Cisco Prime Network Registrar 10.1 Installation Guide

First Published: 2019-12-16

Last Modified: 2022-10-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

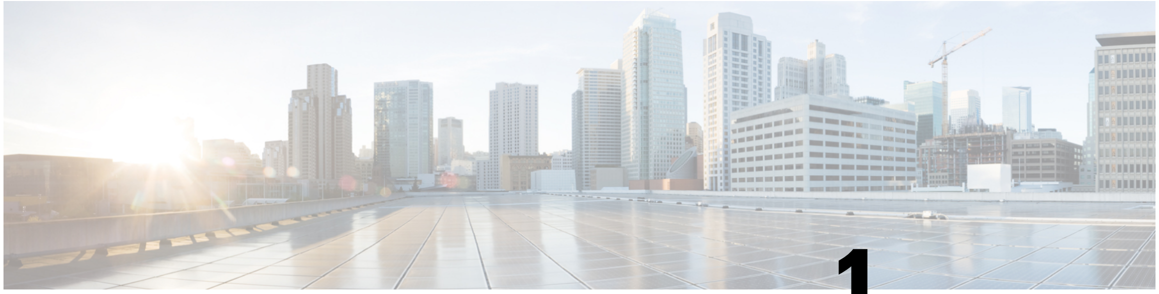
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS



CHAPTER 1

Installation Overview

This chapter contains the following sections:

Overview

This guide describes how to install Cisco Prime Network Registrar Release 10.1 on Windows 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 10.1 Administration Guide*.
- For details about commands available through the Command Line Interface (CLI), see the *Cisco Prime Network Registrar 10.1 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 (refer the below figure).

- Dynamic Host Configuration Protocol (DHCP) server
- Domain Name System (DNS) server
- Caching Domain Name System (CDNS) 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 CLI. These user interfaces can also control server clusters that run on different platforms.

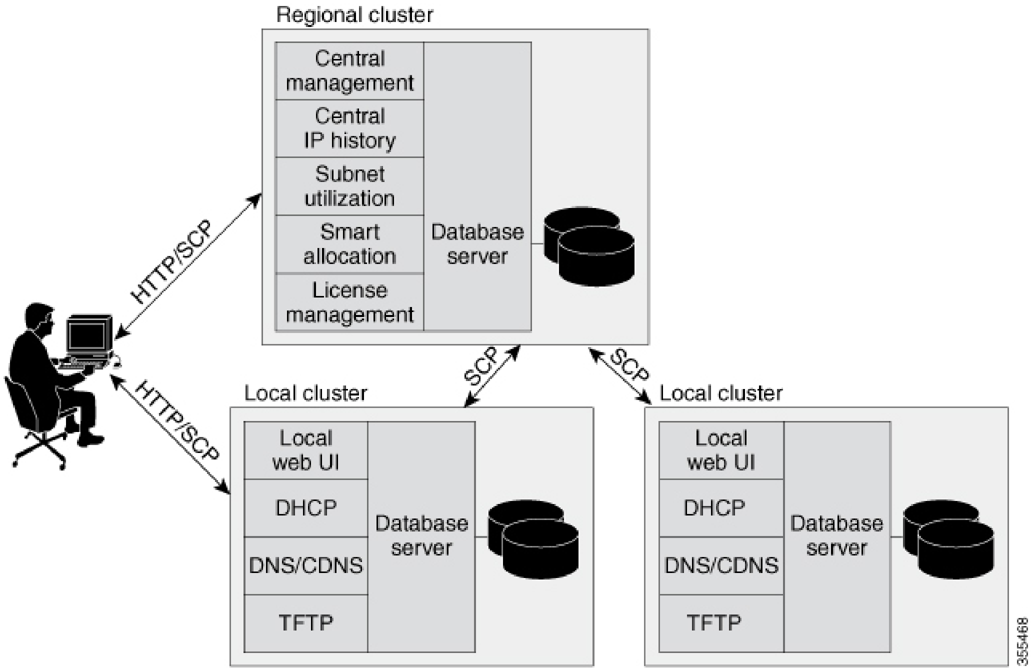
You can install Cisco Prime Network Registrar in either local or regional mode:

- 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 is required for licensing and can be used to centrally manage 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 DHCP utilization and IP lease history data from the local clusters.

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



Sensitive Data Exposure

Most of the data that Cisco Prime Network Registrar deals with is sent over unencrypted networks (especially the last hop to client devices), and is designed by its nature to be shared and available to other devices on the network (either locally or across the Internet).

If you consider the data (or portions of it) that Cisco Prime Network Registrar has as sensitive, we highly recommend you to encrypt your disks using the Linux or Windows support for disk based encryption. This will help protect the data once the disks leave controlled space (that is, reach end of life, when it not possible to erase it properly, or is stolen). You also need to consider how to protect any backups, or other places you may move the data.

CHAPTER 2

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, on page 3
- DHCP-Only Scenarios, on page 4
- DNS-Only Scenarios, on 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, and at least one scope.

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, and 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 an Auth DNS secondary server.
- Configure one machine as a DHCP server, the second machine as an 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

Review the system requirements before installing the Cisco Prime Network Registrar 10.1 software:

- Java—You must have the Java Runtime Environment (JRE) 1.8, or the equivalent Java Development Kit (JDK) installed on your system. (The JRE is available at the Oracle website.)

Note A 64-bit JRE/JDK is required.

- Operating System—We recommend that your Cisco Prime Network Registrar machine run on the Windows or Linux operating systems as described in the Server Minimum Requirements table below. Cisco Prime Network Registrar requires a 64-bit operating system.
- 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 11 and Edge, Mozilla Firefox 69, and Google Chrome 77. Internet Explorer 8 is not supported.
  - The CLI runs in a Windows or Linux command window.

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.

Table 1: Cisco Prime Network Registrar Server Requirements

Component	Operating System	
	Linux	Windows
OS version[1]	Red Hat Enterprise Linux ES/CentOS 6 and 7 64-bit[2] **Note:** The newest level tested with this release is CentOS 7.9.	Windows Server 2012 R2[3]
Minimum disk space	200 GB For best performance, Cisco recommends use of SSD drives.	
Minimum memory	16 GB	
Minimum CPUs[4]	4 CPUs	

[1] Cisco Prime Network Registrar 10.1 is only supported on 64-bit operating systems.

[2] Cisco Prime Network Registrar 10.1 has been tested by Cisco with Red Hat Enterprise Linux ES 6 and 7, running standalone or on VMware (ESXi 6.x) on Cisco Unified Computing System (CUCS). You are not restricted from upgrading these systems as long as the OS and hypervisor changes are backward compatible. Cisco recommends testing the upgraded systems in a lab environment for the intended use cases before deploying to the production systems. Cisco warranty and service apply only to the Cisco Prime Network Registrar software, therefore does not apply to issues in OS, hypervisor, or third-party hardware. The newest levels of hypervisor tested with Cisco Prime Network Registrar are VMware ESXi 7.0 and Openstack Victoria.

[3] Cisco Prime Network Registrar 10.1 supports Windows Server 2012 R2, running standalone or on VMware (ESXi 6.x) on CUCS and other hardware supported by VMware.

[4] Faster CPU and more memory typically result in higher peak performance.

Note Cisco Prime Network Registrar 10.1 is the last release to support Windows. Also, there will be no 9.x or 10.x releases (including patch or maintenance) for Windows, except for Severity 1 issues.

Note Based on the type of clusters you are planning to deploy, see the Capacity and Performance Guidelines appendices for more details.

Important Treat these system requirements as minimal guidelines. We advise you to monitor your deployment and adjust based on the actual usage level you are seeing.

Cisco Network Registrar has been tested against Red Hat Enterprise Linux ES 7.3 and CentOS 7.3+. However, it is anticipated that the end users apply patches and maintenance releases to keep their OS upto date with OS-related bug fixes and security patches. Cisco does not anticipate that these patches/maintenance updates within the same OS major version will cause issues, but as always, it is highly recommended that any updates be lab tested before they are applied to production servers.

System Requirements for Linux OS

To install Cisco Prime Network Registrar on Red Hat Enterprise Linux or CentOS, the following x86_64 (64-bit) packages must be installed (over and above the Java Run-Time):

Table 2: Packages to Install

Package Name	Package Version
OpenLDAP	2.4
OpenSSL	1.0
libstdc++	4.x
libgcc	4.x
zlib	1.x
krb5-libs	1.x

The installer will report any packages that may be missing before beginning the installation process.

Note To know the kind of Linux system you are on, use the following command:

more /etc/redhat-release

Recommendations

When Cisco Prime Network Registrar is deployed on virtual machines, review the following recommendations:

- Do NOT deploy HA DNS or DHCP failover partners on the same physical server (in separate VMs). This will not provide high availability when the server goes down. Ideally, the high available/failover partners should be sufficiently "separate" that when one fails (because of a hardware, power, or networking failure), the other does not.
- When deploying multiple Cisco Prime Network Registrar VMs on the same physical server (or servers served by a common set of disk resources), you should stagger the automatic nightly shadow backups (by default, they occur at 23:45 in the server's local time). To know how to alter this time, see the *"Setting Automatic Backup Time" section in the Cisco Prime Network Registrar 10.1 Administration Guide*.

Note It may be acceptable to not follow the above recommendations for lab environments; but they must be followed for production.

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
- Linux—**install_cnr** script that uses Red Hat Package Manager

License Files

Cisco Prime Network Registrar 10.1 license file contains two sets of licenses that cover the permanent and subscription parts of the license. The permanent licenses are similar to the licenses issued for 8.x and 9.x versions. For Cisco Prime Network Registrar 10.1, the licensing is done according to the services that you require.

The perpetual portion of the license will continue to use the mappings established for Cisco Prime Network Registrar 8.3 and later.

Following are the types of licenses 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 the 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.

A corresponding subscription license is issued for each permanent Cisco Prime Network Registrar 10.x license. The expiration date for each subscription license is set to the subscription period. Following are the types of licenses available:

- sub-system —Licenses the CCM services.
- sub-dhcp—Licenses the DHCP services.
- sub-count-dhcp—Licenses the authoritative DNS services.
- sub-dns—Licenses the Caching DNS services.
- sub-count-dns—Licenses an incremental number of active leases..
- sub-cdns—Licenses an incremental number of RRs.

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-cdns and count-cdns

Note Licenses for Cisco Prime Network Registrar 9.x or earlier are not valid for Cisco Prime Network Registrar 10.x. You should have a new license for Cisco Prime Network Registrar 10.x. For the 10.x Regional, if one has 9.x CDNS clusters, the 9.x CDNS licenses must be added on the Regional server (9.x CDNS clusters will use 9.x licenses, and 10.x CDNS clusters will use 10.x licenses).

