DNS Push Notifications

- DNS Push Notifications, on page 1

DNS Push Notifications

DNS Push Notifications is a mechanism where a client is asynchronously notified when changes to DNS records occur. The feature allows the Authoritative DNS server to accept TCP connections from DNS Push Notification clients and accept subscription requests for specific DNS record names and optionally record types. Once the subscription is accepted, the client will receive update notifications whenever the subscribed to record is changed. Also if the record exists at the time of subscription, the client will receive an initial update notification of the existing record.

DNS Push Notifications Configuration Settings

DNS Push Notifications comes with pre-configured settings but it is not enabled by default. In order to use DNS Push Notifications the push-notifications setting must be enabled at the DNS Server level and on the desired zone(s). DNS Push Notifications can be enabled on any CNR DNS server that hosts the zone we want notifications on. This can be primary and secondary zones.

Note DNS server must be reloaded for DNS Push Notification changes to take effect.

Use the below DNS Server Level Attributes to enable DNS Push Notifications:

Table 1: DNS Server Level Attributes

Attribute	Description
push-notifications	Enables or disables Push Notification support in the DNS server. The default is disabled.
pn-port	Specifies the TCP port number that the DNS server uses to listen for DNS Push Notifications connections. The default is 5352. The available range is 1-65535, but cannot be the same as the DNS server port.
pn-acl	Specifies the access control for Push Notifications. The default is any.

pn-max-conns	Specifies the maximum number of individual DNS Push Notification connections the server will allow. Once the maximum has been reached, no new connections will be allowed. The default is 5000. The available range is 1-65535.
pn-max-conns-per-client	Specifies the maximum number of DNS Push Notification connections per client (IP address) the server will allow. Once the maximum has been reached, the client will not be allowed to make new connections. A value of 0 indicates no limit should be applied. The default is 0. The available range is 0-1000.
pn-conn-ttl	Specifies the maximum time to live for each DNS Push Notification connection. Once the TTL has been reached, the connection is forced close. The default is 30 minutes. The available rate ranges from 1m to 24hr.
pn-tls	Enables or disables tls support for DNS Push Notification in the DNS server. Following two files required to enable TLS: 1. **data/dns/dpn/certificate.pem** Defines a file that contains the certificate to be used for tls communication between dns server and push notification client. The format of the file is the standard X.509. The files must be in the data/dns/dpn directory. 2. **data/dns/dpn/key.pem** Defines a file that contains the private key to be used for tls communication between dns server and push notification client. The format of the file is the standard base64 privacy enhanced mail (PEM) format. Default is no private key file. The files must be in the data/dns/dpn directory.

Advertising DNS Push Notifications to the Clients

DNS Push Notification clients discover the DNS Push Notification server(s) by doing a standard DNS queries for the **_dns-push-tls._tcp.<zone>** SRV record. SRV record points clients to the appropriate DNS server. Therefore you can always dedicate one or more secondary servers for push notifications functionality and leave the other servers for general DNS protocol queries, updates, etc. The SRV record has the following format:

```
_dns-push-tls._tcp TTL IN SRV priority weight port target
```

Note Port should match the pn-port in the DNS Push Notifications configuration.

One or more SRV records can be listed on the zone. Each SRV record specifies a unique DNS Push Notification server. The client is responsible for sorting the SRV records accordingly and choosing which server to contact and retrying or trying other servers when others are not available.

Enabling DNS Push Notifications on the Zone

Local Advanced Web UI

Step 1 On the **Edit Zone** Page, under the **Push Notifications** section, enable **push-notifications**.

Step 2 Click **Save** to save the changes.

Step 3 On the **Manage DNS Authoritative Server** page, under the **Push Notifications** section, enable **push-notifications**.

Step 4 Click **Save** to save the changes and reload the DNS Authoritative Server.

CLI Commands

```
nrcmd> zone <name> enable push-notifications

nrcmd> zone <name> addRR dns-push-tls.tcp SRV <priority> <weight> 5352 <target>
```

Note Also the target refers to the DNS server's FQDN and A/AAAA records may also need to be added.

```
nrcmd> dns enable push-notifications

nrcmd> dns reload
```

Note Restart the DNS Server to apply the configuration changes successfully.

