Installing and Upgrading Cisco Prime Network Registrar

This chapter contains the following sections:

Installing Cisco Prime Network Registrar

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

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

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

Note From Cisco Prime Network Registrar 9.1, Linux and Windows installer provide an option to prompt for web service port, by default same as the web UI port. This will be prompted only if web services feature is enabled. For a new installation, default value of the web service port will be same as the default value for web UI port or the newly input web UI port. For subsequent installations, the port values will be picked from the conf files.

Caution Many distributions of Red Hat and CentOS Linux come with a firewall and connection tracking installed and enabled by default. Running a stateful firewall on the same OS and DNS will cause a significant decrease in server performance. Cisco strongly recommends **NOT** to use a firewall on the DNS server's operating system. If disabling the firewall is not possible, then connection tracking of DNS traffic MUST be disabled. For more information, see the *"DNS Performance and Firewall Connection Tracking" section in the Cisco Prime Network Registrar 10.1 Administration Guide*.

Step 2 Download and install JRE 1.8, or the equivalent JDK, if you have not already done so. These are available at 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\jdk1.8\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 17**.

Note You must use 128-bit SSL to disable weak ciphers in the web UI. For more information, see 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 the 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 Modifying ACLs in Windows Installations.

Step 4 Download the distribution file from Cisco.com, if needed. Then:

- Windows—The cpnr_*version*-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**.

- 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:

  a. Download the distribution file from Cisco.com, if needed.

  b. Navigate to a directory in which you want to uncompress and extract the installation files. It can be the same directory into which the distribution was downloaded.

  c. Uncompress and unpack the .gtar.gz file. Use **gtar** with the **-z** option:

  ```
  gtar -zxpf cpnr_10_1-linux-x86_64.gtar.gz
  ```

  The command creates the cpnr_10_1 directory into which the Cisco Prime Network Registrar installation files are extracted.

  d. Run the **install_cnr** script as follows:

  ```
  # ./cpnr_10_1/Linux/install_cnr
  ```

  The installation script does some checks to assure you are using a supported operating system version and that the required packages are installed, and will report if there are any issues and stop the installation.

Step 5 Specify whether you want to install Cisco Prime Network Registrar in the local or regional cluster mode:

Note Since a regional server is required for license management, install the regional server 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**.

- Linux—Enter **1** for a local, or **2** for regional. For a new installation, the default is 1. For an upgrade, the default depends on what was previously installed.

Step 6 On Linux, specify if you want to run Cisco Prime Network Registrar Local Server Agent as a non-root *nradmin* user. If you choose to run Cisco Prime Network Registrar for a non-root user, a user *nradmin* is created with the requisite privileges to run the Cisco Prime Network Registrar services. When running Cisco Prime Network Registrar as a non-root user *(nradmin*), some changes occur in the CLI operation of the product . Though it is still possible to run as

root, it is not recommended. Instead, create regular Linux users and add them to the *nradmin* group. Users in this group will have full access to the Cisco Prime Network Registrar files. To start and stop Cisco Prime Network Registrar, these users may use the new **cnr_service** program which is in *install-path*/bin/cnr_service).

Note The root user is only needed for installation and uninstallation.

Step 7 Note these Cisco Prime Network Registrar installation default directories and make any appropriate changes to meet your needs:

Note An installation directory path with spaces is not supported on Windows (except for system directories, such as "Program Files").

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

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—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—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

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 8 If there are no defined administrators, create an administrator by providing the username and password. You have to confirm the password entered.

If you are installing a regional, continue; else go to **Step 10**.

Step 9 Enter the filename, as an absolute path, for your base license (see License Files).

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 Prime Network Registrar 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 Starting Cisco Prime Network Registrar for details.

Step 10 Register the local to the regional by providing the regional IPv4 or IPv6 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.

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 11 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 until the upgrade process is completed.

Step 12 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**.
- Linux—Local cluster (*/opt/nwreg2/local.sav*); Regional cluster (*/opt/nwreg2/regional.sav*).

