キャッシュ DNS サーバーの管理

Cisco Prime Network Registrar では、権威サービスとキャッシュサービスは分離され、2 つの個別サーバーで処理されます。この章では、キャッシュ DNS サーバーのパラメータを設定する方法について説明します。この章のタスクに進む前に、ドメイン ネーム システムの概要を参照してください。DNS の基本が説明されています。

DNS キャッシュ サーバー プロパティの設定

キャッシュ DNS サーバーのプロパティを設定できます。次のようなものがあります。

- **一般的なサーバー プロパティ**：「一般的なキャッシュ DNS サーバープロパティの設定 （2 ページ）」を参照
- **ログ設定**：「ログ設定の指定 （3 ページ）」を参照
- **パケットロギング**：「パケットロギングの有効化 （3 ページ）」を参照
- **アクティビティの概要の設定**：「アクティビティ サマリー設定の指定 （5 ページ）」を参照
- **トップネームの設定**：「トップ ネーム設定の指定 （19 ページ）」を参照
- **セキュリティイベントの設定**：「セキュリティイベントのロギング （20 ページ）」を参照
- **証明書の設定**：「証明書の設定の指定 （26 ページ）」を参照
- **TLS の設定**：「TLS 設定の指定 （27 ページ）」を参照
- **HTTPS 設定**：「HTTPS 設定の指定 （30 ページ）」を参照
- **キャッシングの設定**：「プリフェッチ タイミングの設定 （33 ページ）」を参照
- **キャッシュ TTL**：「キャッシュ TTL の設定 （33 ページ）」を参照

- **スマートキャッシング**：「スマートキャッシュの有効化 （34 ページ）」を参照
- **ルート ネームサーバー**：「ルート ネームサーバーの定義 （37 ページ）」を参照
- **UDP ポート**：「UDP ポートの動的割り当て （37 ページ）」を参照
- **最大メモリ キャッシュ サイズ**：「最大メモリ キャッシュ サイズの設定 （37 ページ）」を参照
- **リゾルバの設定**：「リゾルバ設定の指定 （38 ページ）」を参照
- **ネットワークの設定**：「ネットワーク設定の指定 （40 ページ）」を参照
- **詳細設定**：「詳細設定の指定 （40 ページ）」を参照
- **キャッシュのフラッシュ**：「DNS キャッシュのフラッシュ （41 ページ）」を参照
- **DNS キャッシュ ポイズニングの防止**：「DNS キャッシュ ポイズニングの検出と防止 （42 ページ）」を参照
- **応答しないネームサーバーの処理**：「応答しないネームサーバーの処理 （43 ページ）」を参照

一般的なキャッシュ DNS サーバープロパティの設定

ログ設定、キャッシュの基本設定、SNMP トラップ、ルートネームサーバーなどのキャッシング DNS の一般的なサーバー プロパティを表示できます。

以下のサブセクションでは、最も一般的なプロパティ設定をいくつか説明します。これらのリストは「DNS キャッシュ サーバー プロパティの設定 （1 ページ）」に記載されています。

ローカル Web UI

ステップ 1 サーバーのプロパティにアクセスするには、**Deploy** メニューの **DNS** サブメニューで **CDNS Server** を選択して [DNS キャッシュ サーバーの管理（Manage DNS Caching Server）] ページを開きます。

ステップ 2 [展開（Deploy）] メニューから [**CDNS サーバー（CDNS Server**）] タブを選択するか、左ペインの [**CDNS サーバー（CDNS Server**）] タブをクリックすると、[ローカル CDNS サーバー（local CDNS Server）] ページが自動的に選択されます。このページには、すべてのキャッシング DNS サーバー属性が表示されます。

ステップ 3 **Save** をクリックして、キャッシング DNS サーバー属性の変更を保存します。

CLI コマンド

cdns show を使用してキャッシュ DNS サーバーのプロパティを表示します（構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **cdns** コマンドを参照してください）。

ログ設定の指定

log-settings 属性により、キャッシング DNS サーバーログに記録する詳細イベントが決まります。これらの追加の詳細をロギングすることが、問題の分析に役立ちます。ただし、詳細なロギングを長期間にわたって有効のままにしておくと、ログファイルがいっぱいになり、重要な情報が失われる可能性があります。

オプションは次のいずれかです。

- **activity-summary**：サーバー統計情報の概要を定期的にロギングします。
- **config**：サーバーの設定とサーバーの初期化解除に関するロギングを制御します。
- **query**：サーバーへのすべての DNS クエリがロギングされます。
- **scp**：SCP メッセージ処理に関するロギングを制御します。
- **server-detailed-ops**：サーバー運用の詳細なロギングを制御します。
- **server-ops**：サーバー運用の高レベル ロギングを制御します。
- **name-servers**：例外およびフォワーダのネームサーバーが応答しなくなった場合、または再び応答した場合に、ロギングを有効にします。

immediate-response-stats 属性（Advanced モードで使用可能）を使用すると、クエリがすぐに応答された場合の応答時間統計情報を収集できます。この機能を無効にすると、関連する統計情報（*immediate-response-count*、*immediate-response-average*、*and immediate-response-median*）はゼロになります。

パケットロギングの有効化

Cisco Prime Network Registrar では、キャッシング DNS サーバーのパケットロギングをサポートすることで、キャッシング DNS サーバーアクティビティの分析とデバッグを行えるようにしています。パケットロギングの設定によって、パケットロギングのタイプ（概要または詳細）、ログに記録されたパケットのタイプ、およびメッセージが記録されるログファイルが決まります。デフォルトでは、キャッシング DNS サーバーはパケットログメッセージをログに記録しません。

次のサーバーレベルの属性を使用して、キャッシング DNS サーバーのパケットロギングを有効にします。

表 *1:* キャッシング *DNS* サーバーのパケットロギングの属性

属性	説明
パケットロギング（*packet-logging*）	CDNS のログに記録されるパケットロギングのタイプを決定します。ログに記録されるパケットのタイプは、packet-log-settings 属性で制御できます。 • **disabled**：この設定は、パケットロギングを無効にします。 • **summary**：この設定は、1 行の概要でのパケットロギングを有効にします。 • **detail**：この設定は、詳細なパケットトレースを有効にします。 （注） この設定は、ログに記録される情報量を大幅に増加させる可能性があり、デバッグの目的で一時的にのみ使用する必要があります。 注：パケットロギングはデバッグやトラブルシューティングに役立ちますが、DNS サーバーのパフォーマンスに影響します。したがって、実稼働環境でパケットロギングを有効のままにしておくことはお勧めしません。
パケットロギングファイル（*packet-logging-file*）	パケットロギングが有効の場合のパケットロギングメッセージの宛先ログを決定します。 • **cdns**：パケットロギングメッセージは標準 CDNS ログファイル（cdns_log *）に記録されます。 • **packet**：パケットロギングメッセージは別の CDNS パケットログファイル（cdns_query_log *）に記録されます。
パケットロギング設定（*packet-log-settings*）	パケットロギングが有効になっている場合にログに記録するパケットのタイプを決定します。パケットロギングを有効にするには、*packet-logging* 属性を設定します。 • **query-in**：この設定は、着信クエリパケットのロギングを有効にします。これらは、DNS クライアントから着信するパケットです。 • **query-out**：この設定は、発信クエリパケットのロギングを有効にします。これらは、アップストリーム DNS サーバーへのクエリです。 • **response-in**：この設定は、着信クエリ応答パケットのロギングを有効にします。これらは、アップストリーム DNS サーバーからの応答です。 • **response-out**：この設定は、発信クエリパケットのロギングを有効にします。これらは DNS クライアントへの応答です。

ローカルの高度な Web UI

ステップ 1 [DNS キャッシングサーバーの管理（Manage DNS Caching Server）] ページの [パケットロギング（Packet Logging）] セクションで、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* 属性では、対象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

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

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

パケットロギングが有効になっている場合にログに記録するパケットのタイプを設定するには、**cdns set packet-log-settings**=*value* を使用します。

（注） *packet-logging* 属性と *packet-log-settings* 属性をすぐに有効にするのに、キャッシング DNS サーバーのリロードは必要ありません（ログ設定と同様）。ただし、*packet-logging-file* 属性には、キャッシング DNS サーバーのリロードが必要です。

アクティビティ サマリー設定の指定

（注） アクティビティの概要の設定を指定するには、[ログ設定（Log Settings）] で *activity-summary* をオンにする必要があります。

[統計間隔（Statistics Interval）] 属性（*activity-summary-interval*）を使用して、アクティビティの概要情報をロギングする間隔を指定できます。デフォルト値は 60 秒です。

キャッシング DNS サーバーは、統計タイプ（*activity-summary-type*）属性でオンになっているオプションに基づき、サンプル統計または合計統計、あるいはその両方をログに記録します。デフォルト値は「sample」です。

[統計設定（Statistics Settings）]（*activity-summary-settings*）属性でオンになっているオプションによってログに記録される統計のカテゴリが決まります。次の設定を使用できます。

- **cache**：RR キャッシュの統計をログに記録します。

  cache設定のログに表示されるアクティビティサマリーの統計のリストについては、キャッシュ統計 （7 ページ）を参照してください。

- **firewall**：DNS ファイアウィールの統計をログに記録します。

  firewall 設定のログに表示されるアクティビティサマリーの統計のリストについては、ファイアウォールの統計情報 （8 ページ）を参照してください。

- **memory**：メモリ使用率の統計をログに記録します。

  memory 設定のログに表示されるアクティビティサマリーの統計のリストについては、メモリの統計情報 （9 ページ）を参照してください。

- **query**：着信クエリに関する統計をログに記録します。

  query 設定のログに表示されるアクティビティサマリーの統計のリストについては、クエリ統計 （9 ページ）を参照してください。

- **query-type**：照会対象の RR タイプに関する統計をログに記録します。

  query-type 設定のログに表示されるアクティビティサマリーの統計のリストについては、タイプ別クエリの統計 （11 ページ）を参照してください。

- **rate-limit**：レート制限イベントの数を記録します。

  rate-limiting 設定のログに表示されるアクティビティサマリーの統計のリストについては、レート制限の統計情報 （12 ページ）を参照してください。

- **resol-queue**：解決キューの統計をログに記録します。

  resol-queue 設定のログに表示されるアクティビティサマリーの統計のリストについては、解決キューの統計 （13 ページ）を参照してください。

- **responses**：クエリ応答に関する統計をログに記録します。

  responses 設定のログに表示されるアクティビティサマリーの統計のリストについては、応答統計 （14 ページ）を参照してください。

- **security**：セキュリティイベントに関連する統計をログに記録します。

  security 設定のログに表示されるアクティビティサマリーの統計のリストについては、セキュリティ統計 （16 ページ）を参照してください。

- **system**：システム使用率に関する統計情報をログに記録します。

  system 設定のログに表示されるアクティビティサマリーの統計のリストについては、システム統計 （17 ページ）を参照してください。

- **top-names**：照会されたトップネームとヒット数をログに記録します。

  top-names 設定のログに表示されるアクティビティサマリーの統計のリストについては、トップネームの統計情報 （17 ページ）を参照してください。

- **upstream**：アップストリームクエリの数をログに記録します。

  upstream 設定のログに表示されるアクティビティサマリーの統計のリストについては、アップストリームの統計 （18 ページ）を参照してください。

アクティビティサマリーの統計

次のセクションでは、*activity-summary-settings* の各カテゴリの下にあるログに表示されるアクティビティサマリーの統計のリストについて説明します。

