Cisco Prime Network Registrar 8.3 Release Notes

March 9, 2015

These release notes provide an overview of the new and changed features in Cisco Prime Network Registrar 8.3, and describe how to access information about the known problems in Cisco Prime Network Registrar 8.3.

Note: You can access the most current Cisco Prime Network Registrar documentation, including these release notes, online at:
http://www.cisco.com/en/US/products/ps11808/tsd_products_support_series_home.html.

Contents

This document contain 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.

In addition, for IP address management, you can deploy Cisco Prime Network Registrar IPAM, or you can integrate it with the DHCP and DNS components of Cisco Prime Network Registrar.

Before you Begin

Before you install Cisco Prime Network Registrar 8.3, review the system requirements and licensing information available in the *Cisco Prime Network Registrar 8.3 Installation Guide.*

Note: If you are migrating to Cisco Prime Network Registrar 8.3 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 Network Registrar 7.x or earlier are not valid for Cisco Prime Network Registrar 8.x.

Cisco Prime Network Registrar IPAM is licensed separately from Cisco Prime Network Registrar DHCP, DNS, and Caching DNS. When installing IPAM, you will be asked to install as a separate process using a separate license key. To receive the IPAM license, you must purchase Cisco Prime Network Registrar IPAM, either individually, or as part of a Cisco Prime Network Registrar suite.

For more details about Licensing, see the License Files section in the Overview chapter of the *Cisco Prime Network Registrar 8.3 Installation Guide*.

The Cisco Prime Network Registrar 8.3 kit contains the following files and directories:

- Solaris—Solaris 10 installation kit.

Note: Cisco Prime Network Registrar 8.3 will be the last release to support Solaris.

- Linux5—Red Hat Linux ES 5.x or 6.x installation kit.
- Windows—Windows Server 2008 R2 installation kit.
- Docs—Pointer card, Bugs, Enhancement List.

Market Segment Specific Licensing

Cisco Prime Network Registrar introduced separate licenses for the components (System, DHCP, DNS, and CDNS) in release 8.0. For information on the Cisco Prime Network Registrar component-based license set, see the License Files section of the *Cisco Prime Network Registrar 8.3 Installation Guide*.

From Releases 8.1.2 and 8.1.3, Cisco Prime Network Registrar license types are offered specific to market segments. Market-specific licensing generates license keys for use by market segments, that is, Service Provider, Smart Grid, and others. Cisco Prime Network Registrar features are enabled based on the market segment specific license you choose.

Cisco Prime Network Registrar currently offers the following two sets of market segment based licenses:

- PNR
- PNR-SG

Note: If the licenses for both market segments are installed, then only the PNR license will be active.

The PNR license offers features designed for the Enterprise and Service Provider market segment whereas the PNR-SG license offers features designed for the Smart Grid market segment.

The regional server which uses the PNR-SG license can be converted to PNR by installing the PNR license. Local cluster licenses will be converted automatically at the next compliance check, or can be manually updated by resynchronizing the local cluster.

For a given market segment license, only the counts from corresponding market segment license will apply.

For example, if the PNR count license is applied when the PNR-SG base license is active, the Right to Use count will not be updated. If the PNR-SG count license is applied when the PNR base license is active, the Right to Use count will not be updated.

PNR Licenses

The PNR license provides all the features available for the Cisco Prime Network Registrar release you install. If your license set was issued for a release earlier than 8.1.2, it is a PNR license.

PNR-SG Licenses

The PNR-SG license offers the following PNR features with the exception of (identified as not necessary for Smart Grid Implementations):

- Tenants
- External Authentication
- Extensions
- Lightweight Directory Access Protocol (LDAP)
- TCP Listeners (client notification)
- Trivial File Transfer Protocol (TFTP)
- Router Interface Configuration (RIC)
- Regional lease history and subnet utilization
- BYOD

Note: Before you install Cisco Prime Network Registrar 8.3, review the system requirements and licensing in the *Cisco Prime Network Registrar 8.3 Installation Guide*.

Interoperability

Cisco Prime Network Registrar 8.3 uses individual component licenses. This allows users to purchase and install DHCP services, Authoritative DNS and Caching DNS services, and IPAM services individually, or as a suite.

When you purchase the full set of Cisco Prime Network Registrar components, you receive a license package for IPAM, and a separate license for Cisco Prime Network Registrar DHCP and DNS components (Authoritative and Caching DNS).

Customers ordering the DDI 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 Cisco Prime Network Registrar IPAM license is installed separately and does not use the regional server.

The synchronization between version 8.3 and pre-8.3 local clusters must be done from an 8.3 regional cluster. Cisco Prime Network Registrar 8.3 protocol servers interoperate with versions 7.2 or later except as noted below.