Step 13 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.

- 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 14 Enter CCM management SCP port number that the server agent uses for internal communication between servers. The default value is 1234 for local cluster and 1244 for regional cluster.

Step 15 Enter the location of JRE 1.8 or JDK 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.
- 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 16 Choose whether to enable the web UI to use a Non-secure (HTTP) or Secure (HTTPS) connection for web UI logins:

- Windows—Choose **Non-secure (HTTP) only**, **Secure (HTTPS) only (default)**, or **Both HTTP and HTTPS**.
- Linux—Enter **1** for Non-secure (HTTP) only, **2** for Secure (HTTPS) only (default), or **3** for both HTTP and HTTPS.

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 17**.
- If you choose HTTP connection, click **Next**, and go to **Step 18**.

Step 17 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.

Note From Cisco Prime Network Registrar 10.1 onwards, the keystore password is encrypted by default. If you want to change the keystore password later, you can use the plain text password. However, for better security, you should use the encrypt script present in the *install-path*/usrbin directory to generate the encrypted password. This encrypted password should be updated in server.xml. After making the change, you must restart Cisco Prime Network Registrar.

Step 18 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 19 Choose **Yes** if you want to enable the Cisco Prime Network Registrar web services.

Step 20 Enter a port number for the web service connection. The defaults are:

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

Note For Web services user have an option to enter a different port number.

Step 21 Select the security mode to be configured. **Required. Fail if the connection cannot be secured.** is selected by default. Click **Next**.

Step 22 If you are installing a regional, select **Yes** to enable the BYOD service.

The Cisco Prime Network Registrar installation process begins. 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**.
- 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 23 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.
- Linux—Use the *install-path*/usrbin/cnr_status command to verify the status. See Starting and Stopping Servers.

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 an Earlier Product Version, on page 9.

Upgrade Considerations

Cisco Prime Network Registrar 10.1 supports direct upgrades from 8.3 (Linux and Windows), and later, on the same platform.

Cisco Prime Network Registrar does not support Red Hat 3.x, 4.x, and 5.x. Back up your Cisco Prime Network Registrar data and upgrade your operating system before installing this latest release. (See System Requirements for currently supported operating systems.)

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.

Upgrading on Windows

To upgrade to Cisco Prime Network Registrar 10.1:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements).

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 Uninstall the previous version of Cisco Prime Network Registrar. Your existing configuration data will remain in place after the uninstall.

Step 4 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 2012 R2. See the documentation supplied by Microsoft for information about how to install/upgrade Windows servers.

Note If you install Windows Server 2012 R2 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 5 Install Cisco Prime Network Registrar 10.1 on the Windows Server 2012 R2 machine. For installation instructions, see Installing Cisco Prime Network Registrar, on page 1. 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 Prime Network Registrar configuration and license information handy as you may need to re-enter this information during the Cisco Prime Network Registrar installation.

Note While upgrading to Cisco Prime Network Registrar 10.1, you have an option to enter a different port number only for Web services.

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 Linux

To upgrade to Cisco Prime Network Registrar 10.1:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements).

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 Stop the Cisco Prime 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 Prime Network Registrar Local/Regional server agent:

- If local:
  - RHEL/CentOS 6.x—**/etc/init.d/nwreglocal stop**
  - RHEL/CentOS 7.x—**systemctl stop nwreglocal**
- If Regional:
  - RHEL/CentOS 6.x—**/etc/init.d/nwregregion stop**
  - RHEL/CentOS 7.x—**systemctl stop nwregregion**

Step 4 Install Cisco Prime Network Registrar 10.1. For installation instructions, see Installing Cisco Prime Network Registrar, on page 1.

Reverting to an Earlier Product Version

The Cisco Prime Network Registrar installation program provides the capability to archive the existing product configuration and data when you upgrade to a newer version and to revert to an earlier 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.

