Cisco Prime Network Registrar 11.0 Installation Guide

First Published: 2021-04-23

Last Modified: 2022-09-09

CONTENTS

CHAPTER 1

Installation Overview

This chapter contains the following sections:

Overview

This guide describes how to install Cisco Prime Network Registrar Release 11.0 on Linux operating system. 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, see the *Cisco Prime Network Registrar 11.0 Administration Guide*.

- For details about commands available through the Command Line Interface (CLI), see the *Cisco Prime Network Registrar 11.0 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
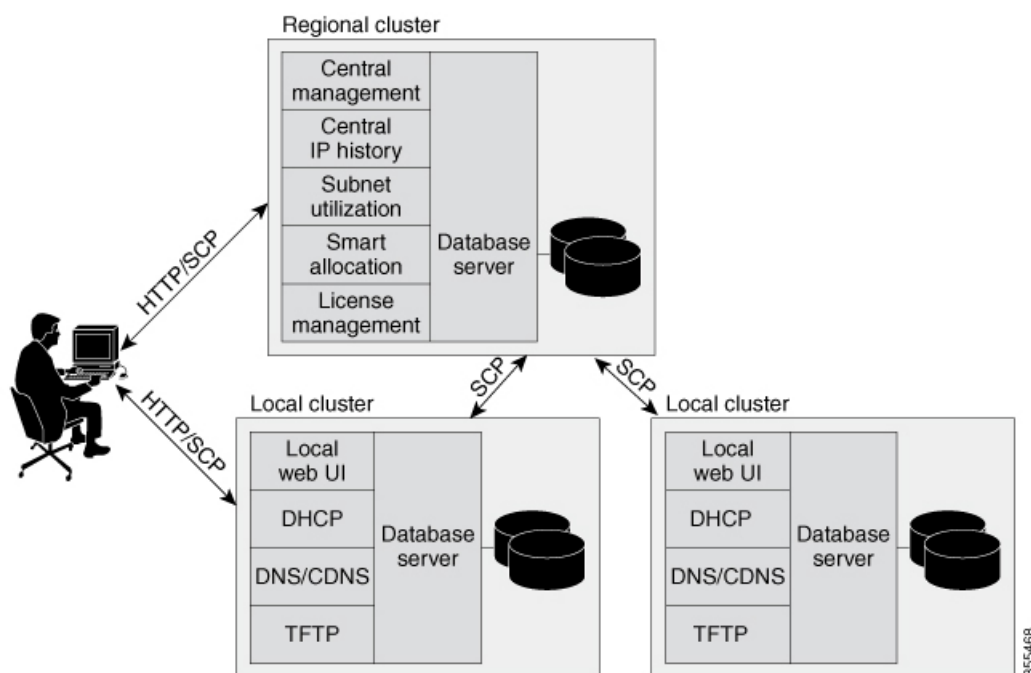
Sensitive Data Exposure

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 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

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.

Installation Requirements

This chapter contains the following sections:

System Requirements

Review the system requirements before installing the Cisco Prime Network Registrar 11.0 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—Ensure that your Cisco Prime Network Registrar machine runs on the Linux Operating Systems as described in the Server 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 Edge 89, Mozilla Firefox 86, and Google Chrome 89. Internet Explorer is not supported.

  - The CLI runs in a 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	Minimum Requirement
OS version[1]	Red Hat Enterprise Linux ES/CentOS 7 and 8 64-bit[2]. **Note:** The newest level tested with this release is RHEL 8.3.
Minimum disk space	200 GB For best performance, Cisco recommends use of SSD drives.
Minimum memory	16 GB
Minimum CPUs[3]	4 CPUs

[1] Cisco Prime Network Registrar 11.0 is only supported on 64-bit operating systems.

[2] Cisco Prime Network Registrar 11.0 has been tested by Cisco with Red Hat Enterprise Linux ES 7 and 8, running standalone or on VMware (ESXi 7.0) 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] 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 8.3 and CentOS 8.1. 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

The following x86_64 (64-bit) packages (over and above the Java Run-Time) are required to install Cisco Prime Network Registrar on Red Hat Enterprise Linux or CentOS. If you use the **yum** or **dnf** commands to install Cisco Prime Network Registrar, then these packages are installed as part of the installation process if

required. If you use the **rpm** command to install Cisco Prime Network Registrar, then you must install these packages separately.

Table 2: Packages to Install

Package Name	Package Version	
	For RHEL/CentOS 7.x	**For RHEL/CentOS 8.x**
glibc	2.17 or later	2.28 or later
krb5-libs	1.15.1 or later	1.17 or later
ldns	(Included with Cisco Prime Network Registrar)	1.7.0 or later
libcurl (built with OpenSSL)	7.29.0 or later	7.61.1 or later
libevent	(Included with Cisco Prime Network Registrar)	2.1.8 or later
libgcc	4.8.5 or later	8.3.1 or later
libicu	(Included with Cisco Prime Network Registrar)	60.3 or later
libstdc++	4.8.5 or later	8.3.1 or later
libxml2	2.9.1 or later	2.9.7 or later
net-snmp-libs	5.7.2 or later	5.8 or later
openldap	2.4.44 or later	2.4.46 or later
openssl-libs	1.0.2k or later	1.1.1c or later
tcl	8.5.13 or later	8.6.8 or later
zlib	1.2.7 or later	1.2.11 or later

To find out the packages required, you can also issue the following command on your Linux system if you have downloaded the RPM:

rpm -qpR *rpm_package_file*

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 11.0 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 the **yum install**, **rpm -i**, or **dnf install** command.

Note If you use the **rpm -i** command to install Cisco Prime Network Registrar, you may have to install the dependencies manually.

License Files

Cisco Prime Network Registrar 11.0 supports both Smart Licensing and traditional licensing.