Note You should not delete any of the individual licenses loaded from the file. If required, you may delete older versions of DNS and DHCP licenses after the upgrade. Older versions of CDNS licenses must be retained if the servers are not upgraded.

Note Subscription licenses, if provided, should be installed to assure upgrades to future releases.

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

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)

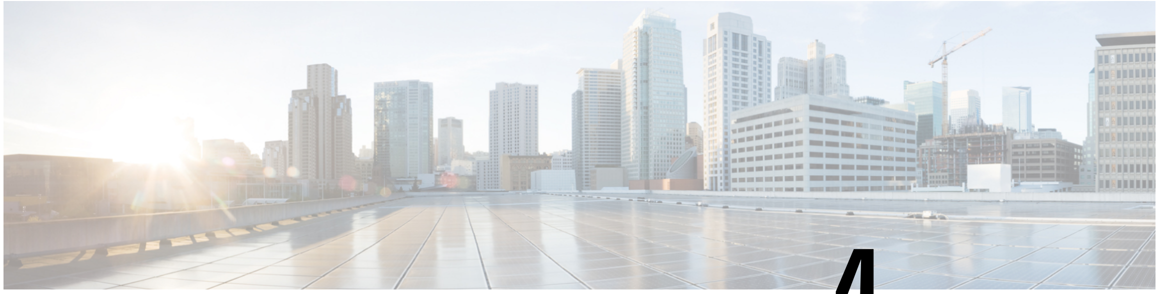
  Active leases include the number of leases in use by a client (and thus not available to another client) which also includes reservations and leases in transition.

- **Auth DNS services**—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 the *"Failover Scenarios" section in the "Configuring DHCP Failover" chapter in the Cisco Prime Network Registrar 10.1 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.



CHAPTER 4

Preparing for the Installation

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

Installation Checklist

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

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

Table 3: Installation Checklist

Task	Checkoff
Does my operating system meet the minimum requirements to support Cisco Prime Network Registrar 10.1? (See System Requirements, on page 7)	□
Does my hardware meet the minimum requirements? (See System Requirements, on page 7)	□
If necessary, have I excluded Cisco Prime Network Registrar directories and subdirectories from virus scanning? (See Backup Software and Virus Scanning Guidelines, on page 15)	□
On Windows, are other applications closed, including any virus-scanning or automatic-backup software programs? Is the Debugger Users group included in the Local Users and Groups?	□
Do I have the proper software license? (See License Files, on page 10)	□
Am I authorized for the administrative privileges needed to install the software?	□
Does the target installation server have enough disk space?	□
Is this a new installation or an upgrade?	□
Is the cluster mode of operation regional or local?	□

Task	Checkoff
Is this a full or client-only installation?	□
Is the 64-bit JRE/JDK installed on the system? If so, where?	□
Should the web UI use an HTTP or HTTPS connection, or both?	□
Am I upgrading from an earlier version of Cisco Prime Network Registrar? If so:	□
• Are there any active user interface sessions?	□
• Is my database backed up?	□
• Am I upgrading from a supported version (Cisco Prime Network Registrar 8.3 and later)?	□
Are the required packages for Linux installed? (See System Requirements for Linux OS, on page 9)	□

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 and install the prerequisite software.

Obtaining Cisco Prime Network Registrar License Files

When you purchase Cisco Prime Network Registrar 10.1, you receive a FLEXlm license file in an e-mail attachment from Cisco, after you register the software.

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

To obtain a license file:

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 10.1 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 in the default locations, exclude the following directories and their subdirectories:

Note In this document, 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 Linux default local cluster paths of /opt/nwreg2/local and /var/nwreg2/local, the *install-path* may represent these paths.

- Windows:

  install-path\data (for example, C:\NetworkRegistrar\Local\data and C:\Network Registrar\Regional\data)

  install-path\logs (for example, C:\NetworkRegistrar\Local\logs and C:\Network Registrar\Regional\logs)

- Linux:

  install-path/data (for example, /var/nwreg2/local/data and /var/nwreg2/regional/data)

  install-path/logs (for example, /var/nwreg2/local/logs and /var/nwreg2/regional/logs)

CHAPTER 5

Installing and Upgrading Cisco Prime Network Registrar

This chapter contains the following sections:

Installing Cisco Prime Network Registrar

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

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

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

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

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

Step 2 Download and install JRE 1.8, or the equivalent JDK, if you have not already done so. These are available at the Oracle website.

Note On Windows, add the full path of the bin subdirectory of your Java installation folder to your PATH environment variable; for example, C:\Program Files (x86)\Java\jdk1.8\bin.

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

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

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore k-file

Enter keystore password: password

What is your first and last name? [Unknown]: name

What is the name of your organizational unit? [Unknown]: org-unit

What is the name of your organization? [Unknown]: org-name

What is the name of your City or Locality? [Unknown]: local

What is the name of your State or Province? [Unknown]: state

What is the two-letter country code for this unit? [Unknown]: cc

Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc correct? [no]: yes

Enter key password for <tomcat> (RETURN if same as keystore password):
```

The keystore filename (k-file) is its fully qualified path. You will be entering the keystore path and password in **Step 17**.

Note You must use 128-bit SSL to disable weak ciphers in the web UI. For more information, see Enhancing Security for Web UI, on page 61.

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

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

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

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

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

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

Caution The Cisco Prime Network Registrar installation program for Windows does not try to modify ACLs to restrict access to the installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities to manually change file and directory permissions. See Modifying ACLs in Windows Installations, on page 37.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 6 On Linux, specify if you want to run Cisco Prime Network Registrar Local Server Agent as a non-root *nradmin* user. If you choose to run Cisco Prime Network Registrar for a non-root user, a user *nradmin* is created with the requisite privileges to run the Cisco Prime Network Registrar services. When running Cisco Prime Network Registrar as a non-root user *(nradmin*), some changes occur in the CLI operation of the product . Though it is still possible to run as root, it is not recommended. Instead, create regular Linux users and add them to the *nradmin* group. Users in this group will have full access to the Cisco Prime Network Registrar files. To start and stop Cisco Prime Network Registrar, these users may use the new **cnr_service** program which is in *install-path/*bin/cnr_service).

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

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

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

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

Windows default locations:

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

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

Linux default locations:

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

- Log files—/var/nwreg2/regional/logs
- Temporary files—/var/nwreg2/regional/temp

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

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

Step 9 Enter the filename, as an absolute path, for your base license (see License Files, on page 10).

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 IPv4 or IPv6 address and SCP port.

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

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

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

Step 11 After you register local to the regional, you can select the required services from the licensed services.

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

Step 12 Choose whether to archive the existing binaries and database in case this installation does not succeed. The default and recommended choice is **Yes** or **y**:

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

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

Step 13 Choose the appropriate installation type: server and client (the default), or client-only:

- Windows—Choose **Both server and client (default)** or **Client only**. Click **Next.** The Select Port window appears.

- Linux—Entering **1** installs the server and client (the default), or **2** installs the client only.

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

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

Step 15 Enter the location of JRE 1.8 or JDK selected in **Step 2**. (The installation or upgrade process tries to detect the location.):

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

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

Step 16 Choose whether to enable the web UI to use a Non-secure (HTTP) or Secure (HTTPS) connection for web UI logins:

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

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

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

Step 17 If you enabled HTTPS web UI connectivity, you are prompted for the location of the necessary keystore and keystore files:

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

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

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

Step 18 Enter a port number for the web UI connection. The defaults are:

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

- HTTPS regional cluster—8453

On Windows, click **Next**.

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

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

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

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

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

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

The Cisco Prime Network Registrar installation process begins. Status messages report that the installer is transferring files and running scripts. This process may take a few minutes.

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

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

Step 23 Verify the status of the Cisco Prime Network Registrar servers:

- Windows—In the Services control panel, verify that the Cisco Prime Network Registrar Local Server Agent or Cisco Prime Network Registrar Regional Server Agent is running after rebooting the system when the installation has completed successfully.
- Linux—Use the *install-path*/usrbin/cnr_status command to verify the status. See Starting and Stopping Servers, 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 25.

Upgrade Considerations

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

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

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

Upgrading on Windows

To upgrade to Cisco Prime Network Registrar 10.1:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements, 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 2012 R2. See the documentation supplied by Microsoft for information about how to install/upgrade Windows servers.

Note If you install Windows Server 2012 R2 instead of upgrading and the disk is reformatted, you must restore the Cisco Prime Network Registrar data to the C:\NetworkRegistrar\{Local | Regional}\data folder.

Step 5 Install Cisco Prime Network Registrar 10.1 on the Windows Server 2012 R2 machine. For installation instructions, see Installing Cisco Prime Network Registrar, on page 17. Ensure that you specify the path where your existing data can be found, for example, C:\NetworkRegistrar\{Local | Regional}, to run the upgrade.

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

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

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

Upgrading on Linux

To upgrade to Cisco Prime Network Registrar 10.1:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements, 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 Prime Network Registrar server agent and backup the current system (or at least the Cisco Network Registrar\Program Files\Network Registrar\ directories and contents). To stop the Cisco Prime Network Registrar Local/Regional server agent:

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

Step 4 Install Cisco Prime Network Registrar 10.1. For installation instructions, see Installing Cisco Prime Network Registrar, on page 17.

Reverting to an Earlier Product Version

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

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

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

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

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

Step 2 Uninstall Cisco Prime Network Registrar using the procedure described in the Uninstalling Cisco Prime Network Registrar, on page 39.

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

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

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

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

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

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

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

b) Using the fully qualified path to the archive directory, extract the archive. These examples assume the default archive location provided during installation.

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

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

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

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

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

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

Step 8 Start the Cisco Prime Network Registrar server agent:

- Windows:
    - Local—**net start nwreglocal**
    - Regional—**net start nwregregion**
- Linux—Local:
    - RHEL/CentOS 6.x—**/etc/init.d/nwreglocal start**
    - RHEL/CentOS 7.x—**systemctl start nwreglocal**
- Linux—Regional:
    - RHEL/CentOS 6.x—**/etc/init.d/nwregregion start**
    - RHEL/CentOS 7.x—**systemctl start nwregregion**

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

Moving a Local Cluster to a New Machine

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

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

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

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

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

- Windows:

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

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

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

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

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

Step 4 Install Cisco Prime Network Registrar (local cluster) on the new server. The installation will detect an upgrade and will do so based on the copied data.

This procedure preserves your original data on the old machine.

Re-apply any custom configuration changes (such as those outlined in Enhancing Security for Web UI, on page 61) after the installation.

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

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

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

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

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

Moving a Regional Cluster to a New Machine

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

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

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

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

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

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

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

- Windows:

  net stop nwregregion

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

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

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

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

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

Step 4 Install Cisco Prime Network Registrar (regional cluster) on the new server. For more information, see Installing Cisco Prime Network Registrar, on page 17.

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

Re-apply any custom configuration changes (such as those outlined in Enhancing Security for Web UI, on page 61) after the installation.

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

Step 5 Start the Cisco Prime Network Registrar web UI or CLI. For more information, see Starting Cisco Prime Network Registrar, on page 33.

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

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

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

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

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

Troubleshooting the Installation

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

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

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

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

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

- Windows:
  - Local cluster: C:\Program Files(x86)\Network Registrar\Local\debug_install.cmd
  - Regional cluster: C:\Program Files\Network Registrar\Regional\debug_install.cmd

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

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

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

Troubleshooting Local Cluster Licensing Issues

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

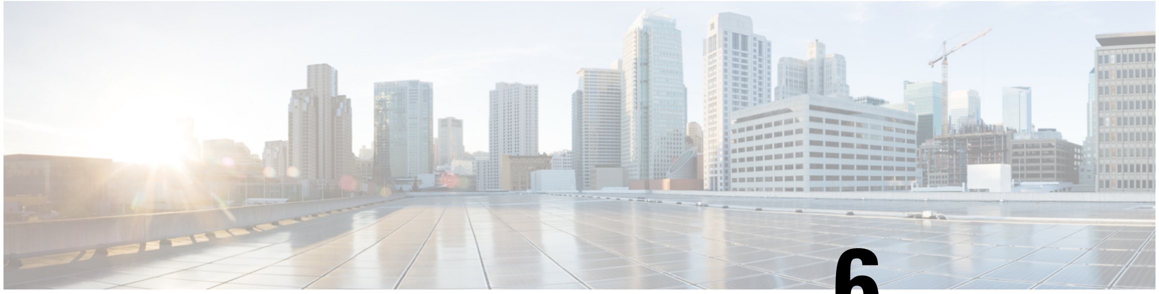
To register a local cluster with the regional cluster:

Step 1 Install Cisco Prime Network Registrar (local cluster) on the server and create the admin user for the local cluster. For more information, see Installing and Upgrading Cisco Prime Network Registrar, on page 17.

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

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

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



CHAPTER 6

Next Steps

This chapter contains the following sections:

Configuring Cisco Prime Network Registrar

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

- Get started with Cisco Prime Network Registrar—See Cisco Prime Network Registrar 10.1 Quick Start Guide.

- Set up DHCP addresses, DHCP failover, and DNS update—See Cisco Prime Network Registrar 10.1 DHCP User Guide.

- Set up Authoritative and Caching DNS services—See Cisco Prime Network Registrar 10.1 Caching and Authoritative DNS User Guide.

- Perform administrative tasks, such as local and regional administration, set up Cisco Prime Network Registrar virtual appliance, and so on—See Cisco Prime Network Registrar 10.1 Administration Guide.

- Configure and manage Cisco Prime Network Registrar via CLI—See Cisco Prime Network Registrar 10.1 CLI Reference Guide.

- Configure and manage Cisco Prime Network Registrar via REST API—See Cisco Prime Network Registrar 10.1 REST APIs Reference Guide.

Starting Cisco Prime Network Registrar

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

To enter license information in web UI or CLI:

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

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