キャッシュ統計

cache activity-summary-settings は、RR キャッシュの統計をログに記録します。

サンプルログメッセージ：

```
10/06/2021 10:22:44 cdns Activity Stats 0 22173 [Cache] Sample since Wed Oct 6 10:21:44
 2021: hits=number, misses=number, prefetches=number, message-overflow=number,
rrset-overflow=number, remote-ns-overflow=number, key-overflow=number, smart-cache=number
```

表 *2:* キャッシュ統計

アクティビティサマリー名	統計[1]	説明
hits	cache-hits	キャッシュから応答されたクエリの合計数。
misses	cache-misses	キャッシュ内で見つからなかったクエリの合計数。
prefetches	cache-prefetches	実行されたプリフェッチの数。
rrset-overflow	mem-cache-exceeded	RRSet キャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
message-overflow	mem-query-cache-exceeded	メッセージキャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
remote-ns-overflow	remote-ns-cache-exceeded	リモートネームサーバーキャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
key-overflow	key-cache-exceeded	キーキャッシュが設定された制限を超えた回数。これは、設定された制限がその環境に対して小さすぎる可能性があることを示しています。
smart-cache	smart-cache	スマートキャッシュが有効になっている場合に、CDNS サーバーがスマートキャッシュ応答を使用した合計回数。

[1] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

ファイアウォールの統計情報

firewall activity-summary-settings は、DNS ファイアウォールの使用状況に関する統計をログに記録します。

サンプルログメッセージ：

```
11/18/2021 12:39:20 cdns Activity Stats 0 22322 [Firewall] Sample since Thu Nov 18
12:38:20 2021: redirected=number, dropped=number, refused=number, redirect-nxdomain=number,
 rpz=number
```

表 *3*: ファイアウォールの統計情報

アクティビティサマリー名	統計[2]	説明
dropped	firewall-dropped	DNS ファイアウォールがクエリをドロップした回数。
redirected	firewall-redirected	DNS ファイアウォールがクエリをリダイレクトした回数。
refused	firewall-refused	DNS ファイアウォールがクエリを拒否した回数。
redirect-nxdomain	firewall-redirect-nxdomain	DNS ファイアウォールがクエリを NXDOMAIN 応答とともにリダイレクトした回数。
rpz	firewall-rpz	DNS ファイアウォール RPZ ルールが着信クエリと一致した回数。

[2] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

メモリの統計情報

memory activity-summary-settings は、メモリ使用量に関する統計をログに記録します。

サンプルログメッセージ：

```
10/06/2021 10:22:44 cdns Activity Stats 0 22303 [Memory] Current: mem-cache-process=number,
 mem-cache-rrset=number, mem-cache-message=number, mem-mod-iterator=number,
mem-mod-validator=number
```

表 *4:* メモリの統計情報

アクティビティサマリー名	統計[3]	説明
mem-cache-process	mem-process	CDNSプロセスのメモリの推定値（バイト数）。
mem-cache-rrset	mem-cache	RRSetキャッシュに割り当てられたメモリ（バイト数）。*rrset-cache-size* 設定が変更されない限り、割り当てられたメモリはサーバーのリロード後も維持されることに注意してください。
mem-cache-message	mem-query-cache	メッセージキャッシュに割り当てられたメモリ（バイト数）。*msg-cache-size* 設定が変更されない限り、割り当てられたメモリはサーバーのリロード後も維持されることに注意してください。
mem-mod-iterator	mem-iterator	CDNS イテレータ モジュールによって使用されたメモリ（バイト数）。
mem-mod-validator	mem-validator	CDNS バリデータ モジュールによって使用されたメモリ（バイト数）。

[3] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラ *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

クエリ統計

query activity-summary-settings は、着信クエリに関連する統計をログに記録します。

サンプルログメッセージ：

```
03/06/2022 16:52:11 Activity Stats 0 22171 [Query] Total since Wed Mar 2 12:49:50 2022:
 total=number, acl-failures=number, udp=number, tcp=number, ipv4=number, ipv6=number,
tls=number, tls-errors-in=number, tls-errors-out=number, https=number,
https-errors-in=number, edns=number, dnssec=number, dns64-aaaa=number, dns64-ptr=number,
```

```
 dns64-ns=number, unwanted-class=number, https-query-buffer=number,
https-response-buffer=number
```

表 *5:* クエリ統計

アクティビティサマリー名	統計[4]	説明
total	queries-total	CDNS サーバーが受信したクエリの合計数。
acl-failures	queries-failing-acl	ACL 障害のためにドロップまたは拒否されたクエリの数。
tcp	queries-over-tcp	CDNS サーバーが TCP を介して受信したクエリの合計数。この統計は、HTTPS 経由でクエリを受信した場合にも増加します。
udp	該当なし	CDNS サーバーが UDP を介して受信したクエリの総数。
ipv4	該当なし	CDNS サーバーが受信した IPv4 クエリの総数。
ipv6	queries-over-ipv6	CDNS サーバーが受信した IPv6 クエリの総数。
tls	queries-over-tls	CDNS サーバーが TLS を介して受信したクエリの総数。この統計は、HTTPS 経由でクエリを受信した場合にも増加します。
tls-errors-in	tls-errors-in	インバウンド DNS クエリの試行で発生した TLS 関連エラーの総数。
tls-errors-out	tls-errors-out	アウトバウンド DNS クエリの試行で発生した TLS 関連エラーの総数。
https	queries-over-https	CDNS サーバーが HTTPS 経由で受信したクエリの総数。
https-errors-in	queries-over-https- failed	HTTPS エラーで失敗したクエリの総数。
edns	queries-with-edns	EDNS OPT RR が存在するクエリの数。
dnssec	queries-with-edns-do	EDNS OPT RR with DO（DNSSEC OK）ビットがセットされているクエリの数。
dns64-aaaa	dns64-a2aaaa-conversions	dns64 がタイプ A の RR をタイプ AAAA の RR に変換した回数。
dns64-ptr	dns64-ptr-conversions	dns64 が IPv4 PTR RR を IPv6 PTR RR に変換した回数。

アクティビティサマリー名	統計[4]	説明
unwanted-class	queries-unwanted-class	不要なクラスを含むクエリの総数。
https-query-buffer	https-query-buffer	メモリバッファの HTTPS クエリの数。
https-response-buffer	https-response-buffer	メモリバッファの HTTPS 応答の数。

[4] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

タイプ別クエリの統計

query-type activity-summary-settings は、照会対象の RR タイプに関する統計をログに記録します。

サンプルログメッセージ：

```
01/30/2023 12:23:11 cdns tid: 0 Activity Stats 0 22172 [Query-by-Type] Sample since Mon
 Jan 30 12:22:11 2023: A=number, AAAA=number, ANY=number, CNAME=number, PTR=number,
MX=number, NS=number, SOA=number, DS=number, DNSKEY=number, RRSIG=number, NSEC=number,
NSEC3=number, HTTPS=number, SVCB=number, TXT=number, SRV=number, NAPTR=number, Other=number
```

表 *6:* タイプ別クエリの統計

アクティビティサマリー名	統計[5]	説明
A	queries-type-A	受信されたクエリの数。
AAAA	queries-type-AAAA	受信された AAAA クエリの数。
ANY	queries-type-ANY	受信された ANY クエリの数。
CNAME	queries-type-CNAME	受信されたクエリの数。
PTR	queries-type-PTR	受信されたクエリの数。
NS	queries-type-NS	受信された NS クエリの数。
SOA	queries-type-SOA	受信された SOA クエリの数。
MX	queries-type-MX	受信された MX クエリの数。
DS	queries-type-DS	受信された DS クエリの数。

アクティビティサマリー名	統計[5]	説明
DNSKEY	queries-type-DNSKEY	受信された DNSKEY クエリの数。
RRSIG	queries-type-RRSIG	受信された RRSIG クエリの数。
NSEC	queries-type-NSEC	受信された NSEC クエリの数。
NSEC3	queries-type-NSEC3	受信された NSEC3 クエリの数。
HTTPS	queries-type-HTTPS	受信された HTTPS（TYPE 65）クエリの数。
SVCB	queries-type-SVCB	受信された SVCB（TYPE 64）クエリの数。
NAPTR	queries-type-NAPTR	受信された NAPTR RR クエリの数。
SRV	queries-type-SRV	受信された SRV RR クエリの数。
TXT	queries-type-TXT	受信された TXT RR クエリの数。
Other	queries-type-other	受信されたその他すべてのクエリ。

[5] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

レート制限の統計情報

rate-limiting activity-summary-settings は、レート制限イベントの数をログに記録します。

サンプルログメッセージ：

```
11/30/2021 16:20:37 cdns tid: 0 Activity Stats 0 22388 [Ratelimit] Sample since Tue Nov
 30 16:19:37 2021: client-ratelimited=number, domain-ratelimited=number

11/30/2021 16:20:37 cdns tid: 0 Activity Stats 0 22390 [Ratelimit-Domain] from 16:19:37
 to 16:20:33; interval=number, num-ratelimited=number, total-counted=number,
not-counted=number

11/30/2021 16:20:37 cdns tid: 0 Activity Stats 0 22390 [Ratelimit-Client] from 08:29:43
 to 08:30:43; interval=number, num-ratelimited=number, total-counted=number,
not-counted=number
```