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation**: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).

- **Unified Management**: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- **License Flexibility**: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

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

In case of traditional licenses (FLEXlm), you purchase a perpetual license for a version and use it until Cisco Prime Network Registrar servers are upgraded to a newer major version. In case of Smart Licensing, the

licenses are not installed on the individual Cisco products, instead, they are kept in a centralized system called Cisco Smart Software Manager (CSSM) or CSSM On-Prem (Satellite), in customer specific Smart accounts.

For more details on the Licensing, see the *"Licensing" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

The Cisco Prime Network Registrar 11.0 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, 9.x, and 10.x versions. For Cisco Prime Network Registrar 11.0, 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:

Smart Licensing:

- PNR-System—Licenses the CCM services. This license is mandatory if you want to run Cisco Prime Network Registrar.

- PNR-DHCP—Licenses DHCP/TFTP services and, optionally, an initial count of leases.

- PNR-DNS—Licenses the authoritative DNS services and, optionally, an initial count of RRs.

- PNR-Caching DNS—Licenses Caching DNS services and, optionally, an initial count of servers.

- PNR-PLR—Licenses Permanent License Reservation for all services.

- PNR-DHCP Container—Licenses DHCP services on containers.

- PNR-DNS Container—Licenses authoritative DNS services on containers.

- PNR-Caching DNS Container—Licenses Caching DNS services on containers.

Traditional Licensing:

- 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 11.x license. The expiration date for each subscription license is set to the subscription period.

Following are the types of licenses available:

Smart Licensing:

- PNR-System SIA—Licenses the CCM services. This license is mandatory if you want to run Cisco Prime Network Registrar.

- PNR-DHCP SIA—Licenses DHCP/TFTP services and, optionally, an initial count of leases.

- PNR-DNS SIA—Licenses the authoritative DNS services and, optionally, an initial count of RRs.

- PNR-Caching DNS SIA—Licenses Caching DNS services and, optionally, an initial count of servers.

- PNR-DHCP Container SIA—Licenses DHCP services on containers.

- PNR-DNS Container SIA—Licenses authoritative DNS services on containers.

- PNR-Caching DNS Container SIA—Licenses Caching DNS services on containers.

Traditional Licensing:

- sub-system —Licenses the CCM services.

- sub-dhcp—Licenses the DHCP services.

- sub-count-dhcp—Licenses an incremental number of active leases.

- sub-dns—Licenses the authoritative DNS services.

- sub-count-dns—Licenses an incremental number of RRs.

- sub-cdns—Licenses Caching DNS services.

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

- CCM services—base-system and PNR-System

- DHCP services—base-dhcp, count-dhcp, and PNR-DHCP

- Authoritative DNS services—base-dns, count-dns, and PNR-DNS

- Caching DNS services—base-cdns, count-cdns, PNR-Caching DNS

Note Licenses for Cisco Prime Network Registrar 10.x or earlier are not valid for Cisco Prime Network Registrar 11.x. You should have a new license for Cisco Prime Network Registrar 11.x. For the 11.x regional, if one has 10.x CDNS clusters, the 10.x CDNS licenses must be added on the regional server (10.x CDNS clusters will use 10.x licenses, and 11.x CDNS clusters will use 11.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 11.0 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 16.

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 11.0? (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 19)	☐
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?	☐
Which type of installation is this - regional cluster, local cluster, or client-only?	☐
Is the 64-bit JRE/JDK installed on the system? If so, where?	☐

Task	Checkoff
Am I upgrading from an earlier version of Cisco Prime Network Registrar? If so:	☐
• Are there any active user interface sessions?	☐
• Is my database backed up?	☐
• Am I upgrading from a supported version (Cisco Prime Network Registrar 8.3 and later)?	☐
Are the required packages for Linux installed? (See System Requirements for Linux OS, on page 8)	☐
Is the signature for the Cisco Prime Network Registrar image verified? (see Image Signing, on page 17)	☐

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.

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

Obtaining Cisco Prime Network Registrar License Files

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

Smart Licensing:

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

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

Traditional Licensing:

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

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

To obtain a license file:

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

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

3. Log in to one of the websites described on the certificate, and follow the registration instructions. The PAK number is required for the registration process.

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

A typical license file might look like:

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

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

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

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

Image Signing

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

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

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

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

2. Run the following command:

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

   Meaning: Package is signed, correct GPG key is imported

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

   - Size message indicates that the size of the packaged files has not changed.
   - PGP message indicates that the digital signature contained in the package file is a valid signature of the package file contents, and was produced by the organization that originally signed the package.

- MD5 message indicates that a checksum contained in the package file and calculated when the package was built, matches a checksum calculated by RPM during verification. Because the two checksums match, it is unlikely that the package has been modified.

OK means that each of these tests was successful.

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

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

  Meaning: Package not signed.

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

  Meaning: Wrong public key.

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

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

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

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

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

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

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

    For example:

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

Running Other Protocol Servers

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

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

Backup Software and Virus Scanning Guidelines

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

C H A P T E R **5**

Installing and Upgrading Cisco Prime Network Registrar

This chapter contains the following sections:

Installing Cisco Prime Network Registrar

Starting from Cisco Prime Network Registrar 11.0, there are no configuration questions asked during the installation. Also, it no longer asks for admin credentials and licensing details. You must provide these details when you connect to Cisco Prime Network Registrar for the first time (see Using Cisco Prime Network Registrar, on page 33).

Note that the following paths are used:

- Program files—/opt/nwreg2/{local | regional}

Warning You should NOT add or modify files in the /opt/nwreg2/* directories as these will be overwritten during upgrades or installations. You should add or modify the files only in the /var area. For example, you should add the extensions in the /var/nwreg2/local/extensions area and not in the /opt area.

