Cisco Prime Network Registrar 10.0 Release Notes

First Published: 2018-11-23

These release notes provide an overview of the new and changed features in Cisco Prime Network Registrar 10.0 and describe 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 10.0, review the system requirements and licensing information available in the *Cisco Prime Network Registrar 10.0 Installation Guide*.

Note If you are migrating to Cisco Prime Network Registrar 10.0 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 of the *Cisco Prime Network Registrar 10.0 Installation Guide*.

The Cisco Prime Network Registrar 10.0 kit contains the following files and directories:

- Linux—CentOS 6.5/Red Hat Linux ES 6.5 and later installation kit
- Windows—Windows Server 2012 R2 installation kit
- 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 7.5 operating system. The Cisco Prime Network Registrar virtual appliance is supported on VMware ESXi 5.5 or later platforms, CentOS/RHEL 7.5 KVM Hypervisor, and an OpenStack installation running on CentOS/RHEL 7.5. For more details, see the "Cisco Prime Network Registrar Virtual Appliance" section of the *Cisco Prime Network Registrar 10.0 Installation Guide*.

Licensing

Cisco Prime Network Registrar 10.0 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 and 9.x versions. For Cisco Prime Network Registrar 10.0, the licensing is done according to the services that you require. For more information, see the "License Files" section of the *Cisco Prime Network Registrar 10.0 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 10.0 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 10.0 and pre-10.0 local clusters must be done from a 10.0 regional cluster. Cisco Prime Network Registrar 10.0 protocol servers interoperate with versions 8.1 or later except as noted below.

- Cisco Prime Network Registrar 10.0 protocol servers, except DHCP failover, interoperate with 8.1 or later. DHCP failover interoperates with 8.2 and later.

Note If you are upgrading to 10.0 from 8.1 or earlier, note that the DHCP failover now uses TCP instead of UDP and this requires updating firewalls to allow TCP traffic on failover port (547) instead of UDP. Also, as of 8.2, failover now supports DHCPv6 in addition to DHCPv4 and only simple failover (back office and symmetrical configurations are no longer supported). For more details on the failover changes made in 8.2, see the DHCP Failover (DHCPv4 and DHCPv6) section of the Cisco Prime Network Registrar 8.2 Release Notes.

New Features and Enhancements

This section describes the features added in Cisco Prime Network Registrar 10.0:

Session Management

Cisco Prime Network Registrar 10.0 provides administrator functions to monitor user sessions, manage system configuration for session management, and report login information for each user. Session events are added to provide login and logout details for each user. For more information, see the "Session Management" section of the *Cisco Prime Network Registrar 10.0 Administration Guide*.

GTP Echo Support for Host Health Check

Prior to Cisco Prime Network Registrar 10.0, in the DNS Host Health Check, DNS used ICMPV4 and ICMPV6 to determine the host health. In Cisco Prime Network Registrar 10.0, DNS host health check now also supports GTP echo message to determine whether hosts are available or unavailable, and the end result is the same as the ping (i.e., unresponsive end points are not returned in the query response). For more information, see the "DNS Host Health Check" chapter of the *Cisco Prime Network Registrar 10.0 Caching and Authoritative DNS User Guide*.

Generalized UDP Source Port for DHCP Relay

Cisco Prime Network Registrar 10.0 supports RFC 8357 (Generalized UDP Source Port for DHCP Relay). These are not "configurable" options and require specialized server processing. A new DHCPv6 attribute, *client-relay-port*, is added to the Lease6 objects.

Note You must upgrade both the failover partners to make use of this feature.

Cluster's UUID as DHCPv6 Server Identifier

Prior to 10.0 release, the DHCP server generated a Server ID (DUID) using the DUID-LLT (link layer address plus time) format and wrote this into the lease state database if no stored entry already existed in the database. This server identifier would be used thereafter unless explicitly removed using the leaseadmin tool (**`leaseadmin -d`** *`server-duid`*). This could cause problems if the lease state database was copied and moved to a different cluster unless the leaseadmin tool was used to remove the server identifier from the copied database.

