DNS プッシュ通知

DNS プッシュ通知は、DNS レコードへの変更が発生したときに、クライアントに非同期で通知するメカニズムです。この機能により、権威 DNS サーバーは DNS プッシュ通知クライアントからの TCP 接続を受け入れ、特定の DNS レコード名（およびオプションとしてレコード タイプ）のサブスクリプション要求を受け入れることができます。サブスクリプションが受け入れられたら、サブスクライブされているレコードが変更されるたびに、クライアントは更新通知を受信します。サブスクリプションを始めるときにレコードが存在する場合は、クライアントは既存のレコードの初期更新通知を受信します。

- DNS プッシュ通知のコンフィギュレーション設定 （1 ページ）
- クライアントへの DNS プッシュ通知のアドバタイジング （2 ページ）
- ゾーンでの DNS プッシュ通知の有効化 （3 ページ）
- DNS プッシュ通知統計の表示 （4 ページ）
- DNS プッシュ通知ロギングの有効化 （5 ページ）
- DNS プッシュ通知パケットのロギング （6 ページ）

DNS プッシュ通知のコンフィギュレーション設定

DNSプッシュ通知には事前に設定された設定が含まれていますが、デフォルトでは有効になっていません。DNSプッシュ通知を使用するには、プッシュ通知（*push-notifications*）属性を DNS サーバーレベルと目的のゾーンで有効にする必要があります。DNSプッシュ通知は、通知するゾーンをホストしている Cisco Prime Network Registrar DNS サーバーでも有効にすることができます。これはプライマリゾーンとセカンダリゾーンのどちらでも可能です。

（注） DNS プッシュ通知の変更を有効にするには、DNS サーバーをリロードする必要があります。

DNS プッシュ通知を有効にするには、次の DNS サーバーレベルの属性を使用します。

表 *1 : DNS* サーバー レベルの属性

属性	説明

プッシュ通知（*push-notifications*）	DNS サーバーで DNS プッシュ通知のサポートを有効または無効にします。デフォルトではディセーブルになっています。
ポート（*pn-port*）	DNS プッシュ通知の接続をリッスンするために DNS サーバーが使用する TCP ポート番号を指定します。デフォルトは 5352 です。使用可能な範囲は 1 ～ 65535 ですが、DNS サーバー ポートと同じにすることはできません。
ACL（*pn-acl*）	DNS プッシュ通知のアクセス制御を指定します。デフォルトは none です。
最大接続数（*pn-max-conns*）	サーバーが許可する個々の DNS プッシュ通知接続の最大数を指定します。最大数に達すると、新しい接続は許可されません。デフォルトは 5000 です。指定できる範囲は 1 ～ 65535 です。
クライアント別の最大接続数（*pn-max-conns-per-client*）	サーバーが許可するクライアント（IP アドレス）ごとの DNS プッシュ通知接続の最大数を指定します。最大数に達すると、クライアントによる新しい接続は許可されません。値 0 は、制限を適用しないことを示します。デフォルトは 0 です。指定できる範囲は 0 ～ 1000 です。
接続 TTL（*pn-conn-ttl*）	各 DNS プッシュ通知の接続の最大 TTL を指定します。TTL に到達すると、接続は強制的に切断されます。デフォルトは 30 分です。使用可能なレートの範囲は、1 分～ 24 時間です。
TLS（*pn-tls*）	DNS プッシュ通知に対する TLS のサポートを有効または無効にします。TLS を有効にするには、次の 2 つのファイルが必要です。 • **data/dns/dpn/certificate.pem**：DNS サーバーとプッシュ通知クライアントの間の TLS 通信に使用される証明書を含むファイルを定義します。このファイルの形式は標準 X.509 です。これらのファイルは、data/dns/dpn ディレクトリに存在する必要があります。 • **data/dns/dpn/key.pem**：DNS サーバーとプッシュ通知クライアントの間の TLS 通信に使用される秘密キーを含むファイルを定義します。このファイルの形式は、標準 base64 プライバシー強化メール（PEM）形式です。デフォルトは秘密キーファイルではありません。これらのファイルは、data/dns/dpn ディレクトリに存在する必要があります。