- Cisco Prime Network Registrar 8.2 and later DHCPv4 failover servers do not interoperate with Cisco Network Registrar 8.0, 8.1failover servers.
- The HA protocol version has been updated in Cisco Prime Network Registrar 8.0 and communications with earlier versions is not supported.

Caution:

- By the nature of the EDNS0 protocol, Cisco Prime Network Registrar 8.3 DNS servers interoperate with earlier versions of Cisco Prime Network Registrar DNS (and third party DNS vendors). EDNS0 defines the interoperability with DNS servers that do not support EDNS0. Cisco Prime Network Registrar 8.3 DNS adheres to the RFC and consequently interoperates with earlier versions of Cisco Prime Network Registrar.
- Cisco Prime Network Registrar 8.3 DDNSv6 interoperates with Cisco Network Registrar 7.0 and later DNS servers because of the use of the DHCID RRs (in place of TXT RRs for DDNSv6).
- Cisco Prime Network Registrar 8.3 does not interoperate with Cisco Prime Network Registrar IPAM 8.1.1 or 8.1.2. An updated version of Cisco Prime Network Registrar IPAM is required to interoperate with Cisco Prime Network Registrar 8.3.

New Features and Enhancements

This section describes the features added in Cisco Prime Network Registrar 8.3.

Client-based DNS64 Prefixes

Cisco Prime Network Registrar DNS caching server supports DNS64, synthesizing AAAA (IPv6) records from A (IPv4) records, when an IPv6 client queries for AAAA records. DNS64 also handles reverse queries for the NAT64 prefixes. DNS64 with NAT64 provides access to the IPv4 internet and servers for hosts that have only IPv6 addresses. Cisco Prime Network Registrar 8.3, now supports up to 30 IPv6 prefixes in synthesis of IPv6 address for IPv4-only server instead of single prefix. The requests are matched to DNS64 prefixes using ACLs.

However, while configuring DNS64 on multiple Caching DNS servers, ensure that the same version of Cisco Prime Network Registrar is installed on all the servers.

Internationalized Domain Names

Cisco Prime Network Registrar 8.3 supports the full set of unicode characters to name DNS domains in the web UI, web-services (REST), and Java SDK with limited sort and search capabilities. The web UI displays domain names both in unicode and ASCII Compatibility Encoding format. The search and sort of unicode Domain names is possible only using the ASCII representation. The Cisco Prime Network Registrar CLI does not support unicode characters in this release.

Caching DNS and Authoritative DNS Server on the Same Operating System (DNS Hybrid)

In Cisco Prime Network Registrar 8.3, for small-sized DNS configurations, you can install the Caching DNS and Authoritative DNS servers on the same operating system, without the need for two separate virtual or physical machines.

The configuration is only recommended for smaller DNS configurations where the incoming traffic is low and a separate Caching DNS would not be required. When the Hybrid-mode configuration is enabled, the Caching DNS server detects the Authoritative DNS server on the same operating system and configures the in-memory exceptions to match the Authoritative DNS server zones. Caching DNS and Authoritative DNS needs different interfaces on the same operating system or have Authoritative DNS hidden on a separate port. Most management can be done via the Authoritative DNS configuration and reloads to Authoritative DNS causes Caching DNS to also reload automatically. For more information, see the *Setting up Caching DNS and Authoritative DNS Server on Same Operating System* section in *Cisco Prime Network Registrar 8.3 User Guide.*

DNS Response Policy Zone (RPZ)

Cisco Prime Network Registrar 8.3 supports Response Policy Zones (RPZ). The DNS firewall rules can be set up for specially designated zones on the Authoritative DNS server. The RPZ and RR data combined with DNS Caching server resolver effectively creates a DNS firewall to prevent the misuse of the DNS server.

The RPZ firewall rules utilize both the Authoritative DNS and the Caching DNS servers to provide the RPZ functionality. The Authoritative DNS server stores the data for RPZ and the RPZ rules in the form of resource records (RRs). The Caching DNS server uses DNS Firewall configurations to access the rules and apply them to client queries and responses. For more information, see the *DNS Response Policy Zone (RPZ) Firewall Rules* section in *Cisco Prime Network Registrar 8.3 Caching and Authoritative DNS User Guide.*

Secured Dynamic DNS and Zone Transfer using GSS-TSIG

Cisco Prime Network Registrar 8.3 supports the Dynamic DNS Updates and Zone Transfer through secured GSS-TSIG mechanism.

The RFC 3645 enables TSIG to establish the Generic Security Service (GSS) method of secure key exchange, eliminating the need for manually distributing keys to all GSS clients. RFC 3645 defines an algorithm to use with TSIG, which is based on the Generic Security Service Application Program Interface (GSS API), as specified in RFC2743.

