権威 DNS サーバーの管理

この章では、権威 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。この章のタスクを始める前に、プライマリ ゾーンとセカンダリ ゾーンの基本プロパティの設定方法を説明している「ゾーンの管理」を参照してください。

DNS サーバー プロパティの設定

すでに設定してあるゾーンのプロパティに加えて、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 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 （4 ページ）を参照
- **アクティビティ サマリーの設定**：「アクティビティ サマリー設定の指定 （6 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 （34 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設定 （35 ページ）」を参照
- **証明書の設定**：「証明書の設定の指定 （40 ページ）」を参照
- **TLS の設定**：「TLS 設定の指定 （41 ページ）」を参照

- **ラウンドロビンサーバーの処理**：「ラウンドロビンの有効化 （43 ページ）」を参照
- **加重ラウンドロビンの有効化**：「 重み付けラウンドロビンの有効化 （44 ページ）」を参照
- **増分ゾーン転送の有効化**：「増分ゾーン転送の有効化（IXFR） （45 ページ）」を参照
- **ゾーンクエリの制限**：「ゾーン クエリの制限 （46 ページ）」を参照
- **NOTIFY パケットの有効化**：「NOTIFY の有効化 （46 ページ）」を参照

（注） GSS-TSIG サポートを有効にするには、*tsig-processing* を none に設定し、ddns とクエリの両方をサポートするように *gss-tsig-processing* を「ddns, query」に設定する必要があります。

- **再帰クエリのブロック**：権威サーバーからの再帰クエリのブロック （47 ページ）を参照

一般的な DNS サーバー プロパティの設定

サーバークラスタまたはホストマシンの名前や Cisco Prime Network Registrar DNS サーバーソフトウェアのバージョン番号などの DNS サーバーの一般的なプロパティを表示できます。現在の名前を削除して新しい名前を入力することによって、DNS サーバーの内部名を変更できます。この名前は表記用であり、サーバーの正式な名前は反映されません。Cisco Prime Network Registrar は、正式名のルックアップや DNS 更新にサーバーの IP アドレスを使用します（『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「DNS 更新の管理」の章を参照）。

以下のサブセクションでは、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 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 サーバープロパティにアクセスするには、[展開（**Deploy**）] メニューの [**DNS**] サブメニューで [DNSサーバー（**DNS Server** ）] を選択して [DNS 権威サーバーの管理（Manage DNS Authoritative Server）] ページを開きます。このページには、すべての DNS サーバーの属性が表示されます。

ステップ 2 要件に従って属性を変更します。

ステップ 3 [保存（**Save**）] をクリックして、DNS サーバー属性の変更を保存します。

CLI コマンド

[**dns show**] を使用して、DNS サーバーのプロパティを表示します。

ログ設定の指定

server-log-settings 属性により、DNS ログファイルに記録するイベントが決まります。デフォルトのフラグは、activity-summary、config、update、xfr-in、xfr-out、scp、scavenge、server-operations、および ha です。

イベントに関する追加の詳細をログに記録すると、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有効のままにしておくと、ログファイルがいっぱいにな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**：この設定により、*activity-summary-interval* で指定された間隔で DNS 統計メッセージのロギングが有効になります。ログに記録される統計のタイプは、*activity-counter-log-settings* と *activity-summary-type* で制御できます。
- **config**：この設定により、DNS サーバーの設定および初期化解除メッセージのロギングが有効になります。
- **config-detail**：この設定により、詳細な設定メッセージのロギング（つまり、詳細なゾーン設定のロギング）が有効になります。
- **db**：この設定により、データベース処理メッセージのロギングが有効になります。このフラグを有効にすると、サーバーの組み込みデータベースでのさまざまなイベントについてのインサイトが得られます。
- **dnssec**：この設定により、DNSSEC 処理に関するログメッセージが有効になります。
- **ha**：この設定により、HA DNS メッセージのロギングが有効になります。
- **host-health-check**：この設定により、DNS ホストの正常性チェックに関連付けられているロギングが有効になります。
- **notify**：この設定により、NOTIFY 処理に関連付けられているメッセージのロギングが有効になります。
- **query**：この設定により、QUERY 処理に関連付けられているメッセージのロギングが有効になりました。
- **scavenge**：この設定により、DNS スカベンジングメッセージのロギングが有効になります。
- **scp**：この設定により、SCP メッセージ処理に関連付けられているロギングが有効になりました。
- **server-operations**：この設定により、ソケットやインターフェイスなどに関する一般的なサーバーイベントのロギングが有効になります。
- **tsig**：この設定により、トランザクションシグニチャ（TSIG）に関するイベントのロギングが有効になります。
- **update**：この設定により、DNS 更新メッセージ処理のロギングが有効になります。
- **xfr-in**：この設定により、インバウンドの完全ゾーン転送と増分ゾーン転送のロギングが有効になります。
- **xfr-out**：この設定により、アウトバウンドの完全および増分ゾーン転送のロギングが有効になります。

パケットロギングの有効化

Cisco Prime Network Registrar では、権威 DNS サーバーのパケットロギングをサポートすることで、権威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、権威 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。

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

表 *1*：権威 *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*）	DNS 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 DNS 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、DNS パケットのロギングを無効にします。 • **summary**：この設定は、DNS パケットの 1 行の概要でのロギングを有効にします。 • **detail**：この設定は、DNSパケットの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。 • **dns**：パケットロギングメッセージは標準 DNS ログファイル（name_dns_1_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 DNS パケットログファイル（dns_packet_log*）に記録されます。

属性	説明
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DNSメッセージ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。 • **all-in**：この設定は、すべての着信パケットのロギングを有効にします。 **注**：これは、すべての -in 設定を有効にすることと同じです。 • **all-out**：この設定は、すべての発信パケットのロギングを有効にします。 **注**：これは、すべての -out 設定を有効にすることと同じです。 • **ha-in**、**ha-out**：これらの設定は、それぞれ、ha-heartbeat-in、ha-heartbeat-out および ha-frameack-in、ha-frameack-out 設定によって制御される HA ハートビートおよびフレーム ACK メッセージを除く HA DNS メッセージのロギングを有効にします。 • **ha-heartbeat-in**、**ha-heartbeat-out**：これらの設定は、HA DNS ハートビートメッセージのロギングを有効にします。 • **ha-frameack-in**、**ha-frameack-out**：これらの設定は、HA DNS フレーム ACK メッセージのロギングを有効にします。 • **notify-in**、**notify-out**：これらの設定は、DNS NOTIFY メッセージのロギングを有効にします。 • **query-in**、**query-out**：これらの設定は、DNS QUERY メッセージのロギングを有効にします。 • **update-in**、**update-out**：これらの設定は、DNS UPDATE メッセージのロギングを有効にします。 • **xfr-in**、**xfr-out**：これらの設定は、DNS IXFR および AXFR メッセージのロギングを有効にします。

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、**dns 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、**dns 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、**dns 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、権威 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、権威 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 サマリー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。DNS アクティビティサマリのログメッセージ間の秒数を設定するには、ログ設定（*server-log-settings*）属性の *activity-summary* 属性を有効にします。*activity-summary-interval* 属性のデフォルト値は 60 秒です。

権威 DNS サーバーは、統計タイプ（*activity-summary-type*）属性を確認するオプションに基づいて、サンプルまたは合計統計、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（*activity-counter-log-settings*）属性で確認されるオプションは、DNS サーバーがロギングに使用するアクティビティカウンタを制御します。

（注） *activity-summary-type* と *activity-counter-log-settings* は、DNS サーバーオブジェクトまたはセッションが保存されるとすぐにリロードなしで有効になります。

次の設定を使用できます。

- **cache**：クエリキャッシュ関連のカウンタ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 （8 ページ）を参照してください。

- **db**：データベース関連のカウンタをログに記録します。

db 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、DB 統計（9 ページ）を参照してください。

- **errors** ：エラー関連のカウンタをログに記録します。

  errors 設定のログに表示される活動要約統計のリストについては、エラー統計 （11 ページ）を参照してください。

- **ha**：HA 関連のカウンタをログに記録します。

  ha 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、HA 統計（13 ページ）を参照してください。

- **host-health-check**：DNS ホストの正常性チェックカウンタをログに記録します。

  host-health-check 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、ホストヘルスチェックの統計 （17 ページ）を参照してください。

- **ipv6**：IPv6 関連のカウンタをログに記録します。

  ipv6 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、IPv6 の統計情報 （19 ページ）を参照してください。

- **maxcounters**：maxcounter 関連のカウンタをログに記録します。

  maxcounters 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、マックスカウンタの統計 （20 ページ）を参照してください。

- **performance**：パフォーマンス関連のカウンタをログに記録します。

  performance 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、パフォーマンス統計情報 （21 ページ）を参照してください。

- **query**：クエリ関連のカウンタ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 （23 ページ）を参照してください。

- **security**：セキュリティ関連のカウンタ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 （27 ページ）を参照してください。

- **system**：システム関連のカウンタ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 （30 ページ）を参照してください。

- **top-names**：クエリ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 （31 ページ）を参照してください。

- **update**：DNS 更新関連のカウンタをログに記録します。

update 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、更新の統計 （31 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-counter-log-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-counter-log-settings は、クエリキャッシュ関連のカウンタをログに記録します。

キャッシュ アクティビティ サマリーの統計は、**Query-Cache** 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：

```
10/22/2021 16:47:05 name/dns/1 Activity Stats 0 21333 [Query-Cache] Sample since Fri Oct
 22 16:46:05 2021: size=number, #-records=number, #-rrs=number, nxdomain=number,
hits=number, misses=number, full=number, collisions=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
size	cache-size	インメモリクエリのキャッシュサイズをバイト単位で報告します。
#-records	cache-records	クエリキャッシュに保存されている RR 名セットの総数を報告します。
#-rrs	cache-rrs	クエリキャッシュに保存されている RR の総数を報告します。
nxdomain	cache-nxdomain	クエリキャッシュ内の NXDOMAIN エントリの総数を報告します。
hits	cache-hits	着信クライアントクエリがクエリキャッシュで見つかった回数を報告します。
misses	cache-misses	着信クライアントクエリがクエリキャッシュで見つからなかった回数を報告します。
すべての	cache-full	クエリキャッシュが設定された制限（*mem-cache-size*）にあることが検出された回数を報告します。

アクティビティサマリー名	統計[1]	説明
collisions	該当なし	異なるFQDNが同じメモリ キャッシュ インデックスにマップされた回数を報告します。コリジョン数が多い場合は、設定されたキャッシュサイズが小さすぎる可能性があることを示しています。

[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。権威 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「DNS統計」セクションを参照してください。

DB 統計

db activity-counter-log-settings は、データベースカウンタをログに記録します。

サンプルログメッセージ：

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21344 [Cset-DB] Sample since Fri Oct 22
 16:43:05 2021: reads=number, writes=number, deletes=number, csets-trimmed=number,
conflicts=number, insufficient-history=number, txns=number, txn-commits=number,
txn-aborts=number, txn-locked=number, txn-unlocked=number, check-pts=number,
log-purges=number, #-logs-purged=number

10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21345 [RR-DB] Sample since Fri Oct 22
16:43:05 2021: reads=number, writes=number, deletes=number, check-pts=number,
log-purges=number, #-logs-purged=number, txns=number, txn-commits=number, txn-aborts=number

10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21352 [Cset-Queue] Sample since Fri Oct
 22 16:43:05 2021: cset-count=number, cset-queue-max-size=number, commits=number,
commits-failed=number
```

表 *3 : DB* 統計

アクティビティサマリー名	ロギングサブカテゴリ	統計[2]	説明
txn	RR-DB	rrdb-txn	RR DBデータベース トランザクションの総数を報告します。
txn-commits	RR-DB	rrdb-txn-commits	コミットされたRR DBデータベース トランザクションの総数を報告します。
txn-aborts	RR-DB	rrdb-txn-aborts	中止された RR DB データベース トランザクションの総数を報告します。

アクティビティサマリー名	ロギングサブカテゴリ	統計[2]	説明
reads	RR-DB	rrdb-reads	RR DB 読み取り操作の総数を報告します。
writes	RR-DB	rrdb-writes	RR DB 書き込み操作の総数を報告します。
deletes	RR-DB	rrdb-deletes	RR DB 削除操作の総数を報告します。
check-pts	RR-DB	rrdb-check-pts	RR DB チェックポイント操作の総数を報告します。
log-purges	RR-DB	rrdb-log-purges	RR DB ログの消去操作の総数を報告します。
#-logs-purged	RR-DB	rrdb-log-purges-count	消去された RR DB ログの総数を報告します。
cset-count	Cset-Queue	csetq-count	cset DB に書き込まれるためにキューに入れられた変更セットの総数を報告します。
cset-queue-max-size	Cset-Queue	該当なし	この間隔の間にキューイングされた最大 cset エントリ数。
commits	Cset-Queue	該当なし	最後の間隔で発生した DB コミットの数。
commits-failed	Cset-Queue	該当なし	最後の間隔で失敗した DB コミットの数。
txns	Cset-DB	csetdb-txn	CSET DB データベース トランザクションの総数を報告します。
txn-commits	Cset-DB	csetdb-txn-commits	コミットされた CSET DB データベース トランザクションの総数を報告します。
txn-aborts	Cset-DB	csetdb-txn-aborts	中止された CSET DB データベース トランザクションの総数を報告します。
reads	Cset-DB	csetdb-reads	CSET DB 読み取り操作の総数を報告します。

