data
  - Log files—/var/nwreg2/local/logs
  - Temporary files—/var/nwreg2/local/temp
- Regional cluster:
  - Program files—/opt/nwreg2/regional
  - Data files—/var/nwreg2/regional/data
  - Log files—/var/nwreg2/regional/logs
  - Temporary files—/var/nwreg2/regional/temp

Step 7 If there are no defined administrators, create it by providing the username and password. You have to confirm the password entered.

If you are installing a regional, continue; else go to Step 9.

Step 8 Enter the filename, as an absolute path, for your base license (see the "License Files" section on page 1-4).

Note Ensure that you use the absolute path and not a relative path for your base license as there are chances that there might be changes to the default path from what you started the install with.

Entering the filename during installation is optional. However, if you do not enter the filename now, you must enter it when you first log into the web UI or CLI.

Note If you install Cisco Network Registrar 7.0 or later using a Remote Desktop Connection to the Windows Server, you will not be able to enter the license information during the installation. Cisco Prime Network Registrar will reject the licenses as invalid. You must therefore skip the license information step, and add the license after the installation completes, using either the web UI or CLI. See the"Starting Cisco Prime Network Registrar" section on page 2-13 for details.

Step 9 Register the local to the regional by providing the regional IP address and SCP port.

After the local is registered to the regional, it can provide those services for which the licenses are present in the regional.

Note If you face any problem synchronizing the regional cluster to the local cluster after registration, unset and set the password on the regional cluster, and sync again. This can happen due to time skew of more than five minutes between local and regional clusters.

Tip Include a network time service in your configuration to avoid time differences between the local and regional clusters. This method ensures that the aggregated data at the regional server appears consistently. The maximum allowable time drift between the regional and local clusters is five minutes. If the time skew exceeds five minutes, then the installation process will not be able to correctly register the server with the regional. In this case, unset and set the password on the regional cluster, and sync again.

Step 10 After you register local to the regional, you can select the required services from the licensed services.

Note If a service is not selected, upgrade process will use the existing configuration. To remove a service wait till the upgrade process is completed.

Step 11 Choose whether to archive the existing binaries and database in case this installation does not succeed. The default and recommended choice is **Yes** or **y**:

If you choose to archive the files, specify the archive directory. The default directories are:

- Windows—Local cluster (C:\NetworkRegistrar\Local.sav); Regional cluster (C:\NetworkRegistrar\Regional.sav). Click **Next**.
- Solaris and Linux—Local cluster (/opt/nwreg2/local.sav); Regional cluster (/opt/nwreg2/regional.sav)

Step 12 Choose the appropriate installation type: server and client (the default), or client-only:

- Windows—Choose **Both server and client (default)** or **Client only**. Click **Next.** The Select Port window appears.
- Solaris and Linux—Entering **1** installs the server and client (the default), or **2** installs the client only.

Note Choose **Client only** in a situation where you want the client software running on a different machine than the protocol servers. Be aware that you must then set up a connection to the protocol servers from the client.

Step 13 Enter the location of the Java installation (JRE or JDK 1.5.0_06 selected in Step 2). (The installation or upgrade process tries to detect the location.):

- Windows—A dialog box reminds you of the Java requirements. Click **OK** and then choose the default Java directory or another one. Click **OK**. The Select Connection Type window appears.
- Solaris and Linux—Enter the Java installation location.

Note Do not include the bin subdirectory in the path. If you install a new Java version or change its location, rerun the Cisco Prime Network Registrar installer, then specify the new location in this step.

Step 14 Choose whether to enable the web UI to use a nonsecure (HTTP) or secure (HTTPS) connection for web UI logins:

- Windows—Choose **Non-secure/HTTP (default)**, **Secure/HTTPS (requires JSSE)**, or **Both HTTP and HTTPS**.
- Solaris and Linux—Enter an HTTP port, a secure HTTPS port, or both HTTP and HTTPS ports.

Enabling the secure HTTPS port configures security for connecting to the Apache Tomcat web server (see Step 3 for configuration). (To change the connection type, rerun the installer, and then make a different choice at this step.)

- If you choose HTTPS, or HTTP and HTTPS, click **Next** and continue with Step 15.
- If you choose the default HTTP connection, click **Next**, and go to Step 16.

