## CONTENTS

### CHAPTER 1  Installation Overview  1

- **Overview**  1
- **About Cisco Prime Network Registrar**  1

### CHAPTER 2  Configuration Options  3

- **Mixed DHCP and DNS Scenarios**  3
  - **One-Machine Mixed Configuration**  3
  - **Two-Machine Mixed Configuration**  3
  - **Three-Machine Mixed Configuration**  4
  - **Four-Machine Mixed Configuration**  4
- **DHCP-Only Scenarios**  4
  - **One-Machine DHCP Configuration**  5
  - **Two-Machine DHCP Configuration**  5
- **DNS-Only Scenarios**  5
  - **One-Machine DNS Configuration**  5
  - **Two-Machine DNS Configuration**  5
  - **Three-Machine DNS Configuration**  5

### CHAPTER 3  Installation Requirements  7

- **System Requirements**  7
- **Installation Modes**  9
- **License Files**  9

### CHAPTER 4  Preparing for the Installation  13

- **Installation Checklist**  13
- **Before You Begin**  14
- **Obtaining Cisco Prime Network Registrar License Files**  14
- **Running Other Protocol Servers**  15
Contents

Booting and Configuring Cisco Prime Network Registrar Virtual Appliance 44
Upgrading the Cisco Prime Network Registrar Virtual Appliance 45
Upgrading the Cisco Prime Network Registrar Installation to run on a Cisco Prime Network Registrar Virtual Appliance 45
Upgrading the Cisco Prime Network Registrar Virtual Appliance 47
Next Steps: Cisco Prime Network Registrar Virtual Appliance 48
Configuring Cisco Prime Network Registrar 48
Configuring Cisco Prime Network Registrar with the CLI on Virtual Appliance 50
Configuring the Virtual Appliance to Automatically Power Up 50
Managing the Cisco Prime Network Registrar Virtual Appliance 51

APPENDIX A

Performing a Silent Installation 53
Performing a Silent Installation 53

APPENDIX B

Lab Evaluation Installations 59
Lab Evaluation Installations 59
Installing Cisco Prime Network Registrar in a Lab 60
Testing the Lab Installation 60
Uninstalling in a Lab Environment 60

APPENDIX C

Installing the Cisco Prime Network Registrar SDK 61
Installing on Linux or Solaris 61
Installing on Windows 62
Testing Your Installation 62
Compatibility Considerations 62

APPENDIX D

Enhancing Security for Web UI 65
Enhancing Security for Web UI 65

APPENDIX E

Troubleshooting DHCP Server Out of Memory Aborts on Linux 67
Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions 69
Undo Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions 70
Alternative Workaround for Cisco Prime Network Registrar 8.3 70
Undo Alternative Workaround for Cisco Prime Network Registrar 8.3 71
Contents

Workaround for other Versions 71
Undo Workaround for other Versions 72
Avoiding the Issue on Cisco Prime Network Registrar 8.3 and later on RHEL /CentOS 6.x 72
CHAPTER 1

Installation Overview

This chapter contains the following sections:

- Overview, page 1
- About Cisco Prime Network Registrar, page 1

Overview

This guide describes how to install Cisco Prime Network Registrar Release 8.3 on Windows, Solaris, and Linux operating systems, and how to install the Cisco Prime Network Registrar Virtual Appliance. You can also see the following documents for important information about configuring and managing Cisco Prime Network Registrar:

- For configuration and management procedures for Cisco Prime Network Registrar and Cisco Prime Network Registrar Virtual Appliance, see the Cisco Prime Network Registrar 8.3 Administrator Guide.

- For details about commands available through the command line interface (CLI), see the Cisco Prime Network Registrar 8.3 CLI Reference Guide.

About Cisco Prime Network Registrar

Cisco Prime Network Registrar is a network server suite that automates managing enterprise IP addresses. It provides a stable infrastructure that increases address assignment reliability and efficiency. It includes (see Figure 1: Cisco Prime Network Registrar User Interfaces and the Server Cluster, on page 2):

- Dynamic Host Configuration Protocol (DHCP) server
- Domain Name System (DNS) server
- Caching Domain Name System (CDNS) server
- Router Interface Configuration (RIC) server
- Simple Network Management Protocol (SNMP) server
- Trivial File Transfer Protocol (TFTP) server
You can control these servers by using the Cisco Prime Network Registrar web-based user interface (web UI) or the command line interface (CLI). These user interfaces can also control server clusters that run on different platforms.

You can install Cisco Prime Network Registrar in either local or regional mode:

- **Local mode** is used for managing local cluster protocol servers.
- **Regional mode** is used for managing multiple local clusters through a central management model.

A regional cluster centrally manages local cluster servers and their address spaces. The regional administrator can perform the following operations:

- Manage licenses for Cisco Prime Network Registrar. An installation must have at least one regional cluster for license management purposes.
- Push and pull configuration data to and from the local DNS and DHCP servers.
- Obtain subnet utilization and IP lease history data from the local clusters.
- Manage the router interface configuration (RIC) server that integrates with cable modem termination systems (CMTSs) directly from the regional cluster.

*Figure 1: Cisco Prime Network Registrar User Interfaces and the Server Cluster*
Configuration Options

Cisco Prime Network Registrar DHCP, Authoritative DNS, and Caching DNS components are licensed and managed from the regional server. You need to have a regional server and all services in the local clusters are licensed through the regional cluster. Only a regional install asks for a license file and only the regional server accepts new license files. Then the regional server can authorize individual local clusters based on available licenses.

The sample configuration shown in this chapter is based on the typical use cases described in the following sections:

- Mixed DHCP and DNS Scenarios, page 3
- DHCP-Only Scenarios, page 4
- DNS-Only Scenarios, page 5

Mixed DHCP and DNS Scenarios

You can set up Cisco Prime Network Registrar for a mixed DHCP and DNS configuration with different numbers of machines.

One-Machine Mixed Configuration

Configure both DHCP and Auth DNS servers on a single machine, initially enabling the servers as primaries, and enabling the TFTP server and SNMP traps. Then configure at least one forward zone and corresponding reverse zone, at least one scope, and DNS Update.

Configure both DHCP and Caching DNS servers on a single machine, initially enabling the servers as primaries, and enabling the TFTP server and SNMP traps. Then you can configure forwarders and exception lists.

Two-Machine Mixed Configuration

A mixed DHCP configuration on two machines offers a few alternatives:
- Configure one machine as primary DHCP and Auth DNS server, and the second machine as a secondary Auth DNS server. Then configure a zone distribution and DNS access controls on the first machine and optionally access controls on the second machine.

- Configure one machine as DHCP and Auth DNS main servers and the second machine as DHCP and Auth DNS backup servers. Perform minimal configuration on the backup machine (changing the password, enabling DHCP and Auth DNS, and selecting partner backup roles). On the main machine, build the configuration, creating server pairs and scheduling synchronization tasks with the backup machine.

- Configure one machine as a DHCP server and the second machine as a Auth DNS primary then configure either machine with DNS Update and push the configuration to the other machine.

- Configure one machine with both DHCP server and Auth DNS server and the second machine as a Caching DNS server with the Auth DNS server as the Forwarder.

### Three-Machine Mixed Configuration

A mixed configuration on three machines offers a few additional alternatives:

- Configure one machine as a DHCP server, the second machine as an Auth DNS primary, and the third machine as an Auth DNS secondary. Optionally revisit the machines to make the DHCP main the Auth DNS backup, and make the Auth DNS main the DHCP backup.

- Configure one machine as DHCP failover and Auth DNS High-Availability (HA) main servers, the second machine as DHCP failover and Auth DNS HA backup servers, and the third machine as a Auth DNS secondary server.

- Configure one machine as a DHCP server, the second machine as the Auth DNS server and the third machine as a Caching DNS, with the Auth DNS as the Forwarder.

- Configure one machine as a DHCP primary server and Auth DNS primary, the second machine as a DHCP secondary and Auth DNS secondary server and the third machine as a Caching DNS, with the primary Auth DNS of the first machine as the Forwarder.

### Four-Machine Mixed Configuration

A mixed configuration on four machines could include:

- DHCP and Auth DNS main and backup pairs, with the first machine as a DHCP main, the second machine as a DHCP backup, the third machine as an Auth DNS main configured with DNS Update, and the fourth machine as an Auth DNS backup.

- An add-on to the three-machine scenario, with the first machine as a DHCP main, the second machine as an Auth DNS main, the third machine as DHCP and Auth DNS backups, and the fourth machine as an Auth DNS secondary.

- Configure the first machine as DHCP main, second machine as DHCP backup, third machine as Auth DNS, and Caching in fourth, with Auth DNS as Forwarder.

### DHCP-Only Scenarios

A DHCP-only configuration could be on a single machine or two machines.
One-Machine DHCP Configuration

Initially configure only DHCP, skip the class-of-service and failover options, and revisit the setup to enable class-of-service and policy options.

Two-Machine DHCP Configuration

Configure the first machine as a DHCP main and the second machine as a backup, with minimal backup configuration (changing password, enabling DHCP, and selecting the backup role), and set up the first machine with failover load balancing, optionally scheduling failover synchronization tasks.

DNS-Only Scenarios

A DNS-only configuration could be on one, two, or three machines.

One-Machine DNS Configuration

Initially configure DNS as an Auth primary, Auth secondary, or caching server.

Two-Machine DNS Configuration

Configure the first machine as an Auth DNS primary and the second machine as a secondary, or the first machine as a main primary and the second machine as a backup primary.

Configure the first machine as an Auth DNS and the second machine as Caching DNS.

Three-Machine DNS Configuration

Configure the first machine as an Auth DNS main primary, the second machine as a backup primary, and the third machine as a secondary server.

Configure the first machine as Auth DNS primary, the second machine as secondary, and the third machine as Caching DNS.
CHAPTER 3

Installation Requirements

This chapter contains the following sections:

- System Requirements, page 7
- Installation Modes, page 9
- License Files, page 9

System Requirements

Review the system requirements before installing the Cisco Prime Network Registrar 8.3 software:

- Java—You must have the Java Runtime Environment (JRE) 1.6 or later, or the equivalent Java Development Kit (JDK) installed on your system. (The JRE is available from Oracle on its website.)