  ```
  http://hostname:http-port
  ```

  ```
  https://hostname:https-port
  ```

  where:

  - *hostname* is the actual name of the target host.
  - *http-port* and *https-port* are the default HTTP or HTTPS port that are specified during installation. (See Installing and Upgrading Cisco Prime Network Registrar, on page 17).

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

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

- To start the CLI:

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

    ```
    nrcmd -C cluster-ipaddress -N username -P password
    ```

  - Linux—Navigate to the *install-path*\usrbin directory and enter this command

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

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

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

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

  ```
  nrcmd> license create filename
  ```

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

Starting and Stopping Servers

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

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

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

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

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

Starting and Stopping Servers on Windows

To start and stop servers on Windows:

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

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

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

Starting and Stopping Servers on Linux

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

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

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

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

To start and stop servers on Linux:

Step 1 Log in as superuser.

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

For the RHEL/CentOS 6.x local cluster:

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

For the RHEL/CentOS 7.x local cluster:

```
# systemctl start nwreglocal
```

For the RHEL/CentOS 6.x regional cluster:

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

For the RHEL/CentOS 7.x regional cluster:

```
# systemctl start nwregregion
```

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

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

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

For the RHEL/CentOS 6.x local cluster:

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

For the RHEL/CentOS 7.x local cluster:

```
# systemctl stop nwreglocal
```

For the RHEL/CentOS 6.x regional cluster:

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

For the RHEL/CentOS 7.x regional cluster:

```
# systemctl stop nwregregion
```

Starting or Stopping Servers Using the Local Web UI

To start or stop servers in the local Web UI:

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

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

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

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

Starting and Stopping Servers Using the Regional Web UI

To start or stop servers in the regional Web UI:

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

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

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

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

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

Server Event Logging

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

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

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

⚠

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

Modifying ACLs in Windows Installations

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

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

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

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

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

CHAPTER 7

Uninstalling Cisco Prime Network Registrar

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

To back up your database before uninstalling Cisco Prime Network Registrar, see the *Cisco Prime Network Registrar 10.1 Administration 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

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

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

Step 2 Reboot after the uninstallation completes.

Uninstalling on 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).

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.

CHAPTER 8

Cisco Prime Network Registrar Virtual Appliance

The Cisco Prime Network Registrar virtual appliance includes all the functionality available in a version of Cisco Prime Network Registrar 10.1 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

There are three kits that can be used to install the virtual appliance:

- An OVA which runs on VMware ESXi 6.x
- A KVM kit which runs on a KVM hypervisor
- A cloud image which can be deployed to OpenStack

These kits are effectively identical, and in this guide, when the OVA is discussed, the discussion applies to all three kits unless otherwise noted.

Each of these kits were created to require limited resources: 1 virtual CPU, 8 GB main memory, 6 GB swap partition, and a 7.5 GB system partition with 5.4 GB available (free). The total disk storage required is 14 GB. You will almost certainly want to increase the size of the system disk, and giving the virtual appliance additional virtual CPUs can increase the performance considerably. You should ensure that sufficient resources are available on the host that you are targeting for the deployment to meet these requirements.

You must increase the resources used by the virtual appliance or it will not function successfully. There are two different regimes: running a local cluster, or running a regional cluster and local cluster on the same machine. The recommendations below are for running the virtual appliance(s) on a Jumpstart, but these are also useful starting points for any local or regional cluster deployment. For a local cluster:

- CPU: 1 socket, 8 CPUs
- Memory: 12 GB
- Disk: 100 GB or greater

For a regional cluster running on the same Jumpstart as a local cluster:

- CPU: 1 socket, 7 CPUs
- Memory: Minimum 8 GB
- Disk: 35 GB

You may need substantially more disk space than listed above based on the size of your deployment. You can increase the disk space by resizing the allocated disk and rebooting the appliance.

Installing and Upgrading Cisco Prime Network Registrar Virtual Appliance

You can deploy the virtual appliance in any of the three environments: VMware ESXi 6.x, KVM hypervisor, or OpenStack. After discussing the information that you will need to determine for any deployment, the individual environments are discussed in detail.

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.

Note From Cisco Prime Network Registrar 9.1 and later, you can copy an existing VM to create a new local cluster (snapshot), you must generate a new UUID and re-register it with the regional cluster to avoid duplication of UUID, see the *“Generating new UUID” section in the Cisco Prime Network Registrar 10.1 Administration Guide*.

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 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 addresses 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 on VMware

The Cisco Prime Network Registrar virtual appliance is supported for production use on VMware ESXi 6.x and can be accessed or managed using the VMware vSphere client. 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.

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 is provided as a .ova file.

The names are:

- *cpnr_10_1_local.ova* for the local virtual appliance
- *cpnr_10_1_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.

Step 2 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 on versions prior to ESXi 6.5 and the Deployment Options window appears for ESXi 6.5 or later versions.

The **Thick** provisioned format is selected by default for versions prior to ESXi 6.5 and the **Thin** provisioned format is selected by default for ESXi 6.5 and later versions. You should select the **Thick** regardless of the default value.

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 before clicking the **Power on** button (▶). 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 10.1 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 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 completely, 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, see Configuring Network Access on RHEL/CentOS 7.x Using nmcli, on page 69.

Deploying the Regional Cluster or Local Cluster on a KVM Hypervisor

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 is provided as a .bz2 file.

The names are:

- *cpnr_10_1_local.kvm.tar.bz2* for the local virtual appliance
- *cpnr_10_1_regional.kvm.tar.bz2* 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.

To install Cisco Prime Network Registrar on a KVM hypervisor, extract the distribution tar archive (cpnr_10_1_local.kvm.tar.bz2 or cpnr_10_1_regional.kvm.tar.bz2) using the following command:

```
root$ tar xvjf cpnr_10_1_local.kvm.tar.bz2
```

or

```
root$ tar xvjf cpnr_10_1_regional.kvm.tar.bz2
```

If you are unpacking both the local and the regional KVM kits, you must untar them in separate directories to avoid filename conflicts.

The extraction takes a few minutes and it requires a minimum of 14 GB free disk space. You should see the following files:

- cpnr_10_1_local-disk1.raw—Contains the disk for the virtual machine.
- installonkvm—Installs the virtual machine.
- readme.kvm.txt—Contains the installation instructions.

The cpnr_10_1_local-disk1.raw file is the actual file that will be used as the disk file for the resulting Cisco Prime Network Registrar KVM virtual machine. This file should be placed in the directory where you want it to reside long-term as the "source path" for the virtual disk in the Cisco Prime Network Registrar KVM virtual machine. While you can move it even after the virtual machine is installed, it is easier to start with it in the correct location. You should move the **installonkvm** script along with it. The **installonkvm** script needs to be executable in order to operate correctly.

To proceed with the installation, follow the instructions as specified in the readme.kvm.txt file.

Once the installation is complete, see Configuring Network Access on RHEL/CentOS 7.x Using nmcli, on page 69.

Deploying the Regional Cluster or Local Cluster on OpenStack

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 is provided as a .ova file.

The names are as follows:

- *cpnr_10_1_local.qcow2* for the local virtual appliance
- *cpnr_10_1_regional.qcow2* 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.

To run the local cluster or regional cluster on OpenStack, you must first create a local or regional image out using the **.qcow2** distribution kit.

After this image exists, you may launch an instance of the local or regional cluster. The Flavor you associate with the instance needs at least 1 VCPU, 8 GB of RAM, and at least 14 GB of root disk storage. In order to have an operational instance of Cisco Prime Network Registrar, you must allocate more than the absolute minimum of 14 GB of root disk storage. See System Requirements, on page 41 for the amount of disk space needed for a local or regional cluster.

An instance of Cisco Prime Network Registrar will be created with a fixed IP address. Cisco Prime Network Registrar will automatically use any IP addresses associated with interfaces that it can detect when it is started. If the interface available to Cisco Prime Network Registrar has an IP address allocated to it from a provider network (that is, it is accessible to the clients that need the DHCP or DNS capabilities provided by Cisco Prime Network Registrar), then you can configure Cisco Prime Network Registrar normally.

When you install a Cisco Prime Network Registrar virtual appliance on VMware or using the KVM kit, you configure the root password for the underlying Linux system on the system console when the virtual machine is first booted. However, usually OpenStack instances are created and deployed in such a way as to only allow logins with SSH using an SSH key-pair that is configured as part of the OpenStack instance. Many OpenStack instances do not allow root password login at all, and only allow login using SSH with an SSH key-pair.

A Cisco Prime Network Registrar OpenStack instance can be configured to operate in either of these two regimes:

Option 1: Require root password configuration and allow root login using a password.

Option 2: Disable the root password configuration and login. An SSH key-pair is required to login.

Option 1:

This is the default approach for all Cisco Prime Network Registrar virtual appliance kits, and requires no additional actions. You will launch an instance from the Cisco Prime Network Registrar virtual appliance image, and on first boot you will have to bring up a console window for the Cisco Prime Network Registrar instance, enter a root password for the Linux system, and accept the End User License Agreement. After the first boot, you will not need to access the console. You can also access this instance with an SSH key-pair.

Option 2:

If you wish to deploy the Cisco Prime Network Registrar virtual appliance instance in a way that is more in accordance with the usual practice for OpenStack instance deployment, you can configure the Cisco Prime Network Registrar OpenStack instance to not allow root logins with a password, and require an SSH key-pair to login. If you also wish to allow a password based login for a user other than root with root permissions, instructions on how to configure are listed below.

When you launch an OpenStack instance from web UI, to prevent root password login, you will have to perform specific configuration in the **Configuration** section of the Launch instance dialog. You will need to provide a customization script - which is analogous to User Data in other systems. You will need to configure a script (provided below) which will make the OpenStack instance disable the root password based login. After you deploy an instance configured with this customization script, the only way to gain access to the Linux operating system on the instance is to login via SSH using the **ssh key pair** associated with the instance at the time of launch.

For example, you might login with **ssh -i keypairname.pem root@a.b.c.d**. If you did not associate a key pair with the instance, or have lost access to the key pair, you will not be able to login to the instance. There is no default root password when the instance is created in this way, and the root password login is disabled.

To configure option 2, enter the following in the **Customization Script** text box:

```
# cloud-boothook
 # !/bin/bash
 if [ ! -f /etc/cloud/cloud.cfg.orig ]; then
 cp /etc/cloud/cloud.cfg /etc/cloud/cloud.cfg.orig
 cp /etc/cloud/cloud.cfg.norootpasswd /etc/cloud/cloud.cfg
 fi
```

Note If you choose option 2 and once you gained access to the instance using the **ssh key pair**, if you would like to login with a password as well, you can create a new Linux user using the **useradd** command and make that user a member of the group wheel. You must also give that user a secure password using the **passwd** command. Then you can always login with **ssh** or to the console as that user, and have root privileges.

To create a user to allow password login, use the following command:

```
useradd safeuser -g wheel
passwd safeuser
```

Then, if you need root access, login as **safeuser** and use the following command:

```
sudo su
```

Enter the password for **safeuser**, and you will become a root user.

If the IP addresses that are associated with the available interfaces are fixed addresses (that is, they are only accessible to other instances in OpenStack), then you need to associate a floating address with Cisco Prime Network Registrar instance. This floating address must then be accessible to the clients of the DHCP or DNS service to be provided by the Cisco Prime Network Registrar instance. You will have to configure the DHCP server provided by Cisco Prime Network Registrar to return the IP address of the floating address as its server-id, instead of the fixed IP address that Cisco Prime Network Registrar can detect that is associated with the interface built into the instance. To configure DHCP for this situation, you need to be in Expert mode, and configure the DHCP Policy attribute *dhcp-server-identifier-address* with the floating address allocated to this instance. Then the DHCP server will return the configured IP address (which will be the externally visible IP address of this instance) instead of the IP address that the DHCP server can detect from examining the interface that it is using for communications with clients (which is the fixed IP address).

A local cluster needs to be registered with a regional cluster. After this registration, the regional cluster needs to be able to connect to the local cluster. When the local cluster initially registers with the regional cluster, it sends its IP address to the regional cluster. If the regional cluster can contact the local cluster by using the IP address that the local cluster sees is configured to its network interface, then no action is required. This would be the case if the local cluster has a fixed IP address that is only visible within the OpenStack cloud, but the regional cluster was also in the same cloud. If the regional cluster can ping the IP address that the local cluster sees as the IP address on its network interface, then no additional steps are required. However, in the event that the regional cluster is not local to the OpenStack cloud on which the local cluster is running, and the local cluster has a floating address in addition to a fixed address, then the regional cluster's configuration for the local cluster needs to have its IP address updated to be that of the floating address (and not the fixed address, which is what it will have from the initial registration).

When allocating a local cluster, you should consider allocating 4 or even 8 VCPUs and at least 12 GB of RAM, with more for large systems. Local clusters will absolutely need more than the 7+ GB free space available in the minimal installation. Regional clusters will probably need an additional disk space, but 2 to 4 VCPUs and 8 to 12 GB of RAM will suffice for many installations.

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 7.7 using the data from an existing virtual appliance.

Note The newest operating system version used for Cisco Prime Network Registrar 10.1.3 virtual appliance is CentOS 7.9.

Upgrading a 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.

Note 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 17.

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: **systemctl stop nwreglocal**

Step 3 Tar the existing *install-path*/local/data directory using the following command:

```
tar cvf tarfile.tar data
```

Step 4 Copy the tar file created to the new virtual appliance.

Step 5 Shut down Cisco Prime Network Registrar on the new virtual appliance using the following command:

```
systemctl stop nwreglocal
```

Step 6 Rename the existing database to **.orig** using the following command:

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

Step 7 Untar the latest database, transferred in **Step 4**, using **tar xvf tarfile.tar**.

Step 8 Copy any existing extensions from the system being upgraded to the correct directories on the new virtual appliance.

Step 9 Reboot the Cisco Prime Network Registrar virtual appliance using VMware vSphere.

Upgrading to a new Version of the Virtual Appliance Operating System

To upgrade and to use a new version of the Cisco Prime 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 in Upgrading a Cisco Prime Network Registrar Installation to Run on a Cisco Prime Network Registrar Virtual Appliance, on page 48.

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

Note The new 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. Whenever this pause during the boot process and message appears, Cisco Prime Network Registrar will not be able to start until after the script /opt/nwreg2/local/usrbin/upgrade_cnr (or /opt/nwreg2/regional/usrbin/upgrade_cnr for a regional cluster) has been run. Cisco Prime Network Registrar has been masked using systemctl, and the **upgrade_cnr** script will unmask it before performing the upgrade.

Step 1 Press return on the console to complete the boot process.

Step 2 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.

Upgrading the Cisco Prime Network Registrar Application

If you want to upgrade the installation of Cisco Prime Network Registrar that currently exists on the virtual appliance to a new version of Cisco Prime Network Registrar, follow the procedure in this document to perform a straightforward software product upgrade. The installation of Cisco Prime Network Registrar delivered on the virtual appliance is a regular installation of the Cisco Prime Network Registrar software product.

Next Steps: Cisco Prime Network Registrar Virtual Appliance

Configuring Cisco Prime Network Registrar with the CLI on Virtual Appliance

The Cisco Prime Network Registrar 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. 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 The KVM kit is installed with automatic power up enabled.

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 7.7, 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. On Openstack, you may use the key pair created when you launched the instance.

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 Windows 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 The newest operating system version used for Cisco Prime Network Registrar 10.1.3 virtual appliance is CentOS 7.9.

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.

Post OVA Installation

Follow the below steps to get the latest CentOS updates, latest version of installed packages and security updates before configuring the Cisco Prime Network Registrar.

Note The command **yum update** will update the running system with new and changed software that in most cases did not exist when the Cisco Prime Network Registrar application was tested with the operating system shipped on the virtual appliance. The updates that are installed as part of the **yum update** command do not cause any problems for the Cisco Prime Network Registrar application. However, Cisco cannot guarantee that the Cisco Prime Network Registrar application will perform without any problems when interfacing with software that was not available when our testing was performed. You should perform your own testing to ensure that everything is operating correctly in your environment after a **yum update** command has been executed before placing the updated virtual appliance into production.

Step 1 Login as root.

Step 2 Configure networking.

Step 3 Go to the root prompt and enter the following command:

```
# yum update
```

Step 4 Reboot the system and then configure Cisco Prime Network Registrar.

APPENDIX A

Performing a Silent Installation

This appendix contains the following section:

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.

- Linux:

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

Table 4: Silent-Response File Entries for Linux

Silent-Response File Entry	Description
BACKUPDIR=	Path where to store the current Cisco Prime Network Registrar installation files, but only if PERFORM_BACKUP=y
CCM_LOCAL_SERVICES=	Services (dhcp, dns or cdns) to enable
CCM_PORT=	Central Configuration Management (CCM) port; default value is: • **1234** if CNR_CCM_MODE=local • **1244** if CNR_CCM_MODE=regional
CCM_REGIONAL_IP_ADDR=	IPv4 address of the regional server
CCM_REGIONAL_IPV6_ADDR=	IPv6 address of the regional server
CCM_REGIONAL_SCP_PORT	SCP port number on the regional server
CNR_ADMIN=	Superuser name. To skip configuring the superuser name, value should be CNR_ADMIN=unset.
NRADMIN=	Non-root user. To install Cisco Prime Network Registrar as non-root user, value must be NRADMIN=y.
CNR_PASSWORD=	Superuser password. To skip configuring the superuser password, value should be CNR_PASSWORD=unset.
CNR_CCM_MODE=	CCM mode; set to **local** or **regional**.
CNR_CCM_TYPE=	Reserved for GSS installation. Always set to **cnr**.
CNR_EXISTS=	If set to **y** (recommended), tries to kill any open CLI connections when installing or upgrading; otherwise, basically deprecated.
CNR_LICENSE_FILE=	Fully qualified path to the license file. Set CNR_LICENSE_FILE=unset if CNR_CCM_MODE=local.
CNR_SECURITY_MODE=	Security mode configuration: • Required. Fail if the connection cannot be secured. • Optional. Allow fallback to insecure connection. • Disabled. Do not load security modules at startup.
DATADIR=	Fully qualified path to the data directory.
JAVADIR=	Fully qualified path to the Java installation (JRE 1.8).

Silent-Response File Entry	Description
KEYSTORE_FILE=	If USE_HTTPS=y, the fully qualified path to the keystore file.
KEYSTORE_PASSWORD=	If USE_HTTPS=y, the password used when generating the keystore file.
LOGDIR=	Fully qualified path to the log file directory.
PERFORM_BACKUP=	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).
ROOTDIR=	Fully qualified installation path for the product files; contains bin, classes, cnrwebui, conf, docs, examples, extensions, lib, misc, schema, tomcat, and usrbin subdirectories.
START_SERVERS=	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**.
TEMPDIR=	Fully qualified path to the temp directory.
USE_HTTP=	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**.
USE_HTTPS=	Sets whether or not the web UI server listens for HTTPS connections; one or both of USE_HTTP or USE_HTTPS 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

Silent-Response File Entry	Description
WS_PORT=	Port number that the web service uses for HTTP traffic; default value is: • **8080** if CNR_CCM_MODE=local • **8090** if CNR_CCM_MODE=regional
WS_SEC_PORT=	Port number that the web service uses for HTTPS traffic; default value is: • **8443** if CNR_CCM_MODE=local • **8453** if CNR_CCM_MODE=regional
WEB_SERVICES=	Set to y or n to enable or disable the web services (DNS ENUM and REST API).
CNR_BYOD_ENABLE=	Set to **y** or **n** to enable or disable the BYOD services.

Step 2 Use these commands to invoke the silent installation or upgrade for each instance:

- Windows:

