



Cisco Prime Network Registrar 11.1 キャッシュおよび権威 DNS ユーザーガイド

初版：2022年7月13日

最終更新：2023年2月14日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



目次

第 1 部 :

はじめに 15

第 1 章

ドメイン ネーム システムの概要 1

DNS の仕組み 1

DNS の概念の概要 2

ドメイン 2

ネームサーバー 5

逆引きネームサーバー 6

権威 DNS サーバーとキャッシュ DNS サーバー 7

ハイアベイラビリティ DNS 7

EDNS 7

DNS ビュー 8

第 2 章

DNS サーバー ステータス ダッシュボード 11

ダッシュボードを開く 11

表示タイプ 12

一般ステータス インジケータ 12

アラートレベルのグラフィックインジケータ 13

グラフの拡大と変換 13

凡例 13

テーブル 13

折れ線グラフ 14

面グラフ 15

その他のチャートタイプ 16

ダッシュボード要素のヘルプの取得	17
表示のカスタマイズ	17
表示の更新	18
ポーリング間隔の設定	18
表としてのグラフの表示	18
CSV形式へのエクスポート	18
含めるダッシュボード要素の選択	19
サーバー チャート タイプの設定	19

第 11 部 : **キャッシュ DNS サーバー** 23

第 3 章 **キャッシュ DNS サーバーの管理** 25

DNS キャッシュ サーバー プロパティの設定	25
一般的なキャッシュ DNS サーバープロパティの設定	26
ログ設定の指定	27
パケットロギングの有効化	27
アクティビティ サマリー設定の指定	29
アクティビティサマリーの統計	31
トップ ネーム設定の指定	43
トップネームの統計情報	44
セキュリティイベントのロギング	44
セキュリティイベントの設定	44
セキュリティイベントの統計	48
セキュリティログ	49
セキュリティイベントのリソースの監視	50
証明書の設定の指定	50
TLS 設定の指定	51
TLS 統計情報	54
HTTPS 設定の指定	54
HTTPS 統計	56
HTTP エラー コード	56

プリフェッチ タイミングの設定	57
キャッシュ TTL の設定	57
ローカル Web UI	58
CLI コマンド	58
スマートキャッシュの有効化	58
ルート ネームサーバーの定義	61
UDP ポートの動的割り当て	61
最大メモリ キャッシュ サイズの設定	61
リゾルバ設定の指定	62
ケースのランダム化除外を設定	63
ネットワーク設定の指定	64
詳細設定の指定	64
ラウンドロビンの有効化	64
DNS キャッシュのフラッシュ	65
DNS キャッシュ ポイズニングの検出と防止	66
応答しないネームサーバーの処理	67
ネットワークバッファの調整	68
DNS キャッシュ サーバー コマンドの実行	68
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	69
ローカルの詳細 Web UI	69
<hr/>	
第 4 章	キャッシュ DNS サーバーの詳細 71
フォワーダの使用	71
ローカルおよびリージョン Web UI	72
CLI コマンド	73
例外の使用	73
ローカルおよびリージョン Web UI	74
CLI コマンド	75
DNS64 の管理	76
ローカル詳細およびリージョン詳細 Web UI	76
CLI コマンド	77

DNSSEC の管理	77
ローカルの詳細 Web UI	78
CLI コマンド	78
レート制限のキャッシュ管理	78
クライアントレート制限	78
ドメインレート制限	79
レート制限の管理	80
ドメインごとの制限	81
CLI コマンド	82
DNS ビューの管理	82
同じオペレーティングシステムでのキャッシング DNS サーバーと権威 DNS サーバーの設定	83
DNS ファイアウォールの管理	83
Umbrella を使用するためのキャッシュ DNS の設定	83

第 5 章

キャッシュ DNS のメトリック	85
キャッシュ DNS の一般的なインジケータ	85
データの解釈方法	85
結果に基づくトラブルシューティング	86
DNS キャッシュアクティビティ	86
データの解釈方法	86
結果に基づくトラブルシューティング	86
DNS キャッシュ サーバーの 1 秒あたりのクエリ数	86
DNS キャッシュサーバーの再帰レート制限	86
DNS 着信クエリ	87
データの解釈方法	87
DNS クエリ応答	87
データの解釈方法	88
結果に基づくトラブルシューティング	88
DNS クエリ タイプ	88
データの解釈方法	88

DNS 再帰クエリ時間	88
データの解釈方法	89
結果に基づくトラブルシューティング	89

第 III 部 : **権威 DNS サーバー** 91

第 6 章 **権威 DNS サーバーの管理** 93

DNS サーバー プロパティの設定	93
一般的な DNS サーバー プロパティの設定	94
ログ設定の指定	95
パケットロギングの有効化	96
アクティビティ サマリー設定の指定	98
アクティビティサマリーの統計	100
トップ ネーム設定の指定	126
トップネームの統計情報	126
セキュリティイベントの設定	127
セキュリティイベントの統計	130
セキュリティログ	131
セキュリティイベントのリソースの監視	131
証明書の設定の指定	132
TLS 設定の指定	133
TLS 統計情報	135
ラウンドロビンの有効化	135
重み付けラウンドロビンの有効化	136
増分ゾーン転送の有効化 (IXFR)	137
ゾーンクエリの制限	138
NOTIFY の有効化	138
権威サーバーからの再帰クエリのブロック	139
ドロップ再帰クエリの統計	140
DNS 権威サーバー コマンドの実行	140
DNS サーバーのネットワーク インターフェイスの設定	141

ローカルの詳細 Web UI	141
権威 DNSSEC の管理	141
権威 DNSSEC の有効化	142
ローカルの高度な Web UI	144
CLI コマンド	144
権威 DNSSEC キーの管理	145
ローカル詳細およびリージョン詳細 Web UI	146
CLI コマンド	146
DS レコードのエクスポート	147
権威 DNS サーバーの詳細プロパティの設定	147
SOA 存続可能時間の設定	147
セカンダリ更新時間の設定	148
セカンダリ再試行時間の設定	149
セカンダリ有効期間の設定	149
ローカルおよび外部ポート番号の設定	149
悪意のある DNS クライアントの処理	150
DNS プロパティの調整	150
同じサーバーでのキャッシュ DNS と権威 DNS の実行	151
ローカルの詳細 Web UI	152
CLI コマンド	153
DNS サーバーのトラブルシューティング	153

第 7 章

DNS ホストの正常性チェック	157
DNS ホストの正常性チェックのコンフィギュレーション設定	158
ホストの正常性チェックの有効化	159
ローカルの高度な Web UI	159
CLI コマンド	159
ホストの正常性チェックの RR セットの設定	159
ローカルの詳細 Web UI	159
CLI コマンド	159
DNS ホストの正常性チェックの統計の表示	160

	ローカルの高度な Web UI	160
	CLI コマンド	161
	SRV レコードのホストヘルスチェック	162
<hr/>		
第 8 章	DNS ファイアウォールの管理	163
	DNS ファイアウォールの管理	163
	権威 DNS サーバーでの RPZ プライマリ ゾーンの設定	167
	DNS ファイアウォール ルールの設定	169
	DNS ファイアウォール ルールの優先順位の変更	170
	RPZ の TLS の有効化	171
<hr/>		
第 9 章	ハイ アベイラビリティ DNS の管理	173
	HA DNS 処理の概要	173
	ハイ アベイラビリティ DNS ペアの作成	175
	ローカルおよびリージョンの詳細 Web UI	176
	CLI コマンド	177
	HA DNS ゾーンの同期	177
	ローカルの詳細 Web UI	177
	CLI コマンド	178
	HA DNS 情報のロギングの有効化	178
	ローカル Web UI	178
	CLI コマンド	178
	HA DNS 統計の表示	178
	ローカル Web UI	178
	CLI コマンド	178
<hr/>		
第 10 章	ゾーンの管理	179
	プライマリ DNS サーバーの管理	180
	関連項目	180
	ゾーンテンプレートの作成と適用	180
	ローカル詳細およびリージョン詳細 Web UI	181

CLI コマンド	182
段階モードと同期モード	183
ローカルおよびリージョン Web UI	183
CLI コマンド	184
プライマリ正引きゾーンの設定	184
プライマリ ゾーンを作成	184
プライマリ ゾーンの編集	187
ゾーン ネームサーバー設定の確認	188
ゾーンの同期	188
ゾーンコマンド	189
ゾーンデータのインポートおよびエクスポート	189
プライマリ逆引きゾーンの設定	192
ゾーンとしての逆引きゾーンの追加	192
サブネットからの逆引きゾーンの追加	194
サーバーのゾーン カウントの取得	195
DNS 更新の有効化	195
セカンダリ サーバーの管理	195
セカンダリ正引きゾーンの追加	196
ゾーン転送の有効化	197
サブゾーンの設定	198
サブゾーン名とサーバーの選択	198
サブゾーンの作成と委任	199
サブゾーン委任の編集	200
サブゾーンの委任解除	200
ゾーン分散の管理	201
ゾーン分散マップの準備	201
ゾーン分散の作成	203
レプリカ データからのゾーン分散のプル	205
DNS ENUM ドメインの管理	206
DNS ENUM デフォルトの管理	206
DNS ENUM ドメインの追加	206

DNS ENUM 番号の追加	207
ENUM ドメインのプルとプッシュ	208
ENUM 番号のプルとプッシュ	210

第 11 章

DNS ビューの管理	213
DNS ビューの処理	213
DNS ビューで作業する際に覚えておくべき重要事項	214
DNS ビューの管理	215
ローカルおよび地域 Web UI	215
CLI コマンド	216
DNS ビューの順序変更	216
CLI コマンド	217
DNS ビューの同期	217
DNS ビューのプッシュとプル	217
ローカル クラスタへの DNS ビューのプッシュ	217
リージョン Web UI	217
CLI コマンド	218
ローカル クラスタからの DNS ビューのプル	218
リージョン Web UI	218
CLI コマンド	219

第 12 章

リソース レコードの管理	221
ゾーンのリソース レコードの管理	221
ゾーンへのリソース レコードの追加	222
ローカルおよび地域 Web UI	222
CLI コマンド	223
リソース レコードの編集	223
ゾーンからのリソース レコードの削除	223
ローカルおよび地域 Web UI	223
CLI コマンド	224
ホストのリソース レコードの管理	224

リソース レコード セットの保護	224
ローカルおよび地域 Web UI	224
リソース レコード セットの保護解除	225
CLI コマンド	225
サーバー全体でのレコードとアドレスの検索	226
ローカルの詳細 Web UI	226
ローカルの詳細 Web UI	226
CLI コマンド	227
リソース レコードのフィルタリング	227
ローカルおよびリージョン Web UI	228
CLI コマンド	228
サービス ロケーション (SRV) レコードを使用したネットワークへのサービスのアドバタイ ジング	228
NAPTR リソース レコードを使用した名前空間の名前解決	229
ローカルおよび地域 Web UI	230
CLI コマンド	230
DNS 認証局認証 (CAA) リソースレコード	230
ローカルおよび地域 Web UI	231
CLI コマンド	232
Uniform Resource Identifier (URI) リソースレコード	232
ローカルおよび地域 Web UI	233
CLI コマンド	233

第 13 章**ホストの管理 235**

ゾーンのホストの追加	235
ローカル Web UI	235
CLI コマンド	236
ホストの RR の追加	236
ローカル Web UI	236
CLI コマンド	237
ホストの編集	237

ローカル Web UI	237
CLI コマンド	237
ホストの削除	237
ローカル Web UI	237
CLI コマンド	238

第 14 章

権威 DNS のメトリック	239
DNS の一般的なインジケータ	239
データの解釈方法	239
結果に基づくトラブルシューティング	240
DNS インバウンドゾーン転送	240
データの解釈方法	240
結果に基づくトラブルシューティング	240
DNS ネットワーク エラー	240
データの解釈方法	241
結果に基づくトラブルシューティング	241
DNS アウトバウンドゾーン転送	241
データの解釈方法	241
結果に基づくトラブルシューティング	241
1 秒あたりの DNS クエリ数	242
DNS 関連サーバー エラー	242
データの解釈方法	242
結果に基づくトラブルシューティング	242

付録 A :	リソース レコード	243
	リソース レコード	243

付録 B :	Cisco Prime Network Registrar を使用した DNS エニーキャスト	261
	DNS エニーキャストの基本要件	261
	エニーキャストルーティング	262
	FRRouting	262
	Quagga	263

Script	263
ルータ設定	264
BGP を使用したエニーキャスト設定の例	264
ネットワーク ルータ設定	265
DNS サーバーでの FRRouting の設定	266
デーモンファイルで zebra と bgpd を有効にする	266
FRR Zebra 設定	267
FRR BGP 設定	267
FRR サービスの開始	268
FRR サービスの再起動	268
DNS サーバーでの Quagga の設定	268
Quagga Zebra の設定	268
Quagga BGP の設定	269
BGP デーモンの開始	269
ルータでの診断の実行	269
BGP トラフィック ログのモニター	270
DNS ゾーンの設定	271

付録 C :	DNS のセキュリティと攻撃の防止	273
	Cisco Prime Network Registrar での DNS 攻撃の防止	273



第 1 部

はじめに

- [ドメイン 名前 システムの概要 \(1 ページ\)](#)
- [DNS サーバー ステータス ダッシュボード \(11 ページ\)](#)



第 1 章

ドメインネームシステムの概要

ドメインネームシステム (DNS) は増加するインターネットユーザーに対応しています。DNS は `www.cisco.com` などの名前を `192.168.40.0` などの IP アドレス (または拡張 IPv6 アドレス) に変換して、コンピュータが互いに通信できるようにします。DNS は、World Wide Web などのインターネットアプリケーションを使いやすくします。このプロセスは、友人や親戚に電話をかける時に、相手の電話番号を覚えていなくても、相手の名前を使って自動的にダイヤルすることができます。

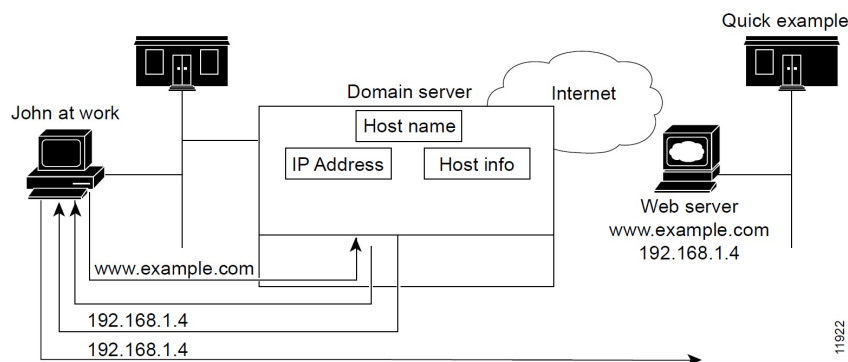
- [DNS の仕組み \(1 ページ\)](#)
- [DNS の概念の概要 \(2 ページ\)](#)

DNS の仕組み

DNS の仕組みを理解するために、ユーザーの典型である John が自分のコンピュータにログインしていると仮定してください。John は ExampleCo 社の Web サイトを表示するために Web ブラウザを起動します (以下の図を参照)。Web サイト名 `http://www.example.com` を入力します。次のアクションを実行します。