アクティビティサマリー名	ロギングサブカテゴリ	統計[2]	説明
writes	Cset-DB	csetdb-writes	CSET DB 書き込み操作の総数を報告します。
deletes	Cset-DB	csetdb-deletes	CSET DB 削除操作の総数を報告します。
csets-trimmed	Cset-DB	csetdb-csets-trimmed	履歴トリムプロセスまたはインライントリムによって CSET DB からトリムされた変更セットの総数を報告します。
check-pts	Cset-DB	csetdb-check-pts	CSET DB チェックポイント操作の総数を報告します。
log-purges	Cset-DB	csetdb-log-purges	CSET DB ログの消去操作の総数を報告します。
#-logs-purged	Cset-DB	csetdb-log-purges-count	消去された CSET DB ログの総数を報告します。

[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。権威 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「DNS 統計」セクションを参照してください。

エラー統計

errors activity-counter-log-settings は、エラー関連のカウンタをログに記録します。

エラー アクティビティ サマリーの統計は、**Errors** 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：

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21492 [Errors] Sample since Fri Oct 22
16:43:05 2021: update-errors=number, update-prereq-fail=number, ixfr-in-errors=number,
ixfr-out-errors=number, axfr-in-errors=number, axfr-out-errors=number,
xfer-in-auth-errors=number, xfer-failed-attempts=number, sent-total-errors=number,
sent-refusal-errors=number, sent-format-errors=number, exceeded-max-dns-packets=number
```

表 *4:* エラー統計

アクティビティサマリー名	統計[3]	説明
update-errors	update-errors	エラーが発生した更新の総数を報告します。これにより、更新の前提条件チェックへの否定応答とTSIG応答が除外されます。更新パケットと CNR UI によって生成された更新の両方がこのカウントに含まれている場合があります。
update-prereq-fail	update-prereq-fail	前提条件の失敗の原因となった更新の総数を報告します。
ixfr-in-errors	ixfr-in-errors	パケット形式エラーを除く、インバウンド IXFR エラーの総数を報告します。
ixfr-out-errors	ixfr-out-errors	パケット形式エラーを除く、送信された IXFRエラー応答の総数を報告します。
axfr-in-errors	axfr-in-errors	パケット形式エラーを除く、インバウンド AXFR エラーの総数を報告します。
axfr-out-errors	axfr-out-errors	パケット形式エラーを除く、送信された AXFR エラー応答の総数を報告します。
sent-total-errors	sent-total-errors	サーバーがエラー（RCODE 値が 0、3、6、7、および 8 以外）で応答した要求の総数を報告します。RFC 1611 を参照してください。
sent-format-errors	sent-format-errors	受信された解析不能な要求の数を報告します。RFC 1611 を参照してください。
sent-refusal-errors	sent-refusal-errors	REFUSED となった要求の数を報告します。RFC 1611 を参照してください。
xfer-in-auth-errors	xfer-in-auth-errors	認証エラーが原因で拒否されたセカンダリ IXFR/AXFR 要求の数を報告します。
xfer-failed-attempts	xfer-failed-attempts	許可拒否を除く、セカンダリ IXFR/AXFR 障害の数を報告します。
exceeded-max-dns-packets	exceeded-max-dns- packets	インバウンドパケットが、*max-dns-packets* で定義された最大 DNS パケット数を超えた回数を報告します。

[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。権威 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「DNS 統計」セクションを参照してください。

HA 統計

ha activity-counter-log-settings は、HA 関連のカウンタをログに記録します。

サンプルログメッセージ：

```
name_dns_1_log:11/19/2021 11:43:23 name/dns/1 Activity Stats 0 20005 [HA-State] Sample
since Fri Nov 19 11:41:35 2021: current=state, last-state-change=time, normal=number,
comm-interrupted=number, negotiate=number, start-up=number, partner-down=number

name_dns_1_log:11/19/2021 12:09:23 name/dns/1 Activity Stats 0 21341 [HA-Requests-Sent]
 Sample since Fri Nov 19 12:08:23 2021: requests-sent=number, last-req-sent=Heartbeat @
 Fri Nov 19 12:09:21 2021 (xid: 207), update=number, heart-beat=number, zone-sync=number,
 rr-sync=number, rr-recon=number, connect=number, negotiate=number, shutdown=number,
truncated=number

name_dns_1_log:11/18/2021 13:07:26 name/dns/1 Activity Stats 0 21342 [HA-Requests-Rcvd]
 Sample since Thu Nov 18 13:04:12 2021: requests-recv=number, last-req-recv=Heartbeat @
 Thu Nov 18 13:07:07 2021 (xid: 207), update=number, heart-beat=number, zone-sync=number,
 rr-sync=number, rr-recon=number, connect=number, negotiate=number, shutdown=number,
truncated=number

11/29/2021  9:02:44 name/dns/1 Activity Stats 0 21343 [HA-Errors] Sample since Mon Nov
29 09:01:44 2021: update-reject=number, resp-mismatch=number, resp-inconsistent=number,
 resp-servfail=number, resp-unknown=number

11/29/2021 14:49:32 name/dns/1 Activity Stats 0 20006 [HA-Zone-Sync] Sample since Mon
Nov 29 14:47:32 2021: sync=number, sync-completed=number, sync-failed=number,
zone-mismatch=number, full-resync=number, conflict=number, merge=number, discard=number
```

表 *5 : HA* 統計

アクティビティサマリー名	ロギングサブカテゴリ	統計[4]	説明
comm-interrupted	HA-State	ha-state-comm-interrupted	サーバーが通信中断状態（HA_STATE_COMMINTR）になるオカレンスの数。
partner-down	HA-State	ha-state-partner-down	サーバーがパートナーダウン状態（HA_STATE_PARTNERDOWN）になるオカレンスの数。
negotiate	HA-State	ha-state-negotiating	サーバーがネゴシエーション状態（HA_STATE_NEGOTIATING）になるオカレンスの数。

アクティビティサマリー名	ロギングサブカテゴリ	統計[4]	説明
current	HA-State	ha-state-current	現在の HA サーバーの状態。
last-state-change	HA-State	ha-state-last-change-time	HA の状態が最後に変化した時刻。
start-up	HA-State	ha-state-startup	サーバーがスタートアップ状態（HA_STARTUP）になるオカレンスの数。
normal	HA-State	ha-state-normal	サーバーが通常状態（HA_NORMAL）になるオカレンスの数。
connect	HA-Requests-Sent	ha-msg-connect-sent	送信された接続確立要求メッセージ（HA_DNS_ESTABLISH_CONNECTION）の数。
rr-recon	HA-Requests-Sent	ha-msg-reconcile-sent	送信されたゾーン調整要求メッセージ（HA_DNS_RECONCILIATION）の数。
heart-beat	HA-Requests-Sent	ha-msg-heartbeat-sent	送信されたハートビート要求メッセージ（HA_DNS_HEARTBEAT）の数。
zone-sync	HA-Requests-Sent	ha-msg-zonesync-sent	送信されたゾーン同期要求メッセージ（HA_DNS_ZONE_SYNC）の数。
rr-sync	HA-Requests-Sent	ha-msg-rrsync-sent	送信された rr-sync 要求メッセージ（HA_DNS_RR_SYNC）の数。
update	HA-Requests-Sent	ha-msg-rrupdate-sent	送信された rr-update 要求メッセージ（HA_DNS_RR_UPDATE）の数。
該当なし	該当なし	ha-msg-resp-sent	送信された応答メッセージの数。応答メッセージは、すべてのタイプの要求メッセージへの受領確認に使用されます。
shutdown	HA-Requests-Sent	ha-msg-shutdown-sent	送信されたシャットダウン要求メッセージの数。
requests-sent	HA-Requests-Sent	ha-msg-req-sent	HA パートナーに送信された HA 要求メッセージの数。

アクティビティサマリー名	ロギングサブカテゴリ	統計[4]	説明
last-req-sent	HA-Requests-Sent	ha-msg-req-sent-time	HA サーバーが HA パートナーに要求メッセージを最後に送信した日時を指定します。
negotiate	HA-Requests-Sent	該当なし	送信されたネゴシエート HA メッセージの数。
truncated	HA-Requests-Sent	該当なし	切り捨てられて送信された HA メッセージの数。
connect	HA-Requests-Rcvd	ha-msg-connect-recv	受信された接続確立要求メッセージ（HA_DNS_ESTABLISH_CONNECTION）の数。
rr-recon	HA-Requests-Rcvd	ha-msg-reconcile-recv	受信されたゾーン調整要求メッセージ（HA_DNS_RECONCILIATION）の数。
heart-beat	HA-Requests-Rcvd	ha-msg-heartbeat-recv	受信されたハートビート要求メッセージ（HA_DNS_HEARTBEAT）の数。
zone-sync	HA-Requests-Rcvd	ha-msg-zonesync-recv	受信されたゾーン同期要求メッセージ（HA_DNS_ZONE_SYNC）の数。
rr-sync	HA-Requests-Rcvd	ha-msg-rrsync-recv	受信された rr-sync メッセージ要求（HA_DNS_RR_SYNC）の数。
update	HA-Requests-Rcvd	ha-msg-rrupdate-recv	受信された rr-update 要求メッセージ（HA_DNS_RR_UPDATE）の数。
該当なし	該当なし	ha-msg-resp-recv	受信された応答メッセージの数。応答メッセージは、すべてのタイプの要求メッセージへの受領確認に使用されます。
shutdown	HA-Requests-Rcvd	ha-msg-shutdown-recv	受信されたシャットダウン要求メッセージの数。
requests-recv	HA-Requests-Rcvd	ha-msg-req-recv	HA パートナーから受信した HA 要求メッセージの数。
last-req-recv	HA-Requests-Rcvd	ha-msg-req-recv-time	HA サーバーが HA パートナーから要求メッセージを最後に受信した日時を指定します。

アクティビティサマリー名	ロギングサブカテゴリ	統計[4]	説明
negotiate	HA-Requests-Rcvd	該当なし	受信したネゴシエート HA メッセージの数。
truncated	HA-Requests-Rcvd	該当なし	切り捨てられて受信した HA メッセージの数。
update-reject	HA-Errors	ha-update-reject	サーバーによって拒否された DNS 更新の数。
resp-mismatch	HA-Errors	ha-zone-mismatch	不一致エラー（HA_DNS_RESP_ERR_MISMATCH）を報告しているゾーンの数。
resp-servfail	HA-Errors	ha-resp-servfail	サーバー障害エラー（HA_DNS_RESP_ERR_SERVFAIL）を報告する応答の数。
resp-inconsistent	HA-Errors	ha-resp-inconsistent	一貫性のないサーバー状態を報告する応答（HA_DNS_RESP_ERR_INCONSISTENT_STATE）の数。
resp-unknown	HA-Errors	ha-resp-unknown	不明なメッセージタイプ（HA_DNS_RESP_ERR_UNKNOWN_MSG_TYPE）の応答の数。
full-resync	HA-Zone-Sync	ha-full-zone-resync	名前セットの調整のためにフルゾーン再同期を必要とするゾーンの数。
conflict	HA-Zone-Sync	ha-sync-conflict	名前セットの調整中に名前が競合するゾーンの数。
discard	HA-Zone-Sync	ha-sync-discard-name	ゾーンを同期するために 1 つの名前セットを廃棄する必要がある名前の競合の数。
merge	HA-Zone-Sync	ha-sync-merge-name	ゾーンを同期するために名前セットをマージできる名前の競合の数。
sync	HA-Zone-Sync	該当なし	同期が要求されたゾーンの数。
sync-completed	HA-Zone-Sync	該当なし	同期が完了したゾーンの数。
sync-failed	HA-Zone-Sync	該当なし	同期が失敗したゾーンの数。

アクティビティサマリー名	ロギングサブカテゴリ	統計[4]	説明
zone-mismatch	HA-Zone-Sync	該当なし	HA メインと HA バックアップで一致しないゾーンの数。

[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。権威 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「DNS 統計」セクションを参照してください。

ホストヘルスチェックの統計

host-health-check activity-counter-log-settings は、DNS ホスト ヘルス チェック カウンタをログに記録します。

ホスト ヘルス チェック アクティビティ サマリーの統計は、**HHC** 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：

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21509 [HHC] Sample since Fri Oct 22
16:43:05 2021: hhc-domains=number, hhc-domains-failed=number, hhc-domains-passed=number,
 hhc-rrs=number, hhc-rrs-passed=number, hhc-rrs-failed=number, hhc-ping-domains=number,
 hhc-ping-domains-failed=number, hhc-ping-domains-passed=number, hhc-ping-rrs=number,
hhc-ping-rrs-passed=number, hhc-ping-rrs-failed=number, hhc-gtp-echo-domains=number,
hhc-gtp-echo-domains-failed=number, hhc-gtp-echo-domains-passed=number,
hhc-gtp-echo-rrs=number, hhc-gtp-echo-rrs-passed=number, hhc-gtp-echo-rrs-failed=number
```