Step 15 If you enabled HTTPS web UI connectivity, you are prompted for the location of the necessary keystore and keystore files:

- For the keystore location, specify the fully qualified path to the keystore file that contains the certificate(s) to be used for the secure connection to the Apache Tomcat web server. This is the keystore file that you created in Step 3.
- For the keystore password, specify the password given when creating the keystore file. On Windows, click **Next**.

Caution Do not include a dollar sign ($) in the keystore password as it will result in an invalid configuration on the Apache Tomcat web server.

Step 16 Enter a port number for the web UI connection. The defaults are:

- HTTP local cluster—8080
- HTTP regional cluster—8090
- HTTPS local cluster—8443
- HTTPS regional cluster—8453

On Windows, click **Next**.

Step 17 Select the security mode to be configured. **Optional. Allow fallback to unsecure connection** is selected by default. Click **Next**.

The Cisco Prime Network Registrar installation process begins. (Solaris prompts you to verify that you want to continue with the installation.) Status messages report that the installer is transferring files and running scripts. This process may take a few minutes:

- Windows—The Setup Complete window appears. Choose **Yes, I want to restart my computer now** or **No, I will restart my computer later,** and then click **Finish**.
- Solaris and Linux—Successful completion messages appear.

Note When you upgrade Cisco Prime Network Registrar, the upgrade process takes place during the installation. Therefore, the installation and upgrade processes take a longer time depending on the number of scopes, prefixes, and reservations that you have configured.

Step 18 Verify the status of the Cisco Prime Network Registrar servers:

- Windows—In the Services control panel, verify that the Cisco Prime Network Registrar Local Server Agent or Cisco Prime Network Registrar Regional Server Agent is running after rebooting the system when the installation has completed successfully.
- Solaris and Linux—Use the *install-path***/usrbin/cnr_status** command to verify status. See the "Starting and Stopping Servers" section on page 2-14.

If the upgrade fails, you can revert to the earlier Cisco Prime Network Registrar version. For details about reverting to the earlier version, see the "Reverting to Earlier Product Version" section on page 2-11.

Upgrade Considerations

Cisco Prime Network Registrar 8.1 supports direct upgrades from 6.3 (Linux, Solaris, and Windows), and later.

Cisco Prime Network Registrar does not support the Red Hat 4.0, 3.0, and Solaris 8 and 9 operating systems. Back up your Cisco Prime Network Registrar data and upgrade your operating system before installing this latest release. (See the "System Requirements" section on page 1-2 for currently supported operating systems.)

Note When upgrading from a pre-7.2 cluster to Cisco Prime Network Registrar 8.1, a platform-specific tool cnr_mcdexport is required. This tool can be downloaded from Cisco.com as an archive file. The archive contains an extensive README file with specific instructions on the process to be followed.

The MCD DB database technology has been in use in Cisco Prime Network Registrar for versions earlier than 7.2. So, if you are upgrading from a pre-7.2 cluster which used the MCD database technology, the cnr_mcdexport kit should be used in extracting the MCD DB data. This MCD DB data, extracted by cnr_mcdexport kit is transferred to new locations during the upgrade procedure.

When you install the software, the installation program automatically detects an existing version and upgrades the software to the latest release. The program first prompts you to archive existing Cisco Prime Network Registrar data. If the program encounters errors during the upgrade, it restores the software to the earlier release.

During an upgrade, Cisco Prime Network Registrar now displays any pre-existing HTTPS configuration defaults for the keystore filename and password to enable a secure connection for web UI logins. If you have enabled HTTPS, and are unaware of the keystore filename and password at the time of the upgrade, you can preserve HTTPS connectivity during the upgrade, and re-enter the defaults when prompted.

Note The default keystore filename and password appear only if you are upgrading from Cisco Prime Network Registrar 6.3.1 or later versions, or reinstalling the Cisco Prime Network Registrar 8.1.

Related Topics

Upgrading on Windows, page 2-10

Upgrading on Solaris/Linux, page 2-11

Upgrading on Windows

To upgrade to Cisco Prime Network Registrar 8.1:

Step 1 Ensure that your environment meets the current system requirements (see the "System Requirements" section on page 1-2).

Step 2 Use the currently installed release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.

Step 3 Ensure that no pending database tasks result from recent edits. You can confirm that the task lists are empty by viewing the CCM and MCD Tasks pages under the Administration menu in the web UI. Wait until both lists are empty before proceeding with the update.

Step 4 Uninstall the previous version of Network Registrar. Your existing configuration data will remain in place after the uninstall. If the version you are upgrading from is already at 7.2 or above, then skip to Step 11.

