Cisco Prime Network Registrar 11.2 Release Notes

First Published: 2023-10-30

This document provides an overview of the new and changed features in Cisco Prime Network Registrar 11.2, and describes how to access information about the known problems.

Note You can access the most current Cisco Prime Network Registrar documentation, including these release notes, online at:

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-registrar/tsd-products-support-series-home.html

This document contains the following sections:

Introduction

Cisco Prime Network Registrar is comprised of these components:

- An Authoritative Domain Name System (DNS) protocol service
- A Caching DNS service
- A Dynamic Host Configuration Protocol (DHCP) service

Cisco offers these components as individually licensed applications or in a mix of suites.

Before You Begin

Before you install Cisco Prime Network Registrar 11.2, review the system requirements and licensing information available in *Cisco Prime Network Registrar 11.2 Installation Guide*.

Note If you are migrating to Cisco Prime Network Registrar 11.2 from an earlier version of Cisco Prime Network Registrar, you must review the release notes for the releases that occurred in between, to fully understand all the changes.

Cisco Prime Network Registrar DHCP, Authoritative DNS, and Caching DNS components are licensed and managed from the Cisco Prime Network Registrar regional server. All services in the local clusters are licensed through the regional cluster. Only a regional install requires a license and only the regional server accepts new licenses. Then the regional server can authorize individual local clusters, based on available licenses.

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, 11.x CDNS clusters will use 11.x licenses).

Warning You MUST upgrade the Cisco Prime Network Registrar 10.x local clusters to 10.1.1 or later before upgrading the regional to 11.x. You should not upgrade the local clusters to 11.0 (or later) directly, as you will not be able to register with the regional until it is upgraded to 11.0 (or later).

Note Smart Licensing is enabled by default in Cisco Prime Network Registrar 11.2. Cisco Prime Network Registrar 11.x regional, working in Smart License mode, does not support pre-11.0 local clusters. For more details, see the *"Using Smart Licensing" section in "Cisco Prime Network Registrar 11.2 Installation Guide"*.

For more details about Licensing, see the *"License Files" section in Cisco Prime Network Registrar 11.2 Installation Guide*.

The Cisco Prime Network Registrar 11.2 kit contains the following files and directories:

- Linux—Cisco Prime Network Registrar RPM application for RHEL 8.x/AlmaLinux 8.x
- Docs—Pointer card, Bugs, and Enhancement List
- Container—Container for Docker on Red Hat UBI 8.8
- Kubernetes—Sample YAML files for deployment of Cisco Prime Network Registrar container on Kubernetes

The Cisco Prime Network Registrar 11.2 also ships as a virtual appliance which includes all the functionality available in Cisco Prime Network Registrar along with the AlmaLinux 8.8 operating system. The Cisco Prime Network Registrar virtual appliance is supported on VMware ESXi 7.x platforms, and OpenStack. For more

details, see the *"Cisco Prime Network Registrar Virtual Appliance" section in Cisco Prime Network Registrar 11.2 Installation Guide*.

Note The Linux distribution packaged with the optional pre-built VM downloads for Cisco Prime Network Registrar is Open Source software and not owned or supported by Cisco. Customers seeking support for Linux should reach out to third party software providers.

Note Cisco Prime Network Registrar has been tested against Red Hat Enterprise Linux ES 8.8 and AlmaLinux 8.8. 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.

Licensing

Cisco Prime Network Registrar 11.2 supports both Smart Licensing and traditional licensing. However, it does not support the hybrid model, that is, you can use only one of the license types at a time. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Cisco Prime Network Registrar 11.x is licensed in two parts: Permanent License and SIA License. The SIA License entitles upgrades to future releases. If you are on SIA from Cisco Prime Network Registrar 10.x, or on unexpired SWSS contract from Cisco Prime Network Registrar 9.x, you can upgrade until either of those entitlements expire. For PAK-based licensing, you must install the PAK onto the Cisco Prime Network Registrar regional server. For Smart Licensing, the licenses are delivered to your Smart Account. Smart Licensing is enabled by default in Cisco Prime Network Registrar 11.2, but can be overridden after installation. For Cisco Prime Network Registrar 11.2, the licensing is done according to the services that you require. For more information, see the *"License Files" section in Cisco Prime Network Registrar 11.2 Installation Guide*.

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.

Interoperability

Cisco Prime Network Registrar 11.2 uses individual component licenses. This allows users to purchase and install DHCP services, Authoritative DNS services, and Caching DNS services individually, or as a suite.