```
setup.exe -s -f1path+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.

- Linux:

```
install_cnr -r response-file
```

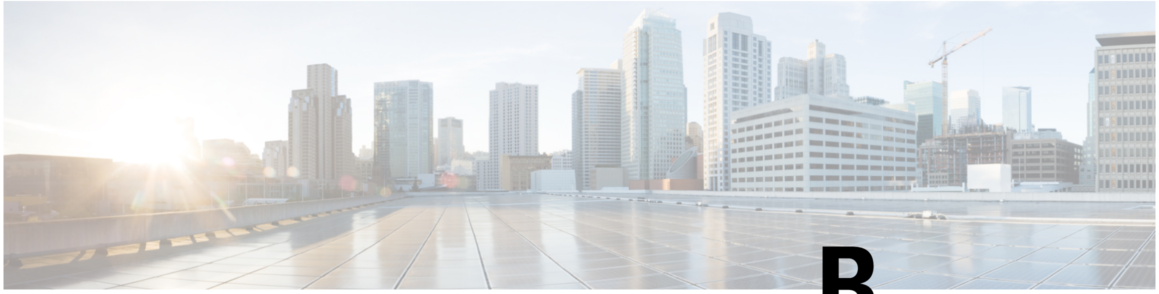
Step 3 If you want to uninstall the product:

- Windows—Generate an uninstallation response file and execute:

```
setup.exe -s -f1uninstall_response_file
```

- Linux—Invoke the silent uninstallation (this command is noninteractive except during an error):

```
uninstall_cnr
```



APPENDIX B

Lab Evaluation Installations

This appendix contains the following sections:

Lab Evaluation Installations

This appendix describes how to install, upgrade, and uninstall Cisco Prime Network Registrar regional and local clusters on a single 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 Linux machine, according to the procedures in Installing Cisco Prime Network Registrar, on page 17. 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 40.

No option exists to uninstall only the regional or local cluster in a dual-mode installation environment.

APPENDIX C

Installing the Cisco Prime Network Registrar SDK

This section documents how to install the Cisco Prime Network Registrar SDK on the Linux and Windows platforms. Before installing the SDK, ensure that you have JRE 1.8, or the equivalent 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

To install the Cisco Prime Network Registrar SDK on a Linux 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, 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.

Review the *"SDK Compatibility Considerations" sections of the Cisco Prime Network Registrar 10.1 Release Notes* for the intervening Cisco Prime Network Registrar versions, as these highlight any significant SDK compatibility considerations.

APPENDIX D

Enhancing Security for Web UI

This appendix contains the following section:

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. In case you want to harden the system, adjust the ciphers as below:

Note The default installation of Cisco Prime Network Registrar 10.1 works with Transport Layer Security (TLS) 1.2. You can change the configuration to make it work with the older TLS versions, if needed.

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:

Note The values for **port**, **keystoreFile**, and **keystorePass** must match the values that you have configured in your system.

```
<Connector port="8443"

maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

maxHttpHeaderSize="8192"

enableLookups="false"

disableUploadTimeout="true"

acceptCount="100" scheme="https" secure="true"

clientAuth="false"

ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA"

keystoreFile="conf/.keystore"

sslProtocol="TLSv1.2"

sslEnabledProtocols="TLSv1.2"/>
```

Step 3 Restart Cisco Prime Network Registrar for the changes to take effect.

APPENDIX E

Hardening Guidelines

This appendix contains the following section:

Hardening Guidelines

If you consider hardening the system, you should consider the following hardening guidelines:

- Refer to the host platform's hardening guides. For example:
    - Red Hat 6:

      https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

    - RHEL/CentOS 7.x:

      https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Security_Guide/Red_Hat_Enterprise_Linux-7-Security_Guide-en-US.pdf

      https://www.cisecurity.org/benchmark/red_hat_linux/

      https://www.cisecurity.org/benchmark/centos_linux/

    - Windows Server 2012:

      https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf

    - NSA hardening guide collection:

      https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

Note The above links reference external websites and Cisco is not responsible for keeping them up-to-date. They are provided for reference only. If you find that the content is outdated or if you cannot access the links, please contact the website owner for updated information.

- Disable or block the ports that are not used by Cisco Prime Network Registrar. The Cisco Prime Network Registrar documentation outlines the port usage and also the issues with using firewall items, such as connection tracking.
  - For a list of ports used by Cisco Prime Network Registrar, see the *"Default Ports for Cisco Prime Network Registrar Services" section in the Cisco Prime Network Registrar 10.1 Administration Guide*. Note that some are defaults and may have been changed during install or configuration.
  - For connection tracking related issues, see the *"DNS Performance and Firewall Connection Tracking" section in the Cisco Prime Network Registrar 10.1 Administration Guide*.
- Install Cisco Prime Network Registrar using the non-root account and use the security features (that is, https and require secure SCP sessions).
- Confirm that any product directories (primarily, /opt/nwreg2/* and /var/nwreg2/*) are locked down as appropriate. Note that you may need to adjust the protection based on your needs (such as for performing offline backups and viewing logs).
- DNS specific considerations include:
  - Use DNS Security Extensions (DNSSEC):

    DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks. DNSSEC provides protection against malicious or forged answers by adding digital signatures into DNS data, so each DNS response can be verified for integrity and authenticity.

    Cisco Prime Network Registrar 9.0 and earlier Authoritative DNS Server do not support signing of zones. Starting from Cisco Prime Network Registrar 10.0, Authoritative DNSSEC support adds authentication and integrity to DNS zones. With this support, Cisco Prime Network Registrar DNS server is able to support both secure and unsecure zones. For more information, see the *"Managing Authoritative DNSSEC" section in the Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*.
  - Secure DNS server activity with ACLs:
    - Restricting Zone Queries—The *restrict-query-acl* attribute on the DNS server serves as a default value for zones that do not have *restrict-query-acl* explicitly set.
    - Restricting Zone Transfer Requests—Use the *restrict-xfer-acl* attribute to filter the zone transfer request to the known secondary servers.
    - Restricting DDNS Updates—Use the *update-acl* attribute to filter DDNS packet from the known DHCP servers.
  - Secure zone transfers and DNS updates using TSIG or GSS-TSIG:

    Zone transfer in secure mode supports both HMAC-MD5 based TSIG and GSS-TSIG. You can add an optional TSIG key or GSS-TSIG keys (see the *"Transaction Security" or "GSS-TSIG " sections in the Cisco Prime Network Registrar 10.1 DHCP User Guide*) to the master server address by hyphenating the entry in the format *address–key*. For each entry, click **Add IP Key**.

    For more information, see the *"Creating a Zone Distribution" section in the Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*
  - Randomize Query IDs and Source Ports.

    - DNS Rate Limiting—See the *"Managing Caching Rate Limiting" section in the Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*.
    - Separate Recursive Server and Authoritative Server roles.

- DHCP specific considerations include:
    - Assure DHCPv4 and DHCPv6 traffic from the "external" sources is blocked on routers and that only valid relay agents are enabled to forward packets to the DHCP servers.
    - Use DHCP Guard and similar services on switches:

      See https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.html

      See https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/ip6-dhcpv6-guard.pdf

    - Use the Chatty Client Filter—See the *"Preventing Chatty Clients by Using an Extension" section in the Cisco Prime Network Registrar 10.1 DHCP User Guide*.

- Consider using external user authentication as password rules (that is, change frequency, length, and difficulty checks) can typically be implemented for Active Directory (LDAP) and RADIUS users. See the *"External Authentication Servers" section in the Cisco Prime Network Registrar 10.1 Administration Guide*.

APPENDIX F

Optimizing VM Performance

See the following sections for optimizing VM performance:

Recommended UCS Settings

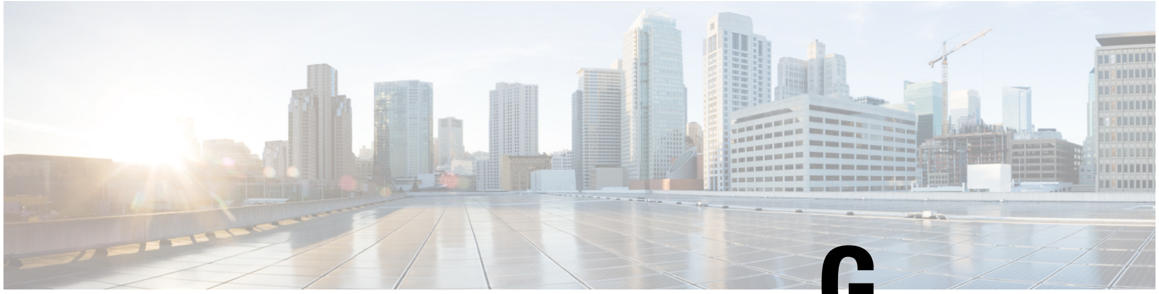
On UCS servers with RAID configured, for improved performance, it is recommended to set the Requested Write Cache Policy on the RAID controller as **Write Back** instead of **Write Through** (the default setting). The downside of using the Write Back option is that you may lose some data if a system failure occurs before the data in the cache is written to disk. Therefore, we recommend to set the Requested Write Cache Policy on the RAID controller to **Write Back Good BBU**. In this mode, the controller enables Write Back caching when the Battery Backup Unit (BBU) is installed and charged. It provides a good balance between data protection and performance.