表 *6*：ホストヘルスチェックの統計

アクティビティサマリー名	統計[5]	説明
hhc-domains	hhc-domains	ホスト ヘルス チェックでチェックされたドメインの合計数を報告します。
hhc-domains-failed	hhc-domains-failed	ホスト ヘルス チェックに失敗したドメイン チェックの合計数を報告します。RR セット内のすべての RR がダウンしている場合、この統計値は増加します。
hhc-domains-passed	hhc-domains-passed	ホスト ヘルス チェックに合格したドメイン チェックの合計数を報告します。RR セット内のいずれかの A/AAAA RR がアップしている場合、この統計値は増加します。

アクティビティサマリー名	統計[5]	説明
hhc-rr	hhc-rr	ホストヘルスチェックでチェックされたRRの総数を報告します。
hhc-rrs-passed	hhc-rrs-passed	ホストヘルスチェックに合格したRRの総数を報告します。
hhc-rrs-failed	hhc-rrs-failed	ホストヘルスチェックで不合格となったRRの総数を報告します。
hhc-ping-domains	hhc-ping-domains	pingによるホストの正常性チェックで確認されたドメインの総数を報告します。
hhc-ping-domains-failed	hhc-ping-domains-failed	pingによるホストの正常性チェックで不合格となったドメインの総数を報告します。RRセット内のすべてのRRがダウンしている場合、この統計値は増加します。
hhc-ping-domains-passed	hhc-ping-domains-passed	pingによるホストの正常性チェックで合格したドメインの総数を報告します。RRセット内のいずれかのRRがアップしている場合、この統計値は増加します。
hhc-ping-rrs	hhc-ping-rrs	pingによるホストの正常性チェックで確認されたRRの総数を報告します。
hhc-ping-rrs-failed	hhc-ping-rrs-failed	pingによるホストの正常性チェックで不合格となったRRの総数を報告します。
hhc-ping-rrs-passed	hhc-ping-rrs-passed	pingによるホストの正常性チェックで合格したRRの総数を報告します。
hhc-gtp-echo-domains	hhc-gtp-echo-domains	gtp-echoによるホストの正常性チェックで確認されたドメインの総数を報告します。
hhc-gtp-echo-domains-failed	hhc-gtp-echo-domains-failed	gtp-echoによるホストの正常性チェックで不合格となったドメインの総数を報告します。RRセット内のすべてのRRがダウンしている場合、この統計値は増加します。
hhc-gtp-echo-domains-passed	hhc-gtp-echo-domains-passed	gtp-echoによるホストの正常性チェックで合格したドメインの総数を報告します。RRセット内のいずれかのRRがアップしている場合、この統計値は増加します。
hhc-gtp-echo-rrs	hhc-gtp-echo-rrs	gtp-echoによるホストの正常性チェックで確認されたRRの総数を報告します。

アクティビティサマリー名	統計[5]	説明
hhc-gtp-echo-rrs-failed	hhc-gtp-echo-rrs-failed	gtp-echo によるホストの正常性チェックで不合格となった RR の総数を報告します。
hhc-gtp-echo-rrs-passed	hhc-gtp-echo-rrs-passed	gtp-echo によるホストの正常性チェックで合格した RR の総数を報告します。

[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。権威 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「DNS 統計」セクションを参照してください。

IPv6 の統計情報

ipv6 activity-counter-log-settings は、IPv6 関連のカウンタをログに記録します。

IPv6 アクティビティサマリーの統計は、**Perform** 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：

```
11/26/2021 15:25:36 name/dns/1 Activity Stats 0 03523 [Perform] Sample since Fri Nov 26
 15:24:36 2021: pkts-in=number, pkts-out=number, pkts-in-udp=number, pkts-out-udp=number,
 pkts-in-tcp=number, pkts-out-tcp=number, ipv4-pkts-in=number, ipv4-pkts-out=number,
ipv6-pkts-in=number, ipv6-pkts-out=number,  queries=number, updates=number,
notifies-in=number, notifies-out=number, notify-errors=number, ixfrs-in=number,
ixfrs-out=number, ixfrs-full-resp=number, axfrs-in=number, axfrs-out=number,
xfrs-in-at-limit=number, xfrs-out-at-limit=number, responses-with-NOTIMP=number,
total-zones=number, total-rrs=number
```

表 *7: IPv6* の統計情報

アクティビティサマリー名	統計[6]	説明
ipv6-pkts-in	ipv6-packets-in	受信された IPv6 パケットの総数。
ipv6-pkts-out	ipv6-packets-out	送信された IPv6 パケットの総数。

[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。権威 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「DNS 統計」セクションを参照してください。

マックスカウンタの統計

maxcounters activity-counter-log-settings は、マックスカウンタ関連のカウンタをログに記録します。

マックスカウンタ アクティビティ サマリーの統計は、**Max-Counters** 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：

```
10/22/2021 16:40:05 name/dns/1 Activity Stats 0 21353 [Max-Counters] Sample since Tue
Oct 19 19:32:39 2021: concurrent-xfrs-in=number, concurrent-xfrs-out=number,
ha-update-latency-max=number, ha-batch-count-limit=number, ha-rr-pending-list=number,
ha-rr-active-list=number, ha-persisted-edit-list=number, packet-queue-size=number,
dns-concurrent-packets=number, pn-conn-max-conns=number, tcp-pkts-dropped=number
```

表 *8:* マックスカウンタの統計

アクティビティサマリー名	統計[7]	説明
concurrent-xfrs-in	concurrent-xfrs-in	最後のサンプリング期間中にインバウンド転送を処理する同時スレッドの最大数を報告します。
concurrent-xfrs-out	concurrent-xfrs-out	最後のサンプリング期間中にアウトバウンド転送を処理する同時スレッドの最大数を報告します。
ha-batch-count-limit	ha-batch-count-limit	最後のサンプリング期間中に *ha-dns-max-batch-count* 制限に達した回数を報告します。
ha-rr-pending-list	ha-rr-pending-list	最後のサンプリング期間中に HA DNS バックアップサーバーからの確認応答を待機している、保留リスト内の RR の最大数を報告します。
ha-rr-active-list	ha-rr-active-list	最後のサンプリング期間中に、HA DNS バックアップサーバーへの送信を待機しているアクティブリスト内の RR の最大数を報告します。
ha-persisted-edit-list	ha-persisted-edit-list	最後のサンプリング期間中に編集リストデータベースに保持されていた名前の最大数を報告します。
ha-update-latency- max	ha-update-latency-max	最後のサンプリング期間中の最大 DNS 更新遅延を秒単位で報告します。遅延は、更新が保留リストに残っている時間として測定されます。

アクティビティサマリー名	統計[7]	説明
dns-concurrent- packets	dns-concurrent-packets	サンプリング期間中にDNSサーバーによって処理された同時パケットの最大数を報告します。
tcp-pkts-dropped	該当なし	*tcp-max-active-connections* を超えた、DNSサーバーによってドロップされたTCP接続の数を報告します。

[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。権威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「DNS統計」セクションを参照してください。

パフォーマンス統計情報

performance activity-counter-log-settings は、パフォーマンス関連のカウンタをログに記録します。

パフォーマンス アクティビティ サマリーの統計は、**Perform** 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：

```
10/22/2021 16:40:05 name/dns/1 Activity Stats 0 03523 [Perform] Sample since Tue Oct 19
 19:32:39 2021: pkts-in=number, pkts-out=number, pkts-in-udp=number,pkts-out-udp=number,
 pkts-in-tcp=number, pkts-out-tcp=number, ipv4-pkts-in=number, ipv4-pkts-out=number,
ipv6-pkts-in=number, ipv6-pkts-out=number,  tcp-pkts-dropped=number, queries=number,
updates=number,notifies-in=number, notifies-out=number, notify-errors=number,
ixfrs-in=number, ixfrs-out=number, ixfrs-full-resp=number, axfrs-in=number,
axfrs-out=number, xfrs-in-at-limit=number, xfrs-out-at-limit=number,
responses-with-NOTIMP=number, total-zones=number, total-rrs=number
```

表 *9:* パフォーマンス統計情報

アクティビティサマリー名	統計[8]	説明
ipv4-pkts-in	ipv4-packets-in	受信されたIPv4パケットの総数を報告します。
ipv4-pkts-out	ipv4-packets-out	送信されたIPv4パケットの総数を報告します。

アクティビティサマリー名	統計[8]	説明
該当なし	updated-rrs	データベースエラーの有無にかかわらず、CPNR UI からの更新を含めて、追加および削除された RR の総数を報告します。
updates	update-packets	成功した DNS 更新の数を報告します。
クエリー	queries-total	DNS サーバーが受信したクエリの総数。
ixfrs-out	ixfrs-out	成功したアウトバウンド増分転送の数を報告します。
ixfrs-in	ixfrs-in	フルゾーン転送になった増分要求を含めて、成功したインバウンド増分転送の数を報告します。
ixfrs-full-resp	ixfrs-full-resp	IXFR 要求に応答してアウトバウンドのフルゾーン転送の数を報告します。これらは、IXFR エラー、連続性に欠ける履歴、またはゾーン内での変更の過多が原因である可能性があります。
axfrs-in	axfrs-in	成功したインバウンド AXFR の数を報告します。
axfrs-out	axfrs-out	*ixfrs-full-resp* でカウントされたものを含めて、成功したアウトバウンドのフルゾーン転送の数を報告します。
xfrs-in-at-limit	xfrs-in-at-limit	同時転送の上限に達したインバウンド転送の回数を報告します。
xfrs-out-at-limit	xfrs-out-at-limit	同時転送の上限に達したアウトバウンド転送の回数を報告します。
notifies-out	notifies-out	アウトバウンド通知の数を報告します。送信された各通知パケットは個別にカウントされます。
notifies-in	notifies-in	インバウンド通知の数を報告します。受信された各通知パケットは個別にカウントされます。
notify-errors	該当なし	通知要求の処理中に検出されたエラー。
total-zones	該当なし	設定済みゾーンの総数。

アクティビティサマリー名	統計[8]	説明
total-rrs	該当なし	すべての設定済みゾーンにおける RR の総数。
responses-with-NOTIMP	responses-with-NOTIMP	実装されていない OP コードを持つ要求の数を報告します。
pkts-in	packets-in	受信されたパケットの総数を報告します。
pkts-out	packets-out	送信されたパケットの総数を報告します。
pkts-in-udp	packets-in-udp	受信された UDP パケットの総数を報告します。
pkts-out-udp	packets-out-udp	送信された UDP パケットの総数を報告します。
pkts-in-tcp	packets-in-tcp	受信された TCP パケットの総数を報告します。
pkts-out-tcp	packets-out-tcp	送信された TCP パケットの総数を報告します。
ipv6-pkts-in	ipv6-packets-in	受信された IPv6 パケットの総数を報告します。
ipv6-pkts-out	ipv6-packets-out	送信された IPv6 パケットの総数を報告します。
tcp-pkts-dropped	該当なし	*tcp-max-active-connections* を超えた、DNS サーバーによってドロップされた TCP 接続の数を報告します。

[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。権威 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「DNS 統計」セクションを参照してください。

クエリ統計

query activity-counter-log-settings は、クエリ関連のカウンタをログに記録します。

サンプルログメッセージ：

```
10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21168 [Query] Sample since Fri Oct 22
16:40:05 2021: total=number, dropped=number, acl-failures=number, udp=number, tcp=number,
 ipv4=number, ipv6=number, tls=number, tls-failures=number, dropped-recursive=number,
dropped-unwanted-class=number, dropped-unwanted-type=number

10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21333 [Query-Cache] Sample since Fri Oct
 22 16:43:05 2021: size=number, #-records=number, #-rrs=number, nxdomain=number,
hits=number, misses=number, full=number, collisions=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21331 [Query-Type] Sample since Fri Oct
 22 16:40:05 2021: A=number, AAAA=number, ANY=number, CNAME=number, MX=number,
NAPTR=number, NS=number,PTR=number, SOA=number, SRV=number, TXT=number, DNSKEY=number,
DS=number, RRSIG=number, NSEC=number, CAA=number, URI=number, SVCB=number, HTTPS=number,
 other=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21332 [Query-Responses] Sample since Fri
 Oct 22 16:40:05 2021: total=number, no-error=number, referrals=number, no-data=number,
 nxdomain=number, refused=number, notauth=number, formerr=number, servfail=number,
other=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21524 [DNSSEC] Sample since Fri Oct 22
16:40:05 2021: dnssec-zones=number, dnssec-sign-zone=number, dnssec-queries=number,
dnssec-responses=number, dnssec-requests-dropped=number

03/08/2022 18:40:54 name/dns/1 Activity Stats 0 21613 [TLS] Total since Tue Mar 1 19:52:29
 2022: tls-queries=number, tls-queries-failed=number
```