To eliminate the need for special steps if a lease state database is copied to another cluster, starting with 10.0 release the server can instead use the local cluster's Universal Unique Identifier (UUID) using the DUID-UUID format. This UUID is stored by ccmsrv and is not stored in the lease state database. Therefore, copying just the lease state database will not cause the same server identifier to be used on both clusters.

However, for upgrades from earlier versions, the existing Server ID will continue to be used unless explicitly removed after the upgrade by using the leaseadmin tool. Therefore, if you are upgrading from an earlier release where the server identifier was written to the database, you should use the leaseadmin tool to remove the server identifier stored in the lease state database to move to the cluster UUID based server identifier.

Note When the server identifier changes, existing clients that attempt to renew DHCPv6 leases will fail to get a response until they send a Rebind request (at the "T2" time).

DNSSEC Enhancements

To simplify configuration, the default behavior uses a single KSK for all zones associated with a given tenant. However, they will all rollover at the same time because the zones use the same keys. Key groups let you create different keys for different groups of zones or even individual zones. Each set of keys will then have its own rollover schedule. In Cisco Prime Network Registrar 10.0, the *key-group* attribute is added to specify the zone KSK and ZSK. If set, these keys and any associated rollover keys will be used to sign the zones, instead of all available keys.

The **dnssec-key getStatus** command is added to manage rollover of multiple keys more easily.

Cisco Prime Network Registrar 10.0 supports CDS and CDNSKEY Resource Records (as described in RFC 7344 and RFC 8078) to ease the KSK rollover process in split DNS server setups, where the parent zone is externally owned.

REST API Enhancements

The following REST APIs are added in Cisco Prime Network Registrar 10.0. For more information, see *Cisco Prime Network Registrar 10.0 REST APIs Reference Guide*.

- REST APIs to obtain the utilization data for scopes and prefixes (v4 and v6 utilization)
- REST APIs to apply scope, zone, prefix, and link templates. These can be applied to new or existing configuration objects using the applyTemplate action. General template support is added for other types of configuration objects.
- REST API to get the server system stats for the individual servers. REST support is added for SystemStats and ServerSystemStats classes.

Command Line Interface Enhancements

The following commands are added or attributes modified in the CLI. For more information, see the *Cisco Prime Network Registrar 10.0 CLI Reference Guide*.

New Commands

The following commands are added in the CLI:

- **address-type**—Configures a address space type
- **task**—Configures a scheduled task

Modified Commands

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

- **admin**—Creates administrators and assigns them groups and passwords
  - Added the **unlimited-sessions** attribute.
- **ccm**—Configures and controls the CCM server
  - Added the following attributes:

admin-failed-login-limit, admin-suspended-timeout, admin-token-session-limit, admin-user-session-limit, and log-settings

- **dns**—Configures and controls the DNS server
  - Updated the **getStats** command to include the **update** statistics.

    dns getStats [**performance** | **query** | **update** | **errors** | **security** | **maxcounters** | **ha** | **ipv6** | **dns-pn** | **cache** | **datastore** | **top-names** | **dns-hhc** | **all**] [**total** | **sample**]
  - Updated the **rollover-ksk** command to inlude the **key-group** attribute.

    dns rollover-ksk [**tenant-id**=<value>] [**next-key**=<keyname> | **key-group**=<value>]
  - Added the **update=16** flag to the **activity-counter-log-settings** attribute.
  - Added the **minimize-ttls** attribute.
- **dnssec-key**—Manages Authoritative DNSSEC Key objects
  - Added the following command:

    dnssec-key getStatus
  - Added the following attributes:

    key-group, rollover-due-date, and status
- **export**—Exports configuration information to a file
  - Added the following command:

    export changeLog <filename> [<attribute>=<value> ...] [**-all**]
- **lease6**—Manages DHCP lease6 objects
  - Added the **client-relay-port** attribute.
- **prefix**—Configures IPv6 network prefixes for use in DHCPv6
  - Added the **range-end** and **range-start** attributes.
- **prefix-template**—Configures a prefix template
  - Added the following attributes:

    range-end-expr, range-start-expr, and restrict-to-admin-allocation
- **zone**—Configures a DNS zone
  - Updated the **rrSet** command to include the **gtp-echo** option.

    zone <name> **rrSet** <rr-name> [**set** <host-health-check=off/ping/gtp-echo>] [**get** <host-health-check>] [**unset** <host-health-check>] [**show**]
  - Added the **key-group** attribute.