- Operating system—We recommend that your Cisco Prime Network Registrar machine run on the Windows, Solaris, or Linux operating systems as described in Table 1: Cisco Prime Network Registrar Server Minimum Requirements, on page 8. Cisco Prime Network Registrar is supported on 32-bit or 64-bit operating systems.

Cisco Prime Network Registrar supports running in VMWARE ESXi 5.0 or later environment.

Note

Cisco Prime Network Registrar applications are 32-bit executable programs and the system should support 32-bit applications (Java JRE/JDK, OpenLDAP library (for RedHat)).

- User Interface—Cisco Prime Network Registrar currently includes two user interfaces: a web UI and a CLI:
  - The web UI has been tested on Microsoft Internet Explorer 9 and Mozilla Firefox 21 and later. Internet Explorer 8 is not supported.
  - The CLI runs in a Windows, Solaris, or Linux command window.
For the CLI, the number of concurrent active user sessions and processes on a cluster can be no more than 14.

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.

**Table 1: Cisco Prime Network Registrar Server Minimum Requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Solaris</strong></td>
</tr>
<tr>
<td>OS version</td>
<td>Solaris 10</td>
</tr>
<tr>
<td>Disk space</td>
<td>2 x 73/146 SAS drives</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>16 GB</td>
</tr>
</tbody>
</table>

1. Cisco Prime Network Registrar 8.3 supports Solaris Sparc only, 128-KB block sizes in the Solaris 10 ZFS and running in Solaris LDOM environments.
2. Cisco Prime Network Registrar is supported on 32-bit and 64-bit operating systems.
3. Cisco Prime Network Registrar 8.3 supports Red Hat Enterprise Linux ES 5.0 and Red Hat Enterprise Linux ES 6.0, running standalone or on VMWare (ESX Server 5.0 or later) on Cisco Unified Computing System (CUCS) and other hardware supported by VMWare.
4. Cisco Prime Network Registrar 8.3 supports Windows Server 2008, running standalone or on VMWare (ESX Server 5.0 or later) on Cisco Unified Computing System (CUCS) and other hardware supported by VMWare.
5. Higher I/O bandwidth usually results in higher average leases per second.
6. Serial Attached SCSI.
7. Serial Advanced Technology Attachment (Serial ATA).
8. Faster CPU and more memory typically result in higher peak leases per second.
System Requirements for Linux OS (RH 5.x, RH6.x and CentOS 6.5)
The Linux OS has the following (32-bit) packages. To support External Authentication using AD feature ensure installation of the following:

- krb5-libs
- cyrus-sasl-gssapi

System Requirements for Red Hat Enterprise Linux ES 6.x (64-bit)
To run Cisco Prime Network Registrar on Red Hat Enterprise Linux ES 6.x (64-bit), ensure the following:

1. The Linux operating system has the following packages to support the Cisco Prime Network Registrar (32-bit) applications:
   - glibc.i686
   - libgcc.i686
   - glibc-common
   - libstdc++
   - compat-libstdc++
   - cyrus-sasl-lib

2. Java Runtime Environment (JRE) (32-bit) is installed along with the dependencies.

Installation Modes
The modes of installation that exist for the local and regional clusters are new installations and upgrades from a previous version. These installations or upgrades are performed by using operating system-specific software installation mechanisms:

- Windows—InstallShield setup program
- Solaris—pkgadd command
- Linux—install_cnr script that uses Red Hat Package Manager

License Files
Cisco Prime Network Registrar license is a perpetual license. The license enables specific components which you have licensed.

Previously, Cisco Network Registrar was licensed as a single system with a single license type called ip-node. For Cisco Prime Network Registrar 8.3, the licensing is done according to the services that you require. The following are the types of licences available:

- base-system—Licenses the CCM services. This license is mandatory if you want to run Cisco Prime Network Registrar.
- base-dhcp—Licenses DHCP/TFTP services and, optionally, an initial count of leases
• **base-dns**—Licenses authoritative DNS services and, optionally, an initial count of RRs
• **base-cdns**—Licenses caching DNS services and, optionally, an initial count of servers
• **count-dhcp**—Licenses an incremental number of active leases
• **count-dns**—Licenses an incremental number of RRs
• **count-cdns**—Licenses an incremental number of caching server instances

The different services provided by Cisco Prime Network Registrar are associated with the different license types as follows:

• **CCM services**—**base-system**
• **DHCP services**—**base-dhcp** and **count-dhcp**
• **Authoritative DNS services**—**base-dns** and **count-dns**
• **Caching DNS services**—**base-system** and **base-cdns**

---

**Note**

You should have at least one base license for a server to enable that service.

---

**Note**

Cisco Prime Network Registrar IPAM uses a separate license and install process. For more information, see *Cisco Prime Network Registrar 8.1.3 IPAM Installation Guide*.

License management is done from the regional cluster when Cisco Prime Network Registrar is installed. You must install the regional server first, and load all licenses in the regional server. When you install the local cluster, it registers with regional to obtain its license.

When you install the regional, you are prompted to provide the license file. You can store the license file in any location provided the location and file are accessible during the installation.

The utilization of licenses are calculated by obtaining statistics from all the local clusters in the Cisco Prime Network Registrar system for all counted services (DHCP, DNS, and CDNS). The regional CCM server maintains the license utilization history for a predetermined time period.

Utilization is calculated for different services as:

• **DHCP services**—total number of active DHCP leases (including v4 and v6)
• **Auth DNS services**—the total number of DNS resource records (all RR types)
• **Caching DNS services**—total number of Caching DNS servers being run in the Cisco Prime Network Registrar system

The services on each local cluster will be restricted based on the services for which licenses are present.

When you configure DHCP failover, only simple failover is operational and supported (see Failover scenarios section in the Configuring DHCP Failover chapter of the *Cisco Prime Network Registrar 8.3 DHCP User Guide*).

To learn about obtaining the license files for Cisco Prime Network Registrar, see *Obtaining Cisco Prime Network Registrar License Files*, on page 14.
Market Segment Specific Licensing

From release 8.1.2, Cisco Prime Network Registrar license types are offered specific to market segments. Market specific licensing generates license keys for use by market segments, that is, Service Provider, Smart Grid, and so on. Cisco Prime Network Registrar features are enabled based on the market segment specific license you choose. For example, the PNR license offers features designed for the Service Provider market segment whereas the PNR-SG license offers features designed for the Smart Grid market segment.

Cisco Prime Network Registrar offers the following market segment specific licenses:

- Prime Network Registrar—PNR
- Prime Network Registrar Connected Grid—PNR-SG
- Prime IP Express—PNR—ENT

Note

If the licenses for all market segments are installed, then only the PNR license will be active.

The regional server which uses the PNR-SG license can be converted to PNR by installing the PNR license. Local cluster licenses will be converted automatically at the next compliance check, or can be manually updated by resynchronizing the local cluster.

For a given market segment license, only the counts from corresponding market segment license will apply. For example, if the PNR count license is applied when the PNR-SG base license is active, the Right to Use count will not be updated. If the PNR-SG count license is applied when the PNR base license is active, the Right to Use count will not be updated.

PNR Licenses

The PNR license provides all the features available for the Cisco Prime Network Registrar release you install. If your license set was issued for a release before 8.1.2, it is a PNR license.

PNR-SG Licenses

The PNR-SG license disables the following PNR features which have been identified as not necessary for Smart Grid implementations:

- Tenants
- External Authentication

The DHCP service PNR-SG license offers you the PNR features with the exception of:

- Extensions
- Lightweight Directory Access Protocol (LDAP)
- TCP Listeners (client notification)
- Trivial File Transfer Protocol (TFTP)
- Router Interface Configuration (RIC)
- Regional lease history and subnet utilization
- BYOD
Prime IP Express—NETREG-ENT

To know the list of features supported by Prime IP Express—NETREG-ENT licenses see *IP Express Installation Guide*. 
Preparing for the Installation

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

- Installation Checklist, page 13
- Before You Begin, page 14
- Obtaining Cisco Prime Network Registrar License Files, page 14
- Running Other Protocol Servers, page 15
- Backup Software and Virus Scanning Guidelines, page 15
- Server Event Logging, page 16
- Modifying ACLs in Windows Installations, page 16

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 2: Installation Checklist

<table>
<thead>
<tr>
<th>Task</th>
<th>Checkoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does my operating system meet the minimum requirements to support Cisco Prime Network Registrar 8.3? (See the System Requirements, on page 7 section.)</td>
<td>☐</td>
</tr>
<tr>
<td>Does my hardware meet the minimum requirements? (See the System Requirements, on page 7 section.)</td>
<td>☐</td>
</tr>
<tr>
<td>If necessary, have I excluded Cisco Prime Network Registrar directories and subdirectories from virus scanning? (See the Backup Software and Virus Scanning Guidelines, on page 15 section.)</td>
<td>☐</td>
</tr>
<tr>
<td>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?</td>
<td>☐</td>
</tr>
</tbody>
</table>
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, on page 7).

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.