表 *10*：クエリ統計

アクティビティサマリー名	ロギングサブカテゴリ	統計[9]	説明
hits	Query-Cache	mem-cache-hits	mem-cache ルックアップのヒット数を報告します。
misses	Query-Cache	mem-cache-misses	mem-cache ルックアップミスの数を報告します。
dropped	クエリ	queries-dropped	エラーなしでドロップされたパケットの数を報告します。サーバー、TSIG、または更新のポリシーによって制限されたクエリは含まれますが、DNSの更新、要求、および通知は除外されます。
該当なし	該当なし	queries-with-edns	処理された OPT RR パケットの数を報告します。
total	クエリ	queries-total	DNSサーバーが受信したクエリの総数。
udp	クエリ	queries-over-udp	DNS サーバーが UDP を介して受信したクエリの総数。

アクティビティサマリー名	ロギングサブカテゴリ	統計[9]	説明
tcp	クエリ	queries-over-tcp	DNS サーバーが TCP を介して受信したクエリの総数。
ipv4	クエリ	queries-over-ipv4	DNS サーバーが受信した IPv4 クエリの総数。
ipv6	クエリ	queries-over-ipv6	DNS サーバーが受信した IPv6 クエリの総数。
tls	クエリ	queries-over-tls	DNS サーバーが TLS を介して受信したクエリの総数。
tls-failures	クエリ	queries-over-tls-failed	TLS ハンドシェイク中に失敗した TLS クエリの総数。
dropped-recursive	クエリ	queries-dropped-recursive	ドロップされた再帰クエリの数。
dropped-unwanted-class	クエリ	queries-dropped-unwanted-class	不要なクラスが原因でドロップされたクエリの総数。クラス IN のクエリのみが許可されます。
dropped-unwanted-type	クエリ	queries-dropped-unwanted-type	不要なタイプが原因でドロップされたクエリの総数。不要な RR タイプは、DNS サーバーの属性 *query-types-unwanted* で指定します。
acl-failures	クエリ	queries-failed-acl	クエリ ACL（*restrict-query-acl*）の失敗数を報告します。
total	Query-Responses	query-answers-total	クエリ応答の総数を報告します。
no-error	Query-Responses	query-answers-with-NOERROR	正当に応答されたクエリの数を報告します。
nxdomain	Query-Responses	query-answers-with-NXDOMAIN	そのような名前応答がないために失敗したクエリの数を報告します。
no-data	Query-Responses	query-answers-with-NODATA	データなしの応答（空の応答）で失敗したクエリの数を報告します。
notauth	Query-Responses	query-answers-with-NOTAUTH	権限のない応答で失敗したクエリの数を報告します。
referrals	Query-Responses	query-answers-with-referral	他のサーバーに参照された要求の数を報告します。

アクティビティサマリー名	ロギングサブカテゴリ	統計[9]	説明
refused	Query-Responses	query-answers-with-REFUSED	拒否されたクエリの数を報告します。
formerror	Query-Responses	query-answers-with-FORMERR	rcode が FORMERR のクエリ応答の数を報告します。
servfail	Query-Responses	query-answers-with-SERVFAIL	rcode が SERVFAIL のクエリ応答の数を報告します。
other	Query-Responses	query-answers-with-other-errors	他のエラーがあるクエリの数を報告します。
dnssec-queries	DNSSEC	queries-dnssec	DNSSEC 関連の RR（EDNS オプション DO ビット）を応答に含めるように要求するクエリの総数を報告します。
A	Query-Type	queries-type-A	受信されたクエリの数。
AAAA	Query-Type	queries-type-AAAA	受信された AAAA クエリの数。
CNAME	Query-Type	queries-type-CNAME	受信されたクエリの数。
PTR	Query-Type	queries-type-PTR	受信されたクエリの数。
NS	Query-Type	queries-type-NS	受信された NS クエリの数。
SOA	Query-Type	queries-type-SOA	受信された SOA クエリの数。
MX	Query-Type	queries-type-MX	受信された MX クエリの数。
NAPTR	Query-Type	queries-type-NAPTR	受信された NAPTR クエリの数。
other	Query-Type	queries-type-other	受信されたその他すべてのクエリ。
ANY	Query-Type	queries-type-ANY	受信された ANY クエリの数。
SRV	Query-Type	queries-type-SRV	受信された SRV クエリの数。
TXT	Query-Type	queries-type-TXT	受信された TXT クエリの数。
DNSKEY	Query-Type	queries-type-DNSKEY	受信された DNSKEY クエリの数。
DS	Query-Type	queries-type-DS	受信された DS クエリの数。
RRSIG	Query-Type	queries-type-RRSIG	受信された RRSIG クエリの数。
NSEC	Query-Type	queries-type-NSEC	受信された NSEC クエリの数。

アクティビティサマリー名	ロギングサブカテゴリ	統計[9]	説明
CAA	Query-Type	queries-type-CAA	受信された CAA クエリの数。
URI	Query-Type	queries-type-URI	受信された URI クエリの数。
SVCB	Query-Type	queries-type-SVCB	受信された SVCB（TYPE 64）クエリの数。
HTTPS	Query-Type	queries-type-HTTPS	受信された HTTPS RR（TYPE 65）クエリの数。
tls-queries	TLS	tls-queries	DNS サーバーが TLS を介して受信したクエリの総数。
tls-queries-failed	TLS	tls-queries-failed	TLS ハンドシェイク中に失敗した TLS クエリの総数。

[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。権威 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「DNS 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-counter-log-settings は、セキュリティ関連のカウンタをログに記録します。

サンプルログメッセージ：

```
10/22/2021 16:44:05 name/dns/1 Activity Stats 0 21492 [Errors] Sample since Fri Oct 22
16:43:05 2021: update-errors=number, update-prereq-fail=number, ixfr-in-errors=number,
ixfr-out-errors=number, axfr-in-errors=number, axfr-out-errors=number,
xfer-in-auth-errors=number, xfer-failed-attempts=number, sent-total-errors=number,
sent-refusal-errors=number, sent-format-errors=number, exceeded-max-dns-packets=number

10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21332 [Query-Responses] Sample since Fri
 Oct 22 16:40:05 2021: total=number, no-error=number, referrals=number, no-data=number,
 nxdomain=number, refused=number, notauth=number, formerr=number, servfail=number,
other=number

11/19/2021 16:59:41 name/dns/1 Activity Stats 0 21524 [DNSSEC] Sample since Fri Nov 19
16:58:41 2021: dnssec-zones=number, dnssec-sign-zone=number, dnssec-queries=number,
dnssec-responses=number, dnssec-requests-dropped=number

11/26/2021 16:16:45 name/dns/1 Activity Stats 0 21491 [TSIG] Sample since Fri Nov 26
16:15:45 2021: tsig-packets=number, badtime=number, badkey=number, badsig=number,
badtime-resp=number, badkey-resp=number, badsig-resp=number

12/08/2021 12:58:42 name/dns/1 Activity Stats 0 21389 [RPZ] Sample since Wed Dec 8
12:57:03 2021: rpz-queries=number, rpz-hits=number, rpz-misses=number
```

```
01/30/2023 22:25:47 dns_security Activity Stats 0 21634 [Security-Events-Categories]
Sample since Mon Jan 30 22:24:47 2023: total=number, requests=number, alarm=number,
amplification=number, dos=number, poisoning=number, snooping=number, tunneling=number
```

表 *11* : セキュリティ統計

アクティビティサマリー名	ロギングサブカテゴリ	統計[10]	説明
xfer-in-auth-errors	エラー	unauth-xfer-reqs	ゾーン転送での ACL 認証の失敗の数を報告します。
該当なし	該当なし	unauth-update-reqs	DNS 更新での ACL 認証の失敗の数を報告します。（CPNR UI からの）管理 RR 更新は除外されます。
refused	Query-Responses	restrict-query-acl	DNS クエリでの ACL 認証の失敗の数を報告します。
該当なし	該当なし	blackhole-acl-dropped-requests	*blackhole-acl* の対象のサーバーによってドロップされた DNS 要求の数を報告します。
tsig-packets	TSIG	rcvd-tsig-packets	パケットタイプに対して TSIG 処理が有効になっている場合に、処理された TSIG RR パケットの数を報告します。
badtime-resp	TSIG	detected-tsig-bad-time	着信 TSIG パケットの不正なタイムスタンプの数を報告します。
badkey-resp	TSIG	detected-tsig-bad-key	着信 TSIG パケット内の不正キー名（無効キーまたは未知のキーを持つキー名）の数を報告します。
badsig-resp	TSIG	detected-tsig-bad-sig	着信 TSIG パケットの不正な署名の数を報告します。
badtime	TSIG	rcvd-tsig-bad-time	TSIG パケットの送信後に受信された BADTIME エラーの数を報告します。
badkey	TSIG	rcvd-tsig-bad-key	TSIG パケットの送信後に受信された BADKEY エラーの数を報告します。
badsig	TSIG	rcvd-tsig-bad-sig	TSIG パケットの送信後に受信された BADSIG エラーの数を報告します。
dnssec-zones	DNSSEC	dnssec-zones	DNSSEC が有効になっているゾーンの数を報告します。

アクティビティサマリー名	ロギングサブカテゴリ	統計[10]	説明
dnssec-sign-zone	DNSSEC	dnssec-sign-zone	サーバーが DNSSEC ゾーンに署名した回数を報告します。
dnssec-queries	DNSSEC	dnssec-queries	DNSSEC 関連の RR（EDNS オプション DO ビット）を応答に含めるように要求するクエリの総数を報告します。
dnssec-responses	DNSSEC	dnssec-responses	DNNSEC 対応クエリ（EDNS オプション DO ビット）への応答の総数を報告します。
dnssec-requests-dropped	DNSSEC	dnssec-requests-dropped	サーバーが DNSSEC ゾーンに署名しているためにドロップされた DNS 要求の総数を報告します。
rpz-queries	RPZ	queries-rpz	RPZ のクエリの数を報告します。
rpz-hits	RPZ	query-answers-rpz-hits	RPZ の RR に一致した RPZ クエリの数を報告します。
rpz-misses	RPZ	query-answers-rpz-misses	RPZ の RR に一致しなかった RPZ クエリの数を報告します。
total	Security-Events-Categories	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。
alarm	Security-Events-Categories	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。
amplification	Security-Events-Categories	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-Categories	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。
poisoning	Security-Events-Categories	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。

アクティビティサマリー名	ロギングサブカテゴリ	統計[10]	説明
スヌーピング	Security-Events-Categories	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。
トンネリング	Security-Events-Categories	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。

[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。権威 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「DNS 統計」セクションを参照してください。

システム統計

system activity-counter-log-settings は、システム関連のカウンタをログに記録します。

システム アクティビティ サマリーの統計は、**System** 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：

```
10/22/2021 16:41:05 name/dns/1 Activity Stats 0 21493 [System] Sample since Fri Oct 22
16:40:05 2021: pid=number, cpu=number, memory=number, virtual=number, conntrack-max=number,
 conntrack-count=number, conntrack-usage=number
```

表 *12*：システム統計

アクティビティサマリー名	説明
pid	ADNS プロセスの PID。
cpu	ADNS プロセスによって使用される CPU の量。
memory	ADNS プロセスによって使用されるメモリの量。
virtual	ADNS プロセスによって使用される仮想メモリの量。
conntrack-max	Linux ファイアウォール接続の達した最大数。
conntrack-count	Linux ファイアウォール接続の現在の数。
conntrack-usage	使用中の Linux ファイアウォール接続の割合。

トップネームの統計情報

top-names activity-counter-log-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。

トップ ネーム アクティビティ サマリーの統計は、**Top-Names** 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：

```
10/22/2021 16:55:05 name/dns/1 Activity Stats 0 21508 [Top-Names] from 16:53:05 to
16:54:05; interval=number, total-counted=number
```

表 *13*：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[11]	説明
interval	該当なし	データ収集期間の長さ。
total-counted	total-counted	この収集期間にカウントされたクエリの総数を報告します。

[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。権威 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「DNS 統計」セクションを参照してください。

更新の統計

update activity-counter-log-settings は、DNS 更新関連のカウンタをログに記録します。

サンプルログメッセージ：

```
10/29/2021 15:56:31 name/dns/1 Activity Stats 0 21550 [Update] Sample since Fri Oct 29
15:55:31 2021: total=number, failed-acl=number, prereq-only=number, dropped=number,
simulated=number, udp=number, tcp=number, ipv4=number, ipv6=number, deletes=number,
adds=number, refreshes=number, rrs=number, A=number, AAAA=number, DHCID=number, TXT=number,
 other=number

10/29/2021 15:56:31 name/dns/1 Activity Stats 0 21551 [Update-Responses] Sample since
Fri Oct 29 15:55:31 2021: total=number, no-error=number, failures=number, refused=number,
 notauth=number, notzone=number, formerr=number, servfail=number, prereq-failures=number,
 yxdomain=number, yxrrset=number, nxdomain=number, nxrrset=number
```