For each unique connection between GSS and TSIG enabled applications, a unique security context is required in GSS-TSIG. Establishing a security context involves a negotiation between GSS-TSIG-client application and GSS-TSIG-server application. After the security context is established, it has a finite lifetime during which it can be used to create and verify the transaction signature on messages between the two applications. The GSS-API implementation uses Kerberos V5 authentication protocol as its underlying security mechanism.

Cisco Prime Network Registrar REST APIs

The Representation State Transfer APIs (REST APIs) provide an alternative method to the Cisco Prime Network Registrar for provisioning selected functions. You can use the REST APIs to service a set of standard requests for all persisted (non-transient) classes in the service definition.

Either XML or JSON formatted objects, are specified as input or output parameters, as applicable. Request parameters are used to further qualify the client requests formed by URLs that identify the requested resource.

Miscellaneous Licensing Enhancements

In Cisco Prime Network Registrar 8.3, you can register a local cluster that is behind a NAT instance by initiating the registration from the local cluster. To register a local cluster that is spanned by a NAT instance, you must ensure that Cisco Prime Network Registrar 8.3 or later is installed on both the regional and local clusters. For more information, see the *Registering a Local Cluster that is Behind a NAT* section in the *Cisco Prime Network Registrar 8.3 Administration Guide.*

Resource Limit Alarms

Resource limit alarms enable you to monitor the Cisco Prime Network Registrar system resources and provides an indication when one or more product resources have entered potentially dangerous levels and requires attention.

Resource limit alarms are designed to convey the resource limit information in an organized and consolidated way. You can reset the predefined threshold levels for both critical and warning levels for each monitored resource. Cisco Prime Network Registrar reports the current status, the current value, and the peak value of the resources monitored in the web UI and CLI. The peak value is compared to the configured warning or critical limit for the resource limit alarm and the status of the resource limit alarm is displayed as OK, Warning or Critical.

The resource limit alarms are updated at regular intervals based on the polling interval configured. If SNMP traps are enabled for the resource limit alarms, Cisco Prime Network Registrar generates SNMP traps when the monitored resources exceed the critical or warning levels.

Cisco Prime Network Registrar displays the alarm in the web UI and CLI until the resulting condition no longer occurs and the peak value is reset.

Installing Protocol Servers without Super User Privilege

In Cisco Prime Network Registrar 8.3, you can now run Cisco Prime Network Registrar Local Server Agent as a non-root *nradmin* user on Linux. If you choose to run Cisco Prime Network Registrar for a non-root user, a user *nradmin* is created with the requisite privileges to run the Cisco Prime Network Registrar services. For more information, see the *Installing Cisco Prime Network Registrar* section in *Cisco Prime Network Registrar 8.3 Installation Guide.*

Supports CentOS 6.5

The operating system in Cisco Prime Network Registrar 8.3 Regional and Local virtual appliance is updated from CentOS 6.0 to CentOS 6.5. The Cisco Prime Network Registrar 8.3 OVAs are built using a new Packer process, unlike the previous versions built using VMWare Studio. Packer process is transparent and enables the resulting build process to adapt easily to other OS versions and to future products. The new packaging includes a change from an OVF contained in a .zip file, to a single .ova file. This simplifies deployment, since unpacking the .zip containing multiple files to get at the .ovf file, is avoided.

The process of configuring network in Cisco Prime Network Registrar 8.3 is script based where the user needs to run 'configurenetwork' command on completion of deployment. After booting up, if the system identifies the database and the code versions to be dissimilar, it directs to run a script to upgrade the database. At every login, the version of Cisco Prime Network Registrar running is displayed. For more information, see the *System Requirements* section in *Cisco Prime Network Registrar 8.3 Installation Guide*.

Note: To avoid the leap second issue in the existing installation, you need to apply the CentOS patch to your system.

Web UI Enhancements

Cisco Prime Network Registrar 8.3 supports a new web UI with improved usability that supports.

- Enhanced display of attribute groups.
- Customer display using widgets for special attributes.

The web UI enhancements in Cisco Prime Network Registrar 8.3 provide improved look and feel which is consistent with the Cisco Prime suit of products.

External Authentication using Active Directory

Cisco Prime Network Registrar 8.3 supports authentication of users against Microsoft Active Directory.

Existing AD user accounts can be used to log into the Cisco Prime Network Registrar webUI/CLI/SDK local and regional clusters by adding the user to the Cisco Prime Network Registrar access privileged group.

Cisco Prime Network Registrar CCM server uses Kerberos, LDAPv3, and DNS to provide secure, centralized authentication for the identified users in AD and to determine if an authenticated user is authorized to access Cisco Prime Network Registrar.