表 *7:* レート制限の統計情報

アクティビティサマリー名	ロギングサブカテゴリ	統計[6]	説明
client-ratelimited	Ratelimit	client-rate-limit	クライアントのレートが制限された回数。
domain-ratelimited	Ratelimit	domain-rate-limit	ドメインのレートが制限された回数。
interval	Ratelimit-Domain	該当なし	データ収集期間の長さ。
num-ratelimited	Ratelimit-Domain	該当なし	レート制限されたドメインの総数。
total-counted	Ratelimit-Domain	該当なし	ドメインのレートが制限された合計回数。
not-counted	Ratelimit-Domain	該当なし	ドメインレート制限テーブルがオーバーフローした回数。
interval	Ratelimit-Client	該当なし	データ収集期間の長さ。
num-ratelimited	Ratelimit-Client	該当なし	レート制限されたクライアントの総数。
total-counted	Ratelimit-Client	該当なし	クライアントのレートが制限された合計回数。
not-counted	Ratelimit-Client	該当なし	クライアントレート制限テーブルがオーバーフローした回数。

[6] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

解決キューの統計

resol-queue activity-summary-settings は、解決キューの統計をログに記録します。

サンプルログメッセージ：

```
10/06/2021 10:22:44 cdns Activity Stats 0 22174 [Resolution-Queue] Sample since Wed Oct
 6 10:21:44 2021: num-entries=number, user-queries=number, system-queries=number,
average-num-entries=number, max-num-entries=number, entries-overwritten=number,
exceeded-limit=number, replies-sent=number, exceeded-max-target-count=number
```

表 *8*: 解決キューの統計

アクティビティサマリー名	統計[7]	説明
num-entries	requestlist-total	再帰応答を待ってキューに入れられた要求の合計数。
user-queries	requestlist-total-user	再帰応答を待ってキューに入れられたユーザー要求の合計数。
system-queries	requestlist-total-system	再帰応答を待ってキューに入れられたシステム要求の合計数。
average-num-entries	requestlist-total-average	要求リストの平均要求数。
max-num-entries	requestlist-total-max	要求リストの最大要求数。
entries-overwritten	requestlist-total-overwritten	新しいエントリによって上書きされた要求リスト上の要求の数。
exceeded-limit	requestlist-total-exceeded	要求リストがいっぱいになったためにドロップされた要求の数。
replies-sent	recursive-replies-total	キャッシュで見つからず、外部解決が必要であったクエリ応答の総数。
exceeded-max-target-count	exceeded-max-target-count	許可されるネーム サーバー グルー ルックアップの最大数を超えたクエリの数。

[7] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

応答統計

responses activity-summary-settings は、クエリ応答に関する統計をログに記録します。

サンプルログメッセージ：

```
10/06/2021 10:22:44 cdns Activity Stats 0 22175 [Responses] Sample since Wed Oct 6
10:21:44 2021: no-error=number, no-data=number, formerr=number, servfail=number,
nxdomain=number, notimp=number, refused=number, notauth=number, other-errors=number,
secure=number, unsecure=number, rrset-unsecure=number, unwanted=number
```

表 *9*: 応答統計

アクティビティサマリー名	統計[8]	説明
no-error	answers-with-NOERROR	NOERROR の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
nxdomain	answers-with- NXDOMAIN	NXDOMAIN の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
no-data	answers-with-NODATA	NODATA の疑似 rcode がクライアントに返される結果となった応答の数。
other-errors	answers-with-other-errors	NODATA の疑似 rcode がクライアントに返される結果となった応答の数。
secure	answers-secure	正しく検証された応答の数。
unsecure	answers-unsecure	正しく検証されなかった応答の数。
rrset-unsecure	answers-rrset-unsecure	バリデータによって偽としてマークされた RRSet の数。
unwanted	answers-unwanted	望ましくない、または未承諾の応答の数。高い値は、スプーフィングの脅威を示している可能性があります。
refused	answers-with-REFUSED	REFUSED の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
servfail	answers-with-SERVFAIL	SERVFAIL の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
formerr	answers-with-FORMERR	FORMERR の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
notauth	answers-with-NOTAUTH	NOTAUTH の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。
notimp	answers-with-NOTIMP	NOTIMP の rcode がクライアントに返される原因となった、キャッシュまたは再帰からの応答の数。

[8] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラ *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

セキュリティ統計

security activity-summary-settings は、着信クエリに関連する統計をログに記録します。

セキュリティ アクティビティ サマリーの統計は、**Security-Events-Categories** サブカテゴリ下のログに記録されます。

サンプルログメッセージ：

```
01/30/2023 12:00:10 cdns_security tid: 0 Activity Stats 0 22439
[Security-Events-Categories] Sample since Mon Jan 30 11:59:09 2023: total=number,
requests=number, alarm=number, amplification=number, dos=number, firewall=number,
malware=number, phishing=number, poisoning=number, snooping=number, tunneling=number
```

表 *10*：セキュリティ統計

アクティビティサマリー名	統計[9]	説明
total	security-events	DNS セキュリティイベントリソース制限アラームのトリガーに使用される、構成可能な間隔内で検出およびキャプチャされたセキュリティイベントの総数。
alarm	security-events-alarm	DNS セキュリティイベントリソース制限アラームのトリガーに使用される、構成可能な間隔内で検出およびキャプチャされたセキュリティイベントの総数。
アンプ攻撃	security-events-amplification-attack	検出およびキャプチャされたアンプ攻撃によるセキュリティイベントの総数。
dos	security-events-dos	検出およびキャプチャされた潜在的な DoS 攻撃によるセキュリティイベントの総数。
ファイアウォール	security-events-firewall	ファイアウォールの制限によるセキュリティイベントの総数。
マルウェア	security-events-malware	検出およびキャプチャされたマルウェアによるセキュリティイベントの総数。

アクティビティサマリー名	統計[9]	説明
フィッシング	security-events-phishing	検出およびキャプチャされたDNSフィッシングによるセキュリティイベントの総数。
ポイズニング	security-events-poisoning	検出およびキャプチャされた DNS キャッシュポイズニングによるセキュリティイベントの総数。
スヌーピング	security-events-snooping	検出およびキャプチャされた DNS キャッシュスヌーピングによるセキュリティイベントの総数。
トンネリング	security-events-dns-tunneling	検出およびキャプチャされたDNSトンネリングによるセキュリティイベントの総数。

[9] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシュ DNS サーバー統計情報の完全なリストについては、『*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイド』の付録「Server Statistics」の「CDNS Statistics」セクションを参照してください。

システム統計

system activity-summary-settings は、システムの使用状況に関する統計をログに記録します。

サンプルログメッセージ：

```
10/26/2021 6:04:44 cdns tid: 0 Activity Stats 0 22375 [System] Current:
conntrack-max=number, conntrack-count=number, conntrack-usage=number
```

表 *11* : システム統計

アクティビティサマリー名	説明
conntrack-max	許可される接続トラッキングエントリの最大数。
conntrack-count	現在使用されている接続トラッキングエントリの数。
conntrack-usage	使用中の接続トラッキングエントリの割合。

トップネームの統計情報

top-names activity-summary-settings は、照会されたトップネームとヒット数をログに記録します。

サンプルログメッセージ：

```
10/26/2021 12:07:08 cdns Activity Stats 0 22371 [Top-Names] from 12:06:48 to 12:06:58;
interval=number, total-counted=number
```

表 *12*：トップネームの統計情報

アクティビティサマリー名	統計[10]	説明
interval	該当なし	データ収集期間の長さ。CDNS *top-names-max-age* 設定に対応し、各ログエントリのトップネームを収集する必要がある期間を制御します。それから、設定可能なトップネームの数（デフォルトは 10）と、それらの名前に対するクエリの数をリストします。
total-counted	total-counted	この収集期間にカウントされたクエリの総数。

[10] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

アップストリームの統計

upstream activity-summary-settings は、アップストリームのクエリの数を記録します。

サンプルログメッセージ：

```
05/05/2022 20:16:47 cdns tid: 0 Activity Stats 0 22442 [Upstream] Sample since Thu May
5 20:15:47 2022: upstream-queries-total=number, upstream-queries-udp=number,
upstream-queries-tcp=number, upstream-queries-tls=number
```

表 *13*：アップストリームの統計

アクティビティサマリー名	統計[11]	説明
upstream-queries-total	該当なし	送信されたアップストリームクエリの総数。
upstream-queries-udp	upstream-queries-udp	UDP を使用して送信されたアップストリームクエリの数。

アクティビティサマリー名	統計[11]	説明
upstream-queries-tcp	upstream-queries-tcp	TCP を使用して送信されたアップストリームクエリの数。
upstream-queries-tls	upstream-queries-tls	TLS を使用して送信されたアップストリームクエリの数。

[11] この列にリストされている統計は、Web UI および CLI に表示されるサーバー統計です。REST API コールには、ダッシュのないキャメルケースの統計名が付けられます（つまり、queries-total は REST API で queriesTotal です）。アクティビティサマリーと統計は同じサーバーデータに対応していますが、アクティビティサマリー名はログメッセージのスペースを節約するために短縮されていることに注意してください。キャッシング DNS サーバー統計情報の完全なリストについては、*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの付録「サーバーの統計情報」の「CDNS 統計」セクションを参照してください。

トップ ネーム設定の指定

top-names 属性は、トップ ネーム データを収集する必要があるかどうかを指定します。これが有効になっていると、照会されたトップ ネームのキャッシュ ヒットのスナップショットが、*top-names-max-age* 値で設定される各間隔で収集されます。アクティビティ サマリー統計で報告されるトップ ネームのリストは、最新のスナップショットです。

top-names-max-age 属性を使用すると、トップネームのリストで許可されている照会された名前の最大経過時間を（最終アクセス時刻に基づいて）指定できます。

（注） *top-names-max-age* 属性のデフォルト値は 60 秒です。

top-names-max-count 属性を使用すると、照会されたトップネームのリストの最大エントリ数を指定できます。この制限は、アクティビティサマリーの一部としてロギングされるか、またはトップネームの統計の一部として返されるトップネームのリストに適用されます。デフォルト値は 10 です。

ローカル Web UI

トップネームを有効にするには、[ローカル CDNS サーバーの編集（Edit Local CDNS Server）] タブの [トップ ネームの設定（Top Names Settings）] セクションで、[有効（enabled）] オプションを選択して *top-names* 属性を有効にしてから、[保存（Save）] をクリックして変更内容を保存します。

トップネームの統計情報

[トップネーム（Top Names）] タブに上位 N 個のドメインと重要なその他の統計属性に関する情報が表示されます。

ローカル Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 [ローカル CDNS サーバー（Local CDNS Server）] ページで使用可能な [トップネーム（Top Names）] タブをクリックします。

CLI コマンド

cdns getStats top-names を使用して、トップネームの統計を表示します。

セキュリティイベントのロギング

DNS は多くのエンドポイントの運用の基本であるため、DNS トラフィックは多くの場合、顧客のネットワークに出入りすることが許可されています。また、トラフィック量が多いため、DNS トラフィックは通常十分に監視されていません。これにより、DNS はさまざまな DNS 攻撃の主要なターゲットになっています。DNS トンネリングまたはデータ漏えいを使用すると、情報を DNS プロトコルの上にペイロードとして運ぶことができます。このデータは、流出したり、コマンド アンド コントロール ホスト（ボットネット）に接続したり、Wi-Fi サービスのキャプティブポータルをバイパスしたりする機密性の高い企業データである可能性があります。