SDK Compatibility Considerations

The following methods are added:

- getAdminFailedLogins—Get the number of failed login attempts since the previous successful login by the current administrator.
- getAdminLastLogin—Get the date and time of the previous successful login by the current administrator.
- setSuspendedAdmin—Suspend or reinstate an administrator account.

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 8.

This section contains the following information:

Resolved Bugs

The following table lists the key issues resolved in the Cisco Prime Network Registrar 10.0 release.

Table 1: Resolved Bugs in Cisco Prime Network Registrar 10.0

Bug ID	Description
CSCvh21633	Zone distribution should update exceptions in replace mode
CSCvj20106	Caches can grow excessively if configured greater than 2GB each
CSCvk12864	DHCPv6 DHCID RR data may be incorrect when client has lookup key
CSCvk48286	Installer does not create appropriate service unit files on CentOS and RHEL 7.x
CSCvm10856	CCM server may hang when updating base licenses

For the complete list of bugs for this release, see the **cpnr_10_0_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 10.0 release.

Table 2: Enhancement Features Added in Cisco Prime Network Registrar 10.0

Bug ID	Description
CSCvb86135	Add CCM server option to set log settings
CSCve08751	DNS activity-summary log settings should take effect without a reload
CSCvg46490	Add option to assign specific DNSSEC keys to a zone
CSCvg46597	Add support for CDS and CDNSKEY Resource Records
CSCvh29435	Allow enabling syslog for individual messages
CSCvh31093	Provide mechanism to override giaddr / link-address for determining client's network location
CSCvh69708	Add address-type command to CLI
CSCvi77306	Allow scheduled tasks to run more frequently
CSCvi77341	Add ability to specify address allocation range for dhcp prefixes
CSCvi82295	Add ability to manage scheduled tasks to CLI
CSCvi86619	Add REST action to apply templates
CSCvi86681	Add ServerSystemStats to REST API
CSCvi86692	Add utilization to REST API
CSCvj00394	Add CLI command to export change log records to CSV file
CSCvj07028	Provide indication that external authentication servers down on login attempt
CSCvj17115	Add lease-requested-prefix-length data item to response dictionary
CSCvj22476	Use cluster's UUID as DHCPv6 server-identifier

For the complete list of enhancement features added in this release, see the **cpnr_10_0_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 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 10.0** 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:

Incorrect DHCPv6 DHCID RR Data when Using Lookup Key

When using lookup keys for DHCPv6 leases, the server may end up using disambiguated (-1) names in DNS for these clients (the original entries will not be deleted). To solve this, you should validate the original name is either the same or no longer in use, and manually remove these entries from the DNS zone(s). This is only an issue for forward zones.

Incorrect DHCID RR Client Data for DHCPv4 DNS Update

If DHCP is configured to use DHCID RRs for DHCPv4 DNS updates, the server may start using disambiguated names (or, if disabled, updates will fail) and old names may fail to be removed. This is because the server used incorrect data to generate the DHCID RR information in versions prior to 10.0.

To avoid these problems, it is highly recommended that you perform the following steps BEFORE upgrading:

Procedure

Step 1 At least the longest lease time period before the expected upgrade time, set the DHCP server's *dns-client-identity* to **regress-to-txt**, enable *force-dns-update* (you may want to record the existing setting to restore it to this at a later time), and reload the DHCP server. This will cause the server to transition the existing entries back to TXT RRs instead of using DHCID RRs.

Step 2 Upgrade the server after the longest lease time after Step 1.

Step 3 Configure the DHCP server's *dns-client-identity* to **transition-to-dhcid** and reload the server. This will cause the server to start to move clients to using the DHCID RRs.