Step 5 Create the C:\NetworkRegistrar\{Local | Regional} directory.

Caution Do not create this directory under C:\Program Files (x86), C:\Program Files, or C:\ProgramData.

Step 6 Move the data, logs, and temp directories manually to the \NetworkRegistrar\{Local | Regional} folder.

Step 7 Modify C:\{Program Files | Program Files (x86)}\{Local | Regional}\conf\cnr.conf to point at the new locations for the data, logs and temp directories.

Step 8 Restart Cisco Prime Network Registrar to ensure that all of the moves or edits were correct and that Cisco Prime Network Registrar is functioning normally.

Step 9 Stop Cisco Prime Network Registrar.

Step 10 Run cnr_mcdexport.exe to export the configuration objects to create an intermediate database. You can download the cnr_mcdexport_windows.tar tool from Cisco.com as an archive file. The archive contains an extensive README file with specific instructions on the process to be followed.

Step 11 Back up your Cisco Prime Network Registrar data on a different machine or a shared network device and upgrade your operating system to Windows Server 2008. See documentation supplied by Microsoft for information about how to install / upgrade Windows servers.

Note If you install Windows Server 2008 instead of upgrading and the disk is reformatted, you must restore the Cisco Prime Network Registrar data to the C:\NetworkRegistrar\{Local | Regional}\data folder.

Step 12 Install Cisco Prime Network Registrar 8.1 on the Windows Server 2008 machine. For installation instructions, see the "Installing Cisco Prime Network Registrar 8.1" section on page 2-3. Ensure that you specify the path where your existing data can be found, for example, C:\NetworkRegistrar\{Local | Regional}, to run the upgrade.

Note Ensure that you keep the old Cisco Network Registrar configuration and license information handy as you may need to re-enter this information during the Cisco Prime Network Registrar installation.

We recommend upgrading the regional cluster before upgrading any local clusters, because an older version of a regional cluster cannot connect to newer local clusters.

Upgrading on Solaris/Linux

To upgrade to Cisco Prime Network Registrar 8.1:

Step 1 Ensure that your environment meets the current system requirements (see the "System Requirements" section on page 1-2).

Step 2 Use the currently installed release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.

Step 3 Ensure that no pending database tasks result from recent edits. You can confirm that the task lists are empty by viewing the CCM and MCD Tasks pages under the Administration menu in the web UI. Wait until both lists are empty before proceeding with the update.

Step 4 Stop the Cisco Network Registrar server agent and backup the current system (or at least the Cisco Network Registrar\Program Files\Network Registrar\ directories and contents). To stop the Cisco Network Registrar server agent:

- If local—`/etc/init.d/nwreglocal stop`
- If regional—`/etc/init.d/nwregregion stop`

Step 5 If the version you are upgrading from is already at 7.2 or above, then skip to Step 6. Run cnr_mcdexport to export the configuration objects to create an intermediate database. You can download the cnr_mcdexport_linux4.tar (or cnr_mcdexport_linux5.tar or cnr_mcdexport_solaris.tar) tool from CCO. The archive contains an extensive README file with specific instructions on the process to be followed.

Step 6 Install Cisco Prime Network Registrar 8.1. For installation instructions, see the "Installing Cisco Prime Network Registrar 8.1" section on page 2-3.

Reverting to Earlier Product Version

The Cisco Prime Network Registrar installation program provides the capability of reverting to an earlier version and archiving the existing product configuration and data when upgrading to a newer version of the product. If you chose this option, and the upgrade process fails, use the following procedure to revert to the earlier product version and configuration:

Caution To complete this process, you must have access to the product installer and license key or license file for the earlier Cisco Prime Network Registrar version. Any attempt to proceed otherwise may destabilize the product.

If the installer had successfully performed the upgrade but you want to roll back to the earlier version at some later point, this procedure can result in network destabilization and data loss; for example, you will lose updates made to the Cisco Prime Network Registrar database after the upgrade, including DHCP lease data and DNS dynamic updates.

To revert to earlier version of the product:

Step 1 Verify that the archive directory that you specified during the upgrade process exists and is valid. These examples assume the default archive location provided during installation. Ensure that the path to the cnr_data_archive directory reflects the value of the archive directory that you specified during installation. If you are using:

- Windows—C:\NetworkRegistrar\{Local.sav | Regional.sav}
- Solaris and Linux—/opt/nwreg2/{local.sav | regional.sav}

Step 2 Uninstall Cisco Prime Network Registrar using the procedure described in the "Uninstalling Cisco Prime Network Registrar" section on page 2-16.