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}
- 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.

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 *Cisco Prime Network Registrar Installation Guide* 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**
- Linux—Local:
  - RHEL/CentOS 6.x—**/etc/init.d/nwreglocal stop**
  - RHEL/CentOS 7.x—**systemctl stop nwreglocal**
- Linux—Regional:
  - RHEL/CentOS 6.x— **/etc/init.d/nwregregion stop**
  - RHEL/CentOS 7.x— **systemctl stop nwregregion**

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.

a) Change to the root directory of the filesystem. On Windows, this directory would be the base drive (such as C:\); on Linux, it would be /.

b) 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.

- Linux:
  - Change to the root directory of the filesystem using **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**
- Linux—Local:
  - RHEL/CentOS 6.x—**/etc/init.d/nwreglocal start**
  - RHEL/CentOS 7.x—**systemctl start nwreglocal**
- Linux—Regional:
  - RHEL/CentOS 6.x—**/etc/init.d/nwregregion start**
  - RHEL/CentOS 7.x—**systemctl start nwregregion**

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

Moving a Local Cluster to a New Machine

Before you begin, ensure that the new machine meets the current system requirements (see System Requirements).

The following steps can be used to upgrade the cluster to a later Cisco Prime Network Registrar version (that is, it is not required that the same version of Cisco Prime Network Registrar be installed in Step 4; a later version that supports upgrades from the earlier version can be installed). This procedure MUST ONLY be used when migrating from Linux to Linux or Windows to Windows releases; these steps are not valid if migrating to a different server operating system platform.

The following procedure uses the default installation directories, and thus may need to be adjusted based on the paths used for the installation.

To move an existing Cisco Prime Network Registrar installation to a new machine on the same platform:

Step 1 Stop the server agent on the old local server.

- Windows:

  Local—**net stop nwreglocal**
- Linux—Local:
  - RHEL/CentOS 6.x—**/etc/init.d/nwreglocal stop**
  - RHEL/CentOS 7.x—**systemctl stop nwreglocal**

Step 2 Tar/zip up the /var/nwreg2/local/data directory and everything below it. Also, tar/zip up the following files on the old local server. Note that these are using the Linux default installation paths.

- /opt/nwreg2/local/conf/cnr.conf
- /opt/nwreg2/local/conf/cert directory and its contents
- /opt/nwreg2/local/conf/cnr_cert_config
- /opt/nwreg2/local/conf/public.der
- /opt/nwreg2/local/conf/priv/*
- Any customer extensions for DHCP in the /opt/nwreg2/local/extensions/dhcp/dex directory (except libdextension.so) and /opt/nwreg2/local/extensions/dhcp/tcl directory

Note Depending on the options selected when the product was installed, not all of these files may exist.

Step 3 Copy the tar/zip files to the respective locations on the new server, and untar/unzip the files.

Step 4 Install Cisco Prime Network Registrar (local cluster) on the new server. 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.

Re-apply any custom configuration changes (such as those outlined in Enhancing Security for Web UI) after the installation.

Step 5 Login to the web UI and navigate to the **List Licenses** page under the **Administration** menu.

Step 6 Edit the regional server information as necessary. Ensure that the regional server information provided is where you would like to register your new machine.

Step 7 Click the **Register** button to register with the regional server.

Step 8 If the IP address of the machine has changed, you may need to also update the failover/HA DNS partner to assure it also has the new address of the server. For DHCP, you may need to update the relay agent helper addresses and DNS server addresses.

Note An address change can prevent DHCP clients from renewing promptly (they may not be able to renew until they reach the rebinding time) and can prevent DNS queries from being resolved until clients or other DNS servers receive the updated information.

Moving a Regional Cluster to a New Machine

License management is done from the regional cluster when Cisco Prime Network Registrar is installed. The regional server is installed first and all licenses are loaded in the regional server. When the local cluster is installed, it registers with the regional server to obtain its license.