Obtaining Cisco Prime Network Registrar License Files

When you purchase Cisco Prime Network Registrar 8.3, 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 into 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 8.0 permanent uncounted \
VENDOR_STRING=<Count>1</Count> HOSTID=ANY \ 
NOTICE="<LicFileID>20110919130037832</LicFileID><LicLineID>4</LicLineID> \ 
<PAK></PAK><CompanyName></CompanyName>" SIGN=521EA9F0925C
```

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 the Cisco Prime Network Registrar installation process detects that a conflict exists, it displays a warning message.

On Windows systems, use one of the following methods to change the configuration from the Service Control Manager:

- Stop the Cisco Prime Network Registrar protocol server that conflicts with the Microsoft protocol server by using the Stop function in one of the user interfaces.
- Change the Microsoft servers from a Startup Type of Automatic to Manual or Disabled.

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 on the default locations, exclude the following directories and their subdirectories:

```
In this documentation set, when install-path is used, it refers to all or part of the installation paths that were specified when installing Cisco Prime Network Registrar. As an example using the Solaris and Linux default local cluster paths of /opt/nwreg2/local and /var/nwreg2/local, the install-path may represent these paths.
```
• Windows—
  \texttt{install-path/data} (for example, 	exttt{C:/NetworkRegistrar/Local/data} and 	exttt{C:/Network Registrar/Regional/data})
  \texttt{install-path/logs} (for example, 	exttt{C:/NetworkRegistrar/Local/logs} and 	exttt{C:/Network Registrar/Regional/logs})
• Solaris and Linux—
  \texttt{install-path/data} (for example, 	exttt{/var/nwreg2/local/data} and 	exttt{/var/nwreg2/regional/data})
  \texttt{install-path/logs} (for example, 	exttt{/var/nwreg2/local/logs} and 	exttt{/var/nwreg2/regional/logs})

## 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: \texttt{C:/NetworkRegistrar/Local/logs};
  Regional cluster: \texttt{C:/NetworkRegistrar/Regional/logs}
• Solaris and Linux—Local cluster: \texttt{/var/nwreg2/local/logs};
  Regional cluster: \texttt{/var/nwreg2/regional/logs}

To monitor the logs, use the \texttt{tail -f} command.

\textbf{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 \textbf{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—\texttt{cacls} and \texttt{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 subdirectories contain data that you may want only the Administrators system group to access:

• \texttt{installdir/conf/cnr.conf}
• \texttt{installdir/tomcat/conf/server.xml}
• \texttt{installdir/conf/priv/}
• \texttt{installdir/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.
Installing and Upgrading Cisco Prime Network Registrar

This chapter contains the following sections:

- Installing Cisco Prime Network Registrar, page 19
- Upgrade Considerations, page 25
- Reverting to an Earlier Product Version, page 27
- Moving an Installation to a New Machine, page 29
- Moving a Regional Cluster to a New Machine, page 30
- Troubleshooting the Installation, page 31
- Troubleshooting Local Cluster Licensing Issues, page 32

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
- 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) 1.6 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\jdk1.6\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:

```bash
> 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 16**.

**Note** You must use 128-bit SSL to disable weak ciphers in the web UI. For more information, see *Enhancing Security for Web UI*, on page 65.

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:

```bash
> 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:

```bash
> 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*, on page 16.

**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 cpnr_8_3-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:

   ```bash
gtar -zxpf cpnr_8_3-linux5.gtar.gz
```

   or

   ```bash
gtar -zxpf cpnr_8_3-solaris.gtar.gz
```

   To uncompress the .gtar file that gunzip already uncompressed, omit the -z option:

   ```bash
gtar -xpf cpnr_8_3-linux5.gtar
```

   The command creates the cpnr_8_3 directory into which the Cisco Prime Network Registrar installation files are extracted.

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:

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

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

     ```bash
     # ./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 About Cisco Prime Network Registrar, on page 1):

**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.

- 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** 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 'cpnr_service' program in the path which is in <install directory>/bin/cpnr_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** The installation directory path with spaces is not supported on non-Windows platforms and not recommended on Windows (except for the "Program Files" path).

**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
  - Logs 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
  - Logs files—C:\NetworkRegistrar\Regional\logs
  - Temporary files—C:\NetworkRegistrar\Regional\temp

**Solaris and Linux default locations:**

- **Local cluster**
  - Program files—/opt/nwreg2/local
Step 8 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 10.

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

**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, on page 33 for details.

Step 10 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.

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 till 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**.
- **Solaris and 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.
- 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 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 the Java installation (JRE) 1.6 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.
- 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 16  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 16.
- If you choose the default HTTP connection, click Next, and go to Step 17.

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.

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

Step 21  If you are installing a regional, select Yes to enable BYOD service.

Note  Enabling BYOD service option is available only in Windows and Linux.

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 22  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 Starting and Stopping Servers, on page 34.

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 27.

---

Upgrade Considerations

Cisco Prime Network Registrar 8.3 supports direct upgrades from 7.2 (Linux, Solaris, and Windows), and later, on the same platform.

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 System Requirements, on page 7 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.
Note

• If you are running the Authoritative DNS server, the upgrade process (from pre-8.2 to 8.3) could take a while depending on the number of zones and resource records because of the database changes made to Cisco Prime Network Registrar 8.2.

• There are several significant changes with respect to DHCP failover support when upgrading from a version prior to Cisco Prime Network Registrar 8.2 to Cisco Prime Network Registrar 8.2 or later. For more information, see the Upgrade Considerations for DHCP Failover section in Cisco Prime Network Registrar 8.2 Installation Guide.

• Either cluster of a DHCP failover pair can be upgraded from Cisco Prime Network Registrar 8.2 to Cisco Prime Network Registrar 8.3 and operate successfully with the other cluster that is running Cisco Prime Network Registrar 8.2. You must not run the DHCP failover cross-version for an extended period, and must upgrade both the main and the backup clusters to Cisco Prime Network Registrar 8.3 at the earliest.

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.

DNS Upgrade Considerations

During an upgrade to 8.2/8.3:

• Staged edits will be lost after the upgrade. All the staged edits must be synced to DNS before upgrading.

• RR upgrades are sourced from a valid AUTHZONE.db. If that database is corrupt, missing, or incomplete, the resulting upgrade will miss some or all RRs. The most common situation is upgrading from a shadow backup or database backup, or a dataset that needs to be rebuilt.

• Ensure that the database is fully operational before upgrade.

Upgrading on Windows

To upgrade to Cisco Prime Network Registrar 8.3:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements, on page 7).

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 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 5  Install Cisco Prime Network Registrar 8.3 on the Windows Server 2008 machine. For installation instructions, see Installing Cisco Prime Network Registrar, on page 19. 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 8.3:

Step 1  Ensure that your environment meets the current system requirements (see System Requirements, on page 7).

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 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 4  Install Cisco Prime Network Registrar 8.3. For installation instructions, see Installing and Upgrading Cisco Prime Network Registrar, on page 19.

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}
- 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, on page 37.

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`
- 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.

a) 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 `/`

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.

- Solaris and Linux

Cisco Prime Network Registrar 8.3 Installation Guide
Changetotherootdirectoryofthefilesystem—cd /

Usingthefullyqualifiedpathtothearchivedirectorycontainingthecnr_data_archive.tarfile,extractthearchive. Theseexamplesassumethedefaultarchivelocationprovidedduringinstallation.Ensurethatthepaths
tothe 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.

---

**Moving an Installation to a New Machine**

Before you begin, ensure that the new machine meets the current system requirements (see System
Requirements, on page 7).

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

**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.
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 will get 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.

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
  ```
- Solaris and Linux:
  ```
  # etc/init.d/nwregregion stop
  ```

**Step 2**
Zip up the data directory on the old regional server.

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

**Step 4**
Install Cisco Prime Network Registrar (regional cluster) on the new server. For more information, see **Installing Cisco Prime Network Registrar**, on page 19.

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.

**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**, on page 33.

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

**Step 7**
To list the local clusters:

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

**Step 8**
To synchronize the data as well as the license information:

```
nrcmd-R>cluster <name of local cluster> 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
- 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 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:

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 19. 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 Adding Local Clusters section of Cisco Prime Network Registrar 8.3 CLI Reference Guide.

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

This chapter contains the following sections:

- Starting Cisco Prime Network Registrar, page 33
- Starting and Stopping Servers, page 34
- Starting and Stopping Servers using the Regional Web UI, page 36

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, Installing Cisco Prime Network Registrar, on page 19).

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 8.3 > Network Registrar 8.3 local Web UI (or Network Registrar 8.3 local Web UI (secure) if you enabled secure login).
* On a regional cluster—Choose Start > Programs > Network Registrar 8.3 > Network Registrar 8.3 regional Web UI (or Network Registrar 8.3 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 clusternname -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 8.3 Administrator Guide*. 

---

_Cisco Prime Network Registrar 8.3 Installation 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 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.