Step 3 Other than the contents of the specified archive directory, delete any remaining files and directories in the Cisco Prime Network Registrar installation paths.

Step 4 Reinstall the original version of Cisco Prime Network Registrar. Ensure that you follow the reinstallation procedure described in *Installation Guide for Cisco Network Registrar* that is specific to the original product version.

Step 5 After the installation ends successfully, stop the Cisco Prime Network Registrar server agent:

- Windows—Local: **`net stop nwreglocal`**
  Regional: **`net stop nwregregion`**
- Solaris and Linux—Local: **`/etc/init.d/nwreglocal stop`**
  Regional: **`/etc/init.d/nwregregion stop`**

Step 6 Delete the contents of the Cisco Prime Network Registrar *install-path*/data subdirectory.

Step 7 Extract the contents of the backup file to the reinstalled version of Cisco Prime Network Registrar.

1. Change to the root directory of the filesystem. On Windows, this directory would be the base drive (such as C:\); on Solaris and Linux, it would be /.
2. Using the fully qualified path to the archive directory, extract the archive. These examples assume the default archive location provided during installation.

- Windows—Copy the C:\NetworkRegistrar\{Local.sav|Regional.sav}\cnr_data_archive\ contents to the target Cisco Prime Network Registrar data directory. The following assume the default installation locations for a local cluster:

```
xcopy/s C:\NetworkRegistrar\Local.sav\cnr_data_archive
C:\NetworkRegistrar\Local\data\
```

Note There is also a cnr_file_archive directory which contains the installed files and generally this should not be recovered over a re-installation.

- Solaris and Linux
  - Change to the root directory of the filesystem —cd /.
  - Using the fully qualified path to the archive directory containing the cnr_data_archive.tar file, extract the archive. These examples assume the default archive location provided during installation. Ensure that the paths to the tar executable and cnr_data_archive.tar file reflect the value of the archive directory that you specified during installation.

    ```
    /opt/nwreg2/{local.sav | regional.sav}/tar -xf /opt/nwreg2/{local.sav |
    regional.sav}/cnr_data_archive.tar
    ```

Note There is also a cnr_file_archive.tar which contains the installed files and generally this should not be recovered over a re-installation.

Step 8 Start the Cisco Prime Network Registrar server agent:

- Windows—Local: **net start nwreglocal**
  Regional: **net start nwregregion**
- Solaris and Linux—Local: **/etc/init.d/nwreglocal start**
  Regional: **/etc/init.d/nwregregion start**

Step 9 Verify if the previous configuration, including scopes and zones, is intact.

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 (nonsecure login) or HTTPS (secure login) website:

  http://*hostname*:*http-port*
  https://*hostname*:*https-port*

  where:
  - The *hostname* is the actual name of the target host.
  - The *http-port and the https-ports* are the default HTTP or HTTPS port that are specified during installation. (See the installation procedure, Step 16 on page 2-8).

  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 8.1 > Network Registrar 8.1 local Web UI** (or **Network Registrar 8.1 local Web UI (secure)** if you enabled secure login).
  - On a regional cluster—Choose **Start > Programs > Network Registrar 8.1 > Network Registrar 8.1 regional Web UI** (or **Network Registrar 8.1 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>

- Solaris and 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 the 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 this 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 User Guide*.

Related Topics

Starting and Stopping Servers on Windows, page 2-14

Starting and Stopping Servers on Solaris or Linux, page 2-15

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 Solaris or Linux

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

To start and stop servers on Solaris or Linux:

Step 1 Log in as superuser.

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

```
# /etc/init.d/nwreglocal start ;for the local cluster
# /etc/init.d/nwregregion start ;for the regional cluster
```

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:

```
# /etc/init.d/nwreglocal stop ;for the local cluster
# /etc/init.d/nwregregion stop ;for the regional cluster
```

Moving an Installation to a New Machine

Before you begin, ensure that the new machine meets the current system requirements (see the "System Requirements" section on page 1-2).

To move an existing Cisco Prime Network Registrar installation to a new machine:

Step 1 Stop the server agent on the old machine.

- Windows—Local: **net stop nwreglocal**;
  Regional: **net stop nwregregion**
- Solaris and Linux—Local: **/etc/init.d/nwreglocal stop**;
  Regional: **/etc/init.d/nwregregion stop**

Step 2 Zip up the data directory on the old machine.