- Data files—/var/nwreg2/{local | regional}/data

- Log files—/var/nwreg2/{local | regional}/logs

- cnr.conf file—/var/nwreg2/{local | regional}/conf

Also, Cisco Prime Network Registrar 11.0 installation configures the following by default:

- Type of web security—HTTPS only (default port, 8443 for local and 8453 for regional)

- Web services—REST API enabled (on HTTPS port, no separate port)

- Security mode—Required

- SCP Port number—CCM on default port (1234 for local and 1244 for regional)

- Run as root—Run as root always. You must create a superuser administrator during first login (see Using Cisco Prime Network Registrar, on page 33).

- Type of installation (local, regional, or client-only)—Depends on the RPM kit used. Following RPM kits are available for Cisco Prime Network Registrar 11.0:

Table 4: RPM Kits

	RHEL/CentOS 7.x	RHEL/CentOS 8.x
Regional cluster	cpnr-regional-11.0-1.el7*.x86_64.rpm	cpnr-regional-11.0-1.el8*.x86_64.rpm
Local cluster	cpnr-local-11.0-1.el7*.x86_64.rpm	cpnr-local-11.0-1.el8*.x86_64.rpm
Client only	cpnr-client-11.0-1.el7*.x86_64.rpm	cpnr-client-11.0-1.el8*.x86_64.rpm
* in the kit name indicates the RHEL minor version that the package was forked from.		

The following steps are applicable for the new installations. To upgrade from earlier versions of Cisco Prime Network Registrar to 11.0, see Upgrading Cisco Prime Network Registrar, on page 25.

To install Cisco Prime Network Registrar, do the following:

Step 1 Log in to the target machine.

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 DNS server's operating system causes significant decrease in the 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 11.0 Administration Guide*.

Step 2 Install the OpenJDK 1.8 or later if you have not already done so. Use the following command:

```
# yum install java-1.8.0-openjdk
```

Note that on some systems, you must use the **dnf install** command.

Step 3 Download the distribution file (RPM kit) from Cisco.com as per your requirement. For the list of RPM kits available for Cisco Prime Network Registrar 11.0, see Table 4: RPM Kits above.

Cisco Prime Network Registrar 11.0 installs both client and server by default. For client only installation, use the appropriate kit as listed in Table 4: RPM Kits above.

Note Choose client only installation in a situation where you want the client software running on a different machine than the protocol servers. You must then set up a connection to the protocol servers from the client.

Step 4 Navigate to the directory in which you saved the downloaded distribution file.

Step 5 Install Cisco Prime Network Registrar using any of the following commands:

 # yum install *filename*

OR

 # rpm -i *filename*

OR

 # dnf install *filename*

Where *filename* is the RPM kit name as listed in Table 4: RPM Kits, on page 22.

Note that the RHEL/CentOS 7.x kits have "el7*" in the name and the RHEL/CentOS 8.x kits have "el8*", where * is the RHEL minor version that the package was forked from.

For example, to install the regional cluster on RHEL/CentOS 7.x, use any of the following commands:

 # yum install cpnr-regional-11.0-1.el7_9.x86_64.rpm

OR

 # rpm -i cpnr-regional-11.0-1.el7_9.x86_64.rpm

OR

 # dnf install cpnr-regional-11.0-1.el7_9.x86_64.rpm

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.

Step 6 Start the Cisco Prime Network Registrar server agent using the following commands (or reboot the system as Cisco Prime Network Registrar is configured to start automatically):

For the local cluster:

systemctl start nwreglocal

For the regional cluster:

systemctl start nwregregional

During start-up, the /var/nwreg2/{local | regional} folder is created. The keystore file is created in the /var/nwreg2/{local | regional}/conf/priv folder and the keystore details are updated in the cnr-priv.conf file.

If you want to use your own certificate, see Installing Your Own Certificate for Web UI Access, on page 30.

Step 7 Verify the status of the Cisco Prime Network Registrar servers. Run either of the following commands:

./cnr_status (available in the *install-path*/usrbin directory)

OR

systemctl status nwreglocal (for the local cluster)

systemctl status nwregregional (for the regional cluster)

After the installation is complete, follow the steps in Using Cisco Prime Network Registrar, on page 33 to start using Cisco Prime Network Registrar. Make sure NOT to modify or add anything in the /opt folder as these files may be overwritten by a future upgrade. You can make changes in the /var folder.

Upgrade Considerations

Cisco Prime Network Registrar 11.0 supports direct upgrades from 8.3 and later.

Cisco Prime Network Registrar 11.0 can run on Red Hat/CentOS 7.x and 8.x. If you are using an earlier version of the operating system, you will first need to upgrade your system to a supported version.

When you install the software, the installation program automatically detects an existing version and upgrades the software to the latest release. Archive the existing Cisco Prime Network Registrar data. If the upgrade fails and fails to start, then you should recover the backup that you made (and perhaps install the old Cisco Prime Network Registrar version). You can also find the backup of the data in the /var/nwreg2/{local|regional} directory, called **upgrade-backup-***date***.tar.gz**. If you did not create your own backup, you can use this backup to restore the databases.

The eventstore is no longer used to track the pending DNS updates. DHCPv4 lease objects are used for this purpose, similar to DHCPv6 DNS updates where leases are used. Therefore, when upgrading from Cisco Prime Network Registrar 10.x or earlier, it is best to upgrade when the DNS update backlog is low as any pending DHCPv4 DNS updates will be lost. The DHCP server logs the DNS update events that it drops using the log message 19669. This will report the lease, pending action, FQDNs, and DNS Update Configuration objects involved for each pending event. These are only logged once as the server removes these events from the eventstore.You can determine the DNS update backlog using the **dhcp getRelatedServers** command and by examining the "requests" count for the DNS servers.