クライアントへの DNS プッシュ通知のアドバタイジング

DNS プッシュ通知クライアントは、DNS プッシュ通知サーバーを検出するために、**_dns-push-tls._tcp.<zone>** SRV レコードの標準 DNS クエリを行います。SRV レコードは、クライアントを適切な DNS サーバーにポイントします。したがって、1 つまたは複数のセカンダ

リサーバーをプッシュ通知機能専用にすることができ、他のサーバーは一般的な DNS プロトコルのクエリや更新などに使用できます。SRV レコードの形式は次のとおりです。

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

（注） ポートは DNS プッシュ通知設定の *pn-port* と一致している必要があります。

1 つまたは複数の SRV レコードをゾーンのリストに表示できます。各 SRV レコードは、一意の DNS プッシュ通知サーバーを指定します。クライアントは、それに応じて SRV レコードをソートし、接続するサーバーを選択して、他のサーバーを使用できないときに再試行または試行します。

ゾーンでの DNS プッシュ通知の有効化

ゾーンでの DNS プッシュ通知を有効にするには、次の手順を実行します。

ローカルの高度な Web UI

ステップ 1 [ゾーンの編集（Edit Zones）] ページの [プッシュ通知（Push Notifications）] セクションで、*push-notifications* を有効にします。

ステップ 2 [**保存（Save）**] をクリックして、変更内容を保存します。

ステップ 3 [DNS権威サーバーの管理（Manage DNS Authoritative Server）] ページの [プッシュ通知（Push Notifications）] セクションで、**push-notifications** を有効にします。

ステップ 4 [**保存（Save）**] をクリックして変更を保存し、DNS 権威サーバーをリロードします。

CLI コマンド

ゾーンで DNS プッシュ通知を有効にするには、次のコマンドを使用します。

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

（注） *target* は DNS サーバーの FQDN を参照し、A/AAAA レコードを追加する必要がある場合もあります。

サーバーレベルでの DNS プッシュ通知を有効にするには、次のコマンドを使用します。

```
nrcmd> dns enable push-notifications
nrcmd> dns reload
```

（注） DNS サーバーを再起動して、設定の変更を正常に適用します。

DNS プッシュ通知統計の表示

次の方法で DNS プッシュ通知の統計を表示できます。

ローカルの基本または高度な Web UI

[DNS権威サーバーの管理（ Manage DNS Authoritative Server）] ページの [統計（Statistics）] タブをクリックして [サーバー統計（Server Statistics）] ページを表示します。DNS プッシュ通知の統計は、[合計統計（Total Statistics）] カテゴリと [サンプル統計（Sample Statistics）] カテゴリの [プッシュ通知の統計（Push Notification Statistics）] セクションに表示されます。

表 *2: DNS* プッシュ通知の統計の属性

属性	説明
pn-conn	成功したプッシュ通知接続の合計数を報告します。
pn-conn-current	成功したプッシュ通知接続の現在の数を報告します。
pn-conn-refused	ACL 許可の失敗が原因で拒否されたタイマープッシュ通知接続の数を報告します。
pn-conn-closed	クライアントによってクローズされたプッシュ通知接続の数を報告します。
pn-conn-max-conns	接続数の上限（*pn-max-conns*）に到達したために許可されなかったプッシュ通知の接続数を報告します。
pn-conn-terminated	サーバーが終了させたプッシュ通知接続の数を報告します。接続の終了のよくある原因は DNS サーバーのリロードです。
pn-conn-terminated-error	エラーが原因で終了したプッシュ通知接続の数を報告します。
pn-conn-terminated-conn-ttl	最大接続 TTL（*pn-conn ttl*）に到達したために終了したプッシュ通知の接続数を報告します。
pn-subscribe	受信したプッシュ通知 SUBSCRIBE 要求の数を報告します。
pn-subscribe-noerror	プッシュ通知サブスクライブ NOERROR 応答の数を報告します。
pn-subscribe-formerr	プッシュ通知サブスクライブ FORMERR 応答の数を報告します。
pn-subscribe-servfail	プッシュ通知サブスクライブ SERVFAIL 応答の数を報告します。

