Cisco Prime Network Registrar 10.1 Release Notes

First Published: 2019-12-16

This document provides an overview of the new and changed features in Cisco Prime Network Registrar 10.1, 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 10.1, review the system requirements and licensing information available in *Cisco Prime Network Registrar 10.1 Installation Guide*.

Note If you are migrating to Cisco Prime Network Registrar 10.1 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 file and only the regional server accepts new license files. Then the regional server can authorize individual local clusters, based on available licenses.

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

For more details about Licensing, see the *"License Files" section in Cisco Prime Network Registrar 10.1 Installation Guide*.

The Cisco Prime Network Registrar 10.1 kit contains the following files and directories:

- Linux—CentOS/Red Hat Linux ES 6.5 and later 6.x or 7.x installation kit
- Windows—Windows Server 2012 R2 installation kit

  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.

- Docs—Pointer card, Bugs, and Enhancement List

The Cisco Prime Network Registrar also ships as a virtual appliance which includes all the functionality available in Cisco Prime Network Registrar along with the CentOS 7.7 operating system. The Cisco Prime Network Registrar virtual appliance is supported on VMware ESXi 6.x platforms, KVM Hypervisor, and OpenStack. For more details, see the *"Cisco Prime Network Registrar Virtual Appliance" section in Cisco Prime Network Registrar 10.1 Installation Guide*.

Licensing

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

Customers ordering the DD bundle would obtain a quantity one of the Caching DNS when they acquire the DNS authoritative license. If they need additional DNS caching licenses they are ordered based on Server count since DNS caching is a server based license.

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

The synchronization between version 10.1 and pre-10.1 local clusters must be done from a 10.1 regional cluster. Cisco Prime Network Registrar 10.1 protocol servers interoperate with versions 8.3 or later.

New Features and Enhancements

This section describes the features added in Cisco Prime Network Registrar 10.1:

- Elastic Lease Times, on page 3
- Caching Rate Limiting, on page 4
- Smart Cache Support, on page 4
- Caching DNS Packet Logging, on page 4
- Exclusion from Case Randomization, on page 4
- Block Recursive Queries, on page 4
- CAA Resource Record Support, on page 5
- URI Resource Record Support, on page 5

Elastic Lease Times

You may need to reconfigure the network because of the need to renumber certain network segments or to make the configuration change effective quickly. Typically, this has been done by reducing the lease times for clients in advance of the change, then applying the change, and restoring the lease times to their original values. In other words, you need to compress the renewal times into a relatively narrow window (maintenance window), and then expand them back to even out the load on the server. These steps are manual and error prone. Cisco Prime Network Registrar 10.1 helps to automate this process and to reduce the renewal load on the DHCP server before, during, and after the maintenance window. For more information, see the *“Elastic Lease Times” section in Cisco Prime Network Registrar 10.1 DHCP User Guide*.

Caching Rate Limiting

Cisco Prime Network Registrar 10.1 supports Rate Limiting, which helps the DNS server from being overwhelmed by a small number of clients. It also protects against upstream query attacks against Authoritative DNS servers. The rate limiting feature helps to mitigate some of the DDoS attacks and prevents the server from being overwhelmed by a small number of clients. This feature allows you to limit the malevolent traffic. For more information, see the *“Managing Caching Rate Limiting” section in Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*.

Smart Cache Support

Whenever Authoritative DNS servers face an outage or are offline for other reasons, this could cause issues with being able to reach Internet services that are likely not impacted. Cisco Prime Network Registrar 10.1 includes support for smart caching, which allows the Caching DNS server to continue to serve the expired data (last known answer) when it cannot reach the authoritative name servers. The Caching DNS server will continue to contact the authoritative name servers and when the name servers are once again functional, the Caching DNS server will update its expired data. For more information, see the *“Enabling Smart Caching” section in Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*.

Caching DNS Packet Logging

Cisco Prime Network Registrar 10.1 supports packet logging for Caching DNS server to help analyze and debug the Caching DNS server activity. Packet logging settings determine the type of packet logging (summary or detail), the type of packets logged, and to which log file the messages are logged. For more information, see the *"Enabling Packet Logging" section in Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*.

Exclusion from Case Randomization

Cisco Prime Network Registrar supports randomizing upstream queries, but there are some name servers that do not maintain the randomized case. Therefore, if you enable case randomization, you may block out valid name servers. The *randomize-query-case-exclusion* attribute in Cisco Prime Network Registrar 10.1 allows you to create an exclusion list, so that you can continue to use case randomization, but exclude selected name servers but still respond with a valid answer. For more information, see the *"Specifying Resolver Settings" section in Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide.*

Block Recursive Queries

Cisco Prime Network Registrar 10.1 supports blocking the recursive queries. This helps the server to not spend resources trying to process these queries. The Drop Recursive Queries (*drop-recursive-queries*) attribute controls whether the DNS server accepts or drops the queries, which have RD flag on. When this attribute is enabled, recursive queries will be dropped by the server. For more information, see the *“Blocking Recursive Queries from Authoritative Server” section in Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*.