BYOD Support

Bring your own device (BYOD) support in Cisco Prime Network Registrar 8.3 is to permit users to use a personal mobile devices for the business communications in a secured way. The advantage of BYOD support is that it supports hands-off, user-driven configuration of device with correct IP Addresses and network settings.

When a BYOD device connects to the network for the first time, the user is redirected to the BYOD self-registration web page to register the device. The web portal registration page populates the device details and prompts the user to authenticate against the active directory server. Upon successful authentication, the device is registered with the DHCP server. The BYOD registration portal is tightly integrated with DHCP, CDNS of Cisco Prime Network Registrar.

To support BYOD feature in Cisco Prime Network Registrar 8.3, the DHCP server and CDNS server (changes are required in backup, if DHCP failover pairs is configured) needs to be configured with specific attributes.

Limitations and Restrictions

This section describes limitations and restrictions you might encounter while using Cisco Prime Network Registrar 8.3.

- The Regional Pull Replica Address Space fails when reservations are being pulled for new failover-pair objects. This problem occurs only if there is a new failover-pair and one or more reservations associated with that failover-pair.

  To work around this issue, repeat the operation twice—first checking Omit Reservations and then without checking Omit Reservations. After the failover-pairs have been pulled, subsequent pull replica address space operations will work correctly.

- In situations where a DHCPv6 server supports clients with multiple leases, the demand on server memory increases. DHCPv4 supports only one lease per client, while DHCPv6 supports multiple leases. Therefore, a server running DHCPv6 cannot support as many leases (clients) as the same server running DHCPv4. For example, one DHCPv6 client might require 2,500 bytes of space compared to 1,000 bytes per DHCPv4 client. This means that a machine that would support one million DHCPv4 clients supports only 400,000 DHCPv6 clients. We recommend that you allow three times the memory for DHCPv6 clients as you would for DHCPv4.

  You must:

  - Be aware of how many prefixes per link are configured. If the configuration has two prefixes on a link, then with default configuration parameters, you have to cut in half the number of clients.
  - Use care if you enable inhibit-all-renews. When enabled, each client would use at least two leases, and perhaps three, depending on the grace and affinity times per prefix.
- Cisco Prime Network Registrar 8.3 works with Java 1.6 or earlier version of Java 1.7. For more details refer CSCur61513.
- The following features are not supported on the Solaris platform:
  - Secured Dynamic DNS and Zone Transfer using GSS-TSIG
  - External Authentication using Active Directory
  - BYOD support

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, page 9.

This section contains the following information:

Resolved Bugs

Table 1 on page 8 lists the key issues resolved in the Cisco Prime Network Registrar 8.3 release.

Table 1 Resolved Bugs in Cisco Prime Network Registrar 8.3

Bug ID	Description
CSCur61513	The Network Registrar installation is successful, but the browser fails to respond when attempting to connect into the Web UI.

For the complete list of bugs for this release, see the cpnr_8_3-buglist.pdf file available at the product download site. See this list especially for information about fixes to customer-reported issues.

Enhancement Features

Table 2 on page 8 lists the key enhancement features added in the Cisco Prime Network Registrar 8.3 release.

Table 2 Enhancement Features Added in Cisco Prime Network Registrar 8.3

Bug ID	Description
CSCup43302	Improved syslog support to include message ids and protocol server names in log messages.

For the complete list of enhancement features added in this release, see the cpnr_8_3-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.

1. Go to http://tools.cisco.com/bugsearch.
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.
3. To search for a specific bug, enter the bug ID in the Search For field and press **Return**.
4. To search for bugs in the current release:

a. Click the **Search Bugs** tab and specify the following criteria:

   a. In the Search For field, enter Prime Network Registrar 8.3 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.

Command Line Interface Enhancements

The following commands were added and attributes modified or deprecated in the CLI (see the *Cisco Prime Network Registrar 8.3 CLI Reference Guide*).

New Commands

Note: For more information, see the *Cisco Prime Network Registrar 8.3 CLI Reference Guide.*

The following new commands were added to the CLI:

- **resource** command—Configures resource limits and allows for viewing and setting resources.
- **auth-ad-server** command–Configures External Authentication Active Directory servers.
- **byod** command—Specifies the configure the BYOD web server in the Regional cluster.
- **gss-tsig** command–Configure GSS-TSIG objects.

Modified Commands

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

- **cdns64** command–Controls and configures DNS64 processing in the DNS Caching server.
- **dns** command–Configures and controls the DNS server.
- **cdns-firewall** command–Configures and controls the DNS firewall processing in the DNS Caching server.

Related Documentation

See Cisco Prime Network Registrar Documentation Overview for a list of Cisco Prime Network Registrar 8.3 guides.

Accessibility Features in Cisco Prime Network Registrar 8.3

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, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the Command Line Interface Enhancements, page 9 section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2015 Cisco Systems, Inc. All rights reserved.