1. John のワークステーションは、`www.example.com` の IP アドレスに関する要求を DNS サーバーに送信します。
2. DNS サーバーがデータベースをチェックして、`www.example.com` が `192.168.1.4` に対応していることを確認します。
3. サーバーは、このアドレスを John のブラウザに返します。
4. ブラウザは、このアドレスを使用して Web サイトを見つけてみます。
5. John のモニターのブラウザにこの Web サイトが表示されます。

図 1: ドメイン名とアドレス



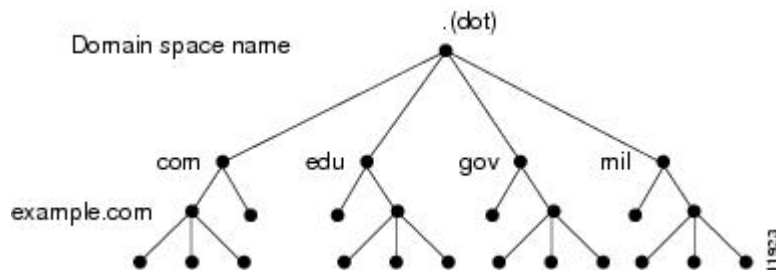
DNS の概念の概要

ここでは、DNS に関する概念について説明します。

ドメイン

John は、DNS サーバーが `www.example.com` の IP アドレスを認識しているため、ExampleCo の Web サイトにアクセスできます。サーバーは、ドメイン名前空間を検索してアドレスを学習しました。DNS はツリー構造として設計されており、各ネームドメインはツリー内のノードです。ツリーの最上位のノードは DNS ルートドメイン (.) です。その下に `.com`、`.edu`、`.gov`、`.mil` といったサブドメインがあります (以下の図を参照)。

図 2: DNS 階層

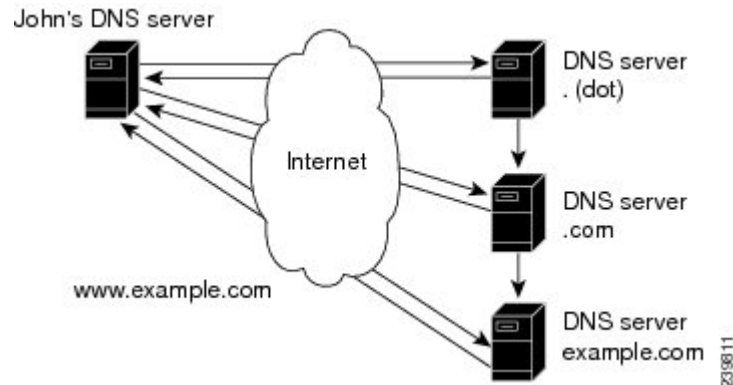


完全修飾ドメイン名 (FQDN) は、ルートに戻るすべてのネットワークドメインのドット区切りの文字列です。この名前は、インターネット上のホストごとに一意です。ドメイン例の FQDN、`example.com.` の場合は、ドメインは `example`、親ドメインは `.com`、ルートドメインは「。」(ドット)です。

ExampleCo アドレスの調査

John のワークステーションが Web サイト `www.example.com` の IP アドレスを要求した場合 (以下の図を参照) :

図 3: DNS 階層名の検索



1. ローカル DNS サーバーがデータベース内で `www.example.com` ドメインを検索しますが、そのドメインを見つけることができません。これは、このサーバーがこのドメインに対する権威ではないことを意味しています。
2. このサーバーは権威ルートネームサーバーに最上位レベル（ルート）ドメイン「.」（ドット）を要求します。
3. ルートネームサーバーは、サブドメインを認識している `.com` ドメインのネームサーバーにクエリを送信します。
4. `.com` ネームサーバーは、`example.com` がサブドメインの 1 つであることを確認して、そのサーバーアドレスで応答します。
5. ローカルサーバーは、`example.com` ネームサーバーに `www.example.com` のロケーションを要求します。
6. `example.com` ネームサーバーは、そのアドレスが `192.168.1.4` であると応答します。
7. ローカルサーバーは、このアドレスを John の Web ブラウザに送信します。

ドメインの確立

ExampleCo には John が到達できる Web サイトがあります。ExampleCo のドメインが認定ドメインレジストリに登録されているからです。ExampleCo は、`.com` サーバーデータベースにもドメイン名を入力し、IP アドレスの範囲を定義するネットワーク番号を要求しました。

この場合のネットワーク番号は `192.168.1.0` です。これには、`192.168.1.1` ~ `192.168.1.254` の範囲内の割り当て可能なホストがすべて含まれています。各アドレスフィールドには、`0` ~ `255` (28) の数字のみを使用できます。これはオクテットと呼ばれます。ただし、番号 `0` ~ `255` はネットワークアドレスとブロードキャストアドレス用にそれぞれ予約されており、ホストには使用されません。

ドメインとゾーンの違い

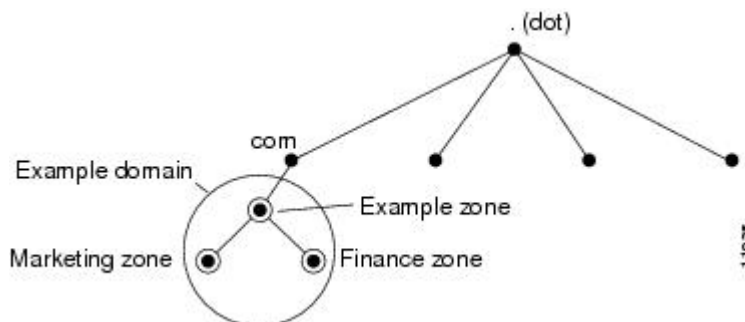
ドメイン名前空間は、DNS ツリーの委任ポイントである、ゾーンと呼ばれるエリアに分割されます。ゾーンには、他のゾーンが権威であるドメインを除いて、特定のポイント以下のすべてのドメインが含まれます。

大抵のゾーンには権威ネームサーバーがあります（複数あることが多い）。組織内で多くのネームサーバーを使用できますが、インターネットクライアントはルートネームサーバーが認識しているネームサーバーのみをクエリできます。他のネームサーバーは、内部クエリだけに応答します。

ExampleCo 社はドメイン `example.com` を登録しました。`example.com`、`marketing.example.com`、`finance.example.com` という 3 つのゾーンを確立しました。ExampleCo は社内のマーケティンググループと財務グループの DNS サーバーに `marketing.example.com` と `finance.example.com` の権限を委任しました。`marketing.example.com` のホストについて `example.com` にクエリすると、`example.com` はそのクエリを `marketing.example.com` ネームサーバーに送信します。

次の図では、ドメイン `example.com` に 3 つのゾーンが含まれています。`example.com` ゾーンは自己に対する権威でしかありません。

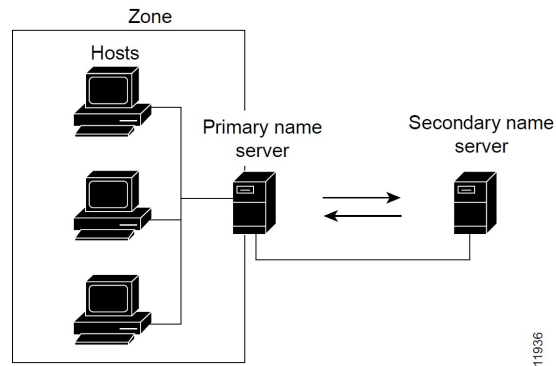
図 4: 委任されたサブドメインを含む `example.com`



ExampleCo にはサブドメインに権限を委任しないという選択肢もありました。その場合には、`example.com` ドメインはマーケティングと財務のサブドメインに対して権威のあるゾーンです。`example.com` サーバーは、マーケティングと財務に関するすべての外部クエリに応答します。

Cisco Prime Network Registrar を使用してゾーンの設定を開始する際には、ゾーンごとにネームサーバーを設定する必要があります。各ゾーンには 1 台のプライマリサーバーがあり、そのサーバーがローカルコンフィギュレーションデータベースからゾーンコンテンツをロードします。各ゾーンには、任意の数のセカンダリサーバーを含めることができます。セカンダリサーバーはプライマリサーバーからデータを取得して、ゾーンコンテンツをロードします。次の図は、セカンダリサーバーが 1 台である場合の構成を示しています。

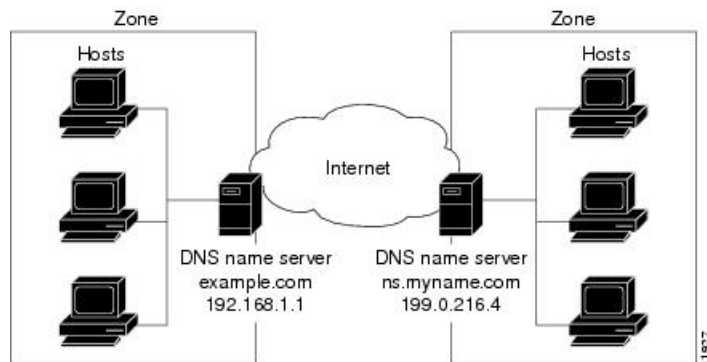
図 5: ゾーンのプライマリ サーバーとセカンダリ サーバー



ネームサーバー

DNS は、クライアント/サーバー モデルに基づいています。このモデルでは、ネームサーバーは DNS データベースの一部に関するデータを保存し、ネットワーク上のネームサーバーに照会するクライアントにそのデータを提供します。ネームサーバーは、物理ホスト上で実行されるプログラムであり、ゾーンデータを保存します。ドメインの管理者は、ゾーン内のホストを記述するすべてのリソースレコード (RR) のデータベースを使用してネームサーバーをセットアップします (下図を参照)。

図 6: クライアント/サーバー名の解決



DNS サーバーは、名前をアドレスに変換するか、名前を解決します。これらのサーバーは FQDN の情報を解釈してそのアドレスを見つけます。

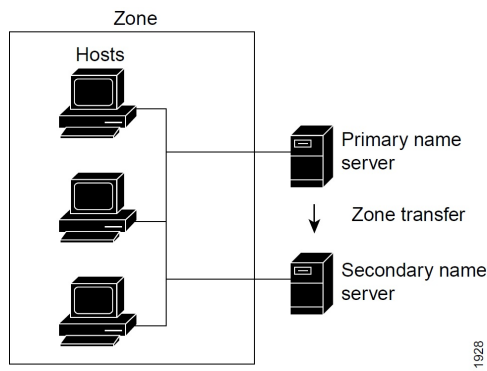
各ゾーンには、ローカル データベースからゾーン コンテンツをロードする 1 台のプライマリ ネームサーバーと、プライマリ サーバーからのデータのコピーをロードする多数のセカンダリ サーバーが必要です (以下の図を参照)。プライマリ サーバーからセカンダリ サーバーを更新するこのプロセスは、ゾーン転送と呼ばれます。

セカンダリ ネームサーバーはプライマリ サーバーへのバックアップとして機能しますが、両方のタイプのサーバーがゾーンに対する権威を持っています。両方とも、クエリへの応答時に得た情報からではなく、ゾーンの権威データベースからゾーン内のホスト名を認識します。クライアントは、両方のサーバーに対して名前の解決を照会できます。

DNS サーバー機能が拡張されて、許可用とキャッシュ用に個別の DNS サーバーが提供されるようになりました。

Cisco Prime Network Registrar DNS ネームサーバーを設定する際には、ゾーンに対するサーバーのロール（プライマリまたはセカンダリ）を指定します。サーバーのタイプは、そのロールのコンテキストでのみ意味があります。権威 DNS サーバーは、ゾーンのプライマリサーバーまたはセカンダリサーバーにのみすることができ、キャッシングサーバーのゾーンは指定しません。

図 7: DNS ゾーン転送



設定方法：

- プライマリ ネームサーバーの設定については、「[プライマリ DNS サーバーの管理 \(180 ページ\)](#)」を参照してください。
- セカンダリ ネームサーバーの設定については、「[セカンダリ サーバーの管理 \(195 ページ\)](#)」を参照してください。

逆引きネームサーバー

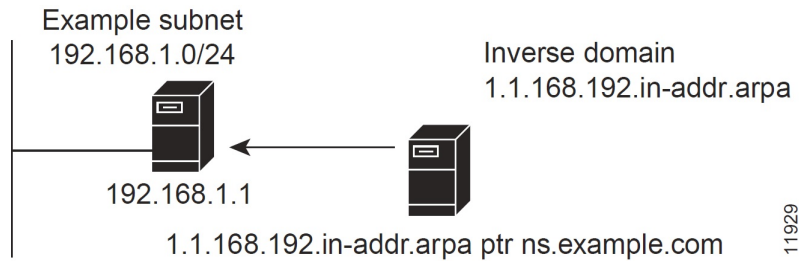
これまで説明した DNS サーバーは、名前からアドレスへの解決を実行します。これは、データベース内で正しいアドレスを検索することで簡単に実行できます。すべてのデータが名前インデックス化されるためです。ただし、特定の出力（コンピュータ ログ ファイルなど）を解釈できるように、アドレスから名前への解決が必要な場合があります。

アドレスのみがわかっている場合にドメイン名を検索するには、名前空間全体を検索する必要があります。DNS は、アドレスを名前として使用するドメイン名前空間（in-addr.arpa または .arpa ドメイン）をサポートすることで、この問題を解決します。この逆引きゾーンには、ネットワーク番号に基づく各ネットワークのサブドメインが含まれます。整合性と自然なグループ化を実現するために、ホスト番号の 4 つのオクテットが逆順に並べられます。

IP アドレスをドメイン名として読み取ると、その名前はリーフからルートという逆順に表示されます。たとえば、ExampleCo ネットワークサブネットは 192.168.1.0/24 です。その逆引きゾーンは 1.168.192.in-addr.arpa. です。DNS サーバーアドレス（192.168.1.1）のみがわかっている場合は、逆ドメインへのクエリによって、example.com にマッピングされるホスト エントリ 1.1.168.192.in-addr.arpa を得られます。

逆ドメインは、次の図に示すように、ポインタ（PTR）RR によって処理されます。

図 8: 逆ドメイン



権威 DNS サーバーとキャッシュ DNS サーバー

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。権威サーバーは、権威ゾーンデータを保持し、自己の権威が及ぶクエリにのみ応答します。キャッシュサーバーは、再帰/キャッシュサーバーであり、権威ゾーンデータを含みません。

ハイアベイラビリティ DNS

ゾーンごとに1つのプライマリ DNS サーバーしか存在できないため、このサーバーに障害が発生すると、ゾーンデータを更新できなくなります。これらの更新は、プライマリ DNS サーバーでのみ発生する可能性があります。DNS リソースレコードを更新するソフトウェア (DHCP サーバーなど) は、更新をプライマリサーバーに直接送信する必要があります。2つ目のプライマリサーバーは、メインのプライマリサーバーをシャドウイングするホットスタンバイにすることができます。これはハイアベイラビリティ (HA) DNS と呼ばれます。