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 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
```
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 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 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

**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.

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

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

**Note** You can only stop and start the SNMP server. Reload is not possible for SNMP servers.
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 Cisco Prime Network Registrar 8.3 Administrator 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, on page 34.

- Uninstalling on Windows, page 37
- Uninstalling on Linux, page 38
- Uninstalling on Solaris, page 38
- Running Performance Monitoring Software on Windows, page 39

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 8.3** 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 Linux

To uninstall Cisco Prime Network Registrar on Linux:

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 checkinstall 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.

**Note** When Cisco Prime Network Registrar is installed as nradmin, the uninstall process will reset the ownership of
all the remaining files back to the superuser (root).

Uninstalling on Solaris

To uninstall Cisco Prime Network Registrar on Solaris:

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.
Running Performance Monitoring Software on Windows

On Windows systems if you uninstall Cisco Prime Network Registrar and try to remove the associated data directories while having software installed that integrates with the Windows Performance Monitor, the software might take possession of certain shared libraries. This action prevents you from removing these files from the Cisco Prime Network Registrar folder and the directory itself. To keep this from happening:

1. Stop the service that is associated with the performance monitoring software.
2. Delete the Network Registrar folder.
3. Restart the service.
The Cisco Prime Network Registrar virtual appliance includes all the functionality available in a version of Cisco Prime Network Registrar 8.3 installed on any Linux operating system.

This chapter describes how to install Cisco Prime Network Registrar virtual appliance and includes the following sections:

- **System Requirements**, page 41
- **Installing and Upgrading Cisco Prime Network Registrar Virtual Appliance**, page 42
- **Upgrading the Cisco Prime Network Registrar Virtual Appliance**, page 45
- **Next Steps: Cisco Prime Network Registrar Virtual Appliance**, page 48

## System Requirements

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

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

---

**Note**

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

---

The Cisco Prime Network Registrar virtual appliance is supported on VMware ESXi 5.0 or later systems that are themselves supported ESXi 5.0 or later systems. VMware provides a bootable program which helps you identify whether the hardware on which it is run supports ESXi 5.0 and later. In some cases, the capabilities that are not available from ESXi 5.0 or later are capabilities that are required to run the Cisco Prime Network Registrar virtual appliance. For example, ESXi 5.0 or later will run on some hardware on which it is not officially supported, and will run only 32 bit operating systems on that hardware. The Cisco Prime Network
Registrar virtual appliance consists of a 64 bit Linux operating system running a 32 bit version of the Cisco Prime Network Registrar application. Thus, the 64 bit OS included with the virtual appliance will not run on the ESXi 5.0 or later platform described above. The hardware platforms on which ESXi 5.0 or later runs in this degraded and unsupported mode are becoming less common over time.

Installing and Upgrading Cisco Prime Network Registrar Virtual Appliance

The Cisco Prime Network Registrar virtual appliance is supported for production use on VMware ESXi 5.0 or later and can be accessed or managed using vSphere client of VMware. The Cisco Prime Network Registrar virtual appliance is made available in an Open Virtual Appliance (OVA) package.

The VMware vSphere client can be connected directly to your ESXi installation, or it can be connected to a vCenter server which in turn is connected to your vSphere installation. Connecting through vCenter provides a number of capabilities that connecting directly to ESXi does not. If a vCenter server is available and associated with the ESXi installation, it should be used.

Preparing to Deploy the Cisco Prime Network Registrar Virtual Appliance

In order to deploy the Cisco Prime Network Registrar virtual appliance and configure its network connection, you have to answer several questions. Some of these questions concern the networking environment in which the virtual appliance is being deployed, and some of them concern values which are unique to the particular virtual appliance being deployed.

The questions that are unique to the installation of this particular virtual appliance are listed below. You must decide on answers to these questions before you deploy the virtual appliance.

- A virtual machine name for the deployed virtual appliance.
- A root password for the underlying Linux CentOS operating system.
- An IPv4 address for the virtual appliance.
- A DNS name associated with the IPv4 address of the virtual appliance.
- A username and password for the initial administrator account for the Cisco Prime Network Registrar application.

The questions concerning the networking environment are as follows. The answers to these questions are not unique to the virtual appliance, but are instead values that are determined by the environment in which you will deploy the virtual appliance:

- The IP address or DNS name of the ESXi installation on which you intend to deploy the virtual appliance.
- The IP address or DNS name of any vCenter server associated with the ESXi installation, above.
- The network mask associated with the IP address of the virtual appliance itself.
- The default gateway address for the virtual appliance.
- The IP address of at least one DNS server that can be accessed by the virtual appliance, although it is best if you have the IP address of two DNS servers to provide additional availability.
Any proxy values necessary for the virtual appliance to access the Internet (if you want the virtual appliance to have access to the Internet).

If this is a local cluster installation, you will need to determine the IP address of the Cisco Prime Network Registrar regional cluster to which this local cluster will connect in order to receive its license information. If this is a regional cluster installation, you can ignore this requirement.

Deploying the Regional Cluster OVA or Local Cluster OVA

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

To install the Cisco Prime Network Registrar virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a zip file.

The names are:

- cpnr_8_3_local.ova for the local virtual appliance
- cpnr_8_3_regional.ova for the regional virtual appliance

Download the virtual appliance of your choice. Every Cisco Prime Network Registrar local cluster installation must connect to a Cisco Prime Network Registrar regional cluster in order to receive the necessary license information required to operate. Thus, before you install a Cisco Prime Network Registrar local virtual appliance you must identify the IP address of the regional cluster to which it will connect to receive the license information.

Using vSphere, connect directly to the ESXi installation or the vCenter server, and select the ESXi installation where the OVA is to be deployed.

If you have a vCenter server available, you can connect the ESXi hypervisor to your existing vCenter server and manage it through that vCenter server. Managing all your VMware hypervisors through a common vCenter server provides many benefits.

The screens that you see while managing the ESXi hypervisor with a vSphere client through a vCenter server are different from the screens that you see while connecting the vSphere client directly to the ESXi hypervisor. You can see additional screens if connected through vCenter server. These screens do not actually provide any benefit for the operations in which you will engage to deploy the Cisco Prime Network Registrar virtual appliance. The benefits to using the vCenter server approach come after the initial deployment of the virtual appliance.

To deploy a Regional Cluster OVA or Local Cluster OVA:

Step 1

From vSphere menu, choose File > Deploy OVF Template.

The Deploy OVF Template Source window appears.
To deploy the OVA file, click **Browse** and navigate to select the OVA file (.ova) available on the local machine where vSphere is running.

*Note* You cannot browse for URLs and you must enter the full path to the file.

**Step 3**
Click **Next**.
The OVF Template Details window appears. It displays the product name, the size of the OVA file, and the amount of disk space that needs to be available for the virtual appliance.

**Step 4**
Verify the OVA template details and click **Next**.

**Step 5**
Provide a name to the new virtual appliance and click **Next**.

*Note* You must enter the same name while configuring the virtual appliance, so make sure you remember this name.

The Disk Format window appears.
The Thick provisioned format is selected by default.

**Step 6**
Click **Next** to continue.

*Note* The virtual appliance is only supported when deployed with thick provisioning.

**Step 7**
To map the networks used in this OVA template to the networks in your inventory, select the current destination network and choose the destination network from the Destination Networks drop-down list. Click **Next**.
The Ready to Complete window appears.

**Step 8**
Click **Finish** to begin deployment of the OVF Template.

---

**Booting and Configuring Cisco Prime Network Registrar Virtual Appliance**

To boot and then configure the Cisco Prime Network Registrar virtual appliance:

*Note* You must set the memory and CPUs based on the requirements prior to clicking the power on. Once you start the VM you cannot change the memory or CPU settings until you shut down.

---

**Step 1**
After deploying the Virtual Appliance OVA, select the virtual machine name in vSphere, right-click on it and select **Open Console**.

**Step 2**
Click the **Power on** button on the console and click in the window after clicking the Power on button. During the initial boot of the newly deployed machine, you will be prompted to enter a root (system) password, which is not the Cisco Prime Network Registrar application password.

*Note* This is the root password for the underlying Linux operating system on which the Cisco Prime Network Registrar 8.3 application is installed. You will be asked to enter this password twice. You will need root access to the underlying Linux operating system at various times in the future, so make sure that you remember this password. The boot process can take a while, both before you are asked for a root password, as well as after you enter the root password.
The End User License Agreement window appears on the first boot. Read the license agreement in its entirety, and only if you understand and accept the license terms, enter y (Yes).

Step 3 Log into the server as the root user.

Step 4 To configure the network for the Virtual Appliance, enter the following command: configurenetwork

Step 5 You should configure the following:

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

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

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

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

**Note** The operating system does not restart at this point.

---

**Upgrading the Cisco Prime Network Registrar Virtual Appliance**

This section describes the procedure for upgrading Cisco Prime Network Registrar to Cisco Prime Network Registrar virtual appliance and upgrading the operating system to CentOS 6.5 using the data from an existing virtual appliance.

**Related Topics**

- Upgrading the Cisco Prime Network Registrar Installation to run on a Cisco Prime Network Registrar Virtual Appliance, on page 45
- Upgrading the Cisco Prime Network Registrar Virtual Appliance, on page 47

---

**Upgrading the Cisco Prime Network Registrar Installation to run on a Cisco Prime Network Registrar Virtual Appliance**

This section describes how to upgrade an existing installation of Cisco Prime Network Registrar to become a Cisco Prime Network Registrar virtual appliance.
This procedure upgrades a current version of Cisco Prime Network Registrar running on a Linux operating system to a current version of the Cisco Prime Network Registrar virtual appliance. If you need to move from a different platform, you have to first convert to the Linux platform prior to upgrading to a virtual appliance. If you need to move from a different version of Cisco Prime Network Registrar to the current version of the virtual appliance, you have to first upgrade to the current version of Cisco Prime Network Registrar on an external Linux system before upgrading to the virtual appliance. See Installing and Upgrading Cisco Prime Network Registrar, on page 19.

To do this follow the steps:

**Step 1**  
Install the Cisco Prime Network Registrar virtual appliance.

**Step 2**  
Shut down the Cisco Prime Network Registrar application being upgraded using the following command:  
```bash  
/etc/init.d/nwreglocal stop  
```

**Step 3**  
Copy the file `cnr_prepareforupgrade` from `/opt/nwreg2/{local | regional}/usrbin` from the virtual appliance system to the Cisco Prime Network Registrar installation being upgraded.  
*Note* You have to choose either local or regional from `{local | regional}` based on the upgrade that you are doing, that is, local upgrade or regional upgrade.  

You can do it using `sftp`, for example:

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

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

**Step 5**  
If the version of Cisco Prime Network Registrar which you are moving to the virtual appliance is a version earlier than Cisco Network Registrar 7.2, then perform the following steps:  
*Note* If you are upgrading from 7.2, you do not require the `cnr_mcdexport` kit because 7.2 clusters do not use the MCD DB database technology and you can skip this step.