DNS Push Notifications Statistics

You can view DNS Push Notifications Statistics through web UI in the following ways:

Local Basic or Advanced Web UI

Click the **Statistics** tab on the **Manage DNS Authoritative Server** page to view the Push Notification Statistics page. The statistics appear under the Push Notification Statistics of both the Total Statistics and Sample Statistics categories.

Table 2: DNS Push Notifications Statistics Attributes

Attribute	Description
pn-conn	Reports the total number of successful Push Notification connections.
pn-conn-current	Reports the current number of successful Push Notification connections.
pn-conn-refused	Reports the number of timer Push Notification connections were refused due to ACL authorization failures.
pn-conn-closed	Reports the number of Push Notification connections closed by the client.
pn-conn-max-conns	Reports the number of Push Notification connections not allowed due to reaching the maximum connections limit (pn-max-conns).
pn-conn-terminated	Reports the number of Push Notification connections terminated by the server. Connection termination is typically caused by reloading the DNS server.
pn-conn-terminated-error	Reports the number of Push Notification connections terminated due to an error.

pn-conn-terminated-conn-ttl	Reports the number of Push Notification connections terminated due to reaching the maximum connection TTL (pn-conn-ttl).
pn-subscribe	Reports the number of Push Notification SUBSCRIBE requests received.
pn-subscribe-noerror	Reports the number of Push Notification subscribe NOERROR responses.
pn-subscribe-formerr	Reports the number of Push Notification subscribe FORMERR responses.
pn-subscribe-servfail	Reports the number of Push Notification subscribe SERVFAIL responses.
pn-subscribe-notauth	Reports the number of Push Notification subscribe NOTAUTH responses.
pn-subscribe-refused	Reports the number of Push Notification subscribe REFUSED responses, due to zone access control (zone query-acl).
pn-unsubscribe	Reports the number of Push Notification UNSUBSCRIBE requests received.
pn-update	Reports the number of Push Notification UPDATE requests sent.
pn-reconfirm	Reports the number of Push Notification RECONFIRM requests received.
pn-keepalive	Reports the number of keep alive requests received.
pn-req-malformed	Reports the number of times that Push Notification requests are malformed. For example, requests having non-zero values in section counts and/or flags where zeros are expected.

DNS Push Notifications statistics can also be logged in the server by enabling the *push-notifications* option present in the Activity Summary Settings section of the Edit Local DNS server page.

CLI Commands

Use **dns getStats dns-pn total** to view the push notification Total statistics and **dns getStats dns-pn sample** to view the sampled counters statistics.

DNS Push Notifications Logging

DNS Push Notifications includes support for logging informational messages. By default, the DNS server is only logs DNS Push Notification configuration and error messages. For additional DNS Push Notification informational logging, the DNS server **server-log-settings** attribute must include **push-notifications**.

Note If you are using the default server-log-settings, you must enable the **default** server-log-settings explicitly.

Local Basic or Advanced Web UI

Step 1 On the **Manage DNS Authoritative Server** page, under the **Log Settings** section, enable **push-notifications**.

Step 2 Click **Save** to save the changes.

CLI Commands

```
nrcmd> dns set server-log-settings=push-notifications
```

Note No DNS reload is required for changing log settings. The changes should take effect immediately.

DNS Push Notifications Packet Logging

DNS Push Notifications include support for summary and detailed packet logging. These messages can be useful for debugging and troubleshooting. By default, the DNS server does not log any packet log messages. Packets can be logged in the form of one line **summary** messages or **detail** packet logging.

Local Advanced Web UI

Step 1 On the **Manage DNS Authoritative Server** page, under the **Packet Logging Settings** section, set **packet-logging** to **summary** or **detail**.

Step 2 Next set **packet-log-settings** to **push-notifications-in** and/or **push-notifications-out**.

Step 3 Click **Save** to save the changes.

CLI Commands

```
nrcmd> dns set packet-logging=summary   or
nrcmd> dns set packet-logging=detail

nrcmd> dns set packet-log-settings=push-notifications-in, push-notifications-out
```

Note DNS reload is not required for changing log settings. The changes should take effect immediately.