CAA Resource Record Support

Cisco Prime Network Registrar 10.1 supports Certification Authority Authorization (CAA) Resource Record type. For more information, see the *"DNS Certification Authority Authorization (CAA) Resource Record" section in Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*.

URI Resource Record Support

Cisco Prime Network Registrar 10.1 supports Uniform Resource Identifier (URI) Resource Record type. For more information, see the *"Uniform Resource Identifier (URI) Resource Records" section in Cisco Prime Network Registrar 10.1 Authoritative and Caching DNS User Guide*

Command Line Interface Enhancements

The following commands are added or attributes modified in the CLI. For more information, see *Cisco Prime Network Registrar 10.1 CLI Reference Guide*.

New Commands

The following commands are added in the CLI:

- **cdns-rate-limit**—Controls and configures DNS rate limiting in the DNS Caching server.
- **dhcp-maintenance-window**—Configures a DHCP maintenance window.

Modified Commands

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

- **expert**—Expert mode commands
  - Deleted the following command:

    ccm sync-to-dhcp [**FailoverPair**]
  - Added the following commands:

    cdns execute flush-ns-cache *ip-address* | **all**—Drops information about all or a specific name server.

    cdns execute dump-ns-cache *filename*—Dumps the contents of the remote-ns-cache to the specified file.

    cdns execute flush-negative—Drops information about non-existing or empty domains.
- **cdns**—Configures and controls the DNS Caching server.
  - Updated the **getStats** command as follows:

    cdns getStats [<**server** | **top-names** | **rate-limit** | **all**> [**total** | **sample**]]
  - Added the **rate-limiting=11** flag to the **activity-summary-settings** attribute.
  - Added the following attributes:

    packet-log-settings, **packet-logging**, **packet-logging-file**, **randomize-query-case**, **randomize-query-case-exclusion**, **smart-cache**, **smart-cache-expiration**, and **smart-cache-expiration-reset**.

  - Updated the description of the **remote-ns-host-ttl** attribute.

- **ccm**—Configures and controls the CCM server.
  - Added the **scp-request-detail=11** and **scp-response-detail=12** flags to the **log-settings** attribute.
  - Added the **scp-request-detail** and **scp-response-detail** attributes.

- **dhcp**—Configures and controls the DHCP server.
  - Added the following command:

    dhcp getRenewalData [*max-buckets*]

  - Added the following attributes:

    distribute-renewals, **distribute-renewals-bucket-interval**, and **distribute-renewals-max-renewal-time**.

- **dns**—Configures and controls the DNS server.
  - Added the **drop-recursive-queries** attribute.
  - Updated the default value of the **edns-max-payload** attribute to **1232**.

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

  Added the **rebind-limit** attribute.

- **lease**—Manages DHCP lease objects.
  - Added the **renewal-tracked=25** flag to the **client-flags** attribute.
  - Added the **lease-rebinding-time** attribute.

- **lease6**—Manages DHCP lease6 objects.

  Added the **renewal-tracked=11** flag to the **client-flags** attribute.

- **link**—Configures IPv6 network links for use in DHCPv6.

  Added the **maintenance** attribute.

- **prefix**—Configures IPv6 network prefixes for use in DHCPv6.

  Added the **maintenance** attribute.

- **resource**—Configures resources limits and allows for viewing and resetting resources.
  - Updated the default value of the **rr-count-critical-level** attribute to **25000000**.
  - Updated the default value of the **rr-count-warning-level** attribute to **20000000**.
  - Updated the default value of the **zone-count-critical-level** attribute to **10000**.
  - Updated the default value of the **zone-count-warning-level** attribute to **8000**.

- **scope**—Specifies the scope's properties.

  Added the **maintenance** attribute.

- **task**—Configures a scheduled task.

  Added the **sync-mode** attribute.

SDK Compatibility Considerations

The following methods are added:

- clearDHCPMaintenance—Clear the DHCP maintenance attributes on scopes and/or prefixes/links.
- getDHCPRenewalData—Get the DHCP Renewal Data.
- getSessionSource—Get the optional session source information if it has been set.
- newSessionFromCluster—Get a new Session object, using the credentials from the specified CCMCluster ScpObj to establish a remote server connection.
- setSessionSource—Set the optional session source information to be logged by ccm for logins.

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 9.

This section contains the following information:

- Resolved Bugs, on page 7
- Enhancement Features, on page 8
- Open Bugs, on page 8
- Using the Bug Search Tool, on page 9

Resolved Bugs

The following table lists the key issues resolved in the Cisco Prime Network Registrar 10.1 release.

Table 1: Resolved Bugs in Cisco Prime Network Registrar 10.1

Bug ID	Description
CSCvn20662	Cisco Prime Network Registrar Denial of Service Vulnerability
CSCvo79126	SNMP server cannot be started if disabled
CSCvo92859	Backup directory is not protected against access
CSCvq63314	Cluster product version may not be updated during upgrade
CSCvr89032	ZD sync implementation is incorrect when ADNS has named views with no zones
CSCvs08424	Regional incorrectly auto propagates views to HA pairs

Bug ID	Description
CSCvs12145	Lock table runs out of available locks during DB operations

For the complete list of bugs for this release, see the **cpnr_10_1_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 features added in the Cisco Prime Network Registrar 10.1 release.