Using Smart Licensing

Cisco Prime Network Registrar 11.x regional, working in Smart License mode, does not support pre-11.0 local clusters. Hence, you must perform the following steps to move to Smart Licensing:

Step 1   Upgrade the Cisco Prime Network Registrar regional cluster to 11.x and disable Smart Licensing (post upgrade). To disable Smart Licensing, see the *"Disabling Smart Licensing" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

Step 2   Load the required traditional licenses on the Cisco Prime Network Registrar 11.x regional cluster.

Step 3   Re-register or resync all the local clusters with the upgraded regional cluster.

> **Warning**   You must upgrade the Cisco Prime Network Registrar 10.x local clusters to 10.1.1 (or later version) before registering them with the 11.x regional cluster. The 10.x local clusters with lower than 10.1.1 version, have issues registering with the 11.x regional cluster.

Step 4   Upgrade all the local clusters to 11.x as per your schedule.

Step 5   After all the clusters are upgraded to 11.x, you can Enable Smart Licensing on regional if you want to move to Smart Licensing. You should perform this step only if you have required licenses in your Smart Account on the CSSM or Satellite. To enable Smart Licensing, see the *"Enabling Smart Licensing" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

Upgrading Cisco Prime Network Registrar

One major change introduced with Cisco Prime Network Registrar 11.0 is to better separate the distributed files (that is, those installed by the RPM) from those that are data and configuration files specific to your installation. Basically, the /opt/nwreg2 area should not include files that are not provided as part of the installation. Everything that is specific to your installation, should now be in the /var/nwreg2 area.

If you used the default paths when previously installing earlier versions of Cisco Prime Network Registrar, the following files will be automatically relocated the first time you start Cisco Prime Network Registrar after installing Cisco Prime Network Registrar 11.0:

- /opt/nwreg2/{local | regional}/conf/cnr.conf will be moved to /var/nwreg2/{local | regional}/conf

- /opt/nwreg2/{local | regional}/conf/priv (and its contents) will be moved to /var/nwreg2/{local | regional}/conf/priv

- /opt/nrweg2/{local | regional}/conf/cert (and its contents) will be moved to /var/nrweg2/{local | regional}/conf/cert

- Any paths in the cnr.conf and cnr-priv.conf will be updated to reflect this move

If the Cisco Prime Network Registrar data area is not in /var/nwreg2/{local | regional}/data, similar moves are done but the resulting paths will use a new conf directory in the parent directory of the data directory. Or, the files may be left where they are.

Note that after upgrading from earlier versions to Cisco Prime Network Registrar 11.0, the following changes will also occur in addition to the above mentioned changes:

- The nwreglocal.env (for local) or nwregregional.env (for regional) file in the /usr/lib/systemd/system directory is used instead of the /opt/nwreg2/{local | regional}/bin/cnr.env file. Therefore, after installing (before starting Cisco Prime Network Registrar), you may need to review if cnr.env changes (such as for LD_LIBRARY_PATH for extensions) need to be applied to the new .env file.

- The web UI keystore is used if one exists or a new one is generated. The existing priv/cnr-priv.conf is used and relocated to /var/nwreg2/{local | regional}.

- HTTPS is used for web UI and REST instead of HTTP. If no port was previously configured for HTTPS, the default (regional | local) ports are used.

- If REST was disabled in the previous install, it gets enabled after the upgrade. If you want to disable REST API, follow the steps in Disabling REST API, on page 36 after upgrading. If REST was previously using a different port than HTTPS, it is no longer supported and the same port is used for HTTPS (web UI) and REST.

Note
From Cisco Prime Network Registrar 10.1 onwards, the keystore password is encrypted by default. Therefore, you do not have to encrypt the keystore password if you are upgrading from 10.1 to 11.0. However, if you are upgrading from pre-10.1 version to 11.0, then you must encrypt the keystore password manually.

To generate the encrypted password, use the encrypt script (**encrypt -s** *<plain-text password>*) present in the *install-path*/usrbin directory. You must update this encrypted password in server.xml and after making the change, you must restart Cisco Prime Network Registrar.

To upgrade to Cisco Prime Network Registrar 11.0:

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

Step 2 Remove the existing installation using the procedure described in Uninstalling Cisco Prime Network Registrar, on page 39. Ensure NOT to do the cleanup operations mentioned at the end (that is, retain the data, cnr.conf, and so on).

Step 3 If the old cnr.conf is in *install-path*/conf, you can upgrade without doing anything. If the old cnr.conf is elsewhere, then create a cnr.conf file in the *install-path*/conf directory that contains the following line:

cnr.confdir=*location of the old cnr.conf file*

Step 4 To reduce issues with Java upgrades, we highly recommend that you edit your cnr.conf file to replace the cnr.java-home entry path with /usr/bin/java (if this is the path that has the version of Java specified in cnr.conf). You can test this by doing:

```
/usr/bin/java -version
```

and

```
cnr.java-home-path/bin/java -version
```

If the two report the same result, you should change the cnr.java-home path to specify /usr/bin/java. If you do this, updates to Java will not require you to update the cnr.java-home path.

Step 5 Install Cisco Prime Network Registrar 11.0. For installation instructions, see Installing Cisco Prime Network Registrar, on page 21.

Step 6 Start the Cisco Prime Network Registrar server agent using the following commands:

• For the local cluster:

```
# systemctl start nwreglocal
```

• For the regional cluster:

```
# systemctl start nwregregional
```

The upgrade process may take some time depending on the size of the configuration and lease/resource record data, and the version from which you are upgrading. You can view the status using the **systemctl status nwreglocal** (for the local cluster) or **systemctl status nwregregional** (for the regional cluster) command. If this shows "trampoline startup, local mode" (for the local cluster) or "trampoline startup, regional mode" (for the regional cluster), it indicates that the services are up or have started. Follow the steps in Using Cisco Prime Network Registrar, on page 33 to start using Cisco Prime Network Registrar.