EDNS

User Datagram Protocol (UDP) を介して 512 バイトを超える DNS メッセージを送信するには、拡張 DNS (EDNS) という DNS プロトコルの拡張を使用する必要があります。EDNS プロトコルは、DNS プロトコルで使用可能なフラグ、ラベルタイプ、および戻りコードの数を増やします。RFC 6891 で定められている EDNS のバージョンは EDNS0 と呼ばれています。EDNS は OPT リソースレコード (OPT RR) という疑似リソースレコードを使用します。OPT RR は通常の DNS と EDNS を区別します。OPT RR は DNS クライアントとサーバーの間のルート伝送にのみ出現します。キャッシュされたり、ディスクに保存されたりすることはありません。DNS クライアントは、EDNS0 OPT RR がより大きな UDP 応答を受け入れることを示す責任があります。

権威サーバーとキャッシング DNS サーバーは、EDNS0 拡張をサポートします。DNS サーバーの UDP ペイロードサイズを変更できます。DNS サーバーの最小 UDP ペイロードサイズは 512 バイトです。UDP パケットの最大サイズは 64 KB です。DNS サーバーのデフォルトサイズは 1,232 KB です。また、DNS サーバーは UDP 応答を 1232 に制限します。



- (注) DNS サーバーは、EDNS0 をサポートしていないクライアントからの要求を処理できますが、EDNS0 をサポートしていないクライアントからの要求を処理するときに拡張機能は使用できません。クライアント要求に対する応答は、デフォルトの 512 バイトのメッセージに挿入されます。クライアントは、クエリに OPT RR を含めることによって、EDNS をサポートしていることを示している場合があります。サーバーが EDNS をサポートしていない場合（またはサポートが無効になっている場合）、サーバーは FORMERR を返し、クライアントは EDNS を使用せずに再試行します。クライアントが報告したサイズ（EDNS 使用またはデフォルトの 512 バイト）を超える応答の場合は、サーバーは結果を省略としてマークし、クライアントは TCP を使用して再試行できます。



- (注) IP フラグメンテーションは、特に大規模な DNS メッセージが発生した場合に、インターネット上で問題となります。フラグメンテーションが動作している場合でも、DNS に十分なセキュリティが確保されていない可能性があります。これらの問題は、次のいずれかの方法で修正できます。a) EDNS バッファ サイズを低く設定して、IP フラグメンテーションのリスクを軽減する、b) DNS 応答が大きすぎて制限したバッファ サイズでは修正できない場合、DNS を UDP から TCP に切り替える。キャッシング DNS サーバーと権威 DNS サーバーのデフォルト EDNS バッファ サイズは、どちらも 1232 バイトです。

EDNS バッファ サイズを設定するには、次のコマンドを使用します。

権威 DNS サーバー：

```
nrcmd> session set visibility=3
nrcmd> dns set edns-max-payload=2000
nrcmd> dns reload
```

キャッシュ DNS サーバー：

```
nrcmd> session set visibility=3
nrcmd> cdns set edns-buffer-size=2000
nrcmd> cdns set max-udp-size=2000
nrcmd> cdns reload
```

DNS ビュー

DNS ビューでは、単一のネームサーバーを使用してゾーンデータの代替バージョンを異なるクライアントのコミュニティに表示できます。

たとえば、example.com の DNS サーバーは、ゾーンの 2 つのビューを維持できます。内部で照会できる example.com のビューには、外部ビューに存在しない多数のホストが含まれていません。各ゾーン ビューは、ゾーンの独立したコピーとして扱われます。DNS サーバーは、ゾーンに関するクエリに応答するときに、各ビューで定義されている一致基準を使用して、クライアントの一致ゾーンを見つけます。その後、そのゾーンコンテンツに基づいてクエリに応答します。

Cisco Prime Network Registrar 11.0 以降では、ゾーンをコピーすることなく、複数のビューからゾーンを参照できます。この目的には、*alternate-view-ids* 属性を使用します。詳細については、[DNS ビューで作業する際に覚えておくべき重要事項 \(214 ページ\)](#) を参照してください。



第 2 章

DNS サーバー ステータス ダッシュボード

Web ユーザー インターフェイス(Web UI)の Cisco Prime Network レジストラーサーバー ステータスダッシュボードには、トラッキングと診断に役立つグラフ、チャート、テーブルを使用して、システム ステータスのグラフィカル ビューが表示されます。これらのダッシュボード要素は、システム情報を整理および統合された方法で伝達するように設計されており、次の項目が含まれます。

- 重要なプロトコルサーバーおよびその他のメトリック
- アラームとアラート
- データベース インベントリ
- サーバーの正常性の傾向

ダッシュボードは、ダッシュボードを表示するシステムがその目的専用であり、プロトコルサーバーを実行しているシステムとは異なる場合があるトラブルシューティングのデスクコンテキストで使用するのが最適です。ダッシュボードシステムは、プロトコルサーバーを実行しているシステムをブラウザでポイントする必要があります。

ダッシュボードインジケータは、予想される通常の使用パターンからの逸脱を考慮して解釈する必要があります。異常なスパイクやアクティビティの低下に気付いた場合は、ネットワーク上で通信障害や停電が発生して調査する必要があります。

- [ダッシュボードを開く \(11 ページ\)](#)
- [表示タイプ \(12 ページ\)](#)
- [表示のカスタマイズ \(17 ページ\)](#)
- [含めるダッシュボード要素の選択 \(19 ページ\)](#)

ダッシュボードを開く

ダッシュボード機能は、地域クラスターでも使用できます。既定では、システム メトリックチャートが提供されます。さまざまなクラスターのサーバー固有の(DHCP、DNS、およびCDNS)チャートを表示できます。これは、[チャートの選択 (Chart Selections)] ページで構成できます。

Web UI でダッシュボードを開くには、[操作 (Operate)]メニューから [ダッシュボード (Dashboard)]を選択します。

表示タイプ

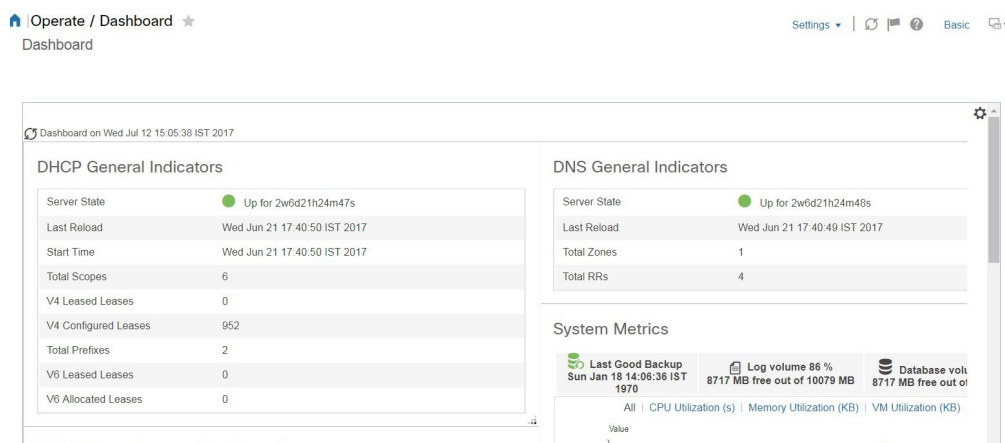
割り当てられた管理者ロールにより DNS とキャッシュ DNS の権限を持っている場合、ダッシュボードのプリセット表示は次のテーブルで構成されます（例については、次の表を参照してください）。

- **システムメトリック**：『Cisco プライムネットワーク レジストラ 11.1 管理ガイド』の「システムメトリック」の項を参照してください。
- **DNS の一般的なインジケータ**：「[キャッシュ DNS のメトリック \(85 ページ\)](#)」と「[権威 DNS のメトリック \(239 ページ\)](#)」を参照してください。



ヒント これらは、プリセットの選択です。選択できる他のダッシュボード要素については、「[含めるダッシュボード要素の選択 \(19 ページ\)](#)」を参照してください。ダッシュボードには、セッション間での選択が保持されます。

図 9: プリセットのダッシュボード要素



各ダッシュボード要素は、最初は、要素に応じて、テーブルまたは特定のパネルチャートとして表示されます。

- **表-テーブル (13 ページ)** を参照。
- **折れ線グラフ - 折れ線グラフ (14 ページ)** を参照。
- **面グラフ - 面グラフ (15 ページ)** を参照。

一般ステータス インジケータ

上の図のサーバー状態の説明の緑色のインジケータに注意してください。これは、情報を提供するサーバーが正常に機能していることを示します。黄色のインジケータは、サーバーの動作

が最適でないことを示します。赤いインジケータは、サーバーがダウンしていることを示します。これらのインジケータは、通常の Web UI の [サーバーの管理 (Manage Servers)] ページのサーバーの状態と同じです。

アラートレベルのグラフィックインジケータ

グラフ化された線とグラフの積み上げ領域は、標準の色と視覚的なコーディングに従って、主要な診断インジケータを一目ですぐに判断できます。グラフは、次の色とテキストのインジケータを使用します。

- **High alerts or warnings** — 線または赤の領域(ハッチングされたテクスチャ付き)。
- **All other indicators** — 線や様々な他の色の領域でデータ要素を区別。グラフでは、緑や黄色は使用しません。

グラフの拡大と変換

別のウィンドウでグラフを拡大するには、パネルグラフの下部にある **グラフリンク** アイコンをクリックし、次に「拡大グラフ」オプションをクリックします(下の図を参照)。拡大表示モードでは、最初に表示されるグラフの種類から別のグラフの種類を選択できます([その他のチャートタイプ \(16 ページ\)](#) を参照)。

図 10: 拡大グラフ



- (注) 拡大されたグラフの自動更新はオフになっています。最新のデータを取得するには、ページの左上にある [ダッシュボード (Dashboard)] の横にある **[更新 (Refresh)]** アイコンをクリックします。

グラフを表に変換するには、「表としてグラフを表示する」の項を参照してください。表をグラフィック・グラフ形式に変換することはできません。

凡例

各グラフには、既定で色分けされた凡例が含まれています。

テーブル

テーブルとして表示されるダッシュボード要素には、行と列にデータが表示されます。以下のダッシュボード要素は、あらかじめ設定されており、テーブルで構成されます(または含める)。

- DHCP DNS の更新

- DHCP アドレスの現在の使用率
- DHCP の一般的なインジケータ
- DNS一般インジケータ
- DNS 一般インジケータのキャッシュ



(注) エキスパートモードでテーブルを表示すると、追加のデータが表示されることがあります。

折れ線グラフ

折れ線グラフとしてレンダリングされるダッシュボード要素には、x 軸と y 軸に対してプロットされた 1 つまたは複数の線を含めることができます。次の表では、3 種類の折れ線グラフについて説明します。

表 1: 折れ線グラフのタイプ

折れ線グラフの種類	説明	表示されるダッシュボード要素
生データ折れ線グラフ	生データに対してプロットされた線。	<ul style="list-style-type: none"> • Java 仮想マシン (JVM) メモリー使用率(エキスパート・モードのみ) • DHCP バッファ容量 • DHCP フェールオーバーステータス(2つのグラフ) • DNS ネットワーク エラー • DNS 関連サーバー のエラー
デルタ折れ線グラフ	2つの連続した生データの差に対してプロットされた線。	<ul style="list-style-type: none"> • DNS インバウンドゾーン転送 • DNS アウトバウンドゾーン転送

折れ線グラフの種類	説明	表示されるダッシュボード要素
レート折れ線グラフ	2つの連続した生データの差に対してプロットされた線は、それらの間のサンプル時間で割った。	<ul style="list-style-type: none"> • DHCP サーバー要求アクティビティ(下の画像を参照) • DHCP サーバー応答アクティビティ • DHCP 応答遅延 • DNS クエリー応答 • DNS 転送エラー



ヒント デルタまたはレートデータを示すグラフの生データを取得するには、エキスパートモードに入り、必要なチャートに移動します。パネルチャートの下にある[**チャートリンク (ChartLink)**] アイコンをクリックしてから [**データテーブル (Data Table)**] をクリックします。生データテーブルは、グラフデータテーブルの下にあります。

図 11: 折れ線グラフの例

Dashboard on Tue Nov 15 16:20:59 IST 2016

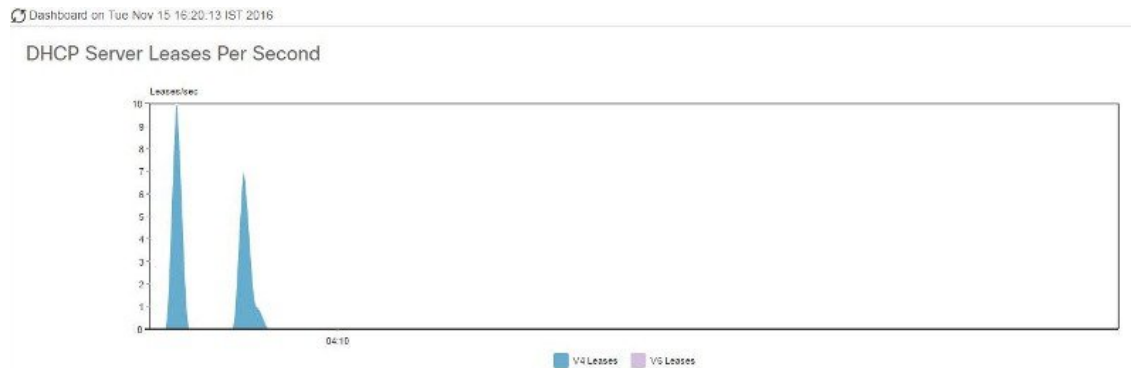
DHCP Server Leases Per Second



面グラフ

面グラフとしてレンダリングされるダッシュボード要素は、複数の関連するメトリックを傾向グラフとしてプロットしますが、一方が積み上げ、最高点が累積値を表すようにします。値は、コントラストの色で個別にシェーディングされます。(面グラフとして図 11: 折れ線グラフの例 (15 ページ) に表示される DHCP サーバー要求アクティビティ チャートの例については、次の図を参照してください)。

図 12: 面グラフの例



これらは、凡例にリストされている順序で積み重ねられ、スタックの下部に左端の凡例項目、スタックの一番上に右端の凡例項目が表示されます。面グラフに事前に設定されているダッシュボード要素は次のとおりです。

- DHCP バッファ容量
- DHCP フェールオーバーステータス
- DHCP 応答遅延
- 1 秒あたりの DHCP サーバーのリース数
- DHCP サーバー要求アクティビティ
- DHCP サーバーの応答アクティビティ
- DNS 受信ゾーン転送
- DNS ネットワーク エラー
- DNS 送信ゾーン転送
- 1 秒あたりの DNS クエリ
- DNS 関連サーバー エラー

その他のチャートタイプ

選択できるその他のグラフの種類は次のとおりです。

- **Line-** [折れ線グラフ \(14 ページ\)](#) で説明した折れ線グラフの 1 つ。
- **Area-** [面グラフ \(15 ページ\)](#) で説明したグラフ。
- **Column-** グラフを横方向に垂直バーで表示し、値軸をグラフの左側に表示します。
- **Scatter-** 散布図は、デカルト座標を使用して、一連のデータの通常 2 つの変数の値を表示するプロットまたは数学図の一種です。