Step 4 A bit after the longest lease time time after Step 3, you can restore the *force-dns-update* setting and also set the *dns-client-identity* to **dhcid**.

Step 5 Reload the server.

Note The above steps will impact dual stack clients for clients that use the DUID format of client identifier (see RFC 4361) that would allow the same name to be used for both DHCPv4 and DHCPv6 leases when the DHCID RR was used. During the window covered by the above steps, the client will have different v4 and v6 names because DHCPv4 updates will use the TXT RR instead of the DHCID RR.

DNS Performance and Firewall Connection Tracking

Caution Many distributions of Redhat and CentOS Linux come with a firewall and connection tracking installed and enabled by default. Running a stateful firewall on the same OS and DNS will cause a significant decrease in server performance. Cisco strongly recommends NOT to use a firewall on the DNS server's operating system. If disabling the firewall is not possible, then connection tracking of DNS traffic MUST be disabled. For more information, see the "DNS Performance and Firewall Connection Tracking" section of the *Cisco Prime Network Registrar 10.0 Administration Guide*.

Performance Impact of Spectre and Meltdown Security Fixes

The fixes for the Spectre and Meltdown vulnerabilities add new overhead for all kernel transitions, which particularly impacts the networking calls used by Cisco Prime Network Registrar. This additional overhead results in considerable degradation in the Cisco Prime Network Registrar performance. For a general explanation of these issues (independent of Cisco Prime Network Registrar), conduct an internet search for “Controlling the Performance Impact of Microcode and Security Patches”.

When operating on a system with the Spectre and Meltdown security fixes in operation, Cisco Prime Network Registrar performance is significantly lower than it is on a system without any of these fixes. However, it is possible to use an up to date system and disable most of the Spectre and Meltdown security fixes.

Disabling the fixes will largely restore the Cisco Prime Network Registrar performance to what it was prior to the implementation of these fixes.

In our testing, with Spectre and Meltdown fixes disabled, DHCP New Lease performance improves by approximately ~20%, and renewal performance improves by approximately ~85%. DNS Non-Cached query performance improves by approximately ~24%, and Cached performance improves by ~29%.

Note These improvements are measured from the degraded performance created by the Spectre and Meltdown fixes themselves. These improvements return the performance of Cisco Prime Network Registrar close to the performance prior to the implementation of the fixes for Spectre and Meltdown.

Using Red Hat Enterprise/CentOS Linux Tunables, you can control the performance impact of the Spectre and Meltdown vulnerability patches of the following CVEs:

- CVE-2017-5754
- CVE-2017-5715
- CVE-2017-5753

It is of paramount importance that you understand that if you decide to disable the Spectre and Meltdown fixes, you may face the very attacks that these fixes are designed to prevent. We are not recommending that you disable these fixes. We are simply informing you of the consequences of running Cisco Prime Network Registrar with them enabled or disabled.

You can disable each of three parameters individually. These do not persist through a reboot. Disable them at runtime with the following three commands. The change is immediately active and does not require a reboot.

```
echo 0 > /sys/kernel/debug/x86/pti_enabled
echo 0 > /sys/kernel/debug/x86/retp_enabled
echo 0 > /sys/kernel/debug/x86/ibrs_enabled
```

This requires that the **debugfs** filesystem be mounted. In RHEL/CentOS 7 the **debugfs** is mounted by default. You can check that **debugfs** is mounted with the following command:

```
mount | grep debugfs
```

If present, you will see the following:

```
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
```

To verify the fixes for these CVEs are correctly disabled, cat the following three files to verify their values are all set to 0.

```
cat /sys/kernel/debug/x86/pti_enabled
cat /sys/kernel/debug/x86/retp_enabled
cat /sys/kernel/debug/x86/ibrs_enabled
```

It is possible to persistently disable the required parameters (i.e., to be effective across a reboot). For an explanation and instructions on how to do this, refer to the vendor site, found through your previous internet search.

Related Documentation

See Cisco Prime Network Registrar Documentation Overview for a list of Cisco Prime Network Registrar 10.0 guides.

Accessibility Features in Cisco Prime Network Registrar 10.0

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.