If you need additional DNS caching licenses, you should order them based on Server count since DNS caching is a server based license.

To install and manage DHCP, DNS, and Caching DNS licenses, you must deploy a regional server. The regional server, among other things, is used to install, count, and manage licensing for these components.

The synchronization between version 11.1 and pre-11.1 local clusters must be done from a 11.1 regional cluster. Cisco Prime Network Registrar 11.2 protocol servers interoperate with versions 9.0 or later.

What's New in Cisco Prime Network Registrar 11.2

The following table lists the new and modified features we documented in the user and installation guides. For information on additional features and fixes that were committed in Cisco Prime Network Registrar 11.2, see Resolved Bugs, on page 9 and Enhancement Features, on page 9.

Feature	Description
Aggressive NSEC and moving negative cache size setting from DNSCachingServer class to CDNSSEC.	In Cisco Prime Network registrar 11.2, the DNS Caching Server supports aggressive NSEC which uses the DNSSEC NSEC chain to synthesize NXDOMAIN and other denials, using information from previous NXDOMAINs answers. It helps to reduce the query rate towards targets that get a very high nonexistent name lookup rate. When the DNSSEC related attributes where moved from the DNSCachingServer class to the then new DnsSec class, the neg-cache-size attribute was left behind. Hence, moved the neg-cache-size attribute from DNSCachingServer class to CDNSSEC. For more information see the *"Managing DNSSEC" section in the Cisco Prime Network Registrar 11.2 Authoritative and Caching DNS User Guide*.
Query Name Minimisation	Cisco Prime Network registrar 11.2 supports QNAME minimisation to minimise the amount of privacy-sensitive data sent from the CDNS to the ADNS server. For more information see the *"Configuring Query Name Minimisation" in the Cisco Prime Network Registrar 11.2 Authoritative and Caching DNS User Guide*.
EDNS0 Client Subnet	In Cisco Prime Network Registrar 11.2, the Client Subnet feature allows the caching DNS server closest to the client attach part of the client's IP address to its upstream queries to signal authoritative servers where in the network the client resides and select the best response. This is done by using the ECS option for the EDNS0 feature of the DNS protocol. For more information see the *"Enabling Client Subnet" section in the Cisco Prime Network Registrar 11.2 Authoritative and Caching DNS User Guide*.

Feature	Description
Container Phase II	Starting Cisco Prime Network Registrar 11.2, there is a new container image created for CDNS service which makes the CDNS service more cloud native (smaller, stateless, horizontally scalable). As a result of this, the CCM Server is removed from the CDNS Container to have the container run standalone. Regional currently has central management for ADNS and DHCP, but there is very little management of CDNS configuration. In order to make the CDNS container stateless and more cloud native, the following classes on regional are exposed: • DNSCachingServer • DnsException • DnsForwarder • Dns64 • CdnsRedirect • CdnsDomainRateLimit • CdnsRateLimit The CDNS container performs the following steps as part of its lifecycle: • Register itself as a CDNS container with regional. • Pull the CDNS configuration from regional and apply it locally. • A check runs from regional on a configured interval to poll the CDNS containers to see if they are still alive and update the licenses accordingly. • On graceful shutdown unregister itself from regional. **Note** CDNS on Kubernetes now supports auto scaling, CDNS service will start only if corresponding license is available on Regional Cluster, so it is highly recommended to use Smart License for CDNS deployment on Kubernetes to make scaling seamless. SNMP Server is not supported on the CDNS Kubernetes Deployment, it is recommended to use the Open Source or Kubernetes native technologies like Prometheus, Grafana etc for monitoring, stats collection, alerting. Cisco Prime Network Registrar CDNS metrics (stats) are exported to be accessible to a monitoring system such as Prometheus through a python client library. For more information, see the *"Deploying Cisco Prime Network Registrar CDNS instance on Kubernetes" section in the Cisco Prime Network Registrar 11.2 Installation Guide*.