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 26.

Reverting to an Earlier Product Version

The Cisco Prime Network Registrar installation program archives the existing product configuration and data when you upgrade to a newer version. If 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 Ensure that the archive file **upgrade-backup-*date*.tar.gz** is available in the /var/nwreg2/{local | regional} directory.

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 archive file, delete any remaining files and directories in the Cisco Prime Network Registrar installation paths.

Step 4 Restore the backup (either the one that you created or the archive file that is created in Step 7).

Step 5 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 6 After the installation ends successfully, stop the Cisco Prime Network Registrar server agent:

- For the local cluster:

```
# systemctl stop nwreglocal
```

- For the regional cluster:

```
# systemctl stop nwregregional
```

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.

 b) Using the fully qualified path to the archive directory, extract the archive.

- Change to the root directory of the filesystem using **cd /**.

- Using the fully qualified path to the archive directory containing the **upgrade-backup-*date*.tar.gz** file, extract the archive.

```
tar xzf /var/nwreg2/{local | regional}/upgrade-backup-date.tar.gz
```

The above command creates the **opt** and **var** folders. The **opt** folder contains only the conf directory.

Step 8 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 5; a later version that supports upgrades from the earlier version can be installed).

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.

```
# systemctl stop nwreglocal
```

Step 2 Tar up /var/nwreg2/local, except /var/nwreg2/local/tomcat. You can also skip the /var/nwreg2/local/data.bak if you prefer not to copy over the latest backup.

Step 3 Copy the tar file to the new server, and untar the files into the same location (/var/nwreg2/local). Ensure that there is no /var/nwreg2/local/tomcat directory (if so, remove it and anything in it).

> **Note** The Step 2 and Step 3 apply to Cisco Prime Network Registrar 11.0 and later. For earlier releases, refer to the documentation of that version.

Step 4 Move the /usr/lib/systemd/system/nwreglocal.env file to the new system.

Step 5 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 51) after the installation.

Step 6 Log in to the web UI and navigate to the **Licenses** page under the **Administration** menu to open the List Licenses page.

Step 7 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 8 Click the **Register** button to register with the regional server.

Step 9 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 5; a later version that supports upgrades from the earlier version can be installed).

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

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

```
# systemctl stop nwregregional
```

Step 2　Tar up /var/nwreg2/regional, except /var/nwreg2/regional/tomcat. You can also skip the /var/nwreg2/regional/data.bak if you prefer not to copy over the latest backup.

Step 3　Copy the tar file to the new server, and untar the files into the same location (/var/nwreg2/regional). Ensure that there is no /var/nwreg2/regional/tomcat directory (if so, remove it and anything in it).

> **Note**　The Step 2 and Step 3 apply to Cisco Prime Network Registrar 11.0 and later. For earlier releases, refer to the documentation of that version.

Step 4　Move the /usr/lib/systemd/system/nwregregional.env file to the new system.

Step 5　Install Cisco Prime Network Registrar (regional cluster) on the new server. For more information, see Installing Cisco Prime Network Registrar, on page 21.

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 51) 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 6　Start the Cisco Prime Network Registrar web UI or CLI. For more information, see Using Cisco Prime Network Registrar, on page 33.

Step 7　Log in as superuser to the CLI for the new regional cluster.

Step 8　To list the local clusters, use the following command:

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

Step 9　To synchronize the data as well as the license information, use the following command:

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

Installing Your Own Certificate for Web UI Access

If you want to use your own certificate for web UI access, do the following:

Step 1 Create a keystore file with self-signed certificate by using **openssl** or **keytool**. Use the utility to define a self-signed certificate, or to request and later import a certificate from an external signing authority:

- 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):
```

  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 51.

- 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 step, 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.

- To create a self-signed certificate using openssl, use the following command:

```
> openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

For more information on certificate management in Cisco Prime Network Registrar, see the *"Certificate Management" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

Step 2 Edit the cnr-priv.conf file (in /var/nwreg2/{local | regional}/conf/priv) as required to point to the new keystore and then specify the password (encrypted). To generate the encrypted password, use the encrypt script (**encrypt -s** <*plain-text password*>) present in the *install-path*/usrbin directory.

Step 3 Restart Cisco Prime Network Registrar.

Whenever Cisco Prime Network Registrar is restarted, the keystore details are applied to the Tomcat configuration.

Troubleshooting the Installation

The log directory is set to these locations by default:

- Local cluster: /var/nwreg2/local/logs

- Regional cluster: /var/nwreg2/regional/logs

If the installation or upgrade does not complete successfully, then:

- Check the contents of the above 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.

- Check the status of the service using the following commands:

  - For the local cluster:

    ```
    # systemctl status -l nwreglocal.service
    ```

  - For the regional cluster:

    ```
    # systemctl status -l nwregregional.service
    ```

- Check the systemd journal using the following commands:

  - For the local cluster:

    ```
    # journalctl -u nwreglocal --since=today
    ```

  - For the regional cluster:

    ```
    # journalctl -u nwregregional --since=today
    ```

  You can change the time interval used in since. For more details, use the **man journalctl** command.

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 21.

When you try to log in for the first time (either in the web UI or CLI) after installing Cisco Prime Network Registrar on the local cluster, you will be prompted to create the superuser and to register with a regional cluster.

Step 2 Log in to 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 11.0 Administration Guide*.

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

Next Steps

This chapter contains the following sections:

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 11.0 Quick Start Guide.

- Set up DHCP addresses, DHCP failover, and DNS update—See Cisco Prime Network Registrar 11.0 DHCP User Guide.