ヒント 各グラフの種類は、異なる方法で、異なる解釈でデータを示しています。どのタイプが最適かを判断できます。

ダッシュボード要素のヘルプの取得

テーブル/グラフウィンドウのヘルプアイコンをクリックすると、各ダッシュボード要素のヘルプウィンドウを開くことができます。

表示のカスタマイズ

ダッシュボードの表示をカスタマイズするには、次の操作を行います。

- データを更新し、自動更新間隔を設定します。
- グラフを展開し、別の形式でレンダリングします。
- グラフィック グラフを表に変換します。
- データをコンマ区切り値 (CSV) 出力にダウンロードします。
- グラフの凡例を表示または非表示にします。
- サーバー グラフの種類を構成します。
- デフォルト表示にリセット

各グラフは次の機能をサポートします。

- サイズ変更
- 新しいセル位置にドラッグ アンド ドロップ
- 最小化
- クローズ

各グラフには、グラフの説明と、説明の下部にあるリンク (詳細..) をクリックすると詳細なヘルプが表示されたヘルプ アイコンが表示されます。



(注) ダッシュボード/グラフに加えられた変更は、[ダッシュボード (Dashboard)] ウィンドウで [保存 (Save)] をクリックした場合にのみ保持されます。

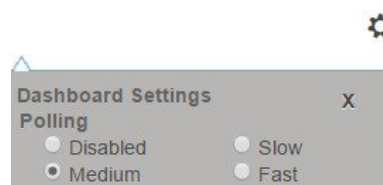
表示の更新

[最新の情報に更新 (Refresh)] アイコンをクリックして、最新のポーリングを選択するように各ディスプレイを更新します。

ポーリング間隔の設定

データのポーリング頻度を設定できます。ダッシュボード表示の右上隅の [ダッシュボード設定 (Dashboard Settings)] アイコンをクリックします。キャッシュされたデータのポーリング間隔を設定するには、4つのオプションがあり、プロトコルサーバーに更新のポーリングを行います (下の図を参照)。

図 13: グラフのポーリング間隔の設定



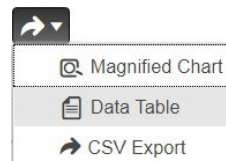
キャッシュされたデータポーリング (したがって、自動更新) 間隔を次の値に設定できます。

- **Disabled**—ポーリングを行わないため、データは自動的に更新されません。
- **Slow**—30 秒ごとにデータを更新します。
- **Medium**—20 秒ごとにデータを更新します。
- **Fast** (プリセット値) —10 秒ごとにデータを更新します。

表としてのグラフの表示

パネルグラフの下部にある [チャートリンク (Chart Link)] アイコンを使用して、チャートリンクオプションを表示します (下の図を参照)。[データテーブル (Data Table)] オプションをクリックすると、グラフィック チャートを表として表示できます。

図 14: 表形式へのグラフ変換の指定



CSV形式へのエクスポート

グラフデータは、カンマ区切り値 (CSV) ファイル (スプレッドシートなど) にダンプできます。パネルグラフの下部にあるチャートリンクコントロール (上の図を参照) で、[CSV形式でエクスポート (CSV Export)] オプションをクリックします。[名前を付けて保存 (Save As)] ウィンドウが表示され、CSV ファイルの名前と場所を指定できます。

含めるダッシュボード要素の選択

ページに表示するダッシュボードエレメントの数を決定できます。DHCPサーバーやDNSサーバーなど、1つのサーバーのアクティビティのみに集中し、他のサーバーの、他のすべてのメトリックを除外する場合があります。このように、ダッシュボードの混雑が少なくなり、要素が大きくなり、読みやすくなります。それ以外の場合は、すべてのサーバーアクティビティの概要を表示し、結果として小さな要素を表示する場合があります。

[ダッシュボードの設定 (Dashboard Settings)] アイコンをクリックし、[ダッシュボードの設定 (Dashboard Settings)] ダイアログの [チャート選択 (Chart Selection)] をクリックすると、メインの [ダッシュボード (Dashboard)] ページから表示するダッシュボード要素を選択できます。リンクをクリックすると、[チャートの選択 (Chart Selection)] ページが開きます (図 15: [ダッシュボード要素の選択 \(20 ページ\)](#) を参照)。

サーバー チャート タイプの設定

メインダッシュボードビューでデフォルトのグラフタイプを設定できます。ダッシュボードのサーバー・グラフをカスタマイズして、特定のグラフ・タイプのみをデフォルトとして表示できます。

既定のグラフの種類を設定するには、表示するメトリック ス グラフに対応するチェック ボックスをオンにし、**Type** ドロップダウンリストからグラフの種類を選択します。既定のグラフの種類は、さまざまなユーザーセッション間で一貫性があり、共有されます (下の図を参照)。

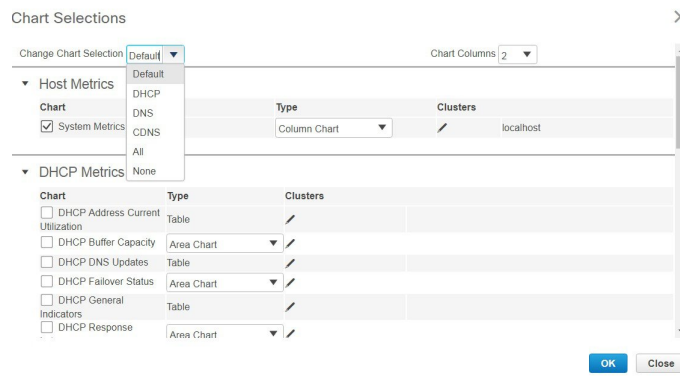


(注) サーバーで構成されたサービスに基づいて、[ダッシュボードの設定 (Dashboard Settings)] > [グラフの選択 (Chart Selection)] ページで CDNS または DNS メトリックを確認できます。



ヒント ダッシュボード要素がグラフの選択リストに表示される順序は、必ずしもページ上での要素の表示順序を決定するものではありません。使用可能な領域を考慮するアルゴリズムによって、グリッドレイアウトの順序とサイズが決まります。ダッシュボード要素の選択を送信するたびにレイアウトが異なる場合があります。選択を変更するには、表示するダッシュボード要素の横にあるチェックボックスをオンにします。

図 15: ダッシュボード要素の選択



上の図は、リージョン Web UI のグラフ選択テーブルを表示します。[クラスター (Clusters)] 列は、リージョンダッシュボードでのみ使用でき、構成されているローカルクラスターの一覧が表示されます。ローカルクラスターを追加するには、[編集 (Edit)] アイコンをクリックし、[ローカルクラスターリスト (Local Cluster List)] ダイアログボックスでローカルクラスター名を選択します。

選択を変更するには、表示するダッシュボード要素の横にあるチェックボックスをオンにします。

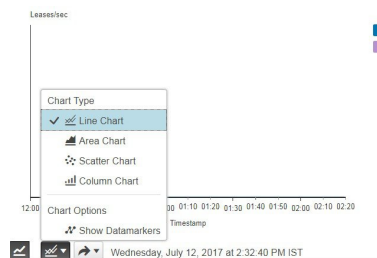
ページの上部にある [チャート選択の変更 (Change Chart Selection)] ドロップダウンリストで特定のグループコントロールを使用できます (上の図を参照)。その内容は：

- すべてのチェックボックスをオフにするには、[なし (None)] を選択します。
- プリセットの選択に戻すには、[デフォルト (Default)] を選択します。DHCP および DNS をサポートする管理者ロール用の事前設定されたダッシュボード要素は次のとおりです。
 - ホストメトリック: システムメトリック
 - DHCP メトリック: 一般的なインジケーター
 - DNS メトリック: 一般的なインジケーター
- DHCP メトリックのみを選択し、**DHCP** を選択します (『Cisco Prime Network Registrar 11.1 DHCP User Guide』の「DHCP Metrics」の項を参照)。
- DNS メトリックのみを選択し、**DNS** を選択します (『Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide』の「Authoritative DNS Metrics」の項を参照)。
- DNS メトリックのみを選択し、**CDNS** を選択します (『Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide』の「Caching DNS Metrics」の項を参照)。
- すべてのダッシュボード要素を選択するには、[すべて (All)] を選択します。

ページの下部にある [OK] をクリックして選択内容を保存するか、または [キャンセル (Cancel)] をクリックして、変更をキャンセルします。

グラフの種類を変更するには、パネルチャートの下部にある [グラフの種類 (Chart Type)] アイコンをクリックし、必要なグラフの種類を選択します (下の図を参照)。使用できるグラフには、折れ線グラフ、棒グラフ、面グラフ、散布図があります。

図 16: グラフの種類の選択





第 II 部

キャッシュ DNS サーバー

- [キャッシュ DNS サーバーの管理 \(25 ページ\)](#)
- [キャッシュ DNS サーバーの詳細 \(71 ページ\)](#)
- [キャッシュ DNS のメトリック \(85 ページ\)](#)



第 3 章

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 \(1 ページ\)](#) 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 \(25 ページ\)](#)
- [DNS キャッシュ サーバー コマンドの実行 \(68 ページ\)](#)
- [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 \(69 ページ\)](#)

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 \(26 ページ\)](#)」を参照
- ログ設定：「[ログ設定の指定 \(27 ページ\)](#)」を参照
- パケットロギング：「[パケットロギングの有効化 \(27 ページ\)](#)」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 \(29 ページ\)](#)」を参照
- トップネームの設定：「[トップネーム設定の指定 \(43 ページ\)](#)」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 \(44 ページ\)](#)」を参照
- 証明書の設定：「[証明書の設定の指定 \(50 ページ\)](#)」を参照
- TLS の設定：「[TLS 設定の指定 \(51 ページ\)](#)」を参照
- HTTPS 設定：「[HTTPS 設定の指定 \(54 ページ\)](#)」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 \(57 ページ\)](#)」を参照
- キャッシュ TTL：「[キャッシュ TTL の設定 \(57 ページ\)](#)」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（58 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（61 ページ）](#)」を参照
- UDP ポート：「[UDP ポートの動的割り当て（61 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（61 ページ）](#)」を参照
- リゾルバの設定：「[リゾルバ設定の指定（62 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（64 ページ）](#)」を参照
- 詳細設定：「[詳細設定の指定（64 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（65 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（66 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（67 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（25 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 2: 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 (<i>packet-logging</i>)	<p>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、<i>packet-log-settings</i> 属性で制御できます。</p> <ul style="list-style-type: none"> • 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。 <p>(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。</p> <p>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。</p>
パケットロギング ファイル (<i>packet-logging-file</i>)	<p>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。</p> <ul style="list-style-type: none"> • cdns : パケットロギングメッセージは標準 CDNS ログファイル (<i>cdns_log *</i>) 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 (<i>cdns_query_log *</i>) に記録されます。
パケットロギング 設定 (<i>packet-log-settings</i>)	<p>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、<i>packet-logging</i> 属性を設定します。</p> <ul style="list-style-type: none"> • 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 \(31 ページ\)](#) を参照してください。
- **firewall** : DNS ファイアウォ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 \(32 ページ\)](#) 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 \(33 ページ\)](#) 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 \(33 ページ\)](#) 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 \(35 ページ\)](#) 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 \(36 ページ\)](#) 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 \(37 ページ\)](#) 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 \(38 ページ\)](#) 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 \(40 ページ\)](#) 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 \(41 ページ\)](#) 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 \(41 ページ\)](#) 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 \(42 ページ\)](#) 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 3: 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 4: 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 5: 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)。 <i>rrset-cache-size</i> 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)。 <i>msg-cache-size</i> 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 6: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 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 7: 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 8: 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 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 9: 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	再帰応答を待つキューに入れられた要求の合計数。
user-queries	requestlist-total-user	再帰応答を待つキューに入れられたユーザー要求の合計数。
system-queries	requestlist-total-system	再帰応答を待つ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 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 10: 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 11: 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 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:
contrack-max=number, contrack-count=number, contrack-usage=number
```

表 12: システム統計

アクティビティサマリー名	説明
contrack-max	許可される接続トラッキングエントリの最大数。
contrack-count	現在使用されている接続トラッキングエントリの数。
contrack-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 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 ¹⁰	説明
interval	該当なし	データ収集期間の長さ。CDNS <i>top-names-max-age</i> 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 *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 14: 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 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 \(167 ページ\)](#) 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があります。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 15: 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 (<code>security-event-logging</code>)	<code>security-event-log-settings</code> 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、 <code>cdns_security_log</code> ファイルに書き込まれます。 <code>security-event-logging</code> および <code>security-event-log-settings</code> 設定の変更は、CDNS サーバーのリロードを必要とせず、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 (<i>security-event-log-settings</i>)	<p>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 <code>cdns_security_log</code> 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、<i>log-settings</i> 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。<i>security-event-logging</i> および <i>security-event-log-settings</i> 設定の変更は、CDNS サーバーのリロードを必要とせずすぐに有効になることに注意してください。</p> <ul style="list-style-type: none"> • 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、<i>packet-inspection</i> 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、アンブ攻撃を示している可能性があります。 <p>デフォルト設定は、<i>configuration</i>、<i>dnssec</i>、<i>packet-inspection</i>、<i>rate-limit</i>、および <i>cisco-umbrella</i> です</p>

属性	説明
セキュリティイベントアラームの設定 (<i>security-event-alarm-settings</i>)	<p>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。<i>security-event-alarm-settings</i> 構成の変更は、DNS サーバーのリロードを必要とせず、すぐに有効になることに注意してください。</p> <ul style="list-style-type: none"> • 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、<i>packet-inspection</i> 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 (<i>security-event-max-qname-size</i>)	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 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-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 17: キャッシング DNS サーバーの TLS 属性

属性	説明
TLS (<i>tls</i>)	<p>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 <code>cdns/tls</code> に配置し、<code>service-key</code> 属性を設定する必要があります。</p> <p>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 <code>cdns/tls</code> に配置し、<code>service-pem</code> 属性を設定する必要があります。</p> <p>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。</p>

属性	説明
TLS ポート (<i>tls-port</i>)	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 (<i>tls-upstream-cert-bundle</i>)	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、 <code><cnr.datadir>/cdns/tls</code>) にかかわらず保管します。 <code>/etc/pki/tls/certs/ca-bundle.crt</code> 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 (71 ページ) を参照)、例外 (例外の使用 (73 ページ) を参照)、およびファイアウォール (RPZ の TLS の有効化 (171 ページ) 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 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。*queries-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 18: TLS 統計属性

属性	説明
<i>queries-over-tls</i>	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。
<i>tls-errors-in</i>	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。
<i>tls-errors-out</i>	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 19: キャッシュ DNS サーバーの HTTPS 属性

属性	説明
HTTPS	<p>キャッシュ DNS の HTTPS サポートを有効または無効にします。</p> <p>DoH は、着信クエリに対してのみサポートされます。</p> <p>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。</p> <p>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 <code>cdns/tls</code> に配置し、<code>service-key</code> 属性と <code>service-pem</code> 属性を設定する必要があります。</p> <p>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 <code>cdns/tls</code> に配置し、<code>service-pem</code> 属性を設定する必要があります。</p>
HTTPS ポート (HTTPS Port) <i>(https-port)</i>	<p>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。</p>

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 20: *HTTPS* 統計属性

属性	説明
<i>queries-over-https</i>	CDNS サーバーが HTTPS 経由で受信したクエリの総数。
<i>queries-over-https-failed</i>	HTTPS エラーで失敗したクエリの総数。
<i>https-query-buffer</i>	メモリバッファの HTTPS クエリの数。
<i>https-response-buffer</i>	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 21: スマートキャッシュ属性

属性	説明
スマートキャッシュ (<i>smart-cache</i>)	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。 <i>smart-cache</i> 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。 <i>smart-cache</i> 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 (<i>smart-cache-expiration</i>)	<i>smart-cache</i> 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 (<i>smart-cache-expiration-reset</i>)	<i>smart-cache</i> が有効で、 <i>smart-cache-expiration</i> 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 (<i>smart-cache-expired-reply-ttl</i>)	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使用する TTL 値を指定します。

属性	説明
プリフェッチ (<i>prefetch</i>)	<p>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。</p> <p><i>Prefetch</i> 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。</p>



(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 \(57 ページ\)](#) 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 ヶ月まで間隔で) 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ーの数に基づいて、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

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ドイングします。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 22: リゾルバ設定の属性

属性	説明
<i>harden-glue</i>	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
<i>randomize-query-case</i>	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をチェックされます。
<i>randomize-query-case-exclusion</i>	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、 <i>randomize-query-case</i> 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、*randomize-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、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があります。

- 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、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

ビジュ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、ビジュ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。非常にビジュ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 \(65 ページ\)](#) 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。



第 4 章

キャッシュ DNS サーバーの詳細

この章では、サーバーの高度な機能のキャッシュ DNS 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 \(1 ページ\)](#) を参照してください。DNS の基本が説明されています。

- [フォワーダの使用 \(71 ページ\)](#)
- [例外の使用 \(73 ページ\)](#)
- [DNS64 の管理 \(76 ページ\)](#)
- [DNSSEC の管理 \(77 ページ\)](#)
- [レート制限のキャッシュ管理 \(78 ページ\)](#)
- [DNS ビューの管理 \(82 ページ\)](#)
- [同じオペレーティングシステムでのキャッシング DNS サーバーと権威 DNS サーバーの設定 \(83 ページ\)](#)
- [DNS ファイアウォールの管理 \(83 ページ\)](#)
- [Umbrella を使用するためのキャッシュ DNS の設定 \(83 ページ\)](#)

フォワーダの使用

転送を行うドメインを指定できます。フォワーダは、IP アドレスとオプションのポート番号のリストまたはサーバーの名前のリスト、あるいはその両方で定義されます。通常、フォワーダはインターネットまたは外部の DNS リソースにアクセスできる他の DNS キャッシングサーバーです。



(注) ホスト名ではなく IP アドレスを使用することを強く推奨します。

フォワーダを使用すると、キャッシング DNS サーバーは、転送ドメインに一致するユーザークエリを別のキャッシング DNS サーバーに転送して解決を実行します。これは、ローカルキャッシング DNS サーバーにインターネットアクセスがない（つまり、ファイアウォールの内側にある）場合に便利です。このような状況では、ローカルゾーンに対して例外を設定し、その後で、すべての外部クエリに対してルート (.) フォワーダを作成するのが一般的です。

フォワーダ名は、転送するドメインに対応します。たとえば、`example.com` クエリを転送する場合は、フォワーダの名前は `example.com` になります。



(注) IPv4 アドレスまたは IPv6 アドレス、あるいはその両方を指定できます。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。



ヒント キャッシング DNS サーバーがすべてのクエリを 1 つ以上の DNS フォワーダに転送するように強制するには、DNS ルート (.) をフォワーダ名として使用します。



(注) デフォルトでは、キャッシング DNS は AS112 および RFC1918 の逆引きゾーンへのアクセスを許可しません。これらは ローカル使用のためだけに予約されている IP アドレス範囲の逆引きゾーンです。これらのゾーンにアクセスするには、ローカルに定義されている逆引きゾーンの例外またはフォワーダを定義します。

Cisco Prime Network Registrar では、個々のフォワーダ オブジェクト レベルで TLS を有効にできます。これを行うには、**有効化** オプションを選択して `tls` 属性を有効にします。これを有効にする場合は、`tls-cert-bundle` を設定し、CA 証明書をロードする必要があります。そのようにしないと、接続を認証できません。認証局バンドルに公開キーを追加するには、フォワーダ 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
```