表 *14 :* 更新の統計

アクティビティサマリー名	ロギングサブカテゴリ	統計[12]	説明
total	更新	update-total	DNS サーバーが受信した更新の総数。
failed-acl	更新	update-failed-acl	ACL または更新ポリシーの認証、あるいはその両方の失敗により拒否された更新の総数。
prereq-only	更新	update-prereq-only	DNS サーバーが受信した前提条件に適合した場合のみの更新の総数。
dropped	更新	update-dropped	DNS サーバーによってドロップされた更新の総数。
simulated	更新	update-simulated	シミュレートされた更新の総数。シミュレートされた RR 更新は NOERROR 応答を返しますが、RR の変更を生じさせません。
udp	更新	update-over-udp	UDP 経由で受信された更新の総数。
tcp	更新	update-over-tcp	TCP 経由で受信された更新の総数。
ipv4	更新	update-over-ipv4	IPv4 経由で受信された更新の総数。
ipv6	更新	update-over-ipv6	IPv6 経由で受信された更新の総数。
deletes	更新	update-delete	DNS の更新によって削除された RR の総数。
adds	更新	update-add	DNS の更新によって追加された RR の総数。
refreshes	更新	update-refresh	DNS の更新によって更新された RR の総数。
rrs	更新	update-total-rrs	DNS 更新要求によって更新された RR の総数。
A	更新	update-type-A	A レコードの更新の総数。
AAAA	更新	update-type-AAAA	AAAA レコードの更新の総数。
DHCID	更新	update-type-DHCID	DHCID レコードの更新の総数。
TXT	更新	update-type-TXT	TXT レコードの更新の総数。

アクティビティサマリー名	ロギングサブカテゴリ	統計[12]	説明
other	更新	update-type-other	特にカウントされていない他のすべてのレコードタイプの更新の総数。
total	Update-Responses	update-resp-total	DNS サーバーから返された更新応答の総数。
no-error	Update-Responses	update-resp-NOERROR	rcode が NOERROR の更新応答の総数。
failures	Update-Responses	update-resp-failures	失敗した更新の総数。
refused	Update-Responses	update-resp-REFUSED	rcode が REFUSED の更新応答の総数。
notauth	Update-Responses	update-resp-NOTAUTH	rcode が NOTAUTH の更新応答の総数。
notzone	Update-Responses	update-resp-NOTZONE	rcode が NOTZONE の更新応答の総数。
formerr	Update-Responses	update-resp-FORMERR	rcode が FORMERR の更新応答の総数。
servfail	Update-Responses	update-resp-SERVFAIL	rcode が SERVFAIL の更新応答の総数。
prereq-failures	Update-Responses	update-resp-prereq-failures	前提条件の失敗（YXDOMAIN、YXRRSET、NXDOMAIN、NXRRSET）を伴う更新応答の総数。
yxdomain	Update-Responses	update-resp-YXDOMAIN	rcode が YXDOMAIN の更新応答の総数。
yxrrset	Update-Responses	update-resp-YXRRSET	rcode が YXRRSET の更新応答の総数。
nxdomain	Update-Responses	update-resp-NXDOMAIN	rcode が NXDOMAIN の更新応答の総数。
nxrrset	Update-Responses	update-resp-NXRRSET	rcode が NXRRSET の更新応答の総数。

[12] 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。権威 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「DNS 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。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。

ローカル Web UI

トップネームを有効にするには、[ローカル DNS サーバーの編集 （Edit Local DNS Server）] タブの [トップネームの設定（Top Names Settings）] セクションで *top-names* 属性を検索し、[有効（enabled）] オプションを選択して有効にしてから、[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。

ローカルの基本または高度な 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 **[DNS]** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS Server）] ページを開きます。

ステップ 3 [ローカル DNS サーバー（Local DNS 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

dns 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設定

Cisco Prime Network Registrar 11.1 では、[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。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 dns_security_log ファイル に書き込まれます。

表 *15*：権威 *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。security-event-logging および security-event-log-settings 設定の変更は、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。 セキュリティイベントログのメッセージは、dns_security_log ファイルに書き込まれます。

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。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 dns_security_log ファイル に書き込まれます。この設定を有効にするには、*security-event-logging* を有効にする必要があります。*security-event-logging* および *security-event-log-settings* 設定の変更は、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。 • 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。 • 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：DNS サーバーが同時パケットの制限（つまり、 *max-dns-packets*）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。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、packet-inspection、および rate-limit 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。 • 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。 • 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：DNS サーバーが同時パケットの制限（つまり、 *max-dns-packets*）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。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。
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。
ブロックリスト ACL （*acl-blocklist*）	このアクセス制御リストにリストされているクライアントからの要求をブロックします。このリストには、ホスト、ネットワークアドレス、およびその他の ACL を含めることができます。リストの ACL と一致するクライアントからの要求はドロップされます。
TSIG 処理 （*tsig-processing*）	DNS トランザクションの TSIG 処理をオンまたはオフにすることができます。デフォルトは、ddnsおよびクエリ要求で有効になっています。

属性	説明
gss-tsig-processing	DNS トランザクションの gss-tsig セキュリティモードを示します。*gss-tsig-processing* と *tsig-processing* の両方が有効になっている場合、gss-tsig セキュリティモードは無効になります。デフォルトはなし（無効）になっています。
gss-tsig-config	DNS サーバーが使用する gss-tsig 設定オブジェクトを識別します。

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 **[DNS]** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS 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、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

dns 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、**dns 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。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 **[セキュリティ統計（Security Statistics）]** セクションに表示されます。

表 *16 :* 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-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

権威 DNS のセキュリティイベントは、dns_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 **[DNS]** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS 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、権威 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。

- **dns-security-events-critical-level**：権威 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。
- **dns-security-events-warning-level**：権威 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 dns-security-events-critical-level = *value* を使用して、権威 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 dns-security-events-warning-level = *value* を使用して、権威 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 セッションのために 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 DNS データディレクトリ（つまり、<cnr.datadir>/dns/tls）に必ず保管するようにしてください。

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 **[DNS]** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS 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 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。このファイルはパスコードで暗号化しないよう注意してください。

- 公開キーファイル（*service-pem*）：DNS が TLS 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 DNS 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

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

dns set service-pem = *value* を使用して、権威 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

Cisco Prime Network Registrar は、キャッシング DNS サーバーに加えて、権威 DNS サーバーで TLS をサポートします。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 秘密キーファイルおよび公開キーファイルを追加するための設定可能なパラメータがあります。

DNS over TLS の詳細については、「キャッシング DNS サーバーの管理」の章にある TLS 設定の指定 の項を参照してください。

（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。

表 *17*：権威 *DNS* サーバーの *TLS* 属性

属性	説明
TLS（*tls*）	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 DNS データディレクトリの dns/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 DNS 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 DNS データディレクトリの dns/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。
TLS ポート（*tls-port*）	TCP TLS サービスを提供するポート番号。DNS サーバーは、このポートで非 TLS クエリを処理しません。

ローカル詳細 Web UI

権威 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 DNS 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>/dns/tls）。そして [DNS権威サーバーの管理（Manage DNS Authoritative 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 **[DNS]** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS 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

dns enable tls を使用して、権威 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。

dns set *attribute=value* を使用して、権威 DNS サーバーの TLS 属性を設定します。

（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。TLS 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 [セキュリティ統計（Security Notification Statistics）] セクションに表示されます。

表 *18 : TLS* 統計属性

属性	説明
tls-queries	DNS サーバーが TLS を介して受信したクエリの総数。
tls-queries-failed	TLS ハンドシェイク中に失敗した TLS クエリの総数。

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 Web UI

[DNS 権威サーバーの管理（Manage DNS Authoritative Server）] ページの [その他のオプションと設定（Miscellaneous Options and Settings）] セクションで、[ラウンドロビン（*round-robin*）の有効化（Enable round-robin）] 属性を探します。[基本（Basic）] モードでは、これはデフォルトで有効になっています。

CLI コマンド

dns 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、**dns enable round-robin** を使用します。

重み付けラウンドロビンの有効化

nameset が同じタイプの複数の RR を用いて設定されている場合は、加重ラウンドロビンのアルゴリズムを使用して、1 つの RR がクエリ応答の最初の RR として返される頻度を決定できます。応答の動作を制御するには、管理者がこれらの RR の重み値を設定できる必要があります。さらに、複数のレコードが返される順序は、クライアントアプリケーションが使用できます。管理者がこの順序を制御する必要があります。

order および *weight* 属性は、Advaned モードで使用できます。

Order

order 属性では、nameset に含まれる同じタイプの他の RR と比較して、RR のソート順序を指定します。同じタイプの RR が昇順で表示されます。これは、照会時に RR が返される順序にもなります。

Weight

RR の重みは、同じサービスを提供する特定のサーバーをから頻繁に返す必要があり、多くの負荷がかかるような場合に使用できます。*weight* 属性では、nameset に含まれる同じタイプの他の RR と比較して、この RR の相対的な重要性を指定します。重みの大きな RR は、名前とタイプのクエリ応答で使用される頻度が高くなります。たとえば、*weight* の RR が 5 に設定されており、別の RR の *weight* が 1 に設定されている場合は、この RR が 5 回使用されてから、別の RR が 1 回使用されます。*weight* が 0（ゼロ）の RR は必ずリストの最後に配置され、ラウンドロビン操作には含まれません。

（注） RR のデフォルトの *weight* は 1 です。ラウンドロビンが有効になっている場合（DNS サーバーまたはゾーンレベルのいずれかで）、クエリごとに RR が最初の位置で 1 回返されます（つまり、従来のラウンドロビン）。

RR セットのすべての重みが 0 の場合、*order* に基づいてクライアントに応答が返されます。RR セットレベルでラウンドロビンを効果的に無効化します。

order および *weight* 属性は、プライマリゾーンでのみ設定できます。これらは HA バックアップ、およびセカンダ サーバーに転送されます。これらの属性は、HA 内のサーバーのいずれか、またはセカンダリサーバーが 9.0 クラスタ以前の場合には転送されません。order と weight が転送されないようにするには、[DNS権威サーバーの管理（Manage DNS Authoritative Server）] ページにある RR メタデータの転送（*xfer-rr-meta-data*）属性を無効にします（これは、セカンダリ DNS サーバーで実行する必要があります）。セカンダリゾーンでは、*order* と *weight* が利用可能で、「リソースレコード」は編集不可となります。

ローカル Web UI

ステップ 1 [設計（Design）] メニューの [認証DNS（Auth DNS）] サブメニューから [正引きゾーン（Forward Zones）] または [逆引きゾーン（Reverse Zones）] を選択し、[ゾーンのリスト/追加（List/Add Zones）] ページを開きます。

ステップ 2 [正引きゾーン（Forward Zone）] または [逆引きゾーン（Reverse Zone）] ペインで、ゾーン名をクリックし、[ゾーンの編集（Edit Zone）] ページを開きます。

ステップ 3 [リソース レコード（**Resource Records**）] タブをクリックします。

ステップ 4 RR 名、TTL（デフォルトの TTL を使用していない場合）、タイプ、およびデータを必要に応じて追加します。

ステップ 5 RR が作成されたら、RR を編集して *order* と *weight* を設定できます（目的の RR の横にある鉛筆アイコンをクリックします）。*order* 属性と *weight* 属性は、[RR 設定（RR Settings）] セクションにあります。

CLI コマンド

zone *name* **addRR** *rr-name rr-type rr-ttl rr-data* [**weight**=*rr-weight*] [**order**=*rr-order*] を使用して、重みと順序を設定します。

リソースレコードを変更するには、**zone** *name* **modifyRR** *rr-name type* [*data*] *attribute=value* [*attribute=value* ...] を使用します。

増分ゾーン転送の有効化（IXFR）

増分ゾーン転送（IXFR、RFC 1995 で説明）では、変更されたデータのみをサーバー間で転送できます。これは動的な環境で特に役立ちます。IXFR は NOTIFY と連携して（「NOTIFY の有効化 （46 ページ）」を参照）ゾーン更新を効率化します。IXFR はデフォルトでは有効になっています。

プライマリ ゾーン サーバーは常に IXFR を提供します。サーバーにセカンダリ ゾーンがある場合にのみ、サーバーで IXFR を明示的に有効にする必要があります（プライマリ ゾーンには設定できません）。特定のセカンダリ ゾーン設定がない場合は、DNS サーバー設定がセカンダリ ゾーンに適用されます。

ローカル Web UI

[DNS 権威サーバーの管理（Manage DNS Authoritative Server）] ページの [ゾーンのデフォルト設定（Zone Default Settings）] セクションで、[要求増分転送（Request incremental transfers (IXFR)）] 属性を確認できます。これはデフォルトで有効になっています。セカンダリゾーンの場合は、*ixfr-expire-interval* 属性を設定して、増分ゾーン転送を微調整することもできます。

この値は、完全ゾーン転送（AXFR）の強制前に、サーバーが IXFR からのみセカンダリ ゾーンを維持するための最長間隔です。事前に定義された値は 0 です。IXFR は常に使用され、有効になっているため、定期的に AXFR に変更されることはありません。次に、[保存（**Save**）] をクリックします。