Cisco Prime Network Registrar キャッシュ DNS はすでに応答ポリシーゾーン（RPZ）をサポートしています。これによってサードパーティの RPZ サービスへの登録や、独自の RPZ の作成が可能です。これにより、悪意のあるアクティビティに関連するドメインをブロックできます。詳細については、権威 DNS サーバーでの RPZ プライマリ ゾーンの設定を参照してください。同様に、Cisco Prime Network Registrar キャッシュ DNS により、クエリ解決の信頼できる送信元として Cisco Umbrella を使用できます。Cisco Umbrella は、既知の脅威をブロックまたはリダイレクトし、処理中のクエリに基づいて新しい脅威や異常なパターンをチェックできる場合もあります。これらに加えて、通常の DNS 要求の検索や 2008 年の Kaminsky スタイルの保護など、異常を検出するための他の小さな機能もあります。Cisco Prime Network Registrar 11.1 は、セキュリティイベントの形式でさまざまなセキュリティトリガーに関する洞察を提供します。

セキュリティイベントの設定

[サーバーの管理（Manage Servers）] ページの *security-event-logging* 属性を使用して、DNS サーバーのセキュリティイベントをログに記録するかどうかを指定できます。**[セキュリティイベ**

ント（Security Events）] セクションで、どのセキュリティイベントのトリガーをログに記録するかを制御することもできます。キャッシュ DNS サーバーがセキュリティイベントを検出し、関連するセキュリティイベントログ設定が有効になっている場合、ログメッセージは cdns_security_log file ファイルに書き込まれます。

security-event-logging が無効になっている場合でも、アクティビティサマリーのためにセキュリティイベントが監視されます。

表 *14*：キャッシュ *DNS* サーバーのセキュリティイベント属性

属性	説明
セキュリティイベントのロギング（*security-event-logging*）	*security-event-log-settings* での設定に基づいて、DNS セキュリティイベントのロギングを有効にします。 セキュリティイベントログのメッセージは、cdns_security_log ファイルに書き込まれます。*security-event-logging* および *security-event-log-settings* 設定の変更は、CDNS サーバーのリロードを必要とせずにすぐに有効になることに注意してください。

属性	説明
セキュリティイベントログの設定 （*security-event-log-settings*）	ログに記録する DNS セキュリティイベントを指定します。CDNS サーバーがセキュリティイベントを検出し、関連するセキュリティイベントログ設定が有効になっている場合、ログメッセージは cdns_security_log file ファイルに書き込まれます。この設定を有効にするには、*log-settings* 属性にセキュリティ設定が含まれている必要があります。*security-event-logging* および *security-event-log-settings* 設定の変更は、CDNS サーバーのリロードを必要とせずにすぐに有効になることに注意してください。 • cisco-umbrella：Cisco Umbrella フォワーダがリダイレクトされたアドレスで応答すると、セキュリティイベントログのメッセージが生成されます。このセキュリティイベントをキャッチするには、Cisco Umbrella フォワーダを設定する必要があることに注意してください。Cisco Umbrella サブスクリプションが必要になる場合があることに注意してください。 • configuration：セキュリティイベントログのメッセージは、DNS サーバー設定（つまり、ACL エラー）に基づいて生成されます。 • dnssec：CDNS サーバーが DNSSEC データの検証に失敗すると、セキュリティイベントログのメッセージが生成されます。DNSSEC の検証の失敗は、キャッシュポイズニングの試行を示している可能性があります。 • packet-inspection：DNS サーバーが要求パケットの問題を検出したことに基づいて、セキュリティイベントログのメッセージが生成されます。これらの問題は、基本的なパケットインスペクション（つまり、*packet-inspection* 設定）によって、またはパケット処理中に検出される場合があります。不正なパケットが多すぎる場合は、DoS 攻撃を示している可能性があります。 • rate-limit：CDNS サーバーが設定済みの IP またはドメインのレート制限に達すると、セキュリティイベントログのメッセージが生成されます。レート制限を必要とする過剰な DNS トラフィックは、アンプ攻撃を示している可能性があります。 デフォルト設定は、configuration、dnssec、packet-inspection、rate-limit、および cisco-umbrella です

属性	説明
セキュリティイベントアラームの設定 （*security-event-alarm-settings*）	リソース制限アラームにカウントされる DNS セキュリティイベント トリガーを指定します。これにより、ユーザーは引き続きすべてのセキュリティイベントの統計とログメッセージを取得できますが、アラームをトリガーするイベントは制限されます。*security-event-alarm-settings* 構成の変更は、DNS サーバーのリロードを必要とせずにすぐに有効になることに注意してください。 • cisco-umbrella：Cisco Umbrella フォワーダがリダイレクトされたアドレスで応答すると、セキュリティイベントログのメッセージが生成されます。このセキュリティイベントをキャッチするには、Cisco Umbrella フォワーダを設定する必要があることに注意してください。Cisco Umbrella サブスクリプションが必要になる場合があることに注意してください。 • configuration：セキュリティイベントログのメッセージは、DNS サーバー設定（つまり、ACL エラー）に基づいて生成されます。 • dnssec：CDNS サーバーが DNSSEC データの検証に失敗すると、セキュリティイベントログのメッセージが生成されます。DNSSEC の検証の失敗は、キャッシュポイズニングの試行を示している可能性があります。 • packet-inspection：DNS サーバーが要求パケットの問題を検出したことに基づいて、セキュリティイベントログのメッセージが生成されます。これらの問題は、基本的なパケットインスペクション（つまり、*packet-inspection* 設定）によって、またはパケット処理中に検出される場合があります。不正なパケットが多すぎる場合は、DoS 攻撃を示している可能性があります。 • rate-limit：CDNS サーバーが設定済みの IP またはドメインのレート制限に達すると、セキュリティイベントログのメッセージが生成されます。レート制限を必要とする過剰な DNS トラフィックは、アンプ攻撃を示している可能性があります。

属性	説明
クエリ名の最大サイズ（*security-event-max-qname-size*）	許可されるクエリ名（QNAME）の最大サイズを指定します。より長いホスト名が検出されると、サーバーは DNS トンネリングカテゴリのパケットインスペクション DNS セキュリティイベントをトリガーし、クエリは拒否されます。0（デフォルト）に設定すると、クエリ名の長さのチェックが無効になります。

ローカルの高度な Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 [セキュリティイベント（Security Events）] セクションで、[security-event-logging] ドロップダウンリストから [有効（enabled）] を選択して、キャッシュ DNS セキュリティイベントのロギングを有効にします。

ステップ 4 *security-event-log-settings* 属性では、対象のチェックボックスをオンにします。

ステップ 5 [**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

cdns enable security-event-logging を使用して、DNS セキュリティイベントのロギングを有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	ログに記録する DNS セキュリティイベントを指定するには、**cdns set security-event-log-settings** = *value* を使用します。	

セキュリティイベントの統計

[DNSキャッシングサーバーの管理（Manage DNS Caching 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。セキュリティイベント統計情報は、[合計統計（Total Statistics）] カテゴリと [サンプル統計（Sample Statistics）] カテゴリの **[セキュリティイベント（Security Events）]** セクションに表示されます。

表 *15 :* セキュリティイベント統計属性

属性	説明
security-events	検出およびキャプチャされたセキュリティイベントの総数。
security-events-alarm	DNS セキュリティ イベント リソース制限アラームのトリガーに使用される、構成可能な間隔内で検出およびキャプチャされたセキュリティイベントの総数。
security-events-amplification-attack	検出およびキャプチャされたアンプ攻撃によるセキュリティイベントの総数。
security-events-dns-tunneling	検出およびキャプチャされた DNS トンネリングによるセキュリティイベントの総数。
security-events-dos	検出およびキャプチャされた潜在的な DoS 攻撃によるセキュリティイベントの総数。
security-events-firewall	検出およびキャプチャされた DNS ファイアウォールによるセキュリティイベントの総数。
security-events-malware	検出およびキャプチャされたマルウェアによるセキュリティイベントの総数。
security-events-phishing	検出およびキャプチャされた DNS フィッシングによるセキュリティイベントの総数。
security-events-poisoning	検出およびキャプチャされた DNS ポイズニングによるセキュリティイベントの総数。
security-events-snooping	検出およびキャプチャされたキャッシュまたはデータのスヌーピングによるセキュリティイベントの総数。

セキュリティログ

キャッシュ DNS のセキュリティイベントは、cdns_security_log ファイルに保存されます。[セキュリティログ（Security Logs）] タブにこのログファイルの内容が表示されます。

ローカル Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 [セキュリティログ（Security Logs）] タブをクリックします。

セキュリティイベントのリソースの監視

[ローカルCCMサーバーの編集（Edit Local CCM Server）] ページで、キャッシュ DNS のセキュリティイベントの警告および重要レベルを構成できます。

ローカルおよびリージョンの詳細 Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。[サーバーの管理（Manage Servers）] ペインの [CCM] をクリックして、[ローカルCCMサーバーの編集（Edit Local CCM Server）] ページを開きます。

ステップ 2 [DNSセキュリティイベント（DNS Security Events）] セクションで、次のフィールドに必要な値を入力します。

- **cdns-security-events-critical-level**：キャッシュ DNS サーバーの DNS セキュリティイベント数の重要レベルを指定します。サーバーのセキュリティイベント数がこの値を超えると、重要な通知がトリガーされます。
- **cdns-security-events-warning-level**：キャッシュ DNS サーバーの DNS セキュリティイベント数の警告レベルを指定します。サーバーのセキュリティイベント数がこの値を超えると、警告通知がトリガーされます。

ステップ 3 [保存（Save）] をクリックします。

CLI コマンド

resource set cdns-security-events-critical-level = *value* を使用して、キャッシュ DNS サーバーの DNS セキュリティイベント数の重要レベルを設定します。

resource set cdns-security-events-warning-level = *value* を使用して、キャッシュ DNS サーバーの DNS セキュリティイベント数の警告レベルを設定します。

証明書の設定の指定

秘密キーファイルと公開キーファイルには、TLS および DoH セッションのためにキャッシュ DNS サーバーが使用する秘密キーと公開キーが含まれています。[サーバーの管理（Manage Servers）] ページでこれらのファイルの名前を指定できます。これらのファイルは tls サブディレクトリの CDNS データディレクトリ（つまり、<cnr.datadir>/cdns/tls）に必ず保管するようにしてください。

openssl ツールを使用して、TLS 秘密キーファイルと公開キーファイルを作成できます。

ローカルの高度な Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 [証明書の設定（Certificates Settings）] セクションで、次のフィールドに秘密キーファイルと公開キーファイルの名前を入力します。