`tls-auth-name` は、フォワーダサーバーの認証名を示します。TLS が有効になっている場合、キャッシング DNS サーバーは、フォワーダサーバーから送信された名前の TLS 認証証明書をチェックします。

Cisco Prime Network Registrar 11.1 以降、`cisco-umbrella` 属性を使用して、フォワーダを Cisco Umbrella CDNS フォワーダとして有効化または無効化できます。これにより、キャッシュ DNS は、アップストリームの Cisco Umbrella サーバーによって検出されたセキュリティイベントをキャプチャしてログに記録できます。

ローカルおよびリージョン Web UI

次の手順でフォワーダを定義します。

ステップ 1 [設計 (Design)]メニューで、**Cache DNS** サブメニューから **[Forwarders]** を選択します。[フォワーダのリスト表示/追加 (List/Add Forwarders)]ページが開きます。

ステップ 2 [フォワーダ (**Forwarders**)]ペインの [フォワーダの追加 (**Add Forwarders**)]アイコンをクリックすると、[フォワーダの追加 (Add Forwarder)]ダイアログボックスが開きます。

ステップ 3 名前として転送するゾーンの名前を入力し、[フォワーダの追加 (**Add Forwarder**)] をクリックします。

(注) すべての外部クエリにフォワーダを使用するには、「.」という名前のフォワーダを作成します。

ステップ 4 [フォワーダの編集 (**Edit Forwarders**)] ページで、ホスト名を入力して [ホストの追加 (**Add Host**)] をクリックするか、フォワーダの IP アドレスを入力して [アドレスの追加 (**Add Address**)] をクリックします。

ステップ 5 [保存 (**Save**)] をクリックします。

CLI コマンド

- フォワーダを使用するためにネームサーバーのアドレス（またはスペースで区切ったアドレス）を指定するには、**cdns addForwarder domain [tls=on | off] [tls-auth-name=name] addr** を使用します。

tls フラグがオンの場合、サーバーは TLS を使用してネームサーバーに接続します。

tls-auth-name が指定されている場合、サーバーはネームサーバーから提供された TLS 証明書でこの名前を確認します。

cdns-forwarder name create attribute=value を使用して、キャッシング DNS フォワーダオブジェクトを作成することもできます。

- 現在のフォワーダのリストを表示するには、**cdns listForwarders** または **cdns-forwarder list** を使用します。
- フォワーダオブジェクトを変更するには、**cdns-forwarder name set attribute=value** を使用します。
- フォワーダまたはフォワーダのリストを削除するには、**cdns removeForwarder domain [addr ...]** または **cdns-forwarder name delete** を使用します。



(注) フォワーダの TLS 関連する変更を有効にするには、キャッシング DNS サーバーを再起動する必要があります。

例外の使用

キャッシング DNS サーバーが標準の解決方法で特定のドメインのネームサーバーに照会しないようにする場合は、例外を使用します。これにより、ルートネームサーバーがバイパスされ、名前解決を処理する特定のサーバー（またはサーバーのリスト）がターゲットとなります。通常、例外はローカル DNS 権威リソース（つまり、会社の社内ゾーン）にアクセスするために使用されます。

たとえば、**example.com** には、**Red** と **Blue** という 2 つの子会社があるとします。各子会社には、**.com** ドメインの下に独自のドメインがあります。**Red** のユーザーが **Blue** のリソースにア

アクセスする場合は、キャッシング DNS サーバーはルートネームサーバーからの委任に従います。

これらのクエリによって不要なトラフィックが発生します。一意のアドレスのない到達不能なプライベートネットワークを使用する外部クエリまたはサイトから内部リソースが除外されることがよくあるため、これらのクエリは失敗に終わる場合があります。

この問題は、例外によって解決します。Red の管理者は、ユーザーが到達する必要がある他のすべての `example.com` ドメインと、対応する 1 つ以上のネームサーバーを指定できます。Red のユーザーが Blue のサーバーに到達するには、Red サーバーは、ルートサーバーからの委任に従う代わりに、Blue のサーバーに照会します。

解決の例外を有効にするには、そのドメインの例外を作成し、権限ネームサーバーの IP アドレスとホスト名、またはそのどちらかを指定します。



(注) 例外には IPv4 アドレスと IPv6 アドレスの両方を含めることができます。例外を有効にするには、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。



警告 権威 DNS サーバーが非標準 DNS ポート (53 以外のポート) を使用しており、例外ゾーンにサブゾーンがある場合、ユーザーは非標準ポートを参照するサブゾーンごとに個別の例外を設定する必要があります。そうしないと、キャッシング DNS サーバーはデフォルトでサブゾーンにポート 53 を使用するため、解決に失敗します。

Cisco Prime Network Registrar では、個々の例外オブジェクトレベルで TLS を有効にできます。これを行うには、**有効化オプション**を選択して `tls` 属性を有効にします。これを有効にする場合は、`tls-cert-bundle` を設定し、CA 証明書をロードする必要があります。そのようにしないと、接続を認証できません。認証局バンドルに公開キーを追加するには、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
```

`tls-auth-name` 属性は、例外サーバーの認証名を示します。TLS が有効になっている場合、キャッシング DNS サーバーは、例外サーバーが送信した名前がある TLS 認証証明書をチェックします。

ローカルおよびリージョン Web UI

ステップ 1 [設計 (Design)]メニューで、**Cache DNS** サブメニューから **[Exceptions]** を選択します。[例外のリスト表示/追加 (List/Add Exceptions)]ページが開きます。

ステップ 2 [例外 (Exceptions)]ペインで **[例外の追加 (AddExceptions)]** アイコンをクリックすると、[例外の追加 (Add Exception)]ダイアログボックスが開きます。

- ステップ 3** [名前 (Name)]フィールドに、例外が必要なドメインまたはゾーンを入力し、[例外の追加 (AddException)]をクリックします。
- ステップ 4** [例外の編集 (Edit Exceptions)]ページで [DNS 名 (DNS Name)]フィールドにホスト名を入力し、[ホストの追加 (Add Host)]をクリックします。アドレスを指定するには、[IP アドレス (IP Address)]フィールドに IP アドレスを入力して、[アドレスの追加 (Add Address)]をクリックします。
- ステップ 5** *prime* 属性がオンになっている場合は、キャッシング DNS サーバーは現在公開されているネームサーバーをゾーンに照会して、それらを使用します。これはサーバーによるルートヒントの扱い方に似ています。
- ステップ 6** [保存 (Save)]をクリックします。

例外リストを削除するには、[例外 (Exceptions)]ペインで例外を選択し、[削除 (Delete)]アイコンをクリックします。例外にネームサーバーを追加または削除するには、[例外のリスト表示/追加 (List/Add Exceptions)]ページで例外名をクリックして、[例外の編集 (Edit Exceptions)]ページを開きます。

CLI コマンド

例外コマンドを使用するのは、キャッシング DNS サーバーがドメイン外の名前をルートネームサーバーに照会するために標準的な名前解決を使用しない場合に限りです。Network Registrar は、これらのサーバーに非再帰クエリを送信します。

- 解決の例外ドメインとサーバーの IP アドレスを追加するには、スペースで区切って、**cdns addException domain [prime=on | off] [tls=on | off] [tls-auth-name=name] [views=on | off] [addr ...]** を使用します。アドレスは、オプションのポート番号 (*addr[@port]*) またはサーバー名 (サーバー名を使用する前に解決できる必要があります) を使用した IPv4 または IPv6 にすることができます。このコマンドを使用するのは、キャッシング DNS サーバーがゾーンの標準的な名前解決を使用しないようにする場合に限りです。

tls フラグがオンの場合、サーバーは TLS を使用してネームサーバーに接続します。

tls-auth-name が指定されている場合、サーバーはネームサーバーから提供された TLS 証明書でこの名前を確認します。

cdns-exception name create attribute=value を使用して、キャッシング DNS 例外オブジェクトを作成することもできます。

- 名前の例外解決が設定されているドメインのリストを表示するには、**cdns listExceptions** または **cdns-exception** リストを使用します。
- ドメイン内のアドレスの例外解決エントリを削除するには、**cdns removeException domain [addr ...]** または **cdns-exception name delete** を使用します。個々のサーバーを指定して削除するか、例外の名前を指定して例外自体を削除できます。
- 例外オブジェクトを変更するには、**cdns-exception name set attribute=value** を使用します。



(注) 例外の TLS に関連する変更を有効にするには、キャッシング DNS サーバーを再起動する必要があります。

DNS64 の管理

NAT64 を使用した DNS64 により、IPv6 アドレスのみを持つホストが IPv4 インターネットとサーバーにアクセスできるようになります。IPv6 クライアントが AAAA レコードを照会して何も見つからない場合は、DNS64 で A レコードから AAAA レコードが合成されます。NAT64 プレフィックスの逆引きクエリも処理されます。

Cisco Prime Network Registrar では、AAAA レコード合成用の複数のプレフィックスを定義できます。



- (注)
- 複数のキャッシュ DNS サーバーで DNS64 を有効にする場合は、すべてのキャッシング DNS サーバーに同じバージョンの Cisco Prime Network Registrar がインストールされていることを確認する必要があります。
 - DNS ファイアウォールのリダイレクトも有効になっている場合は、キャッシュ DNS のリダイレクトは DNS64 の機能よりも優先されます。
 - DNS64 が有効になっている場合は、DNSSEC を有効にすることは推奨されません。DNS64 で応答がシミュレートされ、DNSSEC 検証が失敗する可能性があります。
 - DNS64 を有効にするには、対応する NAT64 サービスがネットワーク上に存在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

次の手順で DNS64 の設定項目を追加、編集、または表示します。

- ステップ 1** [設計 (Design)]メニューの **Cache DNS** サブメニューから **DNS64** を選択し、[DNS64 のリスト/追加 (List/Add DNS64)] ページを開きます。
- ステップ 2** [DNS64] ペインの **[DNS64 の追加 (Add DNS64)]** アイコンをクリックすると、[DNS64 の追加 (Add DNS64)] ダイアログボックスが開きます。
- ステップ 3** [名前 (Name)] フィールドに DNS64 の設定項目の名前を入力します。
- ステップ 4** [DNS64 の追加 (Add DNS64)] をクリックして、設定項目を保存します。[DNS64 の編集 (Edit DNS64)] ページに、編集可能な属性のリストが表示されます。
- ステップ 5** 必要に応じて、属性の値を編集します。 *priority* に対して定義された値によって、クライアントの DNS64 設定の検索順序が決まります。
- ステップ 6** [保存 (Save)] をクリックして、選択した DNS64 の設定項目を保存します。

DNS64 の設定項目を削除するには、[DNS64] ペインで DNS64 エントリを選択し、**[DNS64 の削除 (Delete DNS64)]** アイコンをクリックして、削除を確認します。

CLI コマンド

キャッシング DNS サーバーで DNS64 を作成するには、**cdns64 name create [acl-match-clients=ACL prefix=IPv6 prefix]** コマンドを使用します（シンタックスと属性の説明については、/docs ディレクトリの CLIGuide.html ファイルにある **cdns64** コマンドを参照するか、CLI で **help cdns64** を使用します）。次に例を示します。