CLI コマンド

dns enable ixfr-enable を使用します。デフォルトでは、*ixfr-enable* 属性は有効になっています。

ゾーン クエリの制限

アクセスコントロールリスト（ACL）に基づいて特定のゾーンのみを照会するようにクライアントを制限できます。ACL には、送信元 IP アドレス、ネットワーク アドレス、TSIG キー（『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「トランザクション セキュリティ」の項を参照）、または他の ACL を含めることができます。[権威DNSサーバーの管理（Manage DNS Authoritative Server）] ページの *restrict-query-acl* 属性は、*restrict-query-acl* が明示的に設定されていないゾーンのデフォルト値として機能します。

NOTIFY の有効化

RFC 1996 で説明されている NOTIFY プロトコルを使用すると、ゾーンの変更が生じたことを Cisco Prime Network Registrar DNS プライマリ サーバーがセカンダリに知らせることができるようになります。NOTIFY パケットには、変更が発生したかどうかについてのヒントをセカンダリに提供するゾーンの最新 SOA レコードも含まれます。この場合、シリアル番号は異なります。名前空間が比較的動的である環境で NOTIFY を使用します。

ゾーンプライマリサーバーは、どのセカンダリサーバーが転送元であるかを特定できないため、Cisco Prime Network Registrar は、ゾーン NS レコードに記載されているすべてのネームサーバーに通知します。唯一の例外は、プライマリサーバーの [SOA] フィールドに名前が指定されているサーバーです。ゾーン設定の *notify-list* に IPv4 と IPv6 のアドレスを追加することによって、通知先となるサーバーを追加できます。

（注） 表示されない（つまりゾーンの NS RR として記載されていない）ネームサーバーに通知を送信するには、その IP アドレスを *notify-list* に記載し、通知設定を *notify-list* または *notify-all* にする必要があります。

IXFR と NOTIFY は併用できますが、これは必須ではありません。すべてのセカンダリ即時更新により一定の NOTIFY トラフィックを必要としない、急速に変更するゾーンに対しては NOTIFY を無効にすることができます。そのようなゾーンの場合は、更新時間を短くして、NOTIFY を無効にすることが有効である可能性があります。

（注） セカンダリゾーンでは、通知はデフォルトで有効になっています。通知を受ける第2層のセカンダリサーバーがない場合は、この設定を無効にする必要があります。これにより、不要な通知要求がなくなり、サーバーのパフォーマンスが向上する可能性があります。

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 [ゾーン転送の設定（Zone Transfer Settings）] セクションで *notify* 属性を見つけ、ドロップダウン リストから値を選択します。

ステップ 2 その他の NOTIFY 属性（*notify-min-inverval*、*notify-rcv-interval*、*notify-send-stagger*、*notify-source-port* および *notify-wait*）のいずれかを設定します。

ステップ 3 [保存（**Save**）] をクリックします。

ステップ 4 NS レコードで指定されたものに加えてネームサーバーを追加するには、[**設計（Design**）] メニューから [**権威 DNS（Auth DNS**）] サブメニューで、[**正引きゾーン（Forward Zones**）] または [**逆引きゾーン（Reverse Zones**）] または [**セカンダリ ゾーン（Secondary Zones**）] を選択します。

ステップ 5 [正引きゾーン（Forward Zones）]、[逆引きゾーン（Reverse Zones）] または [セカンダリゾーン（Secondary Zones）] ペインでゾーンをクリックし、[ゾーンの編集（Edit Zones）] ページを開きます。

ステップ 6 [ゾーンの編集（Edit Zone）] ページの *notify-list* 属性を使用して、サーバーの IP アドレスのカンマ区切りリストを追加します。

ステップ 7 *notify* ドロップダウン リストから値を選択します。

ステップ 8 [保存（**Save**）] をクリックします。

CLI コマンド

dns set notify=*value* を使用します。ゾーン レベルで NOTIFY を有効にすることもできます。**zone** *name* **set notify-list** を使用して、NS レコードで指定されたサーバー以外に通知するために、追加のサーバーのカンマ区切りリストを指定できます。

権威サーバーからの再帰クエリのブロック

再帰クエリのブロックにより、サーバーはこれらのクエリを処理しようとしてリソースを消費することがなくなります。再帰クエリのドロップ（*drop-recursive-queries*）属性によって、RD フラグをオンにするクエリを DNS サーバーが受け入れるか、またはドロップするかを制御します。この属性がイネーブルになっている場合、再帰クエリはサーバーによってドロップされます。*drop-recursive-queries* のデフォルト値は disabled です。これは、再帰クエリがドロップされないことを意味します

drop-recursive-queries 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 [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 **[DNS]** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS Server）] ページを開きます。

ステップ 3 **[クエリ設定（Query Settings）]** セクションで、**[有効（Enabled）]** オプションを選択して *drop-recursive-queries* 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） この設定は、DNS サーバーのリロードなしで動的に変更できます。

CLI コマンド

dns enable drop-recursive-queries を使用して、[ドロップ再帰クエリ（Drop Recursive Queries）] を有効にします。

ドロップ再帰クエリの統計

[DNS権限サーバーの管理（Manage DNS Authoritative Server）] ページで、[統計情報（Statistics）] タブをクリックし、[クエリ統計情報（Query Statistics）] セクションの下にある *queries-dropped-recursive* 統計属性を表示します。これは、再帰によってドロップされたクエリの数を示します。queries-dropped カウンタは、再帰クエリがドロップされると増加します。

DNS 権威サーバー コマンドの実行

[コマンド（Commands）] ボタンを使用して、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 [DNS コマンド（DNS 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）。

- **Force all zone transfers**：セカンダリサーバーはプライマリサーバーに変更を定期的に問い合わせます。「ゾーン転送の有効化」を参照してください。
- **Scavenge all zones**：古いレコードを定期的に消去します。『*Cisco Prime Network Registrar 11.1 DHCP ユーザ ガイド*』の「動的レコードのスカベンジング」の項を参照してください。
- **Synchronize All HA Zones**：すべての HA ゾーンを同期します。同期のタイプを選択するオプションがあります。**[Push All Zones From Main to Backup]** オプションは、デフォルトでオンになっています。**[Pull All Zones From Backup to Main]** チェックボックスをオンにすることで、これをオーバーライドできます。

（注） **Synchronize All HA Zones** コマンドはエキスパートモードコマンドであり、サーバーが HA メインサーバーである場合にのみ表示されます。HA バックアップ サーバーの場合、このコマンドは表示されません。ゾーンを個別に同期することもできます。これは [ゾーンのゾーン コマンド（Zone Commands for Zone）] ページで実行できます（「HA DNS ゾーンの同期」を参照）。

（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。

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、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。

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 **DNS** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS 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すると、新しいページが開きますので、そこでインターフェイスのアドレスを変更できます。

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、[サーバーの管理（Manage Servers）] ページに戻ります。

（注） DNS の IPv6 機能を使用するには、DNS サーバーが独立型スタンドアロンである（DNS サーバーが自己のルートであり、すべてのクエリに対する権威である）場合を除いて、IPv4 インターフェイスを設定する必要があります。

権威 DNSSEC の管理

DNSSECにより、データ出自の認証、データの完全性の確認、および認証による存在否定が可能になります。DNSSEC を使用すると、DNS プロトコルが特定のタイプの攻撃（特に DNS スプーフィング攻撃）の影響を受けにくくなります。DNSSEC は、デジタル署名を DNS データに追加することによって、悪意のある応答や偽造された応答を防ぎ、各 DNS 応答の完全性と真正性を検証できます。

Cisco Prime Network Registrar 9.0 以前の権威 DNS サーバーは、ゾーンの署名をサポートしていません。Cisco Prime Network Registrar 10.0 以降は、権威 DNSSEC のサポートにより認証と完全性が DNS ゾーンに付加されます。このサポートにより、Cisco Prime Network Registrar DNS サーバーはセキュアゾーンと非セキュアゾーンの両方をサポートできます。

DNSSEC セキュリティを追加する手順は、次のとおりです。

1. DNSSEC キーとゾーンのリージョンまたはローカル管理を選択します。
2. デフォルトのキー生成に使用される権威 DNSSEC のアルゴリズム、サイズ、ライフタイム、および間隔を確認します。
3. 内部で生成されたキーを使用していない場合は、ゾーン署名用キーとキー署名用キーを作成します。
4. 必要なゾーンに対して、DNSSEC を有効にします。
5. 同じサーバー上で設定されていない場合は、親ゾーンに追加する必要がある署名付きゾーンの DS RR をエクスポートします。

権威 DNSSEC の有効化

権威 DNS サーバーでは、デフォルトで DNSSEC が有効になっています。[権威 DNSSEC の管理（Manage Authoritative DNSSEC）] ページで DNSSEC（*dnssec*）属性（エキスパートモードで使用可能）を使用して無効にできます。この属性を無効にすると、ゾーンの *dnssec* 属性に関係なく、すべてのゾーンのゾーン署名が無効になります。デフォルトでは、ゾーン署名はすべてのゾーンに対して無効になっています。ゾーン署名を有効にするには、ゾーンが公開された後のみに、ゾーン設定の DNSSEC（*dnssec*）属性を有効にする必要があります。ゾーンで DNSSEC を有効にすると、ゾーン署名を実行するために、デフォルトではコア キーが使用され、ゾーン テナントに固有のテナント キーが定義されている場合はそのキーが使用されます。使用可能なキーがない場合は、CCM サーバーでゾーンの新しいキーが生成されます。

（注） RPZ が有効になっている場合は、ゾーンで DNSSEC を有効にすることはできません。その逆の場合も同様です。

表 *19* : 権威 *DNSSEC* 属性

属性	説明
名前	権威 DNSSEC 設定の名前を指定します。
説明	権威 DNSSEC 設定の説明。
キーロールオーバー（*key-rollover*）	リージョナルクラスタまたはローカルクラスタがゾーン署名キー（ZSK）ロールオーバーを実行する必要があるかどうかを示します。 リージョナルゾーン管理を使用する場合は、キーの生成とロールオーバーを一元的に管理するために、この設定をリージョナルに設定する必要があります。

表 *20* : ゾーン署名用キーの属性

属性	説明
アルゴリズム（*zsk-algorithm*）	ZSK に使用される暗号アルゴリズムを指定します。 DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
署名サイズ（*zsk-bits*）	キーのビット数を指定します。64 の倍数にする必要があります。この値は、選択された ZSK アルゴリズム（zsk-algorithm）によって異なります。 DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
キーのライフタイム（*zsk-lifetime*）	ZSK のライフタイムを指定します。これにより、キーがゾーンの署名に使用される時間間隔が定義されます。ZSK キーが作成されたときに deactivation-date を決定するために使用されます。*zsk-rollover-interval* よりも大きい値を設定する必要があります。10 倍の値を推奨します。
キーのロールオーバー間隔（*zsk-rollover-interval*）	ZSK ロールオーバープロセスの時間間隔を指定します。現在のキーに対する deactivation-date より前の新しいキーのリードタイムが決定されます。 偽のゾーン情報を回避するには、ゾーンの最大 TTL と伝達遅延を足した値よりも大きい値をこの間隔として設定する必要があります。

表 *21 :* キー署名用キーの属性

属性	説明
アルゴリズム（*ksk-algorithm*）	キー署名用キー（KSK）に使用される暗号アルゴリズムを指定します。 DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
署名サイズ（*ksk-bits*）	キーのビット数を指定します。64 の倍数にする必要があります。この値は、選択した KSK アルゴリズム（*ksk-algorithm*）によって異なります。 DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
キーのロールオーバー間隔（*ksk-rollover-interval*）	KSK ロールオーバープロセスの時間間隔を指定します。現在のキーに対する deactivation-date より前の新しいキーのリードタイムが決定されます。

ローカルの高度な Web UI

ステップ 1 [**設計（Design**）] メニューから [**セキュリティ（Security**）] サブメニューで [**権威 DNSSEC（Authoritative DNSSEC**）] を選択して、[権威 DNSSEC の管理（Manage Authoritative DNSSEC）] ページを開きます。

ステップ 2 要件に従って、[ゾーン署名キー（Zone Signing Key）] セクションと [キー署名キー（Key Signing Key）] セクションの属性を変更します。

ステップ 3 [**保存（Save**）] をクリックして設定を保存します。

CLI コマンド

dnssec set *attribute=value* [*attribute=value...*] を使用して、権威 DNS サーバーでの DNSSEC 処理を設定します。次に例を示します。

```
nrcmd> dnssec set zsk-algorithm=RSASHA1
```

zone *zonename* **signZone** を使用して、ゾーンの DNSSEC を有効にし、エキスパートモードで実行する場合は、ゾーンのすべての RR に署名を追加します。

リージョン クラスタに接続されている場合は、次の pull および push コマンドを使用できます。プッシュは、クラスタのリストまたは「all」を許可します。

dnssec pull *cluster-name* [**-report-only** | **-report**]

dnssec push *cluster-list* [**-report-only** | **-report**]

権威 DNSSEC キーの管理

DNSSEC で保護されたゾーンを設定するには、まずキーを作成する必要があります。その後、キーを使用してそのゾーンに署名します。キーを手動で作成して、キー属性をカスタマイズすることができます。それ以外は、CCM サーバーが必要に応じて新しいキーを自動的に作成します。