- 秘密キーファイル（*service-key*）：DNS が TLS および DoH セッションに使用する秘密キーを含むファイル名を定義します。
- 公開キーファイル（*service-pem*）：CDNS が TLS および DoH セッションに使用する公開キー証明書を含む pem ファイル名を定義します。マネージド CDNS 証明書を使用する場合、この属性は無視されるため、設定しないでください。

ステップ 4 **[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

cdns set service-key = *value* を使用して、キャッシュ DNS サーバーの秘密キーファイル名を定義します。

cdns set service-pem = *value* を使用して、キャッシュ DNS サーバーの公開キーファイル名を定義します。

TLS 設定の指定

暗号化されていない DNS クエリは、スプーフィングやプライバシーを脅かすその他の攻撃に対して脆弱です。これらの問題に対処するために、Cisco Prime Network Registrar は、権威 DNS サーバーとキャッシング DNS サーバーの両方について RFC 7858 で指定されている DNS over TLS（DoT）をサポートしています。

DNS over TLS は、Transport Layer Security（TLS）プロトコルを介して DNS クエリと応答を暗号化およびラップするためのセキュリティプロトコルです。これにより、クライアントとリゾルバ間のプライバシーとセキュリティが向上します。基本的な接続プロトコルとして TCP を使用し、TLS 暗号化と認証を介したレイヤを使用します。

TLS キー

TLS キーペアは、秘密キーと公開キーで構成されます。これら 2 つのキーは、暗号化アルゴリズムによって相互に関連付けられます。秘密キーは、受信 TLS 接続を受信するサーバーに対して「秘密」であり、秘密にしておく必要があります。サーバーは、証明書を引き渡すことでクライアントに自己紹介します。証明書は、サーバーの公開キーを含む署名付き（「認証済み」）コンテナです。

Cisco Prime Network Registrar では、DNS サーバーは設定可能なポート 853 で TLS をリッスンします。ポート 853 では、TCP TLS 接続のみが許可され、他の接続はドロップされます。DNS サーバーには、TLS を有効または無効にし、TLS 秘密キーファイルと公開キーファイル、およびアップストリームの TLS 証明書バンドルを追加するための設定可能なパラメータがあります。

キャッシング DNS 例外およびフォワーダには、アップストリームの TLS を有効または無効にする構成パラメータがあります。

（注）
- Cisco Prime Network Registrar は、自己署名証明書を生成するコマンドをサポートしていません。ただし、openssl などの簡単に使用できるコマンドラインツールで自己署名証明書を生成することができます。次に例を示します。

  ```
  # openssl req -new -x509 -days 365 -nodes -out public.pem -keyout private.pem
  ```

- TLS は、ハイブリッドモードおよびゾーン転送ではサポートされません。
- TLS キーはパスワードフレーズではサポートされていません。

認証局バンドルへの公開キーの追加

アップストリームクエリの場合は、フォワーダ/例外サーバーの public.pem をキャッシング DNS サーバーにコピーし、次のコマンドを使用して *tls-upstream-cert-bundle* を更新します。

```
scp -r public.pem @client-ip:/etc/pki/ca-trust/source/anchors/

# update-ca-trust
```

上記のコマンドは、/etc/pki/tls/certs/ca-bundle.crt ファイルを更新します。

更新された /etc/pki/tls/certs/ca-bundle.crt ファイルを <cnr.datadir>/cdns/tls にコピーし、ファイル名を *tls-upstream-cert-bundle* に設定します。

表 *16 :* キャッシング *DNS* サーバーの *TLS* 属性

属性	説明
TLS（*tls*）	キャッシング DNS の TLS サポートを有効または無効にします。TLS を有効にする前に、秘密キーファイルを CDNS データディレクトリの cdns/tls に配置し、*service-key* 属性を設定する必要があります。 マネージド CDNS 証明書を使用する場合は、証明書の設定が自動的に設定されます。それ以外の証明書を使用する場合は、公開証明書ファイルを CDNS データディレクトリの cdns/tls に配置し、*service-pem* 属性を設定する必要があります。 TLS サービスを有効または無効にするには、変更を有効にするために Cisco Prime Network Registrar サービスを再起動する必要があります。

属性	説明
TLS ポート（*tls-port*）	TCP TLS サービスを提供するポート番号。キャッシング DNS サーバーは、このポートで非 TLS クエリを処理しません。
TLS証明書バンドルファイル（*tls-upstream-cert-bundle*）	証明書バンドルを含むファイル名を定義します。これらの証明書は、外部ピアへのTLS接続に使用されます。これらの証明書は、アップストリーム DNS サーバーへの接続を認証するために使用されます。ファイルは**tls**サブディレクトリのCDNSデータディレクトリ（つまり、 <cnr.datadir>/cdns/tls）にかならず保管します。/etc/pki/tls/certs/ca-bundle.crt ファイルをコピーするか、またはソフトリンクを作成できます。

TLSは、フォワーダ（フォワーダの使用を参照）、例外（例外の使用を参照）、およびファイアウォール（RPZ の TLS の有効化を参照）レベルで有効にすることもできます。

ローカルの高度な Web UI

キャッシング DNS サーバーの TLS サポートを有効にするには、次の手順を実行します。

始める前に

TLS を有効にする前に、公開証明書と秘密キーファイルを **tls** サブディレクトリの CDNS データディレクトリに配置する必要があります（つまり、<cnr.datadir>/cdns/tls）。そして [DNS キャッシュサーバー管理（Manage DNS Caching Server）] ページの **[証明書の設定（Certificates Settings）]** セクションにある *service-key* 属性および *service-pem* 属性を設定します。管理対象証明書を使用することもできます（*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドの「*Certificate Management*」の項を参照）。

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 **[TLS設定（TLS Settings）]** セクションで、**[有効（Enabled）]** オプションを選択して *TLS* 属性を有効にします。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。

（注） TLS の設定を変更するたびに、Cisco Prime Network Registrar サービスを再起動する必要があります。

CLI コマンド

cdns enable tls を使用して、キャッシュ DNS サーバーの TLS サポートを有効にします。次に、**systemctl restart nwreglocal.service** を使用して、Cisco Prime Network Registrar サービスを再起動します。

キャッシング DNS サーバーの TLS 属性を設定するには、**cdns set** *attribute=value* を使用します。

（注） TLS の設定を変更するたびに、Cisco Prime Network Registrar サービスを再起動する必要があります。

TLS 統計情報

[DNSキャッシングサーバーの管理（Manage DNS Caching 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。*querys-over-tls* 属性は、[合計統計（Total Statistics）] および [サンプル統計（Sample Statistics）] カテゴリの [クエリ詳細（Query Details）] セクションに表示されます。*tls-errors-in* 属性と *tls-errors-out* 属性は、[合計統計（Total Statistics）] カテゴリと [サンプル統計（Sample Statistics）] カテゴリの [サーバー統計（Server Statistics）] セクションに表示されます。

表 *17 : TLS* 統計属性

属性	説明
querys-over-tls	CDNS サーバーが TLS を介して受信したクエリの総数。この統計は、HTTPS 経由でクエリを受信した場合にも増加します。
tls-errors-in	インバウンド DNS クエリの試行で発生した TLS 関連エラーの総数。クエリが正常に受信されたかどうかにかかわらず、エラーが発生する場合があります。
tls-errors-out	アウトバウンド DNS クエリの試行で発生した TLS 関連エラーの総数。クエリが正常に送信されたかどうかにかかわらず、エラーが発生する場合があります。

HTTPS 設定の指定

DNS over HTTPS（DoH）は、DNS クエリを送信し、HTTPS 経由で DNS 応答を取得するためのプロトコルです。DNS クエリと応答の各ペアは、HTTP 交換にマッピングされます。このメソッドの目的は、中間者攻撃による DNS データの盗聴や不正操作を防止することにより、ユーザーのプライバシーとセキュリティを強化することです。これを実現するために、HTTPS プロトコルを使用して、DoH クライアントと DoH ベースの DNS リゾルバ間のデータを暗号化します。通常、DoH には、DoH をサポートすることがわかっているキャッシュサーバーにアクセスするクライアントが含まれます。

Cisco Prime Network Registrar 11.1 は、キャッシュ DNS サーバーで DoH をサポートします。キャッシュ DNS は、着信クエリに対してのみ DoH をサポートします。キャッシュ DNS サーバーは、設定可能なポート 443 で HTTPS をリッスンします。ネットワーク インターフェイスが設定されていない場合、サーバーはすべてのネットワーク インターフェイスの HTTPS ポート、TLS ポート、および DNS ポート（TCP および UDP）でリッスンします。ネットワーク インターフェイスが手動で設定されている場合、サーバーは、設定されたネットワーク インターフェイスの HTTPS ポート、TLS ポート、および DNS ポート（TCP および UDP）でリッスンします。Cisco Prime Network Registrar では、DoH 設定は Web UI、CLI、および REST API で使用できます。

（注）
- Cisco Prime Network Registrar は、自己署名証明書を生成するコマンドをサポートしていません。ただし、openssl などの簡単に使用できるコマンドラインツールで自己署名証明書を生成することができます。
- DoH 設定は、権威 DNS およびアップストリームクエリではサポートされていません。

表 *18* : キャッシュ *DNS* サーバーの *HTTPS* 属性

属性	説明
HTTPS	キャッシュ DNS の HTTPS サポートを有効または無効にします。 DoH は、着信クエリに対してのみサポートされます。 DoH は、RFC 8484 で指定されているように GET および POST メソッドをサポートします。 HTTPS を有効にする前に、秘密キーおよび公開キーファイルを CDNS データディレクトリの cdns/tls に配置し、*service-key* 属性と *service-pem* 属性を設定する必要があります。 マネージド CDNS 証明書を使用する場合は、証明書の設定が自動的に設定されます。それ以外の証明書を使用する場合は、公開証明書ファイルを CDNS データディレクトリの cdns/tls に配置し、*service-pem* 属性を設定する必要があります。
HTTPS ポート（HTTPS Port） （*https-port*）	HTTPS サービスを提供するポート番号。キャッシュ DNS サーバーは、このポートで非 HTTPS クエリを処理しません。