```
nrcmd> cdns64 dns64 create
nrcmd> cdns64 dns64 set acl-match-clients=baaa::56ff:febd:3d6
```

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。プッシュおよび再利用の場合は、クラスターのリストまたは「すべて」を指定できます。

- **cdns64 <name | all > pull < ensure | replace | exact > cluster-name [-report-only | -report]**
- **cdns64 <name | all > push < ensure | replace | exact > cluster-list [-report-only | -report]**
- **cdns64 name reclaim cluster-list [-report-only | -report]**

DNSSEC の管理

DNSセキュリティ拡張機能（DNSSEC）により、サーバーは取得したすべてのリソースレコードのセキュリティステータスを確認できます。詳細モードとエキスパートモードで DNSSEC を管理できます。*dnssec* 属性で DNS 情報の検証を有効にすることができます。*domain-insecure* 属性で、セキュアでないドメイン名を定義します。ドメイン名に対する DNSSEC の信頼チェーンは無視されます。したがって、ドメイン名の上位のトラストアンカーが DS レコードでドメインをセキュアにすることはできません。このような場合に、DS レコードは無視されます。DNSSEC には、DNS ルートサーバーの信頼を確立するためのルートトラストアンカーが必要です。最初の DNSSEC ルートトラストアンカー *root.anchor* は、*.../data/cdns* ディレクトリに保存され、*auto-trust-anchor-file* 属性のデフォルト値です。トラストアンカーを追加できます。追加先は *.../data/cdns* ディレクトリと、ゾーンが RFC 5011 に準拠した自動更新をサポートしている場合は *auto-trust-anchor-file* 属性、それ以外の場合は *trust-anchor-file* 属性です。**cdnssec** コマンドで、Cisco Prime Network Registrar キャッシング DNS サーバーでの DNSSEC 処理を制御および設定します。

アグレッシブネガティブキャッシュのサイズをバイト単位で設定するには、[DNS キャッシュサーバーの管理 (Manage DNS Caching Server)] ページで *neg-cache-size* 属性を使用します。

key-cache-size 属性では、キーキャッシュのサイズをバイト単位で設定します。*prefetch-key* 属性では、DS レコードが検出された場合にキャッシング DNS サーバーが検証プロセスの初期に DNSKEY を取得する必要があるかどうかを設定します。



- (注) DNS64 が有効になっている場合は、DNSSEC を有効にすることは推奨されません。DNS64 で応答がシミュレートされ、DNSSEC 検証が失敗する可能性があります。

ローカルの詳細 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 [Caching DNSSEC] を選択して、[キャッシュ DNSSEC の管理 (Manage Caching DNSSEC)] ページを開きます。
- ステップ 2 DNSSEC 検証の有効化 (*dnssec*) 属性に対して **enabled** オプションを選択して DNSSEC 検証を有効にします。
- ステップ 3 このページには、すべてのキャッシュ DNSSEC 属性が表示されます。要件に従って属性を変更します。
- 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

- キャッシング DNS サーバーで DNSSEC を作成するには、**cdnssec create attribute=value** を使用します。DNSSEC を有効にするには、**cdnssec enable dnssec** を使用します (シンタックスと属性の説明については /docs ディレクトリの CLIGuide.html ファイルにある **cdnssec** コマンドを参照するか、または CLI の **help cdnssec** を使用します)。
- **cdns set neg-cache-size** を使用して、ネガティブ キャッシュ サイズを設定します。

レート制限のキャッシュ管理

レート制限によって、少数のクライアントで DNS サーバーが過負荷になるのを防ぐことができます。また、権威 DNS サーバーに対するアップストリーム クエリ攻撃からも保護します。レート制限機能によって、一部の DDoS 攻撃を軽減し、サーバーが少数のクライアントによって過負荷になるのを防ぐことができます。この機能により、悪意のあるトラフィックを制限することができます。

ローカル Web UI の詳細モードでレート制限を管理できます。レート制限は、クライアントレート制限とドメインレート制限という、個別に管理される 2 つの異なるカテゴリに分割されます。

クライアントレート制限

クライアントレート制限はクライアントごとの QPS に制限を課し、その制限に達すると新しいクエリがドロップされます。クライアントのレートが制限されている場合でも、一部のクエリの通過は許可できます。

[レート制限設定 (Rate Limiting Settings)] タブの *client-rate-limiting* 属性は、IP ベースのクライアントレート制限を有効にします。この設定はデフォルトで有効になっていません。*client-rate-limit-qps* 属性は、レート制限を開始する前の受信クライアント IP の最大 QPS を指定します。デフォルト値は 1000 です。*client-rate-limiting-factor* は、クライアント IP がレート制限されている場合に多数のクエリのうちの 1 つが通過できるように指定します。すべてのクラ

クライアントレート制限の属性については、次の表 23: クライアントレート制限の属性を参照してください。

[キャッシングレート制限の管理 (Manage Caching Rate Limiting)] ページの [クライアントレート制限 (Client Rate Limiting)] タブには、レートが制限されている現在のクライアントとそれらが到達している制限に関する情報が表示されます。このページの表には次の情報が表示されます。

- [クライアント (Client)] : レートが制限されたクライアント IP アドレス。
- [レートが制限された回数 (Number of times rate limited)] : クライアントのレートが制限された合計回数。

表 23: クライアントレート制限の属性

属性	説明
クライアントレート制限 (<i>client-rate-limiting</i>)	IP ベースのクライアントレート制限を有効にします。
クライアントレート制限 QPS (<i>client-rate-limiting-qps</i>)	着信 DNS クライアントのレート制限を指定します。
クライアントレート制限要因 (<i>client-rate-limiting-factor</i>)	<i>client-rate-limiting</i> が有効になっており、クライアントのレートが制限されている場合は、そのクライアントからのこの数のクエリのうちの 1 つを完了できるように指定します。
クライアントレポート最大 (<i>client-report-max-count</i>)	レートが制限されたクライアントのリスト内のエントリの最大数を指定します。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返されるか、統計に含まれるクライアントのリストに適用されます。

ドメインレート制限

ドメインレート制限は、サーバーが DNS ゾーンの権威ネームサーバーに送信する可能性のある QPS に制限を課します。ドメインのレートが制限されている場合でも、一部のクエリの通過を許可できます。

[レート制限設定 (Rate Limiting Settings)] タブの *domain-rate-limiting* 属性は、ドメインベース (ネームサーバーゾーン) のレート制限を有効にします。この設定はデフォルトで有効になっていません。*domain-rate-limit-qps* は、レート制限を開始する前のドメイン/ゾーンの最大 QPS を指定します。デフォルト値は 1000 です。*domain-rate-limiting-factor* は、ゾーンのレートが制限されている場合に、指定されたゾーンへこの多くのクエリのうちの 1 つを通過させることを指定します。すべてのドメインレート制限の属性については、次の表 24: ドメインレート制限の属性を参照してください。

[キャッシング レート制限の管理 (Manage Caching Rate Limiting)] ページの [ドメイン レート制限 (Domain Rate Limiting)] タブには、レート制限されている現在のドメインとヒットしているその制限に関する情報が表示されます。このページの表には次の情報が表示されます。

- **Domain** : レートが制限されたドメイン。
- **Rate Limit Max QPS** : レートが制限されたドメインのリストに記載する最大エントリ数。
- **Number of times rate limited** : ドメインのレートが制限された合計回数。

表 24: ドメインレート制限の属性

属性	説明
ドメインレート制限 (<i>domain-rate-limiting</i>)	ネームサーバーゾーンのレート制限を有効にします。
ドメインレート制限 QPS (<i>domain-rate-limiting-qps</i>)	ネームサーバーゾーンのレート制限を指定します。
ドメインレート制限要因 (<i>domain-rate-limiting-factor</i>)	<i>domain-rate-limiting</i> が有効になっており、ゾーンのレートが制限されている場合、指定されたゾーンへのこの数のクエリのうちの1つが完了できるように指定します。
ドメインごとの制限	<p><i>domain-rate-limiting-qps</i> 以外のレート制限を使用するドメインのリストを指定します。</p> <p>リストのエントリには次の属性があります。</p> <ul style="list-style-type: none"> • domain : このエントリが適用されるゾーン委任ポイントの名前。 • applies-to : このエントリが「domain」で指定されたゾーンにのみ適用するか、または「domain」のサブドメインで指定されたゾーンにのみ適用するか、あるいはその両方に適用するかを指定します。 • rate-limit : このエントリの対象となるゾーンに適用するレート制限。
ドメインレポート最大 (<i>domain-report-max-count</i>)	レートが制限されたドメインのリストの最大エントリ数を指定します。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返されるか、統計に含まれるドメインのリストに適用されます。

レート制限の管理

ローカル Web UI の [キャッシングレート制限の管理 (Manage Caching Rate Limiting)] ページから、クライアントレート制限とドメインレート制限の両方を管理できます。このページには、次の3つのタブがあります。

- [レート制限設定 (Rate Limiting Settings)] : それぞれのカテゴリの下にすべてのレート制限の属性を表示します。
- [ドメインレート制限 (Domain Rate Limiting)] : レートが制限されているドメインのリストを表示します。このタブには、レート制限の最大 QPS やドメインのレートが制限された回数などの情報も表示されます。
- [クライアントレート制限 (Client Rate Limiting)] : レートが制限されているクライアントのリストを表示します。このタブには、クライアントのレートが制限された回数に関する情報も含まれます。



(注) リストの長さは、Client Report Max 属性と Domain Report Max 属性によって制御されます。

ローカルの高度な Web UI

ステップ 1 [設計 (Design)] メニューの [キャッシュ DNS (Cache DNS)] サブメニューで [クライアント レート制限 (Client Rate Limiting)] を選択し、[キャッシングレート制限の管理 (Manage Caching Rate Limiting)] ページを開きます。

ステップ 2 要件に従って、[クライアントレート制限 (Client Rate Limiting)] カテゴリと [ドメインレート制限 (Domain Rate Limiting)] カテゴリの属性を変更します。

- クライアントレート制限を有効にするには、[クライアントレート制限 (Client Rate Limiting)] セクションで *client-rate-limiting* 属性を検索し、**on** オプションを選択して有効にします。
- ドメインレート制限を有効にするには、[ドメインレート制限 (Domain Rate Limiting)] セクションで *domain-rate-limiting* 属性を検索し、**on** オプションを選択して有効にします。

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。



(注) これらの変更を有効にするには、キャッシング DNS サーバーを再起動する必要があります。

ドメインごとの制限

レートを制限するドメインのリストを関連付けられたレート制限値で指定できます。これはドメインまたはそのサブドメイン、あるいはその両方に適用されます。これらのドメインは、*domain-rate-limiting-qps* 以外のレート制限を使用します。[ドメインごとの制限 (Per Domain Limit)] セクションの [追加 (Add)] ボタンを使用してドメインを追加することで、リストを指定できます。



- (注) [ドメインごとの制限 (Per Domain Limit)] を指定する場合、ドメイン名が DNS ゾーンと一致していることが重要です。

ローカルの高度な Web UI

[レート制限設定 (Rate Limiting Settings)] タブの [ドメインレート制限 (Domain Rate Limiting)] セクションで、[ドメインごとの制限 (Per Domain Limit)] の横にある [追加 (Add)] ボタンをクリックします。[ドメインの追加 (Add Domain)] ダイアログボックスで、ドメイン名 (ゾーンの名前) とレート制限値を入力し、ドメインまたはそのサブドメイン、あるいはその両方に適用するかどうかを指定します。次に、[追加 (Add)] ボタンをクリックします。[レート制限の設定 (Rate Limiting Settings)] タブで [保存 (Save)] をクリックして、変更を保存します。

CLI コマンド

- クライアントレート制限機能を有効にするには、**cdns-rate-limit enable client-rate-limiting** を使用します。
- クライアントレート制限の QPS 値を設定するには、**cdns-rate-limit set client-rate-limiting-qps=value** を使用します。次に例を示します。


```
nrcmd> cdns-rate-limit set client-rate-limiting-qps=1000
```
- ドメインレート制限の QPS 値を設定するには、**cdns-rate-limit set domain-rate-limiting-qps=value** を使用します。次に例を示します。


```
nrcmd> cdns-rate-limit set domain-rate-limiting-qps=500
```
- **cdns-rate-limit add [domain=<domain> [[applies-to]=domain | subdomain | both] [[rate-limit]=rate-limit]** を使用して、*domain-rate-limiting-list* 属性のレート制限を指定します。次に例を示します。


```
nrcmd> cdns-rate-limit add example.com both 1000
```
- *domain-rate-limiting-qps* 以外のレート制限を使用するドメインのリストを表示するには、**cdns-rate-limit list** を使用します。
- **cdns getStats rate-limit** を使用して、レート制限統計情報を取得します。

DNS ビューの管理

Cisco Prime Network Registrar キャッシング DNS サーバーは、権威 DNS サーバーの代わりに、クライアント要求を適切なビューに関連付けることができます。これを行うには、キャッシング DNS サーバーで DNS ビューを設定し、[例外の一覧/追加] ページの *uses-views* 属性を **true** に設定します。キャッシング DNS サーバーはクライアントを適切なビューにマッピングし、権威 DNS サーバーに転送されたクエリに適切なビューをタグ付けします。したがって、このような場合、ビューマッピングはキャッシング DNS サーバーによって実行されます。



- (注) キャッシング DNS サーバーはクライアントを *acl-match-clients* にのみマッピングします。*acl-match-destinations* 属性は無視されます。

DNS ビューと例外の設定は、ゾーンディストリビューションによって自動的に同期/設定されます。

DNS ビューの詳細については、[DNS ビューの管理 \(213 ページ\)](#) を参照してください。

同じオペレーティングシステムでのキャッシング DNS サーバーと権威 DNS サーバーの設定

Cisco Prime Network Registrar 10.0 以降では、キャッシング 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るため、2つの独立した仮想マシンまたは物理マシンを使用する必要ありません。DNS ファイアウォールの詳細については、「[DNS ファイアウォールの管理 \(163 ページ\)](#)」を参照してください。

DNS ファイアウォールの管理

Cisco Prime Network Registrar DNS ファイアウォールは、ネットワーク上で機能することが許可されたドメイン名、IP アドレス、およびネームサーバーを制御するメカニズムを提供します。DNS ファイアウォールの詳細については、「[DNS ファイアウォールの管理 \(163 ページ\)](#)」を参照してください。

Umbrella を使用するためのキャッシュ DNS の設定

Cisco Umbrella は、インターネット上の脅威に対する防御の最前線となります。Cisco Prime Network Registrar キャッシング DNS サーバーから Umbrella に切り替えるには、次の CLI コマンドを使用して「.」ドメインのフォワーダを作成する必要があります。