[権威 DNSSEC（Authoritative DNSSEC）] ページの *key-rollover* 属性をローカルまたはリージョナル管理に設定できます。デフォルトは local です。*key-rollover* 属性は、リージョナルまたはローカル クラスタが ZSK ロールオーバーを実行する必要があるかどうかを指定します。ローカル ロールオーバー管理では、キーはローカルプライマリまたはHA メインで管理されます。キーは、CCM HA 同期で HA バックアップにコピーされます。ゾーンが複数のプライマリ サーバーに分散されている場合は、管理するキーが多くなります。リージョン ロールオーバー管理では、キーはリージョン サーバーで管理され、ローカル クラスタにプッシュされます。これにより、分散プライマリサーバーの共通キーセットを管理できます。ゾーンの集中管理では、ゾーンの編集を段階に分けて事前に署名してから、ローカル DNS サーバーと変更内容を同期することもできます。ローカル CCM サーバーで DNS 編集モードが同期に設定されている場合、キーはリージョナルからローカルに自動で同期されます。

ZSK のロールオーバーは自動プロセスです。KSK のロールオーバーは手動で実行する必要があります。**rollover-ksk** コマンドを使用して KSK ロールオーバープロセスを開始します。独自のキーを指定するか、CCM にキーを生成させることができます。

dns rollover-ksk [**tenant-id**=*value*] [**next-key**=*keyname* | **key-group**=*value*]

（注） ラボ設定では、エキスパートモードコマンドである **zone** *name* **removeSignature** を使用して、すべての署名 RR を削除し、そのゾーンの DNSSEC を無効にすることができます。このコマンドは、運用 DNSSEC ゾーンには使用しないでください。署名されなくなる運用 DNSSEC ゾーンでは、RFC 6781：DNSSEC 運用慣行、バージョン 2 のガイドラインに従って、署名レコードをその有効期限後に削除する必要があります。

表 *22*：主要タイムライン属性

属性	説明
アクティベーション日（*activation-date*）	このキーのアクティベーションの日付と時刻を示します。この日時の開始時に、このキーは RR セットの署名に使用されます。

非アクティベーション日（*deactivation-date*）	このキーの非アクティブ化の日付と時刻を示します。この日時まで、このキーはRRセットの署名に使用されます。KSKの場合、この属性は0である必要があります。KSKは、キーのロールオーバープロセスが開始されるまでアクティブのままになります。
削除日（*expiration-date*）	この ZSK が削除される日付と時刻を指定します。0 の場合は、自動削除が無効になり、ユーザーがキーを削除する必要があります。KSKの場合、この属性は0である必要があります。KSKは、キーのロールオーバープロセスが開始されるまでアクティブのままになります。ロールオーバープロセスが完了したら、ユーザーがキーを削除できます。
ロールオーバー期日（*rollover-due-date*）	このキーをロールオーバーする（またはロールオーバーした）日時を指定します。この一時属性は、レポートにのみ使用されます。
キーステータス（*status*）	キーの現在のステータスを指定します。この一時属性は、レポートにのみ使用されます。

ローカル詳細およびリージョン詳細 Web UI

ステップ 1 [**設計（Design）**] メニューから [**セキュリティ（Security）**] サブメニューで [**権威 DNSSEC キー（Auth DNSSEC Keys）**] を選択して、[権威 DNSSEC キーのリスト表示/追加（List/Add Authoritative DNSSEC Keys）] ページを開きます。

ステップ 2 キーを有効にしてゾーンに署名するには、*enable-signing* の属性値を **true** に設定します。

ステップ 3 [キータイムライン（Key Timelines）] セクションでは、必要に応じて、非アクティブにする日付と削除する日付を入力できます。

ステップ 4 [**保存（Save）**] をクリックして設定を保存します。

CLI コマンド

ゾーン署名に権威 DNSSEC キーを作成および管理するには、次の **dnssec-key** コマンドを使用します。

dnssec-key *name* **create** [*attribute=value...*]

dnssec-key *name* **delete** [**-force]**

dnssec-key *name* **show**

dnssec-key *name* **set** *attribute=value* [*attribute=value...*]

dnssec-key getStatus を使用して、ロールオーバープロセスに関連する DNSSEC キーの現在のステータスを確認します。

地域クラスターに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再使用の場合は、クラスターのリストまたは「すべて」を指定できます。

dnssec-key < *name* | **all** > **pull** < **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]

dnssec-key < *name* | **all** > **push** < **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]

dnssec-key *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

DS レコードのエクスポート

Export Delegation Signer（DS）レコードは、DNSSEC が有効になっているゾーンで使用できます。親ゾーンが権威 DNS サーバーで見つかった場合は、DS レコードがゾーンに自動的に追加されます。複数の権威サーバーが展開されていて、親ゾーンが別のローカルクラスタにある場合は、リージョンサーバーのゾーンを管理して、親ゾーンを自動的に更新できます。親ゾーンが外部で所有されている場合は、外部組織によって追加される DS レコードを指定する必要があります。

ローカル詳細およびリージョン詳細 Web UI

DS レコードをエクスポートするには、次の手順を実行します。

ステップ 1 [**設計（Design）**] メニューから [**権威 DNS（Auth DNS）**] サブメニューで [**正引きゾーン（Forward Zones）**] を選択して、[ゾーンの編集（Edit Zone）] ページを開きます。

ステップ 2 [ゾーンの編集（Edit Zone）] ページの [DNSSEC 設定（DNSSEC Settings）] で、DNSSEC 値を true に設定して DNSSEC を有効にします。

ステップ 3 [**保存（Save）**] をクリックして設定を保存します。

ステップ 4 DS レコードをエクスポートするには、 **DS レコード（DS Record）**の横にある [**保存（save）**] アイコンをクリックします。

CLI コマンド

DS レコードをエクスポートした後は、**export dnssec-ds** *zonename filename* コマンドを使用して、同じものを親ゾーンにパブリッシュする必要があります。

権威 DNS サーバーの詳細プロパティの設定

次のサーバー詳細プロパティを設定できます。

- **SOA 存続可能時間**：「SOA 存続可能時間の設定 （56 ページ）」を参照
- **セカンダリ サーバーの属性**：「セカンダリ更新時間の設定 （56 ページ）」を参照
- **ポート番号**：「ローカルおよび外部ポート番号の設定 （58 ページ）」を参照

- **悪意のある DNS クライアントの処理**：「悪意のある DNS クライアントの処理 （58 ページ）」を参照

SOA 存続可能時間の設定

SOA レコード TTL は、通常はゾーンのデフォルト TTL によって決定されます。ただし、SOA TTL を明示的に設定できます。これにより、サーバーが SOA レコード データをキャッシュできる最大秒数が設定されます。たとえば、SOA TTL が 3600 秒（1 時間）に設定されている場合は、1 時間後に外部サーバーはキャッシュから SOA レコードを削除してから、ネームサーバーを再度照会する必要があります。

Cisco Prime Network Registrar は、明示的な TTL 値で権威クエリに応答します。明示的な TTL 値がない場合は、*defttl* ゾーン属性の値で設定されているゾーンのデフォルト TTL が使用されます。

通常は Cisco Prime Network Registrar では、明示的な TTL 値がない RR を使用したゾーン転送で応答する場合に、デフォルトの TTL が前提とされます。ゾーンのデフォルト TTL 値が管理の際に変更された場合は、Cisco Prime Network Registrar は、ゾーン転送を要求するセカンダリ DNS サーバーへの完全ゾーン転送を自動的に強制します。

ローカルおよび地域 Web UI

ステップ 1 [ゾーンのリスト/追加（List/Add Zones）] ページで、ゾーンのデフォルト TTL 属性を設定します。デフォルト値は 24 時間です。

ステップ 2 必要に応じて、SOA レコード専用の TTL である SOA TTL を設定します。デフォルトではゾーンのデフォルト TTL 値に設定されています。

ステップ 3 ゾーンの NS レコード専用の TTL 値を設定することもできます。ネームサーバーで NS TTL 属性値を設定します。この値もデフォルトで、ゾーンのデフォルト TTL 属性値に設定されています。

ステップ 4 [保存（**Save**）] をクリックします。

CLI コマンド

zone *name* **set defttl** を使用します。

セカンダリ更新時間の設定

セカンダリ更新時間は、セカンダリ サーバーがゾーン転送の潜在的なニーズについてプライマリと通信する頻度です。有効な範囲は、期待するゾーン データの変更頻度に応じて 1 時間～1 日です。

NOTIFY はプライマリ データが変更されたときにセカンダリ サーバーに強制的に知らせるので、NOTIFY を使用する場合は、転送間隔が長くならないように、更新時間を大きな値に設定

することができます。NOTIFY の詳細については、「NOTIFY の有効化 （46 ページ）」を参照してください。

ローカルおよび地域 Web UI

[ゾーンのリスト/追加（List/Add Zones）]ページの[セカンダリ更新（Secondary Refresh）]フィールドに更新時間に設定します。 デフォルトは 3 時間です。変更を行ってから、[保存（**Save**）]をクリックします。

CLI コマンド

zone *name* **set refresh** を使用します。デフォルト値は 10,800 秒（3 時間）です。

セカンダリ再試行時間の設定

DNS サーバーは、連続するゾーン転送エラーの間に、セカンダリ再試行時間を適用します。更新間隔が終わり、ゾーン転送のポーリング試行が失敗すると、サーバーは成功するまで再試行を続行します。有効な値は更新時間の 3 分の 1 ～ 10 分の 1 です。デフォルト値は 60 分です。

ローカルおよび地域 Web UI

[ゾーンのリスト/追加（List/Add Zones）] ページの [セカンダリ再試行（Secondary Retry）] フィールドで再試行時間を設定します。 デフォルトは 1 時間です。変更を行ってから、[保存（**Save**）] をクリックします。

CLI コマンド

zone *name* **set retry** を使用します。デフォルト値は 60 分です。

セカンダリ有効期間の設定

セカンダリ有効期間は、セカンダリ サーバーがゾーン転送中にゾーン更新を受信できない場合に、クエリに応答するときにゾーンデータに対する権威を主張できる最長時間です。これを大きな値に設定することで、プライマリ サーバーの長い障害中に存続するのに十分な時間を確保できます。デフォルト値は 7 日間（1 週間）です。

ローカルおよび地域 Web UI

[ゾーンのリスト/追加（List/Add Zones）] ページの [セカンダリ有効期限（Secondary Expire）] フィールドに有効期間に設定します。 デフォルトは 7 日間です。変更を行ってから、[保存（**Save**）] をクリックします。

CLI コマンド

zone *name* **set expire** を使用します。デフォルト値は 7 日間（1 週間）です。

ローカルおよび外部ポート番号の設定

ネームサーバーの新しいグループを試す場合は、要求への応答とリモートデータの要求に非標準ポートを使用できます。ローカルポートと外部ポートの設定で、サーバーが名前解決要求をリッスンする TCP と UDP ポートを制御し、他のネームサーバーへの要求時に接続するポートを制御します。両方の標準値はポート 53 です。通常の動作中にこれらの値を変更すると、サーバーが使用できなくなるように見えます。

デフォルトポートの完全なリストは、の「*Default Ports for Cisco Prime Network Registrar Services*」の項*Cisco* プライムネットワーク レジストラー *11.1* 管理ガイドを参照してください。

ローカルの高度な Web UI

[権威DNSサーバーの管理（Manage DNS Authoritative Server）] ページの [ネットワーク設定（Network settings）] セクションで、[リスニングポート（Listening port）]（*local-port-num*）と [リモートDNSサーバー ポート（Remote DNS Servers Port）]（*remote-port-num*）の属性を目的の値に設定し（どちらもデフォルト値は 53 です）、[保存（**Save**）] をクリックします。

悪意のある DNS クライアントの処理

クエリ要求を解決しようとするときに、DNS サーバーが悪意のある DNS クライアントに遭遇することがあります。クライアントが疑わしい DNS 要求を大量にネットワークに送りつけ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。

悪意のあるクライアントを 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。禁止する悪意のあるクライアントのグローバル ACL を設定するには、*acl-blocklist* 属性を使用します。

ローカルの詳細 Web UI

[DNS権威サーバーの管理（Manage DNS Authoritative Server）] ページで [セキュリティイベント（Security Events）] セクションを展開すると、さまざまな属性とその値が表示されます。*acl-blocklist* 属性には、値（10.77.240.73 など）を入力します。次に [**保存（Save**）] をクリックします。

DNS プロパティの調整

DNS サーバーのプロパティの一部を調整するためのヒントを次に示します。

- [通知送信最小間隔（NOTIFY send min. interval）] DNS サーバー属性（*notify-min-interval*）：同じゾーンでの連続した変更についての通知をサーバーに送信するまでの最小間隔。プリセット値は 2 秒です。非常に大規模なゾーンの場合は、アウトバウンドの完全ゾーン転送の最大送信時間より長くなるように、この値を引き上げることができます。これは、インバウンドの増分ゾーン転送を受信し他のセカンダリ サーバーに完全転送を送信するセカンダリ サーバーに対して推奨されます。これには、増分ゾーン転送をサポートしていない古