Feature	Description
DHCP LDAP over TLS	Starting Cisco Prime Network Registrar 11.2, the communication between LDAP server and Cisco Prime Network Registrar happens over TLS. Both Server and Client Identity Check are supported along with data encryption. For more information, see the *"LDAP over TLS" section in the Cisco Prime Network Registrar 11.2 DHCP User Guide*.
External RPZ Blocklist (CDNS)	In Cisco Prime Network Registrar 11.2, external RPZ blocklist allows CDNS servers to apply DNS policies and control domain resolution. The CDNS querying to external RPZ providers for data by using zone transfers or notifies and stored data in CDNS data directory. To update the RPZ zone file, the CDNS server sends IXFR zone transfers or notifies to RPZ providers based on the Secondary refresh attribute and update the latest information in RPZ file. It greatly increases the performance of processing the RPZ data. For more information see the *"Managing DNS Firewall" section in the Cisco Prime Network Registrar 11.2 Authoritative and Caching DNS User Guide*.
nrcmd text export/import	Starting Cisco Prime Network Registrar 11.2, the cnr_exim exports a configuration in nrcmd format. This allows the configuration to be both human-readable, editable and be able to be imported. The importing happens using nrcmd. For more information see the *"Using the cnr_exim Data Import and Export Tool" section in the Cisco Prime Network Registrar 11.2 Administration Guide*.
Certificate Management	Cisco Prime Network Registrar 11.2 supports to include the private key when required to support the central configuration of all TLS required data. Along with this, the CDNS and ADNS configuration is changed to reference the certificate object by name rather than by certificate type. Also, a support is added to upgrade certificate files into certificate objects. For more information, see the *"Certificate Management" section in the Cisco Prime Network Registrar 11.2 Administration Guide*.
Regional Management of Trust Anchors	In Cisco Prime Network Registrar 11.2 a configuration class is created for trust anchors to allow for central management and adds the Web UI and CLI support and reference that in the CDNS configuration. For more information see the *"Trust Anchor" section in the Cisco Prime Network Registrar 11.2 Authoritative and Caching DNS User Guide*.
Fault alert to notify sync failure	Trap is generated when there is a sync failure between the failover pair and the failure reason is highlighted. Failover pair sync failure notification event is raised as critical alarm.

Command Line Interface Enhancements

The following commands are modified in the CLI. For more information, see *Cisco Prime Network Registrar 11.2 CLI Reference Guide*.

New Commands

The following commands are added in the CLI:

- **cdns-config**—Manage common CDNS server configuration.
- **cdns-trust-anchor**—Manages CDNS trust anchor lists used for DNSSEC validation.

Modified Commands

New attributes are added to, or definitions modified for, the following commands:

- **cdns**—Configures and controls the DNS Caching server.
  - Added the following attributes:

    ecs-always-forward, **ecs-destination**, **ecs-enable**, **query-name-minimisation**, **security-event-alarm-settings**, **security-event-max-qps**, **tls-certificate**, **tls-system-cert-bundle**
  - Revised the description of the following attributes:

    smart-cache, **tls-upstream-cert-bundle**
  - The default setting of the attribute **top-names** changed from enabled to disabled.
  - Removed the following attribute:

    neg-cache-size, **service-key**, **service-pem**
- **cdnssec**—Controls and configures DNSSEC processing in the DNS Caching server.
  - Added the following attributes:

    aggressive-nsec, **neg-cache-size**, **trust-anchor-list**
  - Removed the following attributes:

    auto-trust-anchor-file, **trust-anchor-file**
- **cdns-redirect**—Controls and configures DNS redirect processing in the DNS Caching server.
  - Removed the following attribute:

    rpz-trigger
- **cdns-firewall**—Controls and configures DNS firewall processing in the DNS Caching server.
  - Added the following attributes:

    cdns-firewall < <name> | **all** > **pull** < **ensure** | **replace** | **exact** > <cluster-name> [**-report-only** | **-report**]

    cdns-firewall < <name> | **all** > **push** < **ensure** | **replace** | **exact** > <cluster-list> [**-report-only** | **-report**]

    cdns-firewall <name> **reclaim** <cluster-list> [**-report-only** | **-report**]
- **cdns-forwarder**—Controls and configures DNS Forwarders in the DNS Caching server.
  - Added the following attributes:

cdns-forwarder < <name> | **all** > **pull** < **ensure** | **replace** | **exact** > <cluster-name> [**-report-only** | **-report**]

cdns-forwarder < <name> | **all** > **push** < **ensure** | **replace** | **exact** > <cluster-list> [**-report-only** | **-report**]

cdns-forwarder <name> **reclaim** <cluster-list> [**-report-only** | **-report**]