- Set up Authoritative and Caching DNS services—See Cisco Prime Network Registrar 11.0 Caching and Authoritative DNS User Guide.

- Perform administrative tasks, such as local and regional administration, and so on—See Cisco Prime Network Registrar 11.0 Administration Guide.

- Configure and manage Cisco Prime Network Registrar via CLI—See Cisco Prime Network Registrar 11.0 CLI Reference Guide.

- Configure and manage Cisco Prime Network Registrar via REST API—See Cisco Prime Network Registrar 11.0 REST APIs Reference Guide.

Using Cisco Prime Network Registrar

To administer the local and regional clusters that you have installed, you must create a superuser administrator and enter the appropriate license information. To do this, follow the below steps first time when you connect to Cisco Prime Network Registrar:

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

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

  `https://hostname:https-port`

  where:

    - *hostname* is the actual name of the target host.

    - *https-port* is the default HTTPS port (8443 for local and 8453 for regional).

- To start the CLI, launch nrcmd by entering:

  `install-path/usrbin/nrcmd -R -N username -P password`

  Specify the username and password of the administrator account that you want to create. You will be asked to confirm the password if the superuser administrator account needs to be created (during the first login).

  Note   Specify -R only if you are connecting to a regional cluster.

Step 2 Create a superuser administrator by providing the username and password.

- Web UI—Enter the username and password in the **Admin** and **Password** fields respectively. Then, click the **Add** button.

Step 3 In Cisco Prime Network Registrar 11.0, Smart Licensing is enabled by default. Click the **Configure Smart Licensing** link in the alert window to open the Smart Software Licensing page and set up Smart Licensing. For details, see the *"Use Cisco Smart Licensing" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

If you want to use traditional licensing, then you must disable Smart Licensing first (see the *"Disabling Smart Licensing" section in the Cisco Prime Network Registrar 11.0 Administration Guide*). Then, click **Use Traditional Licensing** and enter the license information as follows:

- 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`

  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 your first login. You can choose the services (dhcp, dns, and cdns) for the local based on the licenses added in the regional cluster.

Step 4 Enter the superuser username and password (created in Step 2) to log in to web UI and CLI.

You may create other administrator accounts to perform certain functions based on the assigned roles. For more information, see the *"Managing Administrators" chapter in the Cisco Prime Network Registrar 11.0 Administration Guide*.

Starting and Stopping Servers

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 11.0 Administration Guide*.

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

To start and stop servers:

Step 1   Log in as superuser.

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

For the local cluster:

```
# systemctl start nwreglocal
```

For the regional cluster:

```
# systemctl start nwregregional
```

Step 3   Verify the status of the Cisco Prime Network Registrar servers. Run either of the following commands:

```
# ./cnr_status
```
(available in the *install-path*/usrbin directory)

OR

```
# systemctl status nwreglocal
```
(for the local cluster)

```
# systemctl status nwregregional
```
(for the regional cluster)

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

For the local cluster:

```
# systemctl stop nwreglocal
```

For the regional cluster:

```
# systemctl stop nwregregional
```

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 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.

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:

• Local cluster: /var/nwreg2/local/logs

• Regional cluster: /var/nwreg2/regional/logs

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

Disabling REST API

When you install Cisco Prime Network Registrar 11.0 or upgrade to 11.0 from previous versions, the REST API gets enabled by default. If you want to disable REST API, then do the following:

Local and Regional Advanced Web UI

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

Step 2   Click **CCM** in the Manage Servers pane on the left. The Edit Local CCM Server page appears. This page displays all the CCM server attributes.

Step 3   Under the **Control Settings** section, set the *is-rest-enabled* attribute value to **false** to disable REST API.

Step 4   Click **Save** to save the changes.

CLI Commands

Use **ccm disable is-rest-enabled** to disable REST.

Use **ccm enable is-rest-enabled** to enable REST.

Uninstalling Cisco Prime Network Registrar

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 11.0 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 Starting and Stopping Servers, on page 34.

Uninstalling Cisco Prime Network Registrar

To uninstall Cisco Prime Network Registrar, run any of the following commands:

rpm -e *kitname*

OR

yum remove *kitname*

OR

dnf remove *kitname*

where *kitname* is either cpnr-local, cpnr-regional, or cpnr-client.

For example, to uninstall the regional cluster, use any of the following commands:

rpm -e cpnr-regional

OR

yum remove cpnr-regional

OR

dnf remove cpnr-regional

Certain configuration and data files that are created during installation and operation remain deliberately after uninstallation. Optionally, delete the data files that are associated with Cisco Prime Network Registrar, as mentioned in the instructions at the end of the uninstallation message.

CHAPTER 8

Cisco Prime Network Registrar on Container

Cisco Prime Network Registrar 11.0 can be run as a Docker container that you can install in your own infrastructure.

The following Docker images are provided for Cisco Prime Network Registrar 11.0:

- Regional container: **cpnr-regional-11.0-1.el8.x86_64_rhel_docker.tar.gz**
- Local container: **cpnr-local-11.0-1.el8.x86_64_rhel_docker.tar.gz**

Note The name of the images will change with releases in future.

Requirements on the Host Machine

- Identify the ports on the host machine to be exposed to ports required by Cisco Prime Network Registrar container. For a complete list of ports used by Cisco Prime Network Registrar services, see the *"Default Ports for Cisco Prime Network Registrar Services"* section in the *Cisco Prime Network Registrar 11.0 Administration Guide*.

- Select an option to persist data of Cisco Prime Network Registrar container on the host machines: Bind mount (where a directory on the host machine is used) or Volume (which is managed by Docker).

- For IPv4, you can use either bridged or macvlan network; Cisco recommends macvlan for better performance.