ローカル詳細 Web UI

キャッシュ DNS サーバーの DoH サポートを有効にするには、次の手順を実行します。

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 [HTTPS設定（HTTPS Settings）] セクションで、[有効（Enabled）] オプションを選択して *HTTPS* 属性を有効にします。[https-port] フィールドに、HTTPS サービスを提供するポート番号を入力します。この値には 1 ～ 65535 の範囲の整数を指定できます。デフォルト値は 443 です。キャッシュ DNS サーバーは、このポートで非 HTTPS クエリを処理しないことに注意してください。

ステップ 4 **[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

cdns enable https を使用して、キャッシュ DNS サーバーで DoH サポートを有効にします。

HTTPS 統計

[DNSキャッシングサーバーの管理（Manage DNS Caching 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。*queries-over-https* 属性は、[合計統計（Total Statistics）] および [サンプル統計（Sample Statistics）] カテゴリの **[クエリ詳細（Query Details）]** セクションに表示されます。*queries-over-https-failed* 属性、*https-query-buffer* 属性、*https-response-buffer* 属性は、[合計統計（Total Statistics）] カテゴリと [サンプル統計（Sample Statistics）] カテゴリの **[サーバー統計（Server Statistics）]** セクションに表示されます。

表 *19 : HTTPS* 統計属性

属性	説明
queries-over-https	CDNS サーバーが HTTPS 経由で受信したクエリの総数。
queries-over-https-failed	HTTPS エラーで失敗したクエリの総数。
https-query-buffer	メモリバッファの HTTPS クエリの数。
https-response-buffer	メモリバッファの HTTPS 応答の数。

HTTP エラー コード

DoH では、次の HTTP エラーコードがサポートされています。

- HTTP_STATUS_OK (200)：DoH はクエリを処理して応答を返すことができます。これは、ネガティブな応答か、SERVFAIL や FORMERR などのエラーである可能性があります。
- HTTP_STATUS_BAD_REQUEST (400)：有効なクエリが受信されませんでした。

- HTTP_STATUS_NOT_FOUND (404)：要求は、http-endpoint（デフォルトまたは dns-query）で設定されたエンドポイント以外のパスに送信されます。
- HTTP_STATUS_PAYLOAD_TOO_LARGE (413)：POST 要求で受信したペイロードが大きすぎます。ペイロードは、要求ヘッダーで通信されるコンテンツの長さを超えることはできません。harden-large-queries が有効になっている場合、ペイロードの長さは 512 バイトに制限されます。
- HTTP_STATUS_URI_TOO_LONG (414)：GET 要求の base64url エンコードされた DNS クエリが大きすぎます。harden-large-queries が有効になっている場合、DNS クエリの長さは 512 バイトに制限されます。
- HTTP_STATUS_UNSUPPORTED_MEDIA_TYPE (415)：要求のメディアタイプはサポートされていません。DoH は現在、「application/dns-message」メディアタイプのみをサポートしています。content-type のない要求は、application/dns-message として扱われます。
- HTTP_STATUS_NOT_IMPLEMENTED (501)：要求で使用されたメソッドは、GET または POST ではありません。

プリフェッチ タイミングの設定

[スマートキャッシュ（Smart Cache）] セクションの Prefetch 属性は、キャッシュを最新の状態に保つためにメッセージキャッシュ要素を有効期限前にプリフェッチする必要があるかどうかを設定するために使用されます。これを **on** にすると、マシンへのトラフィックと負荷は約 10% 増えますが、一般的な DNS 名のクエリ パフォーマンスを向上させることができます。

Prefetch が有効になっている場合、レコードには有効期間の 10 % 以内に相当するプリフェッチ時間が割り当てられます。サーバーはクライアント クエリを処理する際に、レコードを検索し、プリフェッチ時間をチェックします。レコードの有効期間が残り 10% 以内になると、サーバーはレコードが有効期限切れにならないようにクエリを発行します。

キャッシュ TTL の設定

存続可能時間（TTL）は、DNS サーバーが他のネームサーバーから学習したデータをキャッシュできる時間の長さです。キャッシュに追加される各レコードには TTL 値があります。TTL の有効期間が終わると、サーバーはキャッシュされたデータを廃棄し、次にクエリを送信するときには、権威ネームサーバーから新しいデータを取得する必要があります。TTL 属性である *cache-min-ttl* と *cache-max-ttl* は、Cisco Prime Network Registrar がキャッシュされた情報を保持する最小時間と最大時間を示します。これらのパラメータは、キャッシュ内にある TTL 値が非常に大きいか非常に小さいレコードのライフタイムを制限します。

ローカル Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。[サーバーの管理（Manage Servers）] ペインで、[CDNS] をクリックします。

ステップ 2 [ローカルCDNSサーバーの編集（Edit Local CDNS Server）] タブの **[キャッシュ（Caching）]** セクションでは、次の属性を確認できます。

- [最大キャッシュ TTL（Maximum Cache TTL）]（*cache-max-ttl*）属性：必要な値に設定します（デフォルト値は 24 時間）
- [最小キャッシュ TTL（Min Cache TTL）]（*cache-min-ttl*）属性：必要な値に設定します（プリセット値は 0）

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

cdns set cache-max-ttl=*value* を使用して、最大キャッシュ TTL 値を設定します。

cdns set cache-min-ttl =*value* を使用して、最小キャッシュ TTL 値を設定します。

スマートキャッシュの有効化

権威 DNS サーバーが停止したり、その他の理由でオフラインになったりすると、影響を受ける可能性の低いインターネットサービスにアクセスできるという問題が発生する可能性があります。スマートキャッシングを使用すると、キャッシング DNS サーバーが、権威ネームサーバーに到達できない場合でも期限切れのデータ（最新の既知の応答）を引き続き使用できるようになります。キャッシング DNS サーバーは引き続き権威ネームサーバーに接続し、ネームサーバーが再び機能し始めるとキャッシュデータを更新します。

（注） スマートキャッシュ（*smart-cache*）を有効にすると、プリフェッチが自動的に有効になります。

スマートキャッシュの構成設定

Cisco Prime Network Registrar では、キャッシング DNS スマートキャッシュはデフォルトで有効にはなっていません。スマートキャッシュを使用するには、*smart-cache* 属性をキャッシング DNS サーバーレベルで有効にする必要があります。

キャッシング DNS サーバーが期限切れのデータのクエリを受信したときに *smart-cache* 属性が有効になっている場合、キャッシュされた期限切れのデータで応答し続け、[統計（Statistics）] タブの [クエリの詳細（Query Details）] セクションで *smart-cache* カウンタを増分します。

（注） スマートキャッシュは詳細モードで使用でき、変更を有効にするにはキャッシング DNS サーバーをリロードする必要があります。

表 *20 :* スマートキャッシュ属性

属性	説明
スマートキャッシュ（*smart-cache*）	キャッシング DNS サーバーがスマートキャッシングを使用するかどうかを指定します。*smart-cache* が有効になっているときにキャッシュされた応答が期限切れになり、権威ネームサーバーに到達できない場合、キャッシング DNS サーバーは最後の最も知られている応答を引き続き使用します。スマートキャッシュ応答の RRは、0TTL です。スマートキャッシングは、ネットワークの停止や、権威ネームサーバーを使用不能にする可能性のある DDoS 攻撃を軽減するのに役立ちます。 *smart-cache* を有効にすると、プリフェッチが自動的に有効になります。
スマートキャッシュの有効期限（*smart-cache-expiration*）	*smart-cache* が有効になっている場合は、期限切れの RR で応答する時間制限を指定します。 デフォルト値は0で、サーバーがキャッシュに残っている限り、期限切れの応答で応答できます。
スマートキャッシュの有効期限のリセット（*smart-cache-expiration-reset*）	*smart-cache* が有効で、*smart-cache-expiration* が 0 より大きい場合は、有効なクエリの有効期限がリセットされます。これにより、アクティブなクエリが期限切れの応答を返すことができます。また、他のユーザーは、短期間の場合に SERVFAIL 応答を返すことができます。クエリがアクティブになると、期限切れの応答が返されます。デフォルトは無効です。
スマートキャッシュの期限切れの応答の TTL（*smart-cache-expired-reply-ttl*）	スマートキャッシュが有効な場合、期限切れのデータで応答するときに使用する TTL 値を指定します。

属性	説明
プリフェッチ（*prefetch*）	メッセージキャッシュの要素を期限切れになる前にプリフェッチしてキャッシュを最新に保つかどうかを設定します。オンにすると、マシンのトラフィックと負荷が約 10 % 増加しますが、一般的な項目はキャッシュから期限切れになりません。 *Prefetch* が有効になっている場合、レコードには有効期間の 10 % 以内に相当するプリフェッチ時間が割り当てられます。サーバーはクライアントクエリを処理する際に、レコードを検索し、プリフェッチ時間をチェックします。レコードの有効期間が残り 10% 以内になると、サーバーはレコードが有効期限切れにならないようにクエリを発行します。

（注） Cisco Prime Network Registrar 10.1 以降では、*Prefetch* 属性は [スマートキャッシュ（Smart Cache）] セクションで使用できます。これは 詳細モードの機能です。

ローカルの高度な Web UI

スマートキャッシュを有効にするには、次の手順を実行します。

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 **[スマートキャッシュ（Smart Cache）]** セクションで、**[有効（enabled）]** オプションを選択して *smart-cache* 属性を有効にします。

ステップ 4 [**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

スマートキャッシングを有効にするには、**cdns enable smart-cache** を使用します。

smart-cache が有効になっている場合、**cdns set smart-cache-expiration=***value* を使用して、有効期限切れの RR で応答する時間制限を指定します。次に例を示します。

```
nrcmd> cdns set smart-cache-expiration=5m
```

cdns enable smart-cache-expiration-reset を使用すると、*smart-cache* が有効で *smart-cache-expiration* が 0 以上の場合に、アクティブなクエリの有効期限をリセットできます。

ルート ネームサーバーの定義

ルート ネームサーバーは、すべてのトップレベル ドメインの権威ネームサーバーのアドレスを認識します。新しくインストールした Cisco Prime Network Registrar キャッシュ DNS サーバーを初めて起動するときには、現在のルート ネームサーバーを要求する権威としてルート ヒントという事前設定済みルート サーバーを使用します。

Cisco Prime Network Registrar は、ルート サーバー クエリーに対する応答を受信したら、それをキャッシュして、ルート ヒント リストを参照します。キャッシュが期限切れになると、サーバーはプロセスを繰り返します。公式なルートサーバーレコードの TTL は事前に設定されており、別のキャッシュ TTL 値を指定できます（キャッシュ TTL の設定 （33 ページ）を参照）。

設定されているサーバーはヒントにすぎず、完全なセットである必要はありません。情報を変更または拡張する必要があるかどうかを確認するために、ルート サーバーを定期的に（毎月から 6 ヵ月まで間隔で）検索する必要があります。