- **cdns-exception**—Controls and configures DNS Exceptions in the DNS Caching server.
  - Added the following attributes:

    cdns-exception < <name> | **all** > **pull** < **ensure** | **replace** | **exact** > <cluster-name> [**-report-only** | **-report**]

    cdns-exception < <name> | **all** > **push** < **ensure** | **replace** | **exact** > <cluster-list> [**-report-only** | **-report**]

    cdns-exception <name> **reclaim** <cluster-list> [**-report-only** | **-report**]

- **certificate**— Controls and configures Certificates
  - Revised the description of the attribute: **certificate**
  - Added the following attribute:

    certificate <name> **setKey** <key-file>

    An example command is shown below:

    nrcmd> **certificate example setKey cert.key**
  - Added the following attributes:

    configured-by, **key-contents**, **validity-period**

- **dns**—Configures and controls the DNS server.
  - Added the following attributes:

    security-event-alarm-settings, **security-event-max-qps**, and **tls-certificate**
  - Modified the default settings of the attribute **top-names** from enabled to disabled.
  - Deleted the following attributes:

    service-key, **service-pem**

- **failover-pair**— configures a DHCP failover relationship.

  Added the following attribute:

  sync-failure-trap

- **ldap**—Specifies the LDAP remote server's properties.

  Added the following attributes:

  client-certificate, **server-ca-certificate**, **tls**

- **resource**—configures resources limits and allows for viewing and resetting resources

Revised the description of the following attributes:

cdns-security-events-critical-level, **cdns-security-events-warning-level**, **certificate-expiration-critical-level**, **certificate-expiration-warning-level**, **dns-security-events-critical-level**, **dns-security-events-warning-level**

Cisco Prime Network Registrar Bugs

For more information on a specific bug or to search all bugs in a particular Cisco Prime Network Registrar release, see Using the Bug Search Tool, on page 10.

This section contains the following information:

Resolved Bugs

The following table lists the key issues resolved in the Cisco Prime Network Registrar 11.2 release

Table 1: Resolved Bugs in Cisco Prime Network Registrar 11.2

Bug ID	Description
CSCwh17662	CCM Server crashes while performing WebUI search within DHCP server logs
CSCwh16958	DHCP server crashes when client-id is more than 127 bytes and DNS update happens
CSCwa08613	Support adjustable retry count for outbound queries
CSCwd01958	DHCP Server may fail to start after server agent restart

For the complete list of bugs for this release, see the **cpnr_11_2_buglist.pdf** file available at the product download site. See this list especially for information about fixes to customer-reported issues.

Enhancement Features

The following table lists the key enhancement feature added in the Cisco Prime Network Registrar 11.2 release.

Table 2: Enhancement Feature Added in Cisco Prime Network Registrar 11.2

Bug ID	Description
CSCwc00393	Block major and minor version upgrade if product license is out of compliance
CSCwb92206	Add TLS for LDAP communications
CSCwb92139	Fault alert to notify sync fail

Bug ID	Description
CSCvo88170	CDNS Client subnet in DNS queries
CSCwb06836	cnr_exim should be able to export configuration as a series of nrcmd commands
CSCwb92116	Allow customer to integrate Block List from outside databases
CSCwc35959	Enable Aggressive NSEC - RFC-8198
CSCwc35965	Support Query Name Minimisation - RFC-9156
CSCwc35968	Use internal rpz feature
CSCwd81614	DNSSEC trust-anchor-file and auto-trust-anchor-file should be configured as RRs

For the complete list of enhancement features added in this release, see the **cpnr_11_2_enhancements.pdf** file available at the product download site.

Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

Procedure

Step 1 Go to the Cisco Bug Search Tool.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register here.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 4 To search for bugs in the current release, click the **Search Bugs** tab and specify the following criteria:

a) In the Search For field, enter **Cisco Prime Network Registrar 11.2** and press **Return**. (Leave the other fields empty.)

b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

Note To export the results to a spreadsheet, click the **Export All to Spreadsheet** link.

Important Notes

This section contains the important information related to this software release and information in response to recent customer queries. It describes:

Upgrade with Smart License

If previous version is using smart license, make sure all the licenses are in-compliance before performing major or minor version upgrade. If any of the license is out-of-compliance, major or minor version upgrade will fail.

Related Documentation

See Cisco Prime Network Registrar Documentation Overview for a list of Cisco Prime Network Registrar 11.2 guides.

Accessibility Features in Cisco Prime Network Registrar 11.2

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the *What's New in Cisco Product Documentation RSS feed*. RSS feeds are a free service.