NUMA Optimization

If you do not configure the virtual CPUs correctly, you may run into Non-Uniform Memory Access (NUMA) performance issues. To avoid this issue, do not configure a virtual machine from using more virtual CPUs than a single NUMA node. Otherwise, it will be scheduled across multiple NUMA nodes causing memory access degradation. Generally, this means to assign no more virtual CPUs to a virtual machine than the total number of physical cores of a single CPU socket.

Hyperthreading Considerations

When using hyperthreading virtual CPUs, note that the general CPUs utilization is 30% not 100% as threading allows for other work to be done when the main thread is stalled waiting for something. The exact numbers may be different as it depends on the workloads.



APPENDIX G

Configuring Network Access on RHEL/CentOS 7.x Using nmcli

This appendix contains the following section:

Configuring Network Access on RHEL/CentOS 7.x Using nmcli

The **NetworkManager** command-line tool (**nmcli**) provides a command line way to configure networking by controlling NetworkManager. This section provides only an overview with some examples to help you learn how to use nmcli to configure network access on the virtual appliance.

In a departure from previous approaches to network interface configuration, NetworkManager deals with both connections and interfaces (also known as devices). Connections are configured with IP addresses, gateways, DNS servers, and then applied to interfaces (devices). This is a critical change from the past way of configuring network access on CentOS Linux.

There are two nmcli commands that are of general usefulness:

- The **nmcli d** command lists all available network interfaces (devices).
- The **nmcli c** command lists all available configurations.

Use the above two commands frequently as you learn to use nmcli.

Follow the steps below to configure an IP address for an interface on your virtual appliance. Typically, these commands are typed directly into the console of the virtual appliance. If you are already connected through the network (for example, by **ssh**), then making changes to the network interface configuration can be problematic, as you may also lose network connectivity (and thereby your ability to issue nmcli commands) at any point in the process.

Step 1 Make sure that the interface does not block nmcli. The **nmcli d** command lists the existing interfaces. If the interface you want to configure is listed as **unmanaged**, then NetworkManager has been explicitly blocked from configuring this interface. Until you remove this blockage, no nmcli command will have any effect on this interface. Note that you may not need to perform this procedure unless the interface is listed as **unmanaged**. Follow the steps below to allow it to be managed by NetworkManager:

a) Remove the line NM_CONTROLLED-no from the file **/etc/sysconfig/network-scripts/ifcfg-***interface*, where *interface* is the interface name listed in the **nmcli d** command. If there is no file with this name, then you do not need to perform this procedure.

b) Tell the NetworkManager to read the configuration files again by using the following command:

```
nmcli connection reload
```

Note Manual changes to any **ifcfg** file will not be noticed by NetworkManager until the **nmcli connection reload** command is issued.

Step 2 Make sure that there is no current configuration for the interface that you want to configure. If you want the configuration that you create to be the default for the interface and there are multiple configurations associated with an interface, it may lead to confusion when the system reboots. The **nmcli c** command lists the existing configurations. If you see any existing configurations, examine them to see if they apply to the interface you want to configure. An easy way to do this is to use the following command:

```
nmcli con show config | grep interface
```

If you see any output, you should remove the configuration *config* using the following command:

```
nmcli con delete config
```

Note There is often a configuration called "Wired connection 1" which needs to be deleted.

Step 3 Create the configuration and associate it with the interface (device) in one command. This command only creates the configuration and associates it with the interface, it does not apply it to the interface.

```
nmcli con add type ethernet con-name config ifname interface ip4 ip/netmaskwidth gw4 gateway
```

where *config* is the name of the configuration, which can be anything (including the name of the interface), *interface* is the name of the interface (device), *ip* is the IPv4 address, *netmaskwidth* is the network mask width, and *gateway* is the IPv4 gateway address.

For example (type all in one line):

```
nmcli con add type ethernet con-name my-office ifname ens160 ip4 10.10.24.25/24 gw4 10.10.20.174
```

Step 4 Add the DNS server to the configuration for the interface (device):

```
nmcli con mod config ipv4.dns dnsip
```

where *dnsip* is the IPv4 address of the DNS server and *config* is the name of the configuration.

For example:

```
nmcli con mod my-office ipv4.dns 72.63.128.140
```

You can add two DNS addresses as given below:

```
nmcli con mod my-office ipv4.dns "72.63.128.140 72.63.111.120"
```

Note This will replace any previously set DNS servers. To add to an previously set DNS entry, use the + before ipv4.dns as shown below:

```
nmcli con mod test-lab +ipv4.dns "72.63.128.140 72.63.111.120"
```

Step 5 Apply the configuration to the interface, which will bring up the interface if it was not already running:

```
nmcli con up config
```

where *config* is the name of the configuration.

Step 6 Use the following command to examine information about a connection:

```
nmcli -p con show config
```

This will typically scroll off of the console screen, leaving the beginning unreadable. To allow you to move back and forth and examine the output easily, use the following command:

```
nmcli -p con show config | less
```

From this, you can see the entire configuration. You can modify things in the configuration using the following command:

```
nmcli con mod config something.other new-value
```

For example:

```
nmcli con mod my-office wifi-min.key-cntl wpa-psk
```

Step 7 Use the **set-hostname** command to set the hostname for the system:

```
hostnamectl set-hostname hostname.domain
```

Note This must be done before registering the local to the regional. Otherwise, an error will result about "localhost" already existing.

where *hostname* is the hostname you want to use and *domain* is the domain name, ending with .com, .org, and so on. It is important to include the domain name (along with the .com, .org, or whatever ending is appropriate), since this is used as the default for DNS lookups.

For example:

```
hostnamectl set-hostname my-server.gooddomain.com
```

Step 8 After you configure the networking, you **must** restart Cisco Prime Network Registrar for the interfaces to be properly discovered by Cisco Prime Network Registrar. Use the following commands to restart:

- For local cluster:

  ```
  # systemctl restart nwreglocal
  ```

- For regional cluster:

  ```
  # systemctl restart nwregregional
  ```

If you fail to restart, it will result in a misconfigured registration at the regional.

To develop a complete understanding of the usage of nmcli, search the Internet for online resources on nmcli and CentOS 7.7.

APPENDIX H

Changing the IP Address Using nmcli

This appendix contains the following section:

Changing the IP Address Using nmcli

If you need to change the IP address of a local or regional cluster, you can make these changes very easily using nmcli.

Step 1 Find out what connection is associated with the interface you want to change. You can use **nmcli d** to find the devices, and **nmcli c** to see which connections are associated with the device for which you wish to change the IP address.

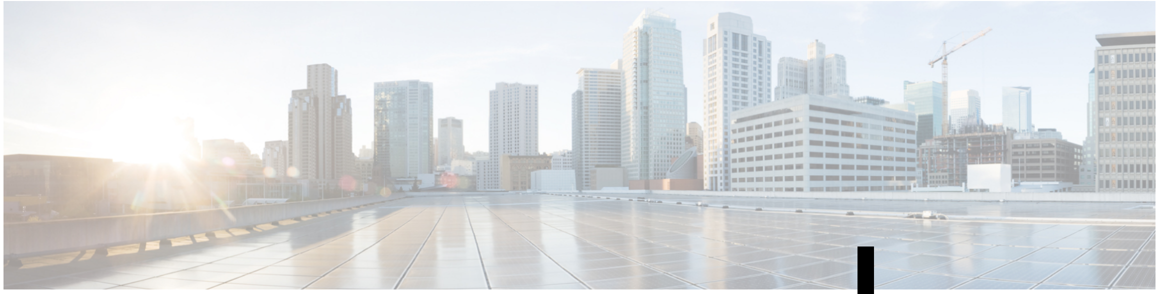
Step 2 Configure the connection with the new IP address:

```
nmcli con mod connection ip4 new-ip-address
```

Step 3 Apply the changed connection to the interface to which it is associated. This will actually change the IP address:

```
nmcli con up connection
```

Step 4 After changing the IP address of any system running Cisco Prime Network Registrar (like the virtual appliance), you need to restart in order to get the management server to recognize the new IP address of the system. For a local cluster, use the **systemctl restart nwreglocal** command or for a regional cluster, use the **systemctl restart nwregregion** command.



APPENDIX I

Authoritative DNS Capacity and Performance Guidelines

This chapter provides information on Authoritative DNS capacity and performance guidelines to help with system sizing for 64-bit Cisco Prime Network Registrar 8.3.5.4 and later.

DNS System Deployment Limits

Cisco Prime Network Registrar makes the following recommendations on maximum Authoritative DNS System configuration sizes. The following recommendations are as per Cisco Prime Network Registrar Authoritative DNS server which can be a primary, primary HA, or secondary server. A redundant DNS architecture will contain multiple of these types of servers all servicing the same data. Therefore, the capacity can be expanded horizontally by introducing a new set of servers. These recommendations are guidelines to ensure a properly functioning DNS deployment.

Note DNSSEC enabled zones (Cisco Prime Network Registrar 9.1 and later versions) will include auto-generated RRs that significantly increase the number of RRs in the zone.

- Maximum of 25 million RRs per Authoritative DNS server (primary, HA pair, or secondary server), ideally not to exceed 2 million RRs per zone. Multiple DNS primary servers can be used for deployments requiring more RRs.
- Maximum of 10000 zones per Authoritative DNS server (primary, HA pair, or secondary server). Multiple DNS primary servers can be used for deployments requiring more zones.
- Maximum of 4 secondary servers per primary or HA pair.
- Maximum of 2 tiers of secondary servers (first tier secondaries and second tier secondaries).
- Maximum of 2 second tier secondary servers per first tier secondary server.

DNS Database Architecture

The Authoritative DNS servers utilize a combination of in-memory cache and on-disk databases to store and maintain authoritative RR data. For sizing purpose, assume an each RR requires 300 bytes of memory for the RR cache and 300 bytes of disk space for the RR DB. The CSET DB has a higher disk space requirement for each RR since it records changes to the RR set, but those changes are capped to the number of history changes kept per zone.

RR DB

- Database that stores all RRs (protected and unprotected) for the zones configured on a DNS server.
- On primary DNS servers, RR data edits are written to the RR DB either through administrative actions (that is, RR adds), or DNS updates and zone scavenging. On secondaries, the RR DB is written through zone transfers.
- The RR DB is required for all ADNS servers (primary/secondary).