```
nrcmd> cdns-forwarder . create addr=208.67.222.222,208.67.220.220
nrcmd> cdns reload
```

設定が完了すると、Cisco Prime Network Registrar キャッシング DNS サーバーは、Cisco Umbrella にすべての解決クエリを転送します（サーバーは引き続きローカルにキャッシュされた応答で応答します）。これを DNS ファイアウォールと組み合わせて、ファイアウォールが明示的にブロックしないクエリに適用できます。

Cisco Prime Network Registrar 11.1 以降、*cisco-umbrella* 属性を使用して、フォワーダを Cisco Umbrella CDNS フォワーダとして有効化または無効化できます。次の CLI コマンドを使用することもできます。

```
nrcmd> cdns-forwarder . enable cisco-umbrella
```

Umbrella セキュリティイベントは、[セキュリティイベント (Security Events)] セクションの *security-event-log-settings* に **cisco-umbrella** が選択されている場合に記録されます。



(注) 例外は通常どおりに機能します。例外によるローカル解決は Umbrella サーバーをバイパスします。



(注) Cisco Umbrella のアドレスは次のとおりです。

- IPv4 アドレス : 208.67.222.222 and 208.67.220.220
- IPv6 アドレス : 2620:119:35::35 and 2620:119:53::53

詳細については、umbrella.cisco.com を参照してください。



第 5 章

キャッシュ DNS のメトリック

次のキャッシング DNS メトリック要素は、ダッシュボードで使用できます。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「*Server Statistics*」にある「*CDNS Statistics*」の項を参照してください。

- [キャッシュ DNS の一般的なインジケータ \(85 ページ\)](#)
- [DNS キャッシュアクティビティ \(86 ページ\)](#)
- [DNS キャッシュ サーバーの 1 秒あたりのクエリ数 \(86 ページ\)](#)
- [DNS キャッシュサーバーの再帰レート制限 \(86 ページ\)](#)
- [DNS 着信クエリ \(87 ページ\)](#)
- [DNS クエリ応答 \(87 ページ\)](#)
- [DNS クエリ タイプ \(88 ページ\)](#)
- [DNS 再帰クエリ時間 \(88 ページ\)](#)

キャッシュ DNS の一般的なインジケータ

ダッシュボード要素 [キャッシュ DNS の一般的なインジケータ (Caching DNS General Indicators)] は、サーバーの状態、最終起動時のリロード時間、およびリソース レコード (RR) の合計数を示します。この表は、[チャートの選択 (Chart Selections)] ページで **CDNS Metrics : Caching DNS General Indicators** を選択すると表示されます。

結果のテーブルに次の情報が表示されます。

- **Server State** : (統計が使用可能かどうかに基づく) アップまたはダウンと、サーバーがこの状態である期間。
- **Last Reload** : 最後のサーバー リロードからの経過時間。
- **Start Time** : サーバー プロセス (Cisco Prime Network Registrar サーバー エージェント) の最終起動日時。

データの解釈方法

このチャートのデータは、サーバー全般の正常性と稼働時間を示しています。目的はサーバーに関する決定を行うことです。たとえば、リロードのタイミングは、設定されているゾーンの数に応じて判断される場合があります。

結果に基づくトラブルシューティング

サーバーの状態が **Down** の場合は、すべての CDNS チャート インジケータに赤色のステータスボックスが表示され、データは使用できません。サーバーが停止している場合は、サーバーを再起動します。

DNS キャッシュ アクティビティ

面グラフとしてレンダリングされる [DNS キャッシング (DNS Caching)] ダッシュボードの要素は、キャッシュのヒットとキャッシュの欠落を追跡します。チャートは、[チャートの選択 (Chart Selections)] ページで [CDNS Metrics: DNS Caching Activity] を選択した場合にのみ使用できます。

結果の面グラフには、次の傾向が表示されます。

- **Cache Hits** : キャッシュから応答されたクエリの合計数。
- **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** : 実行されたプリフェッチの数。

データの解釈方法

このチャートは、再帰処理が必要なクエリの数に対してキャッシュルックアップを使用して正常に応答されたクエリの数を示します。

結果に基づくトラブルシューティング

キャッシュミスが急激に増加している場合は、CDNS ログでエラーを確認します。キャッシュミスが増加しているということは、効率よく応答するためにキャッシュされたクエリを保管するメモリ空き領域が不足している可能性があります。

DNS キャッシュ サーバーの 1 秒あたりのクエリ数

ダッシュボード要素 [DNS キャッシュ サーバーの 1 秒あたりのクエリ数 (DNS Caching Server Queries Per Second)] はチャートとしてレンダリングされ、キャッシュ DNS サーバーの 1 秒あたりのクエリ数を表示します。このチャートは、[チャートの選択 (Chart Selections)] ページで [CDNS Metrics: DNS Caching Server Queries Per Second] を選択した場合に使用できます。

DNS キャッシュサーバーの再帰レート制限

折れ線グラフとしてレンダリングされる [DNS キャッシングサーバーの再帰レート制限 (DNS Caching Server Recursion Rate Limit)] ダッシュボードの要素には、クライアントとドメインに対して制限されたクエリの数が表示されます。このチャートは、[チャートの選択 (Chart

Selections)] ページで [CDNS メトリック : DNS キャッシュサーバーの再帰レート制限 (CDNS Metrics: DNS Caching Server Recursion Rate Limit)] を選択した場合に使用できます。

生成される折れ線グラフには、次のトレンドがプロットされます。

- [クライアントのレート制限 (Client Rate Limit)] : *client-rate-limiting* が有効になっている場合に、クライアントがレート制限された回数。
- **Domain Rate Limit** : *domain-rate-limiting* が有効になっている場合に、ゾーンがレート制限された回数。

DNS 着信クエリ

面グラフとしてレンダリングされるダッシュボードの要素ごとの CDNS 着信クエリは、TCP、IPv6、DNSSEC、EDNS、およびクエリの合計数をトレースします。チャートは、[チャートの選択 (Chart Selections)] ページで [CDNS Metrics: DNS Incoming Queries] を選択した場合に使用できます。

結果の面グラフには、次の傾向が表示されます。

- **TCP** : CDNS サーバーが TCP で受信したクエリの合計数。
- **IPv6** : CDNS サーバーが IPv6 で受信したクエリの合計数。
- **EDNS** : EDNS OPT RR が存在するクエリの数。
- **DNSSEC** : DO (DNSSEC OK) ビットが設定されている EDNS OPT RR のクエリの数。
- **Total** : CDNS サーバーが受信したクエリの合計数。

データの解釈方法

このチャートは、TCP、IPv6、および DNSSEC を使用した CDNS サーバーへのクエリの数、EDNS OPT レコードが存在するクエリの数、および受信したクエリの合計数を示します。

DNS クエリ応答

面グラフとしてレンダリングされる [CDNS クエリ応答 (CDNS Query Responses)] ダッシュボードの要素は、NOERROR、NODOMAIN、No Data、Other Errors、Secure、および Unsecure の戻りコードで応答数を示します。これは、[チャートの選択 (Chart Selections)] ページで [CDNS Metrics: DNS Queries Responses] を選択した場合に表示されます。

結果の面グラフには、次の傾向が表示されます。

- **NOERROR** : NOERROR の rcode がクライアントに戻された、キャッシュまたは再帰からの応答の数。
- **NXDOMAIN** : NXDOMAIN の rcode がクライアントに戻された、キャッシュまたは再帰からの応答の数。
- **NODATA** : NODATA の疑似 rcode がクライアントに戻された応答の数。
- **Other Errors** : その他のエラー。

- **Secure** : DNSSEC によって正しく検証された応答の数。
- **Unsecure** : DNSSEC による検証に失敗した応答の数。

データの解釈方法

このグラフには以下の情報が表示されます。

- クエリに対するキャッシュまたは再帰からの戻りコード NXDOMAIN の応答の数。
- クエリに対する擬似戻りコード NODATA の応答の数。これは、実際の戻りコードが NOERROR であったが、その応答でデータが伝送されなかったことを意味します (NOERROR/NODATA 応答と呼ばれます)。これらのクエリは、NOERROR の数にも含まれています。A レコードが存在し、AAAA がない場合の AAAA ルックアップによく見られます。
- セキュリティで保護された回答の数。応答は正しく検証されました。AD ビットがこれらの応答の一部に設定されていた可能性があり、クライアントが応答の AD ビットを受け入れる準備ができたことを (クエリの DO または AD ビットで) シグナリングしました。
- 正しく検証されなかった応答の数。

通常のシナリオでは、NOERROR は成功した応答コードです。

結果に基づくトラブルシューティング

エラーが増加している場合は、CDNS サーバーの設定を確認します。

DNS クエリ タイプ

面グラフとしてレンダリングされる [DNS クエリタイプ (DNS Queries Type)] ダッシュボードの要素はタイプ別にクエリ数をトレースします。チャートは、[チャートの選択 (Chart Selections)] ページで [CDNS Metrics: DNS Queries Type] を選択した場合に使用できます。

結果の面グラフには、次の傾向が表示されます。

- **A**— 受信したクエリの数。
- **AAAA**— 受信した AAAA クエリの数。
- **CNAME**— 受信した CNAME クエリの数。

データの解釈方法

このグラフには、A、AAAA、CNAME、PTR、その他のタイプの着信クエリの数が表示されません。

DNS 再帰クエリ時間

面グラフとしてレンダリングされる [タイプ別 CDNS クエリ (CDNS Queries by Type)] ダッシュボードの要素は、再帰クエリを完了するまでの時間の平均値と、クエリを完了するまでの

時間の中央値をトレースします。この表は、[チャートの選択 (Chart Selections)] ページで [CDNS Metrics: DNS Recursive Query Time] を選択すると表示されます。

結果の面グラフには、次の傾向が表示されます。

- **Average**— 再帰クエリを完了するまでの時間の平均値。
- **Median**— 再帰クエリを完了するまでの時間の中央値。

データの解釈方法

[平均 (Average)] は、サーバーが再帰処理を必要としたクエリ応答に要した時間を示します。キャッシュから応答されたクエリは、この平均値には含まれないことに注意してください。

[中央 (Median)] は、サーバーが再帰処理を必要としたクエリ応答に要した時間の中央値を示します。中央値は、ユーザー クエリの 50% がこれよりも短い時間で応答されたことを意味します。大きな外れ値が原因で (応答しないサーバーへのクエリであることが多い)、平均値は中央値よりも大きくなる可能性があります。

結果に基づくトラブルシューティング

フォワーダとしてのネームサーバーの接続と設定を確認するか、時間の平均値と中央値の上昇について例外リストを確認します。



第 III 部

権威 DNS サーバー

- [権威 DNS サーバーの管理 \(93 ページ\)](#)
- [DNS ホストの正常性チェック \(157 ページ\)](#)
- [DNS ファイアウォールの管理 \(163 ページ\)](#)
- [ハイアベイラビリティ DNS の管理 \(173 ページ\)](#)
- [ゾーンの管理 \(179 ページ\)](#)
- [DNS ビューの管理 \(213 ページ\)](#)
- [リソースレコードの管理 \(221 ページ\)](#)
- [ホストの管理 \(235 ページ\)](#)
- [権威 DNS のメトリック \(239 ページ\)](#)



第 6 章

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 \(179 ページ\)](#)」を参照してください。

- [DNS サーバー プロパティの設定 \(93 ページ\)](#)
- [DNS 権威サーバー コマンドの実行 \(140 ページ\)](#)
- [DNS サーバーのネットワーク インターフェイスの設定 \(141 ページ\)](#)
- [権威 DNSSEC の管理 \(141 ページ\)](#)
- [権威 DNSSEC キーの管理 \(145 ページ\)](#)
- [権威 DNS サーバーの詳細プロパティの設定 \(147 ページ\)](#)
- [同じサーバーでのキャッシュ DNS と権威 DNS の実行 \(151 ページ\)](#)
- [DNS サーバーのトラブルシューティング \(153 ページ\)](#)

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 \(94 ページ\)](#)」を参照
- ログ設定：「[ログ設定の指定 \(95 ページ\)](#)」を参照
- パケットロギング：[パケットロギングの有効化 \(96 ページ\)](#) 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 \(98 ページ\)](#)」を参照
- トップネームの設定：「[トップネーム設定の指定 \(126 ページ\)](#)」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 \(127 ページ\)](#)」を参照
- 証明書の設定：「[証明書の設定の指定 \(132 ページ\)](#)」を参照
- TLS の設定：「[TLS 設定の指定 \(133 ページ\)](#)」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（135 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（136 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）（137 ページ）](#)」を参照
- ゾーンクエリの制限：「[ゾーンクエリの制限（138 ページ）](#)」を参照
- NOTIFY パケットの有効化：「[NOTIFY の有効化（138 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（139 ページ）](#) を参照

一般的な DNS サーバー プロパティの設定

サーバークラスまたはホストマシンの名前や Cisco Prime Network Registrar DNS サーバース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（93 ページ）](#)」に記載されています。

ローカル Web UI

ステップ 1 サーバード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、詳細なログ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グ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グ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グギング（つまり、詳細なゾーン設定のログギング）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グ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 メッセージのログ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グ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グ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グ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グ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グ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グ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グ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グ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グ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グ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 25: 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 (<i>packet-logging</i>)	<p>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、<i>packet-log-settings</i> 属性で制御できます。</p> <ul style="list-style-type: none"> • 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。 <p>(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。</p> <p>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。</p>
パケットロギング ファイル (<i>packet-logging-file</i>)	<p>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。</p> <ul style="list-style-type: none"> • dns : パケットロギングメッセージは標準 DNS ログファイル (<i>name_dns_1_log*</i>) 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 (<i>dns_packet_log*</i>) に記録されます。

属性	説明
パケットロギング設定 (<i>packet-log-settings</i>)	<p>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、<i>packet-logging</i> 属性を設定します。</p> <ul style="list-style-type: none"> • 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ー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 \(100 ページ\)](#) 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 \(101 ページ\)](#) 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 \(103 ページ\)](#) 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 \(105 ページ\)](#) 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 \(109 ページ\)](#) 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 \(111 ページ\)](#) 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 \(112 ページ\)](#) 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 \(113 ページ\)](#) 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 \(115 ページ\)](#) 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 \(119 ページ\)](#) 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 \(122 ページ\)](#) 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 \(123 ページ\)](#) 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 \(123 ページ\)](#) 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 26: キャッシュ統計

アクティビティサマリー名	統計 ¹²	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 (<i>mem-cache-size</i>) 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 ¹²	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ります。

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 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 27: 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 ¹³	説明
txn	RR-DB	rrdb-txn	RRDB 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 RRDB 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 ¹³	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 RRDB ログの総数を報告します。
cset-count	Cset-Queue	csetq-count	csetDB 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	CSETDB 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 ¹³	説明
writes	Cset-DB	csetdb-writes	CSETDB 書き込み操作の総数を報告します。
deletes	Cset-DB	csetdb-deletes	CSETDB 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 CSETDB 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	CSETDB 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	CSETDB 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 CSETDB ログの総数を報告します。

¹³ 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 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 28: エラー統計

アクティビティサマリー名	統計 ¹⁴	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、 <i>max-dns-packets</i> 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。

¹⁴ 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 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 29: 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 ¹⁵	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 ¹⁵	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 ¹⁵	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 ¹⁵	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 ¹⁵	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。

¹⁵ 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 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 30: 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 ¹⁶	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 ¹⁶	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 ¹⁶	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。

¹⁶ 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 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トの統計は、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 31 : IPv6 の統計情報

アクティビティサマリー名	統計 ¹⁷	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。

¹⁷ 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 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 32: 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 ¹⁸	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 <i>ha-dns-max-batch-count</i> 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、HADNS 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 ¹⁸	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	<i>tcp-max-active-connections</i> 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。

¹⁸ 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 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 サマリートの統計は、**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 33: 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 ¹⁹	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 ¹⁹	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ーの総数。
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	<i>ixfrs-full-resp</i> 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 ¹⁹	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	<i>tcp-max-active-connections</i> 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。

¹⁹ 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 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 34: 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 ²⁰	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 ²⁰	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 <i>query-types-unwanted</i> で指定します。
acl-failures	クエリ	queries-failed-acl	クエリ ACL (<i>restrict-query-acl</i>) 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	正当に回答されたクエリ数を報告します。
nxdomain	Query-Responses	query-answers-with-NXDOMAIN	そのような名前回答がないために失敗したクエリ数を報告します。
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 ²⁰	説明
refused	Query-Responses	query-answers-with-REFUSED	拒否されたクエリの数を表示します。
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表示します。
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 ²⁰	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。

²⁰ 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 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 35: 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 ²¹	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 ²¹	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	DNSSEC 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 ²¹	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。

²¹ 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 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, contrack-max=number,
contrack-count=number, contrack-usage=number
```