ローカル Web UI

[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] タブの [ルート ネーム サーバー（Root Name Servers）] セクションで、追加する各ルートネームサーバーのドメイン名と IP アドレスを入力し、それぞれの後ろにある [ルートのネームサーバーの追加（**Add Root Namerserver**）] をクリックして、[保存（**Save**）] をクリックします。

CLI コマンド

cdns addRootHint *name addr* [*addr ...*] を使用して、ルートサーバーの名前とルートネームサーバーのアドレスを追加します。

UDP ポートの動的割り当て

キャッシング DNS サーバーは、多くの UDP ポート番号を使用します（デフォルトでは最大 48000 万個）。これらの番号は、処理スレッド間で分割されます。多くのポート番号を使用することで、誕生日攻撃によるキャッシュ ポイズニングのリスクが軽減されます。キャッシュ DNS サーバーは、UDP ポートのデフォルト プール（2048）を使用します。UDP ポートのデフォルト プールの最大許容サイズは 4096 です。

現在、Cisco Prime Network Registrar は 1024 ～ 65535 のポート範囲を使用しています。キャッシュ DNS サーバーは、未処理の解決クエリの数に基づいて、ポートを追加または削除することによってプール サイズを調整します。キャッシュ DNS サーバーは、サーバーの実行時に UDP ポートの割り当てと解放を動的に行います。サーバーをリロードすると、すべての UDP ポートが解放され、ランダムに再び選択されます。

最大メモリ キャッシュ サイズの設定

[最大メモリ キャッシュ サイズ（maximum memory cache size）] プロパティは、DNS のインメモリ キャッシュ用に予約するメモリ領域を示します。メモリ キャッシュが大きいほど、キャッ

シュ DNS サーバーが有効期限を過ぎたレコードを再解決しなければならない頻度が低くなります。

ローカルの詳細 Web UI

[ローカル CDNS サーバーの編集（Edit Local CDNS Server）] タブの [キャッシング（Caching）] セクションで、RRSet のキャッシュサイズ（*rrset-cache-size*）属性を目的の値に設定し、[保存（Save）] をクリックします。デフォルトサイズは 1 GB です。

メッセージ キャッシュのサイズを設定するには、[メッセージ キャッシュ サイズ（Message Cache Size）] 属性（*msg-cache-size*）を使用します。メッセージ キャッシュには、クエリ応答が保存されます。デフォルトサイズは 1 GB です。

CLI コマンド

- **cdns set rrset-cache-size** を使用して、RR セット キャッシュ サイズを設定します。
- **cdns set msg-cache-size** を使用して、メッセージ キャッシュ サイズを設定します。

リゾルバ設定の指定

グルー レコードは、定義対象ゾーン内にあるため、通常の DNS 処理によって検出できないネームサーバーの A レコードです。*harden-glue* 属性が有効になっている場合、キャッシング DNS サーバーはクエリ対象ゾーン内に存在しないグルーレコードを無視します。デフォルトでは、*harden-glue* 属性はオンになっています。

ドメインのランダム化により、DNS サーバーは、ランダムに生成されたクエリ名を使用し、アップストリームクエリを送信して解決できます。有効なネームサーバーはクエリ名を変更せずに応答するため、この手法を使用して応答が有効であることを確認できます。

特定の状況では、攻撃者は要求を発行した後、DNS サーバーのキャッシュを不正なデータでポイズニングしようと、偽の応答でサーバーをフラッディングします。ケースをランダム化することで、攻撃のタイプに対するサーバーの保護レベルがさらに高まります。

Cisco Prime Network Registrar ではアップストリーム クエリのランダム化をサポートしていますが、ランダム化されたケースを維持しないネーム サーバーがいくつかあります。したがって、ケースのランダム化をイネーブルにすると、有効なネーム サーバーをブロックする可能性があります。*randomize-query-case-exclusion* 属性を使用すると、除外リストを作成できます。これにより、ケースのランダム化を引き続き使用できますが、維持されないネームサーバーは除外され、有効な回答で応答を続行します。

表 *21 :* リゾルバ設定の属性

属性	説明
harden-glue	グルーがサーバー権限内にある場合にのみグルーを信頼するかどうかを指定します。

属性	説明
randomize-query-case	スプーフィング試行を阻止するために、クエリで 0x20 エンコードランダムビットを使用できるようにします。これにより、権威サーバーに送信されるクエリ名の小文字と大文字が混乱し、応答の大文字と小文字が正しく一致するかどうかがチェックされます。
randomize-query-case-exclusion	アップストリームクエリのランダム化の除外リストを作成できます。この属性は、*randomize-query-case* が有効になっている場合に使用されます。

ケースのランダム化除外を設定

randomize-query-case-exclusion 属性は、[DNS キャッシングサーバーの管理（Manage DNS Caching Server）] ページの [リゾルバ設定（Resolver Settings）] セクションで使用できます。*randomize-query-case* は、デフォルトでは無効になっています。ランダム化クエリケースの除外を使用するには、*randoming-query-case* 属性をキャッシング DNS サーバーレベルで有効にする必要があります。

randomize-query-case 属性と *randomize-query-case-exclusion* 属性の両方が、詳細モードの Web UI で使用できます。

ローカルの高度な Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [CDNS] をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 [リゾルバ設定（Resolver Settings）] セクションで次の手順を実行します。

a) **enabled** オプションを選択して、*randomize-query-case* 属性を有効にします。

b) *randomize-query-case-exclusion* フィールドに、ケースのランダム化から除外するドメインのリスト（カンマ区切り）を入力します。

ステップ 4 **[保存（Save）]** をクリックして、変更内容を保存します。

（注） これらの変更を有効にするには、キャッシング DNS サーバーをリロードする必要があります。

CLI コマンド

ケースのランダム化を有効にするには、**cdns enable randomize-query-case** を使用します。

randomize-query-case-exclusion を設定または設定解除するには、**cdns set** コマンドと **cdns unset** コマンドを使用します。次に例を示します。

```
nrcmd> cdns set randomize-query-case-exclusion="cisco.com"
nrcmd> cdns set randomize-query-case-exclusion="cisco.com, example.com"
nrcmd> cdns unset randomize-query-case-exclusion
```

ネットワーク設定の指定

listen-ip-version 属性では、受け入れて発行する IP パケットを選択できます。IPv4、IPv6、またはその両方を確認できます。*listen-protocol* 属性では、応答して発行するパケットプロトコルを選択できます。UDP、TCP、またはその両方を確認できます。

（注） デフォルトの *listen-ip-version* は IPv4 と IPv6 の両方です。実行しているサーバーが IPv6 をサポートしていない場合は、IPv4 に変更できます。変更しないと、クエリタイムアウトが発生する可能性があります。

詳細設定の指定

minimal-responses 属性は、クエリ応答の authority および data セクションからのレコードが不要な場合に、DNS キャッシュ サーバーがそれらのレコードを省略するのか、含むのかを制御します。この属性を有効にすることで、DNS サーバーがキャッシュ サーバーとして設定されている場合などには、クエリのパフォーマンスが向上する可能性があります。

remote-ns-host-ttl 属性によって、リモートネームサーバーのキャッシュエントリの TTL が設定されます。リモートネームサーバーのキャッシュには、ラウンドトリップタイミング（RTT）、不完全性、および EDNS サポート情報が含まれています。エントリの有効期限が切れると、リモートネームサーバーのキャッシュから削除され、次回サーバーに接続したときに新しいエントリが追加されます。

RTT は、照会するネームサーバーを決定するために使用されることに注意してください。タイムアウトが発生すると、そのサーバーの RTT 値が 2 倍になります。サーバーが応答しなくなると、IP アドレスをプローブするためにいくつかのクエリが選択されるプローブスキームが適用されます。これに失敗すると、ネームサーバーは 15 分間ブロックされ（*remote-ns-host-ttl*）、その後で 1 つのクエリを使用して再プローブされます。したがって、プローブをより頻繁に許可するには、*remote-ns-host-ttl* を減らす必要があります。リモートネームサーバーのキャッシュは、CDNS サーバーのリロード後にはフラッシュされませんが、**cdns execute flush-ns-cache** コマンドを使用するとフラッシュできます。

remote-ns-cache-numhosts 属性を使用して、情報をキャッシュするホストの数を設定できます。

ラウンドロビンの有効化

クエリは、ネームルックアップの複数の A レコードまたは AAA レコードを返す場合があります。ほとんどの DNS クライアントはリスト内の先頭のレコードのみを使用しますが、ラウンドロビンを有効にすることで負荷を共有できます。これにより、同じ名前を解決するクライア

ントが次々に異なるアドレスに循環方式でつながるようになります。DNSサーバーは、クエリのたびにレコードの順序を並べ替えます。これは、サーバーの実際の負荷に基づいたロードバランシングではなく、ロード シェアリング方式です。

ローカルの詳細 Web UI

[ローカル CDNS サーバーの編集（Edit Local CDNS Server）] タブにある [詳細設定（Advanced Settings）] セクションで、*round-robin* 属性を検索します。

CLI コマンド

cdns get round-robin を使用して、ラウンドロビンが有効になっているかどうかを確認します（デフォルトでは有効）。有効でない場合は、**cdns enable round-robin** を使用します。

DNS キャッシュのフラッシュ

Cisco Prime Network Registrar のキャッシュのフラッシュ機能では、サーバーのメモリキャッシュにキャッシュされたデータのすべてまたは一部を削除できます。

ローカル Web UI

ステップ 1 [展開（Deploy）] メニューから **DNS**サブメニューで **CDNS Server** を選択して [DNS キャッシングサーバーの管理（Manage DNS Caching Server）] ページを開きます。

ステップ 2 [DNS キャッシングサーバーの管理（Manage DNS Caching Server）] ページで、[コマンド（Commands）] ボタンをクリックして [CDNS コマンド（CDNS Command）] ダイアログ ボックスを開きます。キャッシュフラッシュのコマンドには 2 つのタイプがあります。

- [CDNS キャッシュのフラッシュ（Flush the CDNS cache）]：特定のゾーン、またはゾーンを指定しない場合はキャッシュ全体のすべてのキャッシュエントリをフラッシュできます。特定のゾーンのすべてのデータを削除するには、[ゾーン（Zone）] フィールドにゾーン名を入力します。キャッシュ全体をクリアするには、[ゾーン（Zone）] フィールドを空のままにします。
- [リソースレコードのフラッシュ（Flush Resource Record）]：[タイプ（type）] フィールドが指定されている場合は、RR 名または RRSet をフラッシュできます。
  - 特定のドメインからの共通RRタイプ（A、AAAA、NS、SOA、CNAME、DNAME、MX、PTR、SRV、NAPTR、および TXT）の削除：[リソースレコードのフラッシュ（Flush Resource Record）] コマンドの FQDN として必要な RR 名を入力し、[RR タイプ（RR type）] フィールドは空のままにします。
  - ドメインに指定された RR タイプの削除：[FQDN] フィールドにドメインを指定し、[RR type（RR タイプ）] フィールドに RR タイプを指定します。