Table 2: Enhancement Features Added in Cisco Prime Network Registrar 10.1

Bug ID	Description
CSCuo78019	Add sync task options in GUI to choose sync types Update and Exact
CSCuv64947	Add DHCPv6 information to DHCP Address Current Utilization dashboard chart
CSCuz94099	Use standard RHEL/CentOS library packages
CSCvn37524	optionList AttrDescArray of OptionDefinitionSet access
CSCvp19912	Extend load balancing to DHCPv6 renewals
CSCvp49553	Improve source information reporting for incoming SCP connections
CSCvp59909	Implement Elastic Lease Time features
CSCvq73812	Add recent option definitions assigned by IETF/IANA
CSCvq75405	Improve local.superusers handling
CSCvr15221	Change default algorithm for DnsSec keys to RSA/SHA-256
CSCvr39515	Support sztp-redirect options (RFC8572) with 2-byte length

For the complete list of enhancement features added in this release, see the **cpnr_10_1_enhancements.pdf** file available at the product download site.

Open Bugs

The following table lists the open bugs in the Cisco Prime Network Registrar 10.1 release.

Table 3: Open Bugs in Cisco Prime Network Registrar 10.1

Bug ID	Description
CSCvs44967	keystore password is not encrypted when setup.exe is invoked from other directories
CSCvs46662	Node-count of license key is zero if Regional is installed on server with AMD processor

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 http://tools.cisco.com/bugsearch.

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 for them at http://tools.cisco.com/RPF/register/register.do.

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 **Prime Network Registrar 10.1** 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:

- System Requirements for Linux OS, on page 9
- Limiting the Risk of IP Fragmentation, on page 10
- local.superusers File Handling, on page 10
- Backup Directory Protection, on page 10
- SCP Connections Reporting, on page 11

System Requirements for Linux OS

Starting from Cisco Prime Network Registrar 10.1, to install Cisco Prime Network Registrar on Red Hat Enterprise Linux or CentOS, the following x86_64 (64-bit) packages must be installed (over and above the Java Run-Time):

Table 4: Packages to Install

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

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

Limiting the Risk of IP Fragmentation

IP fragmentation is a problem on the Internet today, especially when it comes to large DNS messages. Even if fragmentation works, it might not be secure enough for DNS. These issues can be fixed by a) setting the EDNS buffer size lower to limit the risk of IP fragmentation and b) allowing DNS to switch from UDP to TCP when a DNS response is too big to fit in this limited buffer size. The default EDNS buffer size for both the Caching and Authoritative DNS servers is 4096 bytes, but may be lowered to a smaller value (that is, 1232 bytes) to prevent IP fragmentation.

Use the following commands to set the EDNS buffer size:

Authoritative DNS servers:

```
nrcmd> session set visibility=3
nrcmd> dns set edns-max-payload=1232
nrcmd> dns reload
```

Caching DNS servers:

```
nrcmd> session set visibility=3
nrcmd> cdns set edns-buffer-size=1232
nrcmd> cdns set max-udp-size=1232
nrcmd> cdns reload
```

local.superusers File Handling

When using the local.superusers file, all users in the file must now be prefixed with "local$". For more information, see the *"Managing Administrators" section in Cisco Prime Network Registrar 10.1 Administration Guide*.

Backup Directory Protection

When the shadow backup utility creates the backup directory, it will now protect it, so that only the owner has access. However, this is only done if the directory is created - not if it already exists. If you are upgrading, you may want to review the protection and adjust it accordingly.

For example:

- To remove other (world) access, use the following command:

```
chmod o-rwx /var/nwreg2/local/data.bak
```

- To remove group access, use the following command:

```
chmod g-rwx /var/nwreg2/local/data.bak
```

SCP Connections Reporting

In Cisco Prime Network Registrar 10.1, the SCP client provides additional information about the connection when available and can be:

- The source address and port of the incoming HTTP/HTTPS connections (for web UI and REST sessions).
- The source address, port, and user information for the incoming CLI, tools, or SDK sessions. The addresses and ports for the initiating user's SSH connection may also be provided, if available (this is based on the user's SSH_CONNECTION environment variable).
- Other useful indications, such as:
  - “Regional-to-local management” or “Local-to-regional management” for CCM connections between the local and regional clusters.
  - “Local-to-local management” for failover or HA sync, or other CCM-to-CCM connections between the local clusters.
  - Other identifiers, enclosed in < and >, for server related connections that identify the server (and sometimes additional details).

Note As this information is supplied to CCM by the client, it may be subject to spoofing and should be treated as informational, but not authoritative.

For more information, see the *"Active User Sessions" and "Logs for Session Events" sections in Cisco Prime Network Registrar 10.1 Administration Guide*.

Related Documentation

See Cisco Prime Network Registrar Documentation Overview for a list of Cisco Prime Network Registrar 10.1 guides.

Accessibility Features in Cisco Prime Network Registrar 10.1

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.

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