RR Cache

- Increases query performance by storing a subset of the RR DB data (stores entire name sets).
- Most active RR data is stored to RR cache dynamically as part of RR DB lookups generated by DNS query processing.
- The memory foot print of the RR Cache is capped by a configurable DNS server attribute (*mem-cache-size*). When the maximum cache size has been reached, the DNS server will remove older entries from the cache to make room for newer entries. Each RR requires approximately 300 bytes of memory.
- DNS server reload/restart causes the RR cache to be deleted. When the server starts up again, it is rebuilt based on query traffic.
- The RR cache is required for all ADNS servers (primary/secondary).

CSET DB

- Database that stores RR changes (adds, deletes, protection changes, and refreshes) needed to respond to the incremental zone transfer requests (IXFRs).
- RR changes are first stored in the RR DB and then persisted to the CSET DB.
- For DNS servers that do not need to service incremental zone transfers (that is, secondaries that do not send outbound IXFRs), server performance can be increased by disabling persisted change sets (*csetdb-persist-csets*). By default, changes are automatically persisted to the CSET DB.
- DNS maintains only a limited configurable number of changes (*csetdb-htrim-max-cset-kept*) and automatically trims entries when the maximum has been reached. Trimming helps limit the database size. For deployments with DNS updates, it is recommended that the number of changes kept is increased to avoid full zone transfers.
- If the CSET DB is deleted, the DNS server will create an empty database and respond with full zone transfers (AXFRs) until new zone history data is populated into the database.

HA DB

- Database that stores state information about the DNS HA pair as well as data about RR changes during a communications interrupted or partner down event.
- Only applicable on primary HA DNS servers (main and backup).
- If the HA DB is deleted, HA synchronization causes all zone data to be pushed from the HA main to the HA backup.

DNS System Sizing

A Cisco Prime Network Registrar DNS deployment can be categorized as small, medium, or large depending on the number of RRs/zones, DNS update activity, and recovery time during an outage or update. The number of zones can have an impact on the size of the deployment, primarily the number of RRs is the deciding factor. Also, if the DNS deployment requires a large number of RRs/zones, it is recommend that multiple DNS deployments be used - ideally segregating the data appropriately so that related zones/RRs are configured together.

Note To ensure a properly functioning Authoritative DNS system, it is important to monitor system disk space and memory. If the Authoritative DNS server runs out of memory, it will crash. If it runs out of disk space, it will no longer be able to service requests and the databases may become corrupt and unusable.

Regional Management of DNS Deployments

The regional server provides license management of all Cisco Prime Network Registrar local clusters, and allows for central management and replication of Cisco Prime Network Registrar DNS deployments. Follow the below recommendations for system sizing and configuration adjustments to be made when using regional DNS cluster management:

- A minimum of 4 CPUs
- A minimum of 8 GB of RAM
- Disk space should be at minimum an aggregate of the disk size of all the managed DNS (main) primary clusters.
- On large DNS deployments, replication of unprotected RRs should be disabled (*poll-replica-rrs*).

Small Deployment

- 1-1000 RRs and 1-100 zones
- Mainly static data; zone edits are primarily done by administrators.
- Typically consists of one primary and a secondary server.
- DNS Caching server is not required or can be handled by hybrid mode.
- DNS can be recovered from a shadow backup within a matter of minutes with little to no impact on production.

- A minimum of 2 CPUs
- A minimum of 4 GB of RAM
- A minimum of 10 GB of disk space

Medium Deployment

- 1000-100,000 RRs and 100-1000 zones
- A pretty even mix of static and dynamic data; 100 updates per second or less.
- Typically consists of one primary and two to four secondaries.
- Typically consists of two to four DNS Caching Servers. DNS Caching Servers must be deployed on separate machines or VMs.
- DNS can be recovered from a shadow backup within an hour with minimal impact to production.
- A minimum of 4 CPUs
- A minimum of 8 GB of RAM
- A minimum of 25 GB of disk space. On the primaries, the number of change sets kept (*csetdb-htrim-max-cset-kept*) should be increased. The value will depend on how many DNS updates are handled by the system, but should be between 1000 and 5000.

Large Deployment

- 100,000-25,000,000 RRs and 1000-10,000 zones
- Dynamic data makes up a larger percentage of the data; thousands of updates per second.
- Typically consists of two primaries (DNS HA pair) and four secondaries.
- Typically consists of four or more DNS Caching servers.
- DNS recovery is complex and must be done during a maintenance window; DNS servers can take an hour or more to recover from a shadow backup.
- A minimum of 8 CPUs
- A minimum of 16 GB of RAM. The DNS RR cache memory size (*mem-cache-size*) should be increased (approximately 300 bytes per RR, but not to exceed 2,000,000 KB).
- A minimum of 100 GB of disk space. On the primaries, the number of change sets kept (*csetdb-htrim-max-cset-kept*) should be increased. The value will depend on how many DNS updates are handled by the system, but should be between 5000 and 10,000.

APPENDIX J

Caching DNS Capacity and Performance Guidelines

This chapter provides information on Caching DNS capacity and performance guidelines to help with system sizing. The recommendations are based on 64-bit Cisco Prime Network Registrar 8.3.5.4 and up.

DNS System Deployment Limits

Cisco Prime Network Registrar makes the following recommendations on maximum Caching DNS System configuration sizes. A redundant DNS architecture will contain multiple servers, therefore the capacity can be expanded horizontally by adding on new servers. Although Cisco Prime Network Registrar does not put hard limits on many of its configuration objects, these recommended maximums are to ensure a properly functioning DNS deployment.

- Maximum of 100 DNS Views
- Maximum of 500 Exceptions and Forwarders
- Maximum of 3 DNS RPZ Firewall Objects. Note that the RPZ zones can have many thousands of entries.
- Maximum of 12 DNS Firewall Objects (non-RPZ) with no more than 200 domains each
- Maximum of 30 DNS64 Objects

Caching DNS System Sizing

A Cisco Prime Network Registrar Caching DNS deployment can be categorized as small, medium, or large depending on the number of servers and query load. The following sections are an indication of how to provision the Caching DNS server based on the deployment size.

Note To ensure a properly functioning DNS system, it is important to monitor system disk space and memory.

Small Deployment

- Typically consists of 2-4 DNS Caching servers. DNS Caching server maybe co-located with the DNS Authoritative server using hybrid mode.
- Typically less than 1,000 Queries per second
- A minimum of 2 CPUs
- A minimum of 4 GB of RAM
- A minimum of 10 GB of disk space

Medium Deployment

- Typically consists of 2-4 DNS Caching servers. DNS Caching servers must be deployed on separate machines or VMs.
- Typically between 1,000 and 50,000 queries per second
- A minimum of 4 CPUs
- A minimum of 8 GB of RAM
- A minimum of 25 GB of disk space

Large Deployment

- Typically consists of 4 or more DNS Caching servers.
- Typically more than 50,000 queries per second
- A minimum of 8 CPUs
- A minimum of 16 GB of RAM. The DNS RR cache memory size (*mem-cache-size*) should be increased (approximately 300 bytes per RR, but not to exceed 2,000,000 KB).
- A minimum of 50 GB of disk space

Possible Impacts on Caching DNS Server Performance

The following is a list of common system components and Cisco Prime Network Registrar configurations that may have an impact on performance:

- Firewalls and Connection Tracking may have a negative impact on performance especially in medium to large deployments where the firewall may drop a significant amount of DNS traffic.
- Excessive logging—Either enabling too many log settings, packet logging, or debug logging can decrease server performance.
- IPv6 only networks configured to also use IPv4. IPv6 networks should be configured in IPv6 only mode in order to prevent the server wasting cycles on failed IPv4 communication.

APPENDIX K

DHCP Capacity and Performance Guidelines

This section provides capacity and performance guidelines for Cisco Prime Network Registrar 9.0 and later, and also for 64-bit versions of Cisco Prime Network Registrar 8.3.2 and later.

The goal of this section is to provide an understanding of what influences the capacity and performance of the servers to help in planning how to deploy the product and what to consider when purchasing hardware for these systems. These recommendations primarily apply to the Linux releases.

When multiple clusters are running on virtual machines, the underlying physical hardware needs to be at least the sum of the individual virtual machine requirements. Also, it should be noted that high availability solutions (that is, HA-DNS or DHCP failover) should not have both partners located on the same physical machine in virtual environments, as that makes the hardware a single point of failure.

Note These are just guidelines, as actual performance may vary based on variances in the live deployment.

Local Cluster DHCP Considerations

There are two common questions concerning DHCP capacity:

1. How many leases can I put on a single server?
2. If I want to put *n* leases on a server, what sort of server should I purchase or virtual machine should I configure?

Number of Leases Allowed on a Single Server

When discussing about the capacity of a server, the number of DHCP operations per second that the server can support is the most important issue. There are two regimes that affect the operations per second that the server will be required to support:

- **Steady state**: Made up of existing DHCP clients renewing their leases and the arrival of DHCP clients not previously seen by the server.

- **Avalanche**: Made up of a large (possibly vast) quantity of existing DHCP clients, all contending at the DHCP server to get an address. This situation can occur with restoration of power after a failure or perhaps a blanket reset of many customer devices. This can often consist of tens of thousands of DHCP clients all trying to get an IP address from the DHCP server at the same time. It can even be hundreds of thousands of DHCP clients trying to get an IP address.

For the steady state situation, the number of DHCP clients and the lease times of the leases they are granted will dominate the load.

The operations per second required by a DHCP client population is largely driven by the size of that client population coupled with the lease times (both expiration and renewal times) that are granted to that population. These values are all configurable, and so the actual requirements can vary dramatically.

Following table presents a range of these data points showing the operations per second required for various client populations and differing lease times:

Table 5: Client lease Times

Operations per Second						
	Client Lease Times					
Active Leases	30 min	1 hr	1 day	1 week	2 weeks	30 days
1,000	1	1	-	-	-	-
10,000	11	6	-	-	-	-
100,000	111	56	2	-	-	-
500, 000	556	278	12	2	1	-
1,000,000	1,111	556	23	4	2	1
1,500,000	1,667	833	35	5	2	1
2,000,000	2,222	1,111	46	7	3	2
4,000,000	4,444	2,222	93	13	7	3
6,000,000	6,667	3,333	139	20	10	5

The lease times granted to the clients has an overwhelming influence on the steady state operations per second required on the DHCP server. A server's operations likely include a mix of lease times, as lease times for clients without an existing lease are limited by the failover Maximum Client Lead Time (MCLT), and there may be other operations (such as from "bad" clients or lease query requests).

The DHCP server will not collapse under any client load, but it can take seconds to minutes to work through tens or hundreds of thousands of clients. It is for this reason that our recommendations for the operations per second that the server is required to support in steady state tends to be on the lower side; so that the server has plenty of headroom to process the eventual avalanche.