- a) Download the upgrade preparation kit, `cnr_mcdexport_linux5.tar`, from Cisco.com.
- b) Untar the downloaded archive and run the script `cnr_mcdexport`.

**Step 6**  
Tar the existing `install-path/local/data` directory using the command:  
```bash  
tar cvf tarfile.tar data  
```
Step 7 Copy the tar file created to the new virtual appliance.

Step 8 Shut down Cisco Prime Network Registrar on the new virtual appliance using the command:

/etc/init.d/nwreglocal stop

Step 9 Rename the existing database to .orig using the command:

mv /var/nwreg2/local/data /var/nwreg2/local/data.orig

Step 10 Untar the latest database, transferred in Step 4, using tar xvf tarfile.tar.

Step 11 Reboot the Cisco Prime Network Registrar virtual appliance using VMware vSphere.

Upgrading the Cisco Prime Network Registrar Virtual Appliance

To upgrade an existing Cisco Network Registrar virtual appliance, install a new virtual appliance which has the new operating system version on it, and then move the data and configuration from the existing virtual appliance to the new virtual appliance.

To do this follow the steps:

Step 1 Deploy the latest Cisco Prime Network Registrar virtual appliance (with the new OS version) on the ESXi machine where the existing Cisco Prime Network Registrar virtual appliance resides.

Step 2 Shut down Cisco Prime Network Registrar on the existing virtual appliance. Use either /etc/init.d/nwreglocal stop or /etc/init.d/nwregregion stop to stop the application, depending on whether you are operating on a local or regional cluster.

Step 3 Run cnr_prepareforupgrade on the existing appliance.

Step 4 Shut down the virtual machine of the existing appliance.

Step 5 The next few steps will guide you through the process of copying the data disk (which contains the Network Registrar databases) from the existing virtual appliance to the new virtual appliance. You will use vSphere to make the copy. Ensure that you have shut down both virtual appliances before copying.

Step 6 Select the ESXi platform in vSphere. It is not a particular virtual machine that you have to select, but rather the container in which these virtual machines appear.

Step 7 Select the Configuration tab and click the Storage link under Hardware area. You can now see the datastores in the right hand window. Determine the datastore in which the files for your virtual machines reside.

Note You should have selected the datastore when you deployed the virtual machines, if you have more than one datastore. If you have only one, no selection was required at the time of deployment.

Step 8 Right-click the datastore that contains the existing virtual machine. Select Browse Datastore... A Datastore Browser is displayed which shows you the file structure of your ESXi datastore.

Note The directories which you see in the Datastore Browser use the names given to the virtual appliances when they were first deployed, which may or may not be the current names of the virtual appliances. If you changed the name of a virtual appliance after it was deployed, that name change will not be reflected in the file structure in the datastore.

Step 9 Select the folder for the existing virtual appliance from the tree structure displayed at the left pane of the Database Browser window. You can see the files which are associated with the existing virtual appliance in the right pane of the
Database Browser window. Find the existing data disk from the list of files displayed in the right pane. The name of the file of the existing data disk ends with _1.vmdk and is the largest file in the virtual machine.

**Step 10** Right-click the file you found in **Step 9** and select **Copy**.

**Step 11** Select the folder of the new virtual appliance in the left pane of the Datastore Browser window. You can see the files currently associated with the new virtual appliance in the right pane of the window. Right-click in the right pane, and not on a particular file, and select **Paste**. Since the file you are copying may be rather large, you can see a progress popup which shows the copy progress. Close the Datastore Browser window when the copy is complete.

**Step 12** Select the new virtual appliance in the left pane of the vSphere client window and select **Edit virtual machine settings**. The Virtual Machine Properties window is displayed. The Hardware tab is selected by default. If it is not, then select it.

**Step 13** Select Hard disk 2 and click **Remove**. Accept the default **Removal Option** of **Remove from virtual machine** which does not delete the virtual disk file itself, but rather just removes it from the virtual machine.

**Step 14** Select the new virtual appliance again in the left pane of the vSphere client window and select **Edit virtual machine settings** again. Click **Add** in the Virtual Machine Properties window to add the hard disk you copied from the existing virtual machine.

The **Add Hardware** window is displayed.

**Step 15** Choose **Hard Disk** from the list of device types and click **Next**.

**Step 16** Check the **Use an existing virtual disk** check box to allow you to use the virtual disk that you just copied from the existing virtual appliance and click **Next**.

**Step 17** Click **Browse** to locate the disk file path. Select the datastore where you placed the copy of the virtual disk in the Browse Datastore window. Click **Open** and you can see the list of virtual machines on this datastore. Select the directory of the new virtual appliance from the list and click **Open**. You can see the list of virtual disks in the directory for that virtual machine. Probably two of them will be named the same as the new virtual machine, and one of them will be named based on the existing virtual machine. Select the one named for the existing virtual machine and click **OK**. Click **Next**.

**Step 18** Click **Finish** again to accept the **Advanced Options** unchanged.

**Step 19** Click **Next** again to accept the **Advanced Options** unchanged.

This takes you back to the Virtual Machine Properties window, and the list of hardware in the virtual machine now has the **New Hard Disk (adding)** in the list. Click **OK** to finish.

You can now start the new virtual machine. It will have the entire data disk of the existing virtual machine.

**Note** The virtual machine with the upgraded operating system will pause during the boot process and instruct you to upgrade the Cisco Prime Network Registrar database to match the database version of the Cisco Prime Network Registrar application that resides on the new virtual machine.

**Step 20** Run the file and press return on the console to complete the boot process.

**Step 21** Log in as root and run the displayed command.

After boot completion, you should see your existing configuration running with the new version of Cisco Prime Network Registrar on the new virtual machine.

---

**Next Steps: Cisco Prime Network Registrar Virtual Appliance**

**Configuring Cisco Prime Network Registrar**

To access the Cisco Prime Network Registrar Application use the following URLs:
The URLs to manage Cisco Prime Network Registrar are the URLs displayed on the Console screen under **manage the Cisco Prime Network Registrar 8.3 application**.

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

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

To manage the Cisco Prime Network Registrar 8.3 application:

---

**Step 1**
Browse to any URL displayed under **manage the Cisco Prime Network Registrar 8.3 application** (either secure or standard access).

*Note* If you are using secure access for login, choose **I understand the risks** when you get the warning 'This Connection is Untrusted' and click **Add Exception** and **Confirm Security Exception** for this page.

The Cisco Prime Network Registrar New Product Installation page is displayed.

**Step 2**
Enter the Name and Password for the superuser administrator in the New Product Installation > Add Superuser Administrator page.

*Note* This account is different from the root password which you entered earlier. This is an account in the Cisco Prime Network Registrar product for the most privileged Cisco Prime Network Registrar administrator, who will have permission to create additional administrator accounts in the Cisco Prime Network Registrar product.

**Step 3**
Enter the IP address of a CCM regional cluster and the SCP port in use on that cluster. There is no default for the port number, but port number 1244 is often used for the regional cluster. You must register with a regional cluster in order to operate the product.

**Step 4**
Check the services which you wish to use on this virtual appliance.

*Note* You must check the boxes for the services you intend to use on this virtual appliance, or you will not be able to see the user interface for these services in the Web UI. You may select DHCP and select either DNS or CDNS. It is possible to run both DNS and CDNS servers on the same machine at the same time in export mode configuration, but we do not recommend that.

**Step 5**
Click **Register**.

The Configuration Summary page is displayed. It will not have any DHCP or DNS boxes checked, because you do not have any configuration for any of these services yet. If you checked DHCP on the previous page, you can see **DHCP services configured for start on reboot**, and similarly for DNS.

You can now proceed to configure DHCP, DNS, or CDNS servers on this virtual machine.
Configuring Cisco Prime Network Registrar with the CLI on Virtual Appliance

The Cisco Prime Network Registrar command line interpreter (CLI) can be used to configure the virtual appliance in two ways:

- You can use the nrcmd CLI on the virtual appliance directly by first using SSH to connect into the underlying Linux operating system on the virtual appliance. You can use any username and password which you have created on the virtual appliance for the SSH login, and you must use an administrator username and password for the Cisco Prime Network Registrar to use the nrcmd CLI to configure Cisco Prime Network Registrar.

  **Note**  As distributed, there is only one valid user for the Linux operating system—root. While you can login as root to use the Cisco Prime Network Registrar CLI, you might want to add additional users to the system. Use the useradd program to add additional users. You can type `man useradd` for more information on how to add additional users.

- Alternatively, you can use the nrcmd CLI on some other system in the network to configure and manage Cisco Prime Network Registrar on the virtual appliance the same way that you would use it to manage any remote installation of Cisco Prime Network Registrar. This requires installing Cisco Prime Network Registrar (typically only the client-only installation) on the other system.

Configuring the Virtual Appliance to Automatically Power Up

You can configure the ESXi hypervisor to automatically power up the Cisco Prime Network Registrar virtual appliance when power is restored to the ESXi hypervisor layer.

  **Note**  You must manually power up the virtual machine.

To configure automatic power up:

**Step 1**  In the vSphere client, select the ESXi machine to which you are connected. It is not a specific virtual machine that you have to select but the ESXi hypervisor on which they reside.

**Step 2**  Select the **Configuration** tab.

**Step 3**  Click the **Virtual Machine Startup/Shutdown** link under the **Software** area. You should see the virtual machine in the list shown in window.

**Step 4**  Click the **Properties...** link present at the top right corner of the page. If you do not see that, resize the window until you do.

The Virtual Machine Startup and Shutdown page is displayed.

**Step 5**  Check the ** Allow virtual machines to start and stop automatically with the system** check box.

**Step 6**  Select the virtual machine running the Cisco Prime Network Registrar virtual appliance and use the **Move Up** button on the right to move it up into the group labelled **Automatic Startup**

**Step 7**  Click **OK**
This ensures that whenever power is restored to the ESXi hypervisor the Cisco Prime Network Registrar appliance powers up automatically.

Managing the Cisco Prime Network Registrar Virtual Appliance

You can manage the underlying Linux operating system, which is based on CentOS 6.5, by logging in as the root user. You may use SSH to log into the virtual appliance with the username root and the root password you specified when you first booted the virtual appliance.

You will probably want to create additional users on the Linux system so that people can access the Linux system with a username other than root.

The Linux system which is included on the virtual appliance is stripped down to a considerable degree and thus does not include things that are not required to run or manage the Cisco Prime Network Registrar application, such as a window system manager and its associated GUI user interface. However, all the tools necessary to support and manage the Cisco Prime Network Registrar application are included on the Linux operating system used inside of the virtual appliance.

You may also want to take additional steps to secure the SSH connection. For instance, configuring it to prevent logging on as root, and requiring a user to su to gain root privileges after logging on as another user.

You may wish to perform other configuration changes on the underlying Linux operating system in order to lock it down in ways appropriate to your environment.

Note

Cisco Prime Network Registrar customers are solely responsible for keeping their OS up to date regarding patches that they desire to apply and Cisco is not responsible for the same.
Performing a Silent Installation

This appendix contains the following sections:

- Performing a Silent Installation, page 53

Performing a Silent Installation

This appendix describes how to perform a silent installation, upgrade, or uninstallation of the Cisco Prime Network Registrar product. A silent installation or upgrade allows for unattended product installations based on the configuration values that are provided at the time that a silent installation response file was created.

⚠️ Caution

Unpredictable results can occur if you try to use a silent-response file that does not contain the correct settings for the system undergoing the silent installation.

To generate or create a silent-response file:

---

**Step 1**

For each silent installation or upgrade, use these commands to create a separate response file:

- **Windows:**