- For IPv6, you will need to configure the container to have an IPv6 address.

Running Cisco Prime Network Registrar Docker Container

To run Cisco Prime Network Registrar as Docker container, you must first download the Docker image of your choice. Then, do the following:

Step 1   Load the Docker image using the following command:

  • For the regional container:

    # **docker load -i cpnr-regional-11.0-1.el8.x86_64_rhel_docker.tar.gz**

  • For the local container:

    # **docker load -i cpnr-local-11.0-1.el8.x86_64_rhel_docker.tar.gz**

Step 2   Verify that the image is successfully loaded using the following command:

  # **docker image ls**

Step 3   Run the Docker container using the following command:

  • For the regional container:

    # **docker run -d --name cpnr_regional_container --privileged=true -p 8453:8453 -p 1244:1244 --mount type=bind,source=/data/cpnr_regional_data,target=/var/nwreg2/regional cpnr-regional:11.0 /usr/sbin/init**

    In the above command:

      • Default bridge networking driver of Docker is used. Ports needed by container are exposed–8453 is for regional web UI, 1244 for regional configuration management.

      • Data directory of Cisco Prime Network Registrar is /var/nwreg2/regional and mountpoint on the host is /data/cpnr_regional_data

      • The command to be run is /usr/sbin/init

    If it is required to synchronize the timezone of the host and the Docker container, then add the **-v /etc/localtime:/etc/localtime** option to the above Docker run command.

    By default, the core files are available in the /var/lib/systemd/coredump directory of the Docker host machine. To collect the core files via the **cnr_tactool** utility, run the following commands on the Docker host machine:

    # **echo '/data/cpnr_regional_data/core.%p' > /proc/sys/kernel/core_pattern'**
    # **ulimit -c unlimited**

    After running the above commands, the core files will be available in the /data/cpnr_regional_data directory and you can use **cnr_tactool** to collect them.

  • For the local container:

    # **docker run -d --name cpnr_local_container --privileged=true -p 8443:8443 -p 1234:1234 -p 67:67/udp -p 53:53/udp --mount type=bind,source=/data/cpnr_local1_data,target=/var/nwreg2/local cpnr-local:11.0 /usr/sbin/init**

    In the above command:

      • Default bridge networking driver of Docker is used. Ports needed by container are exposed–8443 is for the web UI, 1234 for local configuration management, 67 for DHCP, and 53 for DNS. For other services like SNMP, TFTP see the *"Default Ports for Cisco Prime Network Registrar Services" section in the Cisco Prime Network Registrar 11.0 Administration Guide*.

      • Data directory of Cisco Prime Network Registrar is /var/nwreg2/local and mountpoint on the host is /data/cpnr_local1_data

      • The command to be run is /usr/sbin/init

If it is required to synchronize the timezone of the host and the Docker container, then add the **-v /etc/localtime:/etc/localtime** option to the above Docker run command.

By default, the core files are available in the /var/lib/systemd/coredump directory of the Docker host machine. To collect the core files via the **cnr_tactool** utility, run the following commands on the Docker host machine:

```
# echo '/data/cpnr_local1_data/core.%p' > /proc/sys/kernel/core_pattern'
# ulimit -c unlimited
```

After running the above commands, the core files will be available in the /data/cpnr_local1_data directory and you can use **cnr_tactool** to collect them.

Step 4   Start configuring Cisco Prime Network Registrar.

- For the regional container:

    - To connect using web UI, use https://*hostip*:8453

    - To connect using CLI, use the following command:

        *install-path***/usrbin/nrcmd -R -C** *hostip***:1244 -N** *username* **-P** *password*

- For the local container:

    - To connect using web UI, use https://*hostip*:8443

    - To connect using CLI, use the following command:

        *install-path***/usrbin/nrcmd -C** *hostip***:1234 -N** *username* **-P** *password*

For running DHCP failover and HA DNS, we recommend running two Cisco Prime Network Registrar containers (Main and Backup) in separate hosts, as this avoids single point of failure. Given that bridge network is limited to a single host, using macvlan as networking driver is the best choice. With macvlan, container appears to be directly connected to physical network.

If the Docker daemon allows IPv6, you can use dual-stack macvlan networks, that is, both IPv4 and IPv6:

```
# docker network create --driver=macvlan --ipv6 --subnet=2001:db8:1:1::/64
--gateway=2001:db8:1:1::1 --subnet=10.0.0.0/24 --gateway=10.0.0.1 -o macvlan_mode=bridge
-o parent=eth0 cpnr_macvlan
```

Run Cisco Prime Network Registrar container and attach it to the macvlan network created above:

```
# docker run -d --name cpnr_dhcp_main --network=cpnr_macvlan --ip 10.0.0.20 --ip6
2001:db8:1:1::20 --privileged=true --mount type=bind,source=/data/cpnr_dhcp_main_data,
target=/var/nwreg2/local cpnr-local:11.0 /usr/sbin/init
```

This Cisco Prime Network Registrar container (local) can now be reached at 10.0.0.20 and 2001:db8:1:1::20.

- To connect using web UI over IPv4, use https://10.0.0.20:8443

- To connect using CLI over IPv6, use the following command:

    *install-path***/usrbin/nrcmd -C [2001:db8:1:1::20]:1234 -N** *username* **-P** *password*

Moving an Existing Cisco Prime Network Registrar Cluster to Docker Container

To move to Cisco Prime Network Registrar 11.0 Docker container from an existing Cisco Prime Network Registrar 8.3 or later cluster, do the following:

Step 1 Remove the existing installation using the procedure described in .

Step 2 Delete the /opt/nwreg2 folder. Ensure NOT to delete the /var/nwreg2 folder after uninstallation.

If you are upgrading to Cisco Prime Network Registrar 11.0 Docker Container on the same machine, then skip this Step 3 and proceed to Step 4.