（注） タイプが指定されていない場合は、タイプ A、AAAA、NS、SOA、CNAME、DNAME、MX、PTR、SRV、TXT、および NAPTR がフラッシュされます。

CLI コマンド

- 特定のドメイン以下にあるすべてのキャッシュエントリを削除するには、次のコマンドを使用します。ドメインが指定されていない場合は、キャッシュ内のすべての RR がフラッシュされます。

  ```
  nrcmd> cdns flushCache domain
  ```

- 特定の RR 名に関連付けられたキャッシュから RR をフラッシュするには、次のコマンドを使用します。タイプが指定されている場合は、指定された名前とタイプのエントリがすべてフラッシュされます。タイプが指定されていない場合は、タイプ A、AAAA、NS、SOA、CNAME、DNAME、MX、PTR、SRV、TXT、および NAPTR がフラッシュされます。

  ```
  nrcmd> cdns flushName name type
  ```

DNS キャッシュ ポイズニングの検出と防止

Cisco プロダクト セキュリティ インシデント レスポンス チーム（PSIRT）ドキュメント番号 PSIRT-107064（Advisory ID cisco-sa-20080708-dns）に記載されているとおり、Cisco Prime Network Registrar は、DNS キャッシュポイズニング攻撃（CSCsq01298）などの CDNS 関連の問題に対処するために、キャッシング DNS サーバーのパフォーマンスを向上させます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns

DNS キャッシュ ポイズニング攻撃

キャッシュ ポイズニング攻撃は、DNS キャッシュ内の既存のエントリを変更したり、DNS キャッシュに新しい無効レコードを挿入したりすることができます。この攻撃により、ホスト名が誤った IP アドレスを指すようになります。たとえば、www.example.com が IP アドレス 192.168.0.1 にマッピングされており、このマッピングが DNS サーバーのキャッシュに存在しているとします。攻撃者は DNS キャッシュをポイズンし、www.example.com を 10.0.0.1 にマッピングできます。この場合に、www.example.com にアクセスしようとすると、誤った Web サーバーに接続してしまいます。

転送クエリに対する応答を単一の静的ポートで受信する DNS サーバーは、偽装応答を送信する悪意のあるクライアントの影響を受けやすくなります。

DNS 応答の検証に使用される DNS トランザクション ID と送信元ポート番号は、十分にランダムではなく、簡単に予測できるため、攻撃者は DNS クエリに対する偽装応答を作成できます。DNS サーバーは、このような応答を有効と見なします。

DNS キャッシュ ポイズニング攻撃

DNS キャッシュ ポイズニング攻撃に対する脆弱さを減らすために、DNS サーバーは転送クエリに使用する UDP 送信元ポートをランダム化します。リゾルバの実装がクエリの次の属性に対する応答と一致する必要もあります。

- リモートアドレス
- ローカルアドレス

- ポートのクエリ
- クエリ ID
- 質問名（大文字と小文字の区別なし）
- DNS 信頼性ルールの適用前の質問のクラスとタイプ（[RFC2181]、セクション 5.4.1 を参照）

（注） 応答の送信元 IP アドレスがクエリの宛先 IP アドレスと一致する必要があり、応答の宛先 IP アドレスがクエリの送信元 IP アドレスと一致する必要があります。不一致はフォーマットエラーと見なされる必要があり、応答は無効です。

リゾルバ実装の条件は、次のとおりです。

- 発信クエリには、できるだけ大規模かつ実用的な使用可能ポートの範囲（53、または 1025 以上）から予測不可能な送信元ポートを使用します。
- 複数の未処理クエリがある場合は、複数の異なる送信元ポートを同時に使用します。
- 発信クエリには、使用可能な全範囲（0 ～ 65535）から予測不可能なクエリ ID を使用します。デフォルトでは、CDNS は最大 48000 万個のポート番号を使用します。

キャッシング DNS サーバー属性である *randomize-query-case* が有効になっている場合は、再帰クエリを送信するときのクエリ名は疑似ランダムな camel 形式であり、応答でこの大文字と小文字が変わっていないかどうかがチェックされます。*randomize-query-case* が有効になっている場合は、大文字と小文字が変わった応答は廃棄されます。デフォルトでは *randomize-query-case* は無効になっているため、この機能は無効です。

ローカルの基本または詳細 Web UI

キャッシング DNS サーバーの統計は、[DNS キャッシュ サーバーの管理（Manage DNS Caching Server）] ページの [統計（Statistics）] タブに表示されます。統計には、*answers-unwanted* の値が表示されます。統計テーブルの上部にある [サーバー統計の更新（Refresh Server Statistics）] アイコンをクリックすると、DNS キャッシュサーバーの統計を更新できます。

応答しないネームサーバーの処理

クエリ要求を解決しようとすると、キャッシュ DNS サーバーが無応答のネームサーバーに遭遇することがあります。ネームサーバーがクエリに応答しないか、応答が遅れる可能性があります。これは、ローカル DNS サーバーとリモート ネームサーバーのパフォーマンスに影響します。

無応答のネームサーバーを Cisco Prime Network Registrar で禁止することによって、この問題を解決できます。禁止する無応答のネームサーバーのグローバル ACL を設定するには、*acl-do-not-query* 属性を使用します。

Cisco Prime Network Registrar は、DNS クエリ要求の送信先リモートネームサーバーのリストを受信すると、*acl-do-not-query* リストにあるネームサーバーを確認してこのリストから削除しま

す。逆に、クライアントまたはその他のネームサーバーからのすべての着信 DNS 要求も *acl-blacklist* に照らしてフィルタ処理されます。

acl-query 属性を使用して、サーバーへのクエリを許可するクライアントを指定します。デフォルトでは、どのクライアントもサーバーへのクエリを許可されます。このリストに含まれていないクライアントは、ステータスが拒否（REFUSED）になっている応答を受信します。*acl-blacklist* リスト上のクライアントは、どのような応答も受信しません。

ローカルの詳細 Web UI

[ローカル CDNS サーバーの編集（Edit Local CDNS Server）] タブで [クエリアクセス制御（Query Access Control）] を展開すると、さまざまな属性とその値が表示されます。クエリ禁止（*acl-do-not-query*）属性には、たとえば 10.77.240.73 などの値を入力します。次に [保存（Save）] をクリックします。

ネットワークバッファの調整

ビジー状態のサーバーのためにネットワークバッファを調整する必要がある場合があります。Cisco Prime Network Registrar キャッシュ DNS サーバーは、システム上の他のプロセスに影響を与えることなく、サーバーの受信バッファと送信バッファを実行するために、次のエキスパートモードのパラメータを使用できるようにします。

- **so-rcvbuf**：SO_RCVBUF ソケットオプションを設定して着信クエリ用のバッファスペースを増やし、ビジー状態のサーバーでの短いスパイクによってパケットがドロップされないようにします。オペレーティングシステムは、最大値に上限を設定します。デフォルトは 0 です（システム値を使用）。
- **so-sndbuf**：0 でない場合、SO_SNDBUF ソケットオプションを使用して、発信クエリに使用される UDP ポートのバッファスペースを調整します。非常にビジーな状態のサーバーでは、応答トラフィックのスパイクを処理します。デフォルトは 0 です（システム値を使用）。

（注） これらは展開固有のものであるため、システム管理者は正しいチューニングパラメータを設定する責任があります。

ローカルのエキスパート Web UI

[ローカル CDNS サーバーの編集（Edit Local CDNS Server）] タブで、[ネットワーク設定（Network Settings）] セクションを展開して、**so-rcvbuf** 属性と **so-sndbuf** 属性を表示します。

DNS キャッシュ サーバー コマンドの実行

[コマンド（Commands）] ボタンを使用して、DNS キャッシングサーバーコマンドにアクセスします。[コマンド（Commands）] ボタンをクリックすると、ローカル Web UI に [CDNS コマ

ンド（CDNS Commands）] ダイアログボックスが開きます。コマンドごとに [実行（Run）] アイコンがあります（それをクリックしてから、ダイアログボックスを閉じます）。

- **Flush the CDNS cache**：このコマンドを使用して、インメモリ キャッシュからすべての RR または特定ゾーンの RR をフラッシュできます。DNS キャッシュのフラッシュ （41 ページ）を参照してください。
- **Flush Resource Record**：このコマンドで、インメモリ キャッシュから削除する RR 名と任意でタイプを指定できます。

（注） インメモリキャッシュからすべてのエントリを削除するには、キャッシング DNS サーバーをリロードする必要があります。

（注） サーバーエラーが見つかった場合は、設定エラーがないかサーバーのログ ファイルを調査し、エラーを修正して、このページに戻り、ページを更新します。

キャッシュ DNS サーバーのネットワーク インターフェイスの設定

ローカル Web UI の [サーバーの管理（Manage Servers）] ページから、キャッシング DNS サーバーのネットワーク インターフェイスを設定できます。インターフェイスが明示的に設定されていない場合、サーバーは使用可能なすべてのインターフェイスを使用します。

ローカルの詳細 Web UI

ステップ 1 [操作（**Operate**）] メニューで、[サーバー（Servers）] サブメニューから [サーバーの管理（**Manage Servers**）] を選択し、[サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの **CDNS** をクリックして、[ローカルCDNSサーバーの編集（Edit Local CDNS Server）] ページを開きます。

ステップ 3 [ネットワークインターフェイス（**Network Interfaces**）] タブをクリックすると、サーバーに対して設定できるネットワーク インターフェイスが表示されます。デフォルトでは、サーバーはすべてを使用します。

ステップ 4 インターフェイスを設定するには、インターフェイスの [設定（Configure）] 列の [**設定（Configure**）] アイコンをクリックします。これにより、[設定されたインターフェイス （Configured Interfaces）] テーブルにインターフェイスが追加されますので、インターフェイスを編集または削除できます。

ステップ 5 設定されたインターフェイスの名前をクリックして、設定されたインターフェイスを編集します。ここでは、インターフェイスのアドレス、方向、およびポートを変更できます。

ステップ 6 編集が完了したら、[インターフェイスの変更（**Modify Interface**）] をクリックしてから、[サーバーインターフェイスに移動（**Go to Server Interfaces**）] をクリックして、[ネットワーク インターフェイス（Network Interface）] ページに戻ります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。