いBINDサーバーが含まれます。インバウンドの増分転送によってアウトバウンドの完全転送が中止されることがあります。

- [サーバー間の通知遅延（NOTIFY delay between servers）] **DNS server attribute (（*notify-send-stagger*)**：複数のサーバーの変更通知が重ならないように通知を遅らせるための間隔。プリセット値は1秒ですが、複数のサーバーに分散された多数のゾーン転送をサポートする必要がある場合は、最大 5 秒に引き上げることができます。
- [追加変更までの通知待機（NOTIFY wait for more changes）] **DNS server attribute (（*notify-wait*)**：最初のゾーン変更後に、他のネームサーバーに変更通知を送信するまでの時間。プリセット値は 5 秒ですが、*notify-min-interval* 属性と同じ理由で 15 秒に引き上げることができます。
- [最大メモリキャッシュサイズ（Maximum Memory Cache Size）] **DNS server attribute (（*mem-cache-size*)**：メモリ内のレコードキャッシュのサイズ（KB 単位）。プリセット値は 500000 KB（500 MB）です。これにより、権威 DNS サーバーのクエリを高速化できます。目安としては、この値を権威 RR の数と同等にします。
- **EDNS 最大パケットサイズ DNS サーバー属性（*edns-max-payload*）**：送信側の最大 UDP ペイロードサイズを指定します。これは、要求元が処理できる最大 UDP パケットのオクテット数として定義されます（RFC 6891 を参照）。この属性は、最小 512 バイトから最大 4 KB まで変更できます。この属性のデフォルト値は、DNS サーバー上で 1232 バイトです。

同じサーバーでのキャッシュ DNS と権威 DNS の実行

Cisco Prime Network Registrar にはハイブリッド DNS 機能が含まれています。この機能を使用すると、2つの独立した仮想マシンまたは物理マシンを使用せずに、キャッシュ DNS サーバーと権威 DNS サーバーの両方を同じオペレーティング システムで実行できます。この機能により、キャッシング DNS は DNS の例外を作らずに権威 DNS サーバーとそのゾーンを自動で検出できます。

（注） ハイブリッドモードは、小規模な展開の場合にのみ使用することを推奨します。大規模な展開では、キャッシング DNS と権威 DNS を別々の物理マシンまたは VM に分離することを推奨します。詳細については、 の付録の「*Authoritative DNS Capacity and Performance Guidelines*」と「*Caching DNS Capacity and Performance Guidelines*」を参照してください*Cisco Prime Network Registrar 11.1* インストール ガイド。

（注） ハイブリッドモード設定の場合は、Cisco Prime Network Registrar への SNMP クエリは、キャッシング DNS サーバーの静的値のみを受信し、権威 DNS サーバーの静的値は受信しません。

ハイブリッド モードが正しく機能するには、次の前提条件を満たしている必要があります。

- キャッシング DNS サーバーと権威 DNS サーバーの両方にローカルクラスタのライセンスを取得している必要があります。

- キャッシュ DNS サーバーと権威 DNS サーバーにはそれぞれ独自に設定された一意のネットワーク インターフェイスが必要です。別々のインターフェイスを使用できず、1 つのインターフェイスのみを使用できる場合は、ループバック インターフェイス（127.0.0.1/8, ::1/128）が権威 DNS サーバーで設定され、別のインターフェイス（たとえば、eth0、eth1、ens192 など）がキャッシュ DNS サーバーで設定されている必要があります。

前提条件を満たしたら、権威 DNS サーバーでハイブリッド モードを有効にすることができます。

ハイブリッド モードを有効にすると、サーバーは次のように動作します。

1. 権威 DNS サーバーがリロードされるたびに、キャッシュ DNS サーバーがリロードされます。
2. キャッシング DNS サーバーは権威 DNS サーバーのインターフェイスリストを読み取り、要求の送信先となる IP を検出します。
3. キャッシング DNS サーバーは、すべてのゾーン（正引き、逆引き、セカンダリ）を自動で検出し、それらのゾーンのインメモリ例外を自動で作成します。
4. キャッシング DNS サーバーは、RR TTL 値に関係なく、ハイブリッドモードの応答をキャッシュしません。これにより、クライアントに返される応答に最新の情報が反映されます。

ローカルの詳細 Web UI

ステップ 1 権威 DNS サーバーとキャッシング DNS サーバーでネットワーク インターフェイスを設定するには、次の手順を実行します。

（注） ハイブリッド モードでは、キャッシュ DNS サーバーと権威 DNS サーバーをそれぞれ独自のネットワーク インターフェイスで設定する必要があります。権威 DNS サーバーにループバック インターフェイスを使用できるのは、権威 DNS サーバーがクエリ、通知、またはゾーン転送のための直接アクセスを必要としない場合に限られます。

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。
2. [サーバーの管理（Manage Servers）] ペインの **[DNS]** をクリックして、[ローカルDNSサーバーの編集（Edit Local DNS Server）] ページを開きます。
3. **[ネットワーク インターフェイス（Network Interfaces）]** タブをクリックし、DNS に使用可能なネットワーク インターフェイスを設定します。

   （注） ループバック インターフェイス（127.0.0.1/8, ::1/128）は、DNS ハイブリッド モードの権威 DNS サーバーで設定する必要があります。

4. [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。
5. **[ネットワーク インターフェイス（Network Interfaces）]** タブをクリックし、キャッシュ DNS サーバーに使用可能なネットワーク インターフェイスを設定します。

ステップ 2 権威 DNS サーバーでハイブリッドモードを有効にするには、次の手順を実行します。

1. [展開（Deploy）] メニューの [DNS] サブメニューから [DNS サーバー（DNS Server）] を選択して [DNS 権威サーバーの管理（Manage DNS Authoritative Server）] ページを開きます。
2. [ハイブリッドモード（Hybrid Mode）] セクションで利用可能な *hybrid-mode* および *hybrid-use-adns-addrs* 属性を有効にします。
   - Hybrid Mode（*hybrid-mode*）属性に、**enabled** オプションを選択します。
   - Hybrid Use ADNS Addresses（*hybrid-use-adns-addrs*）属性に **true** オプションを選択します。

（注） *hybrid-use-adns-addrs* 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、ハイブリッドの例外を設定して、*hybrid-adns-addrs* 経由で権威 DNS サーバーに転送します。*hybrid-adns-addrs* 属性のデフォルトは、ハイブリッド DNS 通信の推奨インターフェイスであるループバックアドレス（127.0.0.1）です。*hybrid-use-adns-addrs* 属性が無効になっている場合、キャッシング DNS サーバーは権威 DNS サーバーのすべての設定済みネットワークインターフェイスを使用します。

hybrid-adns-addrs 属性は、ハイブリッドモード通信に使用する 1 つ以上の IP アドレスのリストを指定します。これらのアドレスは、権威 DNS サーバーの設定済みインターフェイスのうち、1 つ以上のインターフェイスと一致する必要があります。デフォルトのループバックアドレス（127.0.0.1）以外のアドレスを使用する場合は、キャッシング DNS サーバーで、発信トラフィック用のインターフェイスも設定する必要があります。

ステップ 3 ハイブリッドモードの設定を有効にするには、権威 DNS サーバーをリロードします。

CLI コマンド

dns set hybrid-mode=enabled を使用して、権威 DNS サーバーでハイブリッドモードの設定を有効にします。**dns set hybrid-use-adns-addrs=true** を使用して、*hybrid-use-adns-addrs* 属性を有効にします。**dns-interface** *name* **set** *attribute=value* または **cdns-interface** *name* **set** *attribute=value* を使用して、インターフェイスを設定します。

DNS サーバーのトラブルシューティング

DNS サーバーを診断するための便利なトラブルシューティングのヒントとツール、およびパフォーマンスを向上させる方法には、次のようなものがあります。

- **Restoring a loopback zone**：ループバック ゾーンは、ホストがループバック アドレス（127.0.0.1）を名前 *localhost* に解決できるようにする逆引きゾーンです。ループバック アドレスは、ホストがネットワーク トラフィックを自己に転送できるようにするために使用されます。ループバック ゾーンは手動で設定することも、既存の BIND ゾーン ファイルからインポートすることもできます。

- **Listing the values of the DNS server attributes**：[展開（Deploy）] メニューの [DNS] サブメニューで [DNS サーバー（DNS Server）] を選択して Web UI で [DNS 権威サーバーの管理（Manage DNS Authoritative Server）] ページを開きます。CLI では **dns show** を使用します。
- **Adjusting certain attribute values that could have inherited preset values from previous releases during an upgrade**：これらのプリセット値は、現在のシステムには最適ではない可能性があり、パフォーマンスの問題を引き起こす可能性があります。新しいプリセット値を使用するには、設定を更新することを強く推奨します。例：現在の最大メモリキャッシュサイズの DNS サーバー属性（*mem-cache-size*）は、500 MB に更新されます。

  設定を保存した後、必ず DNS サーバーをリロードしてください。
- **Choosing from the DNS log settings to give you greater control over existing log messages**：Web UI の [DNS サーバーの編集（Edit DNS Server）] ページでログ設定（*server-log-settings*）属性を使用するか、または CLI で **dns set server-log-settings**=*value* を使用します。この場合、これらの 1 つまたは複数のキーワードまたは数値はカンマで区切って使用します（次の表を参照）。ログ設定を変更した場合は、サーバーを再起動します。

表 *23 : DNS* ログ設定

ログ設定	説明
activity-summary	この設定により、*activity-summary-interval* で指定された間隔で DNS 統計メッセージのロギングが有効になります。ログに記録される統計のタイプは、*activity-counter-log-settings* と *activity-summary-type* で制御できます。
config	この設定により、DNS サーバーの設定および初期化解除メッセージのロギングが有効になります。
config-detail	この設定により、詳細な設定メッセージのロギング（つまり、詳細なゾーン設定のロギング）が有効になります。
dnssec	この設定により、DNSSEC 処理に関するログ メッセージが有効になります。
host-health-check	この設定により、DNS ホストの正常性チェックに関するロギングが有効になります。
db	この設定により、データベース処理メッセージのロギングが有効になります。このフラグを有効にすると、サーバーの組み込みデータベースでのさまざまなイベントについてのインサイトが得られます。
ha	この設定により、HA DNS メッセージのロギングが有効になります。
notify	この設定により、NOTIFY 処理に関するメッセージのロギングが有効になります。

ログ設定	説明
query	この設定により、QUERY 処理に関するメッセージのロギングが有効になりました。
scavenge	この設定により、DNS スカベンジング メッセージのロギングが有効になります。
scp	この設定により、SCP メッセージ処理に関するロギングが有効になりました。
server-operations	この設定により、ソケットやインターフェイスなどに関する一般的なサーバー イベントのロギングが有効になります。
tsig	この設定により、トランザクション シグニチャ（TSIG）に関するイベントのロギングが有効になります。
update	この設定により、DNS 更新メッセージ処理のロギングが有効になります。
xfr-in	この設定により、インバウンドの完全および増分ゾーン転送のロギングが有効になります。
xfr-out	この設定により、アウトバウンドの完全および増分ゾーン転送のロギングが有効になります。

- **Using the dig utility to troubleshoot DNS Server** ：dig（domain information groper）は、DNS ネームサーバーに照会するための柔軟なツールです。DNS ルックアップを実行し、照会先ネームサーバーから返された応答を表示します。dig は柔軟で、使いやすく、出力が明確であることから、ほとんどの DNS 管理者は DNS 問題のトラブルシューティングに dig を使用します。**dig** ユーティリティのヘルプを取得するには、**dig -h** を使用するか、**man dig** を使用します。

- **Using the nslookup utility to test and confirm the DNS configuration**：このユーティリティは、インターネット ネームサーバーにクエリを送信する単純なリゾルバです。**nslookup** ユーティリティのヘルプを取得するには、このコマンドを呼び出した後に、プロンプトで **help** を入力します。意図したルックアップになるように、末尾にドットを付けた完全修飾名のみを使用してください。**nslookup** はネームサーバー自体の逆引きクエリで始まりますが、サーバーの設定のためこれを解決できない場合は失敗に終わる可能性があります。適切なサーバーを照会できるように、**server** コマンドを使用するか、コマンドラインでサーバーを指定します。**–debug** を使用するか、できれば **–d2** を使用して、応答を（**–d2** の場合は送信クエリも）ダンプするフラグを設定します。

通常 dig はコマンドラインの引数とともに使用されますが、ファイルからのルックアップ要求を読み取るためのバッチ操作モードもあります。以前のバージョンとは異なり、dig の BIND9 実装では、コマンドラインから複数のルックアップを発行できます。特定のネームサーバーに照会しない限り、dig は /etc/resolv.conf. にリスト表示されている各サーバーへの照会を試みます。コマンドラインの引数またはオプションが指定されていない場合には、dig はルート「.」

の NS クエリを実行します。dig の通常の呼び出しは dig @server name type のように表示されます。server は照会先ネームサーバーの名前または IP アドレスです。

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。