When you want to move a regional cluster to a new machine, you need to back up the data on the old regional cluster and copy the data to the same location on the new machine.

Note When the regional server goes down or is taken out of service, the local cluster is not aware of this action. If the outage lasts for less than 24 hours, it results in no impact on the functioning of the local clusters. However, if the regional cluster is not restored for more than 24 hours, the local cluster may report warning messages that the local cluster is not properly licensed (in the web UI, CLI, or SDK). This does not impact the operation of the local clusters and the local clusters continue to work and service requests.

The following steps can be used to upgrade the cluster to a later Cisco Prime Network Registrar version (that is, it is not required that the same version of Cisco Prime Network Registrar be installed in Step 4; a later version that supports upgrades from the earlier version can be installed). This procedure MUST ONLY be used when migrating from Linux to Linux or Windows to Windows releases; these steps are not valid if migrating to a different server operating system platform.

The following procedure uses the default installation directories, and thus may need to be adjusted based on the paths used for the installation.

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

Step 1 Stop the server agent on the old regional server:

- Windows:

  net stop nwregregion

- Linux:
  - RHEL/CentOS 6.x—**/etc/init.d/ nwregregion stop**
  - RHEL/CentOS 7.x—**systemctl stop nwregregion**

Step 2 Tar/zip up the /var/nwreg2/regional/data directory and everything below it. Also, tar/zip the following files on the old regional server. Note that these are using the Linux default installation paths.

- /opt/nwreg2/regional/conf/cnr.conf
- /opt/nwreg2/regional/conf/cert directory and its contents
- /opt/nwreg2/regional/conf/cnr_cert_config
- /opt/nwreg2/regional/conf/public.der
- /opt/nwreg2/regional/conf/priv/*

Note Depending on the options selected when the product was installed, not all of these files may exist.

Step 3 Copy the tar/zip files to the respective locations on the new server, and untar/unzip the files.

Step 4 Install Cisco Prime Network Registrar (regional cluster) on the new server. For more information, see Installing Cisco Prime Network Registrar, on page 1.

The installation will detect an upgrade and will do so based on the copied data. This procedure preserves your original data from the old regional server.

Re-apply any custom configuration changes (such as those outlined in Enhancing Security for Web UI) after the installation.

Note When you install Cisco Prime Network Registrar on the new machine, you must choose the data directory on which you have copied the data from the old regional server.

Step 5 Start the Cisco Prime Network Registrar web UI or CLI. For more information, see Starting Cisco Prime Network Registrar.

Step 6 Log in as superuser to the CLI for the new regional cluster.

Step 7 To list the local clusters, use the following command:

```
nrcmd-R> cluster listnames
```

Step 8 To synchronize the data as well as the license information, use the following command:

```
nrcmd-R> cluster cluster-name sync
```

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
- 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
- Linux:

- Local cluster: /opt/nwreg2/local/debug_install.sh
- Regional cluster: /opt/nwreg2/regional/debug_install.sh

If you need help in 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

Troubleshooting Local Cluster Licensing Issues

If your regional cluster and local cluster are located in isolated networks, are separated by a firewall, or the time skew between the regional and local clusters is more than five minutes, then the local cluster may be unable to register with the regional server. The firewall may block the return connection used to validate the local cluster admin credentials that are sent from the local cluster to the regional cluster.

To register a local cluster with the regional cluster:

Step 1 Install Cisco Prime Network Registrar (local cluster) on the server and create the admin user for the local cluster. For more information, see Installing and Upgrading Cisco Prime Network Registrar, on page 1.

When you install Cisco Prime Network Registrar on the local cluster, you can skip the registration of the local cluster with the regional cluster.

Step 2 Log into the regional cluster and add the new local cluster to the regional cluster with the admin credentials. For more information, see the *"Adding Local Clusters" section in the Cisco Prime Network Registrar 10.1 Administration Guide*.

Step 3 To synchronize the data as well as the license information, click the **Resynchronize** icon.