DHCP operations per second

It is difficult to give concrete recommendations regarding the operations per second that the DHCP server can deliver to DHCP clients, since there are many factors that are involved in this aspect of DHCP server performance.

Cisco has measured DHCP server performance in the lab well above 20,000 operations per second. However, that was a DHCP server which was configured specifically for maximal performance (no failover, no logging, no lease history, no extensions, and no LDAP). Almost every feature that you configure in the DHCP server costs some amount of performance; frequently trimming 10 percent or so off of the previous performance. Some features, for instance LDAP lookup or running with the Prime Cable Provisioning (PCP) product, can have a much bigger effect on performance; since the LDAP lookup or PCP interaction with the DPE requires interlocking with a separate server and the round-trip delays that entails, prior to even processing the incoming DHCP request. Failover costs at least 10 percent, basic logging can also cost 10 percent of performance or more. Extensions will cost an unpredictable amount on top of a constant overhead to just call the extension. The time spent in the extension is also synchronous and additive to the time it takes to process every DHCP request.

The upshot of all of this is that there is no way to reasonably predict the operations per second that the DHCP server will be able to supply given a particular load when running on a particular hardware configuration with a particular software configuration.

Also, the operations per second load placed on the DHCP server by the constant requirement to process DHCP RENEW requests from DHCP clients ("steady state") is frequently overshadowed by the requirements to process large "avalanche" loads, where many thousands to tens of thousands of DHCP clients attempt to get service from the DHCP sever in a very short time. These events can be generated by a power outage among the DHCP clients or network element resets that will provoke many thousands of DHCP clients to re-DISCOVER / re-SOLICIT for IP addresses. The DHCP server needs to be able to process these loads, which typically dwarf the loads generated by the steady state RENEWAL traffic.

Cisco recommends that the steady state load on the DHCP server be limited to a few hundred operations per second, in part to ensure that headroom exists to process the avalanche loads presented to the DHCP server in unusual circumstances. We have customers which have high performance hardware and excellent monitoring regimes that run with several hundred operations per second and sometimes more with constant load. They are running successfully, in part because they are careful to ensure that they do not let the avalanche load size get too large; by limiting the number of active leases on each server.

The DHCP server has several features to reduce the load on the server and help it service requests as quickly as possible, especially under avalanche conditions:

- **Defer-lease-extension**

  By default, the server will defer extending a lease to a client if the client "renews" before its expected renewal time. This usually helps out with avalanches if the outage that triggered it was short (less than 1/2 the lease time) as a large number of clients will avoid the need for a disk write (and failover update).

- **Reduced logging when overloaded**

  By default, the server will reduce the logging when the request buffers in use exceeds 67 percent of the configured buffers. As logging can be costly, this allows the server to handle additional capacity when very busy. This feature can be disabled. Note that the server dropping requests under avalanche conditions should be expected, as that is the only way that the server can shed load, and the client will re-transmit the request. Under steady state conditions, if a server is frequently dropping requests, that is probably an indication that it is unable to handle the load.

- **Chatty Client Filter**

Use of this provided extension is highly recommended in all service provider networks. This extension monitors client activity and blocks those clients that are considered to be "chatty". Once a client is blocked, it is unblocked if it quiets down. In many service provider networks, the Chatty Client Filter can reduce the requests to the server by about 50 percent. However, the Chatty Client Filter requires careful tuning and requires reviewing that tuning periodically to assure traffic patterns have not changed. For more details, see the *"Preventing Chatty Clients by Using an Extension" section in the Cisco Prime Network Registrar 10.1 DHCP User Guide*.

- **Discriminating Rate-Limiter**

  The Discriminating Rate-Limiter reduces downtime after an outage in service networks by restricting the rate of DISCOVER and SOLICIT requests while still honoring all RENEW requests. The basic concept is to assure a client that was offered a lease is able to complete getting that lease. For more details, see the *"Setting Advanced DHCP Server Attributes" section in the Cisco Prime Network Registrar 10.1 DHCP User Guide*.

Number of leases you want on a server

If the only thing that mattered was the steady state operations per second load, then looking at the table above and with a one week lease time, you could imagine 12 million or even 24 million leases would pose no problem. However, there are other factors as follows:

- **Avalanche load**: Which may or may not scale with the total leases on a server.
- **Reload time**: The server needs to refresh its in-memory cache whenever it is reloaded, and the reload time scales linearly with the number of active leases in the server.
- **Service interruption impact**: If you have millions of leases to start with, then there is probably a relationship between DHCP clients and customers of some sort. You probably want to avoid having a DHCP server have so many leases that having an entire DHCP failover pair out of service for a few hours would cause an unacceptable risk to your business. While DHCP failover will prevent almost all service interruptions and you probably have no single points of failure, sometimes two things do fail at the same time. It is possible that both servers in a DHCP failover pair will fail for a while, and in the unlikely event that this should happen, the difference between having 2 million DHCP clients on a server and 10 million DHCP clients on a server could be very important. With the reasonable DHCP lease times, only some small percentage of DHCP clients will have their leases expire every hour that a failover pair is out of service.

Recommendations

Cisco strongly recommends that you limit the total active leases on a single DHCP server (or server failover pair) to 6 million leases. In addition, Cisco strongly recommends that you limit the steady-state operations per second requirement to 500 operations per second, in order to have sufficient bandwidth to handle avalanche and other exceptional conditions.

Scale out, not up, beyond some point!

Instead of loading vast quantities of leases into a single DHCP server or failover pair, consider keeping the number of leases to a more modest number, say 3 to 5 million leases. Cisco resource limits set the warning level to be 6 million leases, and it is wise to configure more like 4 million leases per server to allow for growth in the future. While managing multiple failover pairs is more work than just managing one failover pair, the ease of management of a server that is more modestly loaded with 3 to 4 million leases will pay long term dividends, to say nothing of the impact on your business in the unlikely event that an entire server pair should fail for a couple of hours.

Request Latency

It should be noted that the DHCP server's design is optimized to respond to large numbers of requests quickly – it is not optimized to have the lowest latency for each request. This often complicates testing for scale as the server's performance with a few simultaneous requests may not show its true processing power.

Server Considerations

If you do not need a lot of operations per second and do not have a lot of leases on the server, pretty much any server will do. For the purpose of this discussion, we will assume that you want to get the maximum performance possible.

For DHCP, the general recommendations in terms of physical or virtual server considerations are as follows:

1. Disk write performance is the primary consideration. SAN storage, SSD, or 15K RPM HDD disks are recommended. The DHCP server is disk write performance limited, because it must commit to disk any changes to leases (primarily assigning a lease to a new client and extending the lease times on a lease) before responding to a client. Configuration options, such as failover, lease history, and DNS updates also increase the disk write load on the server, as each of these require additional write operations. There are up to 4 writes for a lease on the server that grants, extends (renew/rebind), releases, or expires a lease plus 1 more write on the failover partner as follows:

    - The lease itself (before responding to the client). Generally, this also results in a failover binding update if failover is used.
    - A history record (this only occurs if lease history is enabled and the lease was leased but is no longer).
    - The partner writes the lease when it receives a failover binding update (if failover used).
    - The lease after the receipt of the failover binding update acknowledgement (if failover used).
    - The lease after the DNS update completes (if configured and initiated for the lease).

    A server may also initiate writes at other times for a lease, such as for failover state transitions for the lease, when balancing failover pools, and because of user action (such as to force a lease available). The DHCP server lease state database disk space requirements are generally as follows:

    - 1 KB for each configured or active lease, and
    - If lease history is enabled, 1 KB for each historical record.

    These numbers can be reduced about 30 percent if the lease record compression is enabled (see the DHCP server's *server-flags* attribute).

    Note These numbers need to be multiplied by 3 to accommodate the shadow backups. These numbers just reflect the lease state database and no other system requirements.

2. Memory (RAM) is secondary, with 64-bit support, memory limits are not generally a concern provided the system has sufficient memory. It is important to have sufficient "free" memory for the file system to

be able to keep the entire DHCP lease state database in memory to avoid the need for disk reads. A rough rule of thumb is to assume:

- 1 KB for each configured or active lease for the DHCP server's memory usage. Configuration options, such as DNS update and the length of host and domain names and the amount of option-82 (DHCPv4) or Relay-forward message (DHCPv6) data can influence this rule of thumb.
- 1 KB of "free" memory for the file system cache for each lease (configured or active) and,
- If lease history is enabled, 1 KB of "free" memory for the file system cache for each history record (this will be more difficult to judge as it depends on how frequently leases expire or are released).

3. CPU performance is the least significant as the processing required to service requests is generally low. On the other hand, avalanche processing is largely handled with just CPU cycles and minimal disk writes. So, if you have a large avalanche possibility, invest in a system with good CPU capability and fast network interfaces. Most modern multi-processor systems should be sufficient for modest avalanche loads. For higher capacity/performance applications, both the CPU speed and number of effective processors should be higher. The DHCP server is highly multi-threaded, so that, additional CPU cores will help DHCP server performance up to a point. Due to the requirements for some minimal amount of locking inside the DHCP server, performance will improve when adding up to 12 CPU cores. Beyond 12 CPU cores, there is not much of any performance improvement due to the requirements for synchronization.

Regional Cluster DHCP Considerations

The regional cluster disk space requirements are dictated by several factors for DHCP:

1. **Lease history**—When lease history is enabled at the local clusters, by default, the regional cluster collects this history from the local clusters for longer term storage (the default is to retain these records for 24 weeks, see the CCM server's *trim-lease-hist-age* attribute). As mentioned above for the DHCP server, each lease record (active and historic) should be assumed to require about 1KB, but this should be multiplied by 3 to accommodate backup requirements – thus, 3 KB/lease record. The regional cluster disk space needed will depend on the total number of lease history records, which depends on the number of servers, their lease counts and client activity levels, and the period of time over which the history is to be retained. In very large service provider networks, this can easily be 100 GB or more.

Note These disk space requirements can be reduced to 30 percent for the lease history data by enabling lease record compression in Cisco Prime Network Registrar 9.0 and later (see the CCM server's *lease-hist-compression* attribute).

2. **Network utilization**—The regional cluster also collects subnet and prefix utilization data from the local clusters (by default, every hour and retained for 24 weeks; see the CCM server's *addrutil-poll-interval* and *addrutil-trim-age* attributes). While each record is about 1/2 KB (the scope/prefix names, owner, region, selection tags, and other data cause the size to vary), this can add up if there are many subnets and prefixes, a 10,000 scope/prefix deployment can use 10 GB over a 24 week period (not considering the backup requirements, which make this 30 GB).

INDEX