  ```
  setup.exe -r
  ```

  Complete the installation or upgrade steps as you normally would. This command installs or upgrades Cisco Prime Network Registrar according to the parameters that you specified.

  **Note**

  If Cisco Prime Network Registrar is already installed, `setup.exe` uninstalls the existing version and if Cisco Prime Network Registrar is not installed, then it does the installation.

  It also generates the setup.iss silent-response file based on these parameters. Look for this file in the Windows installation directory, such as C:\WINDOWS. Each time you use the command, the file is overwritten.

  We recommend that you rename or relocate this file before running the silent process in **Step 2**. Rename the file to something distinguishable, such as local-nr-https-install, and relocate it to a temporary folder.

- **Solaris:**
pkgask -d install-path -r response-file nwreg2

Complete the installation or upgrade steps as you normally would. This command installs or upgrades Cisco Prime Network Registrar according to the parameters that you specified.

**Note**  Complete the installation or upgrade steps as you normally would. This action does not actually install or upgrade Cisco Prime Network Registrar, but simply generates a silent-response file by the specified name that includes the installation or upgrade parameters that you want to replicate for additional installations or upgrades. We recommend that you name the file something distinguishable, such as local-nr-upgrade or regional-nr-https-install.

- **Linux:**

  Create a text silent-response file that includes the entries listed in the table below.

### Table 3: Silent-Response File Entries for Linux

<table>
<thead>
<tr>
<th>Silent-Response File Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKUPDIR=</td>
<td>Path where to store the current Cisco Prime Network Registrar installation files, but only if PERFORM_BACKUP=y</td>
</tr>
<tr>
<td>CCM_LOCAL_SERVICES=</td>
<td>Services (dhcp, dns or cdns) to enable</td>
</tr>
<tr>
<td>CCM_PORT=</td>
<td>Central Configuration Management (CCM) port; default value is:</td>
</tr>
<tr>
<td></td>
<td>• <strong>1234</strong> if CNR_CCM_MODE=local</td>
</tr>
<tr>
<td></td>
<td>• <strong>1244</strong> if CNR_CCM_MODE=regional</td>
</tr>
<tr>
<td>CCM_RGNL_IP_ADDR=</td>
<td>IP address of the regional server</td>
</tr>
<tr>
<td>CCM_RGNL_SCP_PORT=</td>
<td>SCP port number on the regional server</td>
</tr>
<tr>
<td>CNR_ADMIN=</td>
<td>Superuser name. To skip configuring the superuser name, value should be CNR_ADMIN= unset.</td>
</tr>
<tr>
<td>NRADMIN=</td>
<td>Non-root user. To install Cisco Prime Network Registrar as non-root user, value must be NRADMIN=y.</td>
</tr>
<tr>
<td>CNR_PASSWORD=</td>
<td>Superuser password. To skip configuring the superuser password, value should be CNR_PASSWORD= unset.</td>
</tr>
<tr>
<td>CNR_CCM_MODE=</td>
<td>CCM mode; set to local or regional.</td>
</tr>
<tr>
<td>CNR_CCM_TYPE=</td>
<td>Reserved for GSS installation. Introduced in Cisco Prime Network Registrar 7.0; always set to cnr.</td>
</tr>
<tr>
<td>CNR_EXISTS=</td>
<td>If set to y (recommended), tries to kill any open CLI connections when installing or upgrading; otherwise, basically deprecated.</td>
</tr>
<tr>
<td>Silent-Response File Entry</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CNR_LICENSE_FILE=</td>
<td>For Cisco Prime Network Registrar 7.x and later only, the fully qualified path to the license file. Set CNR_LICENSE_FILE = unset if</td>
</tr>
<tr>
<td></td>
<td>CNR_CCM_MODE=local for Cisco Prime Network Registrar 8.x.</td>
</tr>
<tr>
<td>CNR_SECURITY_MODE=</td>
<td>Security mode configuration:</td>
</tr>
<tr>
<td></td>
<td>• required - Fail if the connection cannot be secured.</td>
</tr>
<tr>
<td></td>
<td>• optional - Allow fallback to insecure connection.</td>
</tr>
<tr>
<td></td>
<td>• disabled - Do not load security modules at startup.</td>
</tr>
<tr>
<td>DATADIR=</td>
<td>Fully qualified path to the data directory</td>
</tr>
<tr>
<td>JAVADIR=</td>
<td>Fully qualified path to the Java installation (JRE 1.6 or later).</td>
</tr>
<tr>
<td>KEYSTORE_FILE=</td>
<td>If USE_HTTPS=y, the fully qualified path to the keystore file.</td>
</tr>
<tr>
<td>KEYSTORE_PASSWORD=</td>
<td>If USE_HTTPS=y, the password used when generating the keystore file.</td>
</tr>
<tr>
<td>LOGDIR=</td>
<td>Fully qualified path to the log file directory.</td>
</tr>
<tr>
<td>PERFORM_BACKUP=</td>
<td>Specifies whether or not to back up the current installation files, if present. Can be set to y even on a clean installation (see also BACKUPDIR).</td>
</tr>
<tr>
<td>ROOTDIR=</td>
<td>Fully qualified installation path for the product files; contains bin, classes, cnrwebui, conf, docs, examples, extensions, lib, misc, schema, tomcat, and usrbin subdirectories</td>
</tr>
<tr>
<td>START_SERVERS=</td>
<td>Must be set to y for a full installation (with protocol servers) to assure the installation or upgrade is completed; it also results in the Cisco Prime Network Registrar product being started after the install/upgrade. For a client-only installation, must be set to n.</td>
</tr>
<tr>
<td>TEMPDIR=</td>
<td>Fully qualified path to the temp directory.</td>
</tr>
<tr>
<td>USE_HTTP=</td>
<td>Sets whether or not the web UI server listens for HTTP connections; one or both of USE_HTTP or USE_HTTPS must be set to y.</td>
</tr>
</tbody>
</table>
**Silent-Response File Entry** | **Description**
--- | ---
USE_HTTPS= | Sets whether or not the web UI server listens for HTTPS connections; one or both of USE_HTTP or USEHTTPS must be set to y (see also KEYSTORE_FILE and KEYSTORE_PASSWORD).

WEBUI_PORT= | Port number that the web UI uses for HTTP traffic; default value is:

- **8080** if CNR_CCM_MODE=local
- **8090** if CNR_CCM_MODE=regional

WEBUI_SEC_PORT= | Port number that the web UI uses for HTTPS traffic; default value is:

- **8443** if CNR_CCM_MODE=local
- **8453** if CNR_CCM_MODE=regional

CNR_BYOD_ENABLE= | Set to y or n to enable or disable the BYOD services. Enabling BYOD service option is available only in Windows and Linux.

---

**Step 2**

Use these commands to invoke the silent installation or upgrade for each instance:

- **Windows:**
  
  `setup.exe -s -f1 path+response-file`

  **Note** The silent installation fails if you do not specify the `-f1` argument with a fully qualified path to the response file, unless the response file is located in the i386 directory and setup.exe is run from that directory.

- **Solaris:**
  
  `pkgadd -a pkgdir/nwreg2/install/cnradmin -d pkgdir -r response-file nwreg2`

- **Linux:**
  
  `install_cnr -r response-file`

**Step 3**

If you want to uninstall the product:

- **Windows**—Generate an uninstallation response file and execute:
  
  `setup.exe -s -f1 uninstall_response_file`

- **Solaris**—Invoke the silent uninstallation:
  
  `pkgrm -a pkgdir/nwreg2/install/cnradmin -n nwreg2`

- **Linux**—Invoke the silent uninstallation (this command is noninteractive except during an error):
  
  `uninstall_cnr`
Lab Evaluation Installations

This appendix contains the following sections:

- Lab Evaluation Installations, page 59
- Installing Cisco Prime Network Registrar in a Lab, page 60
- Testing the Lab Installation, page 60
- Uninstalling in a Lab Environment, page 60

Lab Evaluation Installations

This appendix describes how to install, upgrade, and uninstall Cisco Prime Network Registrar regional and local clusters on a single Solaris or Linux machine to support smaller test configurations for evaluation purposes.

**Note**

You cannot install both the local and the regional cluster on a single Windows machine.

**Caution**

Installing the regional and local cluster on a single machine is intended only for lab evaluations, and should not be chosen for production environments. The aggregated regional cluster databases are expected to be too large to be reasonably located with a local server that is also running DNS or DHCP services. Running out of free disk space causes these servers to fail.
Installing Cisco Prime Network Registrar in a Lab

To install Cisco Prime Network Registrar on a single machine for evaluation purposes:

Step 1 Check whether the machine has enough disk space to accommodate two separate installations of Cisco Prime Network Registrar.

Step 2 Install or upgrade the local cluster on the Solaris or Linux machine, according to the procedures in Installing Cisco Prime Network Registrar, on page 19. Specify the Local cluster installation.

Step 3 Install or upgrade the regional cluster on the same machine, according to the same procedures. Specify the Regional cluster installation.

Testing the Lab Installation

To test the installation:

Step 1 Start and log in to the web UI for the local cluster, using the URL appropriate to the port number. By default, the local port numbers are **8080** for HTTP connections and **8443** for HTTPS (secure) connections.

Step 2 Add DNS zones and DHCP scopes, templates, client-classes, or virtual private networks (VPNs) as a test to pull data to the regional cluster.

Step 3 Start and log into the web UI for the regional cluster, using the URL appropriate to the port number. By default, the regional port numbers are **8090** for HTTP connections and **8453** for HTTPS (secure) connections.

Step 4 Test the regional cluster for single sign-on connectivity to the local cluster. Try to pull DNS zone distributions, DHCP scopes, templates, client-classes, or VPNs from the local cluster to the regional replica database.

Uninstalling in a Lab Environment

If you need to uninstall Cisco Prime Network Registrar, follow the procedure in Uninstalling on Linux, on page 38 or Uninstalling on Solaris, on page 38.

No option exists to uninstall only the regional or local cluster in a dual-mode installation environment.
Installing the Cisco Prime Network Registrar SDK

This section documents how to install the Cisco Prime Network Registrar SDK on the Linux, Solaris, and Windows platforms. Before installing the SDK, ensure that you have Java Runtime Environment (JRE) 1.6 or later, or the equivalent Java Development Kit (JDK), installed on your system. The Cisco Prime Network Registrar SDK is a separate product and is sold separately.

This appendix contains the following sections:

- Installing on Linux or Solaris, page 61
- Installing on Windows, page 62
- Testing Your Installation, page 62
- Compatibility Considerations, page 62

Installing on Linux or Solaris

To install the Cisco Prime Network Registrar SDK on a Linux or Solaris platform:

**Step 1**

Extract the contents of the distribution .tar file.

a) Create the SDK directory:

```
% mkdir /cnr-sdk
```

b) Change to the directory that you just created and extract the .tar file contents:

```
% cd /cnr-sdk

% tar xvf sdk_tar_file_location/cnrsdk.tar
```

**Step 2**

Export your LD_LIBRARY_PATH and CLASSPATH environment variable:

```
% export LD_LIBRARY_PATH=/cnr-sdk/lib

% export CLASSPATH=/cnr-sdk/classes/cnrsdk.jar:
```
Installing on Windows

To install the Cisco Prime Network Registrar SDK on a Windows platform:

---

**Step 1**  
Extract the contents of the distribution .tar file.  
a) Create the SDK directory:  
> md c:\cnr-sdk  
b) Change to the directory that you just created and extract the .tar file contents:  
> c:  
> cd \cnr-sdk  
> tar xvf sdk_tar_file_location\cnrsdk.tar  
You may optionally use Winzip to extract cnrsdk.tar to the C:\cnr-sdk directory.

**Step 2**  
Set your PATH and CLASSPATH variables:  
> set PATH=%PATH%;c:\cnr-sdk\lib  
> set CLASSPATH=c:\cnr-sdk\classes\cnrsdk.jar;.

---

**Testing Your Installation**

On Linux or Solaris, the following test program verifies that you have set your PATH or LD_LIBRARY_PATH correctly:

% java -jar /cnr-sdk/classes/cnrsdk.jar  
On Windows, the following test program verifies that you have set your CLASSPATH correctly:

> java -jar c:\cnr-sdk\classes\cnrsdk.jar

---

**Compatibility Considerations**

For Java SDK client code developed with an earlier version of the SDK, you can simply recompile most code with the latest JAR file to connect to an upgraded server.  

But in cases where the client code for versions before 7.1 directly manipulates reservation lists in scopes or prefixes, changes are required. These changes are required because the embedded reservation lists in both scopes and prefixes are no longer used. Beginning with version 7.1, individual reservations are stored separately and reference the parent scope or prefix by name.  

The new design provides the following benefits:  

- Reservation edits (add/modify/delete) do not require a scope or prefix edit.  
- Reservations can be indexed directly to allow quick search and retrieval.  
- Edits to scopes or prefixes with a large number of reservations no longer result in large scope or prefix change entry logs.
No changes are required for client code that adds or removes reservations using the addReservation or removeReservation methods. However, these methods are now deprecated because the edit functionality is replaced and extended by the general addObject, modifyObject, removeObject, addObjectList, modifyObjectList, and removeObjectList methods.
Enhancing Security for Web UI

This appendix contains the following sections:

- Enhancing Security for Web UI, page 65

Enhancing Security for Web UI

When connected through the Secured Socket Layer (SSL) protocol using HTTPS, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These ciphers usually include weak cipher session keys and can affect system security. Therefore, you may want to adjust the ciphers to disable the use of weak ciphers in the web UI.

To adjust the ciphers:

Step 1
Open the `server.xml` file in the install-path/tomcat/conf folder in your Cisco Prime Network Registrar installation folder.

Step 2
Add a ciphers statement to the HTTPS connector statement and list down the allowed ciphers as described in the following example:

```
<Connector port="8443"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    maxHttpHeaderSize="8192"
    enableLookups="false"
    disableUploadTimeout="true"
    acceptCount="100" scheme="https" secure="true"
    clientAuth="false"
>
    <!--ciphers statement goes here-->
</Connector>
```

Note: The values for `port`, `keystoreFile`, and `keystorePass` must match the values that you have configured in your system.
The ciphers attribute can carry a comma-separated list of encryption ciphers that this socket is allowed to use. By default, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These contain the weak export-grade ciphers in the list of available ciphers. This results in the web UI supporting weak cipher session keys.

**Note** The ciphers are specified using the Java Secure Socket Extension (JSSE) cipher naming convention.

**Step 3** Restart Cisco Prime Network Registrar for the changes to take effect.
Troubleshooting DHCP Server Out of Memory Aborts on Linux

Some customers have experienced the DHCP server to abort itself, generating a core file with DHCP server log messages indicating that the process is aborting as it was unable to create a thread. Prior to the server abort, memory usage may be seen to increase significantly (100 MB or more) after a reload. This occurs on Linux, typically impacting users who have fairly large configurations (where the DHCP server uses 2 GB or more of memory), and occurs on a reload (after a few to hundreds of reloads). For more information, refer CSCus91865.

When the server aborts either due to the inability to create a thread or loss of memory, the cnrservagt automatically starts a new DHCP server process. Thus, the impact to most users is:

- Slightly longer reloads.
- Large core files (3.5 GB to just over 4 GB) in the /opt/nwreg2/local directory must be periodically removed to avoid running out of disk space. Whether these core files are created and how, depends on the system settings (see man pages for core(5)).
- Server will take a long time while reloading prior to exiting. The server is found to be using 100% CPU on one processor and spending most of its time in memory allocation system calls.

In working with Red Hat on this issue, it was determined to result from the behavior of the glibc MALLOC library, and the pattern of memory allocations and thread usage within the DHCP server - the two do not play nicely.

The MALLOC library uses the concept of ARENAS (memory pools) to improve performance and reduce the need for locks and reducing lock contention. However, at times the ARENAS are reused differently than they were used earlier in the life of the process and memory held by an ARENA is thus not necessarily reused or freed to the system. Thus this can thus result in many ARENAS holding large amounts of memory - increasing the memory required for the DHCP server process. Eventually, most of the memory space is in use (or what is still available is fragmented), and when the server requests the system to create a thread, the system is unable to obtain the necessary contiguous mappable space for the thread - and hence the thread creation fails and the server considers this "fatal" and (by design) aborts itself.

This is known to occur on Red Hat Enterprise Linux (RHEL)/CentOS 5.x with Network Registrar 8.2 and earlier. It may also occur on RHEL/CentOS 6.x with Network Registrar 8.3.

There are several workarounds possible, as described in the following sections. The table below indicates the workaround options:
Table 4: The table below indicates the workaround options:

<table>
<thead>
<tr>
<th>Network Registrar Version</th>
<th>RHEL / CentOS Version</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.3.4 or earlier</td>
<td>5.x</td>
<td>See Workaround for other Versions</td>
</tr>
<tr>
<td></td>
<td>6.x</td>
<td>No action needed.</td>
</tr>
<tr>
<td>7.2.3.5 or later 7.2</td>
<td>5.x</td>
<td>See Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions</td>
</tr>
<tr>
<td></td>
<td>6.x</td>
<td>No action needed.</td>
</tr>
<tr>
<td>8.0 to 8.1.3.2</td>
<td>5.x</td>
<td>See Workaround for other Versions</td>
</tr>
<tr>
<td></td>
<td>6.x</td>
<td>No action needed.</td>
</tr>
<tr>
<td>8.1.3.3 or later 8.1</td>
<td>5.x</td>
<td>See Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions</td>
</tr>
<tr>
<td></td>
<td>6.x</td>
<td>No action needed.</td>
</tr>
<tr>
<td>8.2 to 8.2.2.1</td>
<td>5.x</td>
<td>See Workaround for other Versions</td>
</tr>
<tr>
<td></td>
<td>6.x</td>
<td>No action needed.</td>
</tr>
<tr>
<td>8.2.2.2 or later 8.2</td>
<td>5.x</td>
<td>See Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions</td>
</tr>
<tr>
<td></td>
<td>6.x</td>
<td>No action needed.</td>
</tr>
<tr>
<td>8.3 or later</td>
<td>5.x</td>
<td>See Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions, or Alternative Workaround for Cisco Prime Network Registrar 8.3</td>
</tr>
<tr>
<td>-------------</td>
<td>-----</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>6.x</td>
<td>See Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions, Alternative Workaround for Cisco Prime Network Registrar 8.3, or Avoiding the Issue on Cisco Prime Network Registrar 8.3 and later on RHEL /CentOS 6.x</td>
</tr>
</tbody>
</table>

- Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions, page 69
- Alternative Workaround for Cisco Prime Network Registrar 8.3, page 70
- Workaround for other Versions, page 71
- Avoiding the Issue on Cisco Prime Network Registrar 8.3 and later on RHEL /CentOS 6.x, page 72

**Recommended Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions**

The recommended workaround, available for 7.2.3.5 (and later), 8.1.3.3 (and later), 8.2.2.2 (and later), and 8.3 (and later), is to issue the following Network Registrar CLI (nrcmd) commands on the DHCP cluster:

```bash
session set visibility=3
server-agent dhcp
server-agent dhcp set environment-list=MALLOC_PER_THREAD=1,MALLOC_ARENA_MAX=1
exit
```
**Important**

- This workaround is not available in earlier releases because of CSCu77653 (the cnrservagt was not properly setting the environment variables on the target process).
- You must restart Cisco Prime Network Registrar for these environment variables to take effect. Use /etc/init.d/nwreglocal stop followed by /etc/init.d/nwreglocal start.
- Confirm that the "environment-list" attribute, displayed in the server-agent dhcp command is unset. If it is not unset, you will have to alter the `server-agent dhcp set environment-list` command to include the current environment variables. Once set, these environment variables are preserved during upgrades.
- Run glibc-2.5-38 or later versions, as environment variables are not available in earlier versions of the glibc libraries.
- If using RHEL/CentOS 6.x, you do not need to set the MALLOC_PER_THREAD as this environment variable is not available.

---

**Undo Workaround for Cisco Prime Network Registrar 8.3 and Other Recent Versions**

To undone the workaround for Cisco Prime Network Registrar 8.3 and other versions, use the following nrcmd commands (assuming that there are no other environment variables that have been set):