pn-subscribe-notauth	プッシュ通知サブスクライブ NOTAUTH 応答の数を報告します。
pn-subscribe-refused	ゾーンアクセス制御（*zone query-acl*）に起因するプッシュ通知サブスクライブ拒否応答の数を報告します。
pn-unsubscribe	受信したプッシュ通知 UNSUBSCRIBE 要求の数を報告します。
pn-update	送信されたプッシュ通知 UPDATE 要求の数を報告します。
pn-reconfirm	受信したプッシュ通知 RECONFIRM 要求の数を報告します。
pn-keepalive	受信したキープ アライブ要求の数を報告します。
pn-req-malformed	プッシュ通知要求の形式が間違っていた回数を報告します。たとえば、ゼロが想定されているセクション数やフラグにゼロ以外の値が含まれている要求です。

DNS プッシュ通知の統計をサーバーにロギングすることもできます。それには、[ローカル DNS サーバーの編集（Edit Local DNS server）] ページの [アクティビティ サマリーの設定（Activity Summary Settings）] セクションにある [*push-notifications*] オプションを有効にします。

CLI コマンド

プッシュ通知の合計統計を表示するには、**dns getStats dns-pn total** を使用します。サンプルカウンタ統計を表示するには、**dns getStats dns-pn sample** を使用します。

DNS プッシュ通知ロギングの有効化

DNSプッシュ通知では、情報メッセージのロギングをサポートしています。デフォルトでは、DNS サーバーは DNS プッシュ通知の設定とエラーメッセージのみをログに記録します。追加の DNS プッシュ通知の情報ロギングには、*server-log-settings* 属性に **push-notifications** を含める必要があります。

（注） デフォルトの *server-log-settings* を使用する場合は、デフォルトの server-log-settings を明示的に有効にする必要があります。

ローカルの基本または詳細 Web UI

ステップ 1 [DNS 権威サーバーの管理（Manage DNS Authoritative Server）] ページの [ログ設定（Log Settings）] セクションで **push-notifications** のチェックボックスをオンにします。

ステップ 2 [保存（**Save**）] をクリックして、変更内容を保存します。

CLI コマンド

DNS プッシュ通知に関連付けられたロギングを有効にするには、**dns set server-log-settings=push-notifications** を使用します。

（注） ログ設定を変更するために DNS をリロードする必要はありません。変更がすぐに反映されます。

DNS プッシュ通知パケットのロギング

DNS プッシュ通知には、サマリーおよび詳細パケット ロギングのサポートが含まれます。これらのメッセージはデバッグやトラブルシューティングに役立ちます。デフォルトでは、DNS サーバーはパケット ログ メッセージをロギングしません。パケットは1行の**サマリー**メッセージまたは**詳細**パケット ロギングの形式でロギングできます。

ローカルの詳細 Web UI

ステップ 1 [DNS 権威サーバーの管理（Manage DNS Authoritative Server）] ページの、[パケットロギング（Packet Logging）] セクションにあるドロップダウンリストから **packet-logging** の値を選択します。値は **summary** または **detail** です。

ステップ 2 *packet-log-settings* 属性の場合は、**push-notifications-in** または **push-notifications-out**、あるいはその両方のチェックボックスをオンにします。

ステップ 3 [保存（**Save**）] をクリックして、変更内容を保存します。

CLI コマンド

DNS パケットの 1 行の概要のロギングを有効にするには **dns set packet-logging=summary** を使用します。

DNS パケットの詳細なパケットトレースを有効にするには、**dns set packet-logging=detail** を使用します。

DNS プッシュ通知メッセージのパケットロギングを有効にするには、 **dns set packet-log-settings=push-notifications-in** または **dns set packet-log-settings=push-notifications-out** を使用します。

（注） パケットログの設定を変更するのに DNS をリロードする必要はありません。変更がすぐに反映されます。