Step 3 Copy the zip file over to the same location on the new machine.

Step 4 Install Cisco Prime Network Registrar on the new machine (on Solaris and Linux, use the –a option). The installation will detect an upgrade and will do so based on the copied data.

This procedure preserves your original data on the old machine.

Troubleshooting the Installation

The Cisco Prime Network Registrar installation process creates a log file, install_cnr_log, in the Cisco Prime Network Registrar log file directory. For upgrades, one additional log file is created: lease_upgrade_log. The log directory is set to these locations by default:

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

If the installation or upgrade does not complete successfully, first check the contents of these log files to help determine what might have failed. Some examples of possible causes of failure are:

- An incorrect version of Java is installed.
- Insufficient disk space is available.
- Inconsistent data exists for an upgrade.

If the log messages do not clearly indicate the failure, you can gather additional debug information by using the debug_install utility script. This script appears only if the installation failed and is located by default in the Cisco Prime Network Registrar program files directory:

- Windows:
  - Local cluster: C:\Program Files(x86)\Network Registrar\Local\debug_install.cmd
  - Regional cluster: C:\Program Files\Network Registrar\Regional\debug_install.cmd
- Solaris and Linux:
  - Local cluster: /opt/nwreg2/local/debug_install.sh
  - Regional cluster: /opt/nwreg2/regional/debug_install.sh

If the `## Executing checkinstall script` part of the Solaris **pkgadd** fails, ensure that the /tmp directory has sufficient permissions to allow a nonprivileged installation user ID to write to it.

If you still need help determining the cause or resolution of the failure, forward the output of this script to Cisco Systems for further analysis. To contact Cisco for assistance, see the following Cisco website:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Uninstalling Cisco Prime Network Registrar

The uninstallation procedure differs based on the operating system you are using. You must have administrator or superuser privileges to uninstall Cisco Prime Network Registrar, just as you must to install it.

To back up your database before uninstalling Cisco Prime Network Registrar, see the *Cisco Prime Network Registrar User Guide* for the procedure.

Note Uninstallation stops the Cisco Prime Network Registrar server agents first. If you find that the server processes are not shutting down, see the "Starting and Stopping Servers" section on page 2-14.

Related Topics

Uninstalling on Windows, page 2-17
Uninstalling on Solaris, page 2-17
Uninstalling on Linux, page 2-18

Uninstalling on Windows

To uninstall Cisco Prime Network Registrar on Windows:

Step 1 Choose the Add/Remove Program function from the Windows control panel.

Or,

Choose **Uninstall Network Registrar 8.1** from the Windows Start menu. The uninstallation program removes the server and user interface components but does not delete user data files. Optionally, delete all Cisco Prime Network Registrar data by deleting the Cisco Prime Network Registrar folder.

Note Temporarily stop any service that is related to software that integrates with Performance Monitoring that might interfere with removing shared libraries in the Cisco Prime Network Registrar folder.

Step 2 Reboot after the uninstallation completes.

Uninstalling on Solaris

To uninstall Cisco Prime Network Registrar on Solaris:

Step 1 From the root account, use the **pkgrm** program to remove the **nwreg2** package:

```
pkgrm nwreg2
```

Solaris prompts you to verify that you want to continue with the uninstallation. The uninstallation procedure removes the server and user interface components; but does not delete user data, such as the log and data files. Optionally, delete the database and log files that are associated with Cisco Prime Network Registrar, as mentioned in the instructions at the end of the **pkgrm** process.

Uninstalling on Linux

To uninstall Cisco Prime Network Registrar on Linux:

Step 1 Run the **uninstall_cnr** program from the *install-path*/usrbin directory:

```
./uninstall_cnr
Stopping Server Agent...
Deleting startup files...
Removing Network Registrar...
cannot remove /opt/nwreg2/usrbin - directory not empty
cannot remove /opt/nwreg2/conf - directory not empty
package optnwreg2 not found in file index
Note that any files that have been changed (including your database) have _not_ been
uninstalled. You should delete these files by hand when you are done with them, before you
reinstall the package.
```

The `cannot remove` warnings mean that, although the uninstall program removes the server and user interface components, it cannot delete directories that are not empty. Certain configuration and data files that are created during installation remain deliberately after uninstallation. Optionally, delete the database and log files that are associated with Cisco Prime Network Registrar, as mentioned in the instructions at the end of the **uninstall_cnr** script execution.