```nrcmd
session set visibility=3
server-agent dhcp unset environment-list
exit
```

**Alternative Workaround for Cisco Prime Network Registrar 8.3**

An alternative workaround available in 8.3 (and later), is to use a new cnrservagt feature - `exit-on-stop`. When you enable this feature, it will cause the DHCP server to exit after stopping. On server restart, a new process will be initiated. A reload is a stop followed by a start, so this too will result in the process exiting before a restart. This will avoid the memory issues since it is the reload within the same process that seems to trigger the issue. For more information, see CSCur19708.

However, this alternative workaround is not recommended for 8.3 (and later) since the DHCP server normally retains some information across reloads (statistics and scope utilization history) and retention of the information is not possible if the server process exits. Also, the process PID will change at each reload (rather than just at a Network Registrar restart). This may impact monitoring of tools.

To use this workaround, you can issue the following nrcmd commands:

```nrcmd
session set visibility=3
server-agent dhcp enable exit-on-stop
exit
```

You must then restart Network Registrar for this change to take effect. Once set, these settings are preserved during upgrades.
Undo Alternative Workaround for Cisco Prime Network Registrar 8.3

To undo the alternative workaround for Cisco Prime Network Registrar 8.3, use the following nrcmd commands:

```
session set visibility=3
server-agent dhcp unset exit-on-stop
exit
```

Workaround for other Versions

For all Network Registrar versions, the following workaround are used:

---

**Step 1**
Create the following dhcp.script file in the Network Registrar bin directory (typically /opt/nwreg2/local/bin):

```
#!/bin/csh
setenv MALLOC_PER_THREAD 1
setenv MALLOC_ARENA_MAX 1
/opt/nwreg2/local/bin/dhcp $argv
```

**Step 2**
Ensure that this dhcp.script file is root readable and executable. To make the script executable and readable use:

```
chmod +rx /opt/nwreg2/local/bin/dhcp.script
```

**Note**
Ensure that the dhcp.script file is not writable by anyone but root.

**Step 3**
Start Cisco Prime Network Registrar if it is not already running:

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

**Step 4**
Issue the following nrcmd commands:

```
session set visibility=3
server-agent dhcp set load-path=dhcp.script
exit
```

**Step 5**
Stop Cisco Prime Network Registrar:

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

**Step 6**
Start Cisco Prime Network Registrar:

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

**Important**
- Since this workaround results in the actual DHCP server process running as a separate process (different PID), Network Registrar reports on the shell script process as the DHCP server's PID and not on the actual DHCP server process itself. Therefore, using the web UI dashboard to monitor memory usage for the DHCP server is no longer possible.
- Once set, this change will be preserved during upgrades. Depending on future upgrades, it may be necessary to undo the above steps.
- Run glibc-2.5-38 or later versions only, as environment variables are not available in earlier versions of the glibc libraries.
- If using RHEL/CentOS 6.x, you do not need to set the MALLOC_PER_THREAD as this environment variable is not available.
Undo Workaround for other Versions

To undo the settings, issue the following commands:

**Step 1**  
Start Cisco Prime Network Registrar if not running: `/etc/init.d/nwreglocal start`.

**Step 2**  
Issue the following nrcmd commands:
```
session set visibility=3  
server-agent dhcp set load-path=dhcp  
exit
```

**Step 3**  
Stop Cisco Prime Network Registrar: `/etc/init.d/nwreglocal stop`.

**Step 4**  
Delete the script file (if desired): `rm /opt/nwreg2/local/bin/dhcp.script`.

**Step 5**  
Start Cisco Prime Network Registrar (if desired): `/etc/init.d/nwreglocal start`.

Avoiding the Issue on Cisco Prime Network Registrar 8.3 and later on RHEL /CentOS 6.x

It appears that this issue can be avoided, without the above mentioned workarounds, when using Cisco Prime Network Registrar 8.3 (and later) on RHEL/CentOS 6.x by disabling parallel lease loading (described below).

Loading the leases in parallel decreases the time needed to load DHCPv4 and DHCPv6 leases when the server is starting. But, because an additional thread is used, this seems to expose the issue on RHEL/CentOS 6.x. For more details, see CSCup67709.

To disable parallel lease loading, issue the following nrcmd commands:
```
session set visibility=3  
dhcp set server-flags=+serial-lease-loading  
exit
```

On the next reload, the DHCP server will not use parallel lease loading and revert to the pre-8.3 behavior of loading the leases serially.

This can be undone by using the following nrcmd commands:
```
session set visibility=3  
dhcp set server-flags=-serial-lease-loading  
exit
```
# Index

## A
- Add License page 34
  - web UI; Web UI: Add License page 34
- archive directories 23
- archiving 23

## C
- certificate file 20
  - importing; keytool utility 20
- ciphers 65
  - adjusting 65
- CLI 2, 7, 33, 34
  - license set key command 34
  - requirements 7
  - starting 33
- client-only installation 24
- clusters 21
  - local 21
  - modes 21
  - regional 21
- cnr_status utility 25, 35
- command line interface 2
- connection type 24

## D
- database status 23
- debug_install script 31
- DHCP servers 2
- disk space requirements 8
- DNS servers 2

## E
- error logging 16, 39

## G
- gtar utility 21
- gzip utility 21

## H
- HTTP connection 24
- HTTPS connection 24

## I
- install_cnr utility 21, 56
- install_cnr_log file 31
- installation 1, 9, 13, 19, 20, 21, 22, 24, 25, 31, 35, 53, 59
  - CD 20
  - cluster mode 21
  - connection type 24
  - directory 22
  - Java directory 24
  - JAVA_HOME setting 19
  - JRE/JDK requirements 19
  - lab evaluation 59
  - license keys 13
  - log files 31
    - install_cnr_log 31
    - lease_upgrade_log 31
  - modes 9
    - new 9
  - upgrade with data migration 9
  - upgrade without data migration 9
- network distribution 20
  - overview 1
  - process 19
  - processing messages 25
  - secure login 19
  - silent 53
  - system privileges 19
  - troubleshooting 31
  - types 24
installation (continued)
Web UI port 24
installation:checklist 13
installation;upgrade:checklist 13

J
Java 7, 24
directory 24
requirements 7
Java Development Kit (JDK) 19
Java Runtime Environment (JRE) 19
JAVA_HOME setting 19

K
keystore file 20
keytool utility 20

L
lab evaluation installations 59
lease_upgrade_log file 31
license 11
license keys 9, 13, 33
license set key command (CLI) 34
license types 9
Linux 8, 19, 21, 25, 35, 38, 54, 56
cnr_status 25, 35
gtar 21
gzip 21
install_cnr 21, 56
requirements 8
superuser/root accounts 19
uninstall_cnr 38
uninstallation 38
variable declaration file 54
Local directory 22
local mode 21
Local.sav directory 23
log files 31
logging 16, 39
server events 16, 39
startups 16, 39
Windows 16

M
market segment specific 11

N
Network Registrar 1
about; 1
noninteractive 53
nwreg2 package 21
nwreglocal utility 35
nwregregion utility 35

O
operating system 7, 8
requirements 7
versions 8
OVA 41
overview 1

P
pkgadd utility 21, 56
pkgask utility 54
pkgrm utility 38, 56
processing messages 25

R
RAM requirements 8
Regional directory 22
regional mode 21
Regional.sav directory 23
RIC servers 2
root accounts 19
router interface configuration servers 2

S
sdk 61, 62
compatibility considerations 62
installing 61
secure login 19
self-extracting executable 21
self-signed certificates 20
server-client installation 24
servers 2, 15, 16, 34, 39
DHCP 2
DNS 2
logging events 16, 39
RIC 2
running with other 15
servers (continued)
  starting/stopping 34
setup.exe file 21
silent installations 53
Solaris 19, 21, 25, 35, 38, 53, 56
  cnr_status 25, 35
gtar 21
gzip 21
nwreg2 21
nwreglocal and nwregion 35
pkgadd 21, 53, 56
pkgrm 38, 56
superuser/root accounts 19
uninstallation 38
Start menu 21, 33
  access 33
setup 21
starting 16, 33, 34, 39
  CLI 33
  logging when 16, 39
servers 34
Web UI 33
status of server agents; server agents 25
  checking status 25
stopping servers 34
superuser accounts 19
system privileges 19

T

tail command 16
troubleshooting 31

U

uncompressing the media 21
uninst.exe utility 56
uninstall.cntr utility 38
uninstallation 37, 38, 60
  lab evaluation 60
Linux 38
Solaris 38
Windows 37
unpacking the media 21
upgrade 1, 13, 19, 20, 21, 23, 24, 25, 53, 59
  archive directories 23
  archiving 23
  CD 20
  cluster mode 21
  connection type 24
  database status 23
upgrade (continued)
  Java directory 24
  JAVA_HOME setting 19
  JRE/JDK requirements 19
  lab evaluation 59
  license keys 13
  network distribution 20
  overview 1
  process 19
  processing messages 25
  secure login 19
  silent 53
  system privileges 19
  types 24
  Web UI port 24

V

viewing server logs 16, 39
virtual appliance 42, 43, 44, 45, 48
  automatic power up 48
  booting and configuring 44
  deploying 43
  installing and configuring 42
  managing 45
  upgrading 45
virus scanning 15
  excluding directories; excluding directories for virus scanning 15
VMware vCenter 43
VMware vSphere 43

W

Web UI 2, 7, 24, 33, 65
  ciphers 65
  ports 24
  requirements 7
  starting 33
web-based user interface 2
Windows 8, 16, 21, 33, 37, 56
  logging 16
  program run location 21
  requirements 8
  self-extracting executable 21
  setup.exe file 21
  Start menu 21, 33
  uninst.exe 56
  uninstallation programs 37