Step 3 If you are upgrading to Cisco Prime Network Registrar 11.0 Docker Container on a different machine, then create the source directory tree (for example, /data/cpnr_local1_data for local cluster and/data/cpnr_regional_data for regional cluster) in the machine where you want to create the Docker instance (target machine). Then, transfer the original cluster's /var/nwreg2/{local | regional} directory to this directory. Use the following commands:

- For regional cluster:

```
# mkdir  -p  /data/cpnr_regional_data
# mv  /var/nwreg2/regional  /data/cpnr_regional_data
```

- For local cluster:

```
# mkdir  -p  /data/cpnr_local1_data
# mv  /var/nwreg2/local  /data/cpnr_local1_data
```

Note Copy the cnr.conf file from the /opt/nwreg2/{local | regional}/conf directory to the conf folder in the source directory of the target machine. Use the following commands:

- For regional cluster:

```
# mv /opt/nwreg2/regional/conf /data/cpnr_regional_data/conf
```

- For local cluster:

```
# mv /opt/nwreg2/local/conf /data/cpnr_local1_data/conf
```

Step 4 Create the Docker instance using the following command:

- For regional container:

```
$ docker run -d --name cpnr_container -v /etc/localtime:/etc/localtime --network=mymacvlan
--ip hostip --ip6 ipv6address --privileged=true --hostname=hostip --mount type=bind,
source=/data/cpnr_regional_data,target=/var/nwreg2/regional cpnr_regional:11.0 /usr/sbin/init
```

- For local container:

```
$ docker run -d --name cpnr_container -v /etc/localtime:/etc/localtime --network=mymacvlan
--ip hostip --ip6 ipv6address --privileged=true --hostname=hostip --mount type=bind,
source=/data/cpnr_local1_data,target=/var/nwreg2/local cpnr_local:11.0 /usr/sbin/init
```

Step 5   Verify if the previous configuration, including scopes and zones, is intact in Cisco Prime Network Registrar 11.0 server. Also, verify that the data.bak folder is created which contains the pre-upgrade version's database version as backup.

Note   After performing the above steps, all settings will take their defaults and you may have to take additional steps to reinstall the certificates or change ports. For information, see Installing Your Own Certificate for Web UI Access, on page 30.

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 machine to support smaller test configurations for evaluation purposes.

⚠

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, according to the procedure in Installing Cisco Prime Network Registrar, on page 21. Use the cpnr-local kit.

Step 3 Install or upgrade the regional cluster on the same machine, according to the same procedure. Use the cpnr-regional kit.

Testing the Lab Installation

To test the installation:

Step 1 Start and log in to the web UI for the local cluster. By default, the local port number is **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 in to the web UI for the regional cluster. By default, the regional port number is **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

To remove the local cluster, follow the steps in Uninstalling Cisco Prime Network Registrar, on page 39 and specify cpnr-local for the kit.

To remove the regional cluster, follow the steps in Uninstalling Cisco Prime Network Registrar, on page 39 and specify cpnr-regional for the kit.

Installing the Cisco Prime Network Registrar SDK

This section documents how to install the Cisco Prime Network Registrar SDK. 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 Cisco Prime Network Registrar SDK

To install the Cisco Prime Network Registrar SDK:

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:.
```

Note If you have Cisco Prime Network Registrar installed on the system, then use the /opt/nwreg2/{local|regional}/lib path for LD_LIBRARY_PATH. If you do not have Cisco Prime Network Registrar installed, then you must point to the lib directory into which you untarred the files. If the system is not running as a local or regional cluster, you may want to consider installing the cpnr-client kit (to get access to other command line utilities). You can then specify LD_LIBRARY_PATH as /opt/nwreg2/client/lib.

Testing Your Installation

The following test program verifies that you have set your PATH or LD_LIBRARY_PATH correctly:

```
% java -jar /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 11.0 Release Notes* for the intervening Cisco Prime Network Registrar versions, as these highlight any significant SDK compatibility considerations.

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 11.0 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 /var/nwreg2/{local | regional}/tomcat/conf folder.

Step 2   Use the below recommended sslEnabledProtocols and ciphers, or configure it as per your security requirement. For more details, refer the tomcat SSL/TLS Configuration document available online.

```
<Connector port="${cnrui.https.port}" protocol="com.cisco.cnr.webui.tomcat.SecureHTTP"

relaxedQueryChars='[]'

maxConnections="1024" maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

clientAuth="false"

keystoreFile="..."

keystorePass="..."

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"

compression="on"

compressionMinSize="2048"

noCompressionUserAgents="gozilla, traviata"

URIEncoding="UTF-8"

compressableMimeType="text/html,text/xml,text/plain, text/css,text/javascript,
application/x-javascript,application/javascript"

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

Note The **keystoreFile** and **keystorePass** values are specific to your installation. You should not change these values as it will be overwritten each time Cisco Prime Network Registrar is started.

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

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:
  - 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

  - RHEL/CentOS 8.x:

    https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/Red_Hat_Enterprise_Linux-8-Security_hardening-en-US.pdf

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

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

  - 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 11.0 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 11.0 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 11.0 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 11.0 DHCP User Guide*) to the primary 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 11.0 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 11.0 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 11.0 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 11.0 Administration Guide*.

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 **F**

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.

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

Note   To account for situations where one or more servers are unavailable due to maintenance or outage, it is recommended to include excess capacity in the deployment architecture to accommodate the additional load that must be borne by the remaining live systems. The excess capacity to be deployed or the number of backup systems, will depend on the level of redundancy that you want to achieve. A minimum of n+1 redundancy is recommended.

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 **H**

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.

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 11.0 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 11.0 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 or SSD 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).

I N D E X