表 36: 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。
contrack-max	Linux ファイアウォール接続の達した最大数。
contrack-count	Linux ファイアウォール接続の現在の数。
contrack-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 37: 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 ²²	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。

²² 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 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 更新関連のカウント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 38: 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 ²³	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 ²³	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。

²³ 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 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트리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 39: 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 (<i>security-event-logging</i>)	<i>security-event-log-settings</i> 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。 <i>security-event-logging</i> および <i>security-event-log-settings</i> 設定の変更は、DNS サーバーのリロードを必要とせず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、 <i>dns_security_log</i> 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 (<i>security-event-log-settings</i>)	<p>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 <code>dns_security_log</code> ファイルに書き込まれます。この設定を有効にするには、<i>security-event-logging</i> を有効にする必要があります。<i>security-event-logging</i> および <i>security-event-log-settings</i> 設定の変更は、DNS サーバーのリロードを必要とせずすぐに有効になることに注意してください。</p> <ul style="list-style-type: none"> • 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、<i>packet-inspection</i> 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、<i>max-dns-packets</i>) 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。 <p>デフォルト設定は、<code>configuration</code>、<code>packet-inspection</code>、および <code>rate-limit</code> です。</p>

属性	説明
セキュリティ イベント アラームの設定 (<i>security-event-alarm-settings</i>)	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。 <i>security-event-alarm-settings</i> 構成の変更は、DNS サーバーのリロードを必要とせずすぐに有効になることに注意してください。 <ul style="list-style-type: none"> • 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、<i>packet-inspection</i> 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、<i>max-dns-packets</i>) 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、アンブ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 (<i>security-event-max-qname-size</i>)	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 (<i>acl-blocklist</i>)	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 (<i>tsig-processing</i>)	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、 <i>ddns</i> およびクエリ要求で有効になっています。

属性	説明
<i>gss-tsig-processing</i>	DNS トランザクションの <i>gss-tsig</i> セキュリティモードを示します。 <i>gss-tsig-processing</i> と <i>tsig-processing</i> の両方が有効になっている場合、 <i>gss-tsig</i> 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。
<i>gss-tsig-config</i>	DNS サーバーが使用する <i>gss-tsig</i> 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 40: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ワ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 \(51 ページ\)](#) 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 41: 権威 DNS サーバーの TLS 属性

属性	説明
TLS (<i>tls</i>)	<p>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 <code>dns/tls</code> に配置し、<code>service-key</code> 属性を設定する必要があります。</p> <p>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 <code>dns/tls</code> に配置し、<code>service-pem</code> 属性を設定する必要があります。</p> <p>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。</p>
TLS ポート (<i>tls-port</i>)	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 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 42: TLS 統計属性

属性	説明
<i>tls-queries</i>	DNS サーバーが TLS を介して受信したクエリの総数。
<i>tls-queries-failed</i>	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 の重み値を設定する必要があります。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、Advanced 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、およびセカンダリ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 \(138 ページ\)](#)」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-interval*、*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権威サーバーの管理 (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 \(197 ページ\)](#)」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「動的レコードのスキャベンジング」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 \(177 ページ\)](#)」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 43: 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。

属性	説明
キーロールオーバー (<i>key-rollover</i>)	リージョナルクラスまたはローカルクラスがゾーン署名キー (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 44: ゾーン署名用キーの属性

属性	説明
アルゴリズム (<i>zsk-algorithm</i>)	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 (<i>zsk-bits</i>)	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 (<i>zsk-algorithm</i>) 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 (<i>zsk-lifetime</i>)	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 <i>deactivation-date</i> を決定するために使用されます。 <i>zsk-rollover-interval</i> 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 (<i>zsk-rollover-interval</i>)	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 <i>deactivation-date</i> 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 45: キー署名用キーの属性

属性	説明
----	----

アルゴリズム (<i>ksk-algorithm</i>)	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 (<i>ksk-bits</i>)	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 (<i>ksk-algorithm</i>) 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 (<i>ksk-rollover-interval</i>)	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、CCMHA 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 46: 主要タイムライン属性

属性	説明
アクティベーション日 (<i>activation-date</i>)	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 (<i>deactivation-date</i>)	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 (<i>expiration-date</i>)	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 (<i>rollover-due-date</i>)	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 (<i>status</i>)	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せん。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 \(147 ページ\)](#)」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 \(148 ページ\)](#)」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 \(149 ページ\)](#)」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 \(150 ページ\)](#)」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、転送間隔が長くなるように、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 \(138 ページ\)](#)」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は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 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せん。
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-addr*s 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-addr*s 経由で権威 DNS サーバーに転送します。*hybrid-adns-addr*s 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-addr*s 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-addr*s 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-addr=true** を使用して、*hybrid-use-adns-addr*s 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 47: DNS ログ設定

ログ設定	説明
activity-summary	この設定により、 <i>activity-summary-interval</i> 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、 <i>activity-counter-log-settings</i> と <i>activity-summary-type</i> 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。
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。

ログ設定	説明
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グ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グ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グ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グ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 のように表示されず。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。



第 7 章

DNS ホストの正常性チェック

Cisco Prime Network Registrar 9.0 以前では、DNS は、宛先アドレスが到達可能かどうかにかかわらず、権威設定で RR を使用して A/AAAA クエリに応答します。返された IP アドレスに DNS クエリが行われた時点で到達できるかどうかはわかりません。DNS サーバーまたは DNS クライアントがこの停止を認識していない可能性があります。Cisco Prime Network Registrar 9.1 以降では、権威 DNS サーバーが ICMP エコーメッセージ (ping) を使用してアドレスに ping を実行することで、DNS 権限として動作するホストまたはホストのセットの可用性を定期的に確認できます。Cisco Prime Network Registrar 10.0 以降では、DNS ホストの正常性チェックは、ホストの可用性を確認するために UDP v4 と UDP v6 を使用する GTP-C プロトコルエコーメッセージをサポートします。使用できないことが判明したホストは、クエリ応答に含まれません。サーバーは最初のクエリに対して RR セットのすべての RR で応答します。TTL は `hhc-max-init-ttl` に設定されています。DNS サーバーは、その RR のクエリを受信した後に、RR セット内の RR に対して ping (ICMP ping または GTP-C echo ping) を送信し、後続の A/AAAA クエリには到達可能な RR で応答します。Cisco Prime Network Registrar 11.1 以降では、SRV レコードのホストヘルスチェックを有効にして、対応する A/AAAA レコードのヘルスチェックを自動的に行うことができます。



(注) `host-health-check` 属性が **ping** または **gtp-echo** に設定されているすべての RR は、定期的にモニターされます。モニターリングは、**ping** または **gtp-echo** に設定されている `host-health-check` を使用した RR の最初のクエリを受信した後に開始されます。`host-health-check` が **ping** に設定されている場合、ICMP プロトコルがモニターリングに使用されます。

この機能を活用するには、ping の対象であるシステムのデフォルトのセキュリティ設定で ping への応答が許可されている必要があります。`host-health-check` が **gtp-echo** に設定されている場合、GTP-Cv2 プロトコル (GTP-C エコー要求および応答) がモニターリングに使用されます。

- [DNS ホストの正常性チェックのコンフィギュレーション設定 \(158 ページ\)](#)
- [ホストの正常性チェックの有効化 \(159 ページ\)](#)
- [ホストの正常性チェックの RR セットの設定 \(159 ページ\)](#)
- [DNS ホストの正常性チェックの統計の表示 \(160 ページ\)](#)
- [SRV レコードのホストヘルスチェック \(162 ページ\)](#)

DNS ホストの正常性チェックのコンフィギュレーション設定

DNS ホストの正常性チェックには事前設定があり、DNS サーバーではデフォルトで無効になっています。

DNS ホストの正常性チェックを有効にするには、次の DNS サーバーレベルの属性を使用します。

表 48: DNS サーバー レベルの属性

属性	説明
ホストの正常性チェック (<i>host-health-check</i>)	DNS サーバーで DNS ホストの正常性チェックを有効または無効にします。ホストの正常性チェックが有効になっている場合は、DNS サーバーはアクティブな RR のクエリ応答の TTL として、 <i>hhc-max-ttl</i> を送信します。DNSSEC が有効になっている場合は、DNS サーバーはアクティブではない RR をクエリ応答の RR リストの末尾に追加します。DNSSEC が有効になっていない場合は、DNS サーバーはアクティブではない RR をクエリ応答の RR リストに追加しません。 <i>host-health-check</i> は、デフォルトで DNS サーバーでは無効になっています。 <i>host-health-check</i> を有効にした後に DNS サーバーをリロードします。
ホストの正常性チェック間隔 (<i>hhc-interval</i>)	RR セットの到達可能性をチェックする時間間隔 (秒単位) を指定します。
最大 TTL (<i>hhc-max-ttl</i>)	RR ヘルス ステータスがアップである場合に、クエリ応答で送信する最大 TTL (秒単位) を指定します。デフォルトでは、 <i>hhc-interval</i> の値が使用されます。 (注) RR セットの TTL が <i>hhc-interval</i> または <i>hhc-max-ttl</i> 未満である場合は、RR セットの TTL が応答に使用されます。
最大初期 TTL (<i>hhc-max-init-ttl</i>)	ホストの正常性チェック RR の初回クエリの際にクエリ応答で送信する最大初期 TTL (秒単位) を指定します。 (注) RR セットの TTL が <i>hhc-max-init-ttl</i> 未満である場合は、RR セットの TTL が応答に使用されます。

ホストの正常性チェックの有効化

DNS ホストの正常性チェックを有効にするには、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 [DNS 権威サーバーの管理 (Manage DNS Authoritative Server)] ページの [ホストの正常性チェック (Host Health Check)] セクションで、*host-health-check* 属性に **enabled** オプションを選択します。

ステップ 2 [保存 (Save)] をクリックして変更を保存し、権威 DNS サーバーをリロードします。

CLI コマンド

dns enable host-health-check を使用してホストの正常性チェックを有効にしてから、**dns reload** を使用して DNS サーバーを再起動します。



(注) DNS サーバーを再起動して、設定の変更を正常に適用します。

ホストの正常性チェックの RR セットの設定

ローカルの詳細 Web UI

[設計 (Design)] メニューの [権威 DNS (Auth DNS)] サブメニューから [正引きゾーン (Forward Zones)] を選択し、[正引きゾーンのリスト/追加 (List/Add Forward Zones)] ページを開き、[リソースレコード (Resource Records)] タブをクリックします。RR 名をクリックします。[RR セット設定 (RR Set Settings)] セクションで、[host-health-check] ドロップダウンリストから [ping] の値を選択します。RR セットでこの属性を変更しても、リロードは必要ありません。



(注) ゾーンで DNSSEC が有効になっている場合は、DNS サーバーはアクティブではない RR をクエリ応答の RR リストの最後に追加します。

CLI コマンド

rrSet コマンドは、*rr-name* のリソースレコードに *host-health-check* フラグを設定または解除します。このフラグが設定されている場合は、A レコードと AAAA レコードの正常性がモニターされます。

```
zone name rrSet rr-name [set <host-health-check=off/ping/gtp-echo>] [get <host-health-check>]
[unset <host-health-check>] [show]
```



(注) DNS サーバーは、IPv6 ホスト ヘルス モニターリング用のグローバルユニキャストアドレスをサポートしています。

DNS ホストの正常性チェックの統計の表示

次の方法で、DNS ホストの正常性チェックの統計を表示できます。

ローカルの高度な Web UI

[DNS権威サーバーの管理 (Manage DNS Authoritative Server)] ページの [統計 (Statistics)] タブをクリックして [サーバー統計 (Server Statistics)] ページを表示します。DNS ホストの正常性チェックの統計は、[合計統計 (Total Statistics)] カテゴリと [サンプル統計 (Sample Statistics)] カテゴリの両方の [ホストの正常性チェックの統計 (Host Health Check Statistics)] に表示されます。

表 49: DNS ホストの正常性チェックの統計に関する属性

属性	説明
<i>hhc-domains</i>	ping と 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数を報告します。
<i>hhc-domains-failed</i>	ping と 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。
<i>hhc-domains-passed</i>	ping と 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。
<i>hhc-rr</i>	ping と gtp-echo によるホストの正常性チェックで確認された RR の数を報告します。
<i>hhc-rrs-passed</i>	ping と gtp-echo による正常性チェックで合格した RR の数を報告します。
<i>hhc-rrs-failed</i>	ping と gtp-echo による正常性チェックで不合格となった RR の数を報告します。
<i>hhc-ping-domains</i>	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数を報告します。
<i>hhc-ping-domains-failed</i>	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。

<i>hhc-ping-domains-passed</i>	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。
<i>hhc-ping-rrs</i>	ping によるホストの正常性チェックで確認された RR の数を報告します。
<i>hhc-ping-rrs-failed</i>	ping によるホストの正常性チェックで不合格だった RR の数を報告します。
<i>hhc-ping-rrs-passed</i>	ping によるホストの正常性チェックで合格した RR の数を報告します。
<i>hhc-gtp-echo-domains</i>	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数を報告します。
<i>hhc-gtp-echo-domains-failed</i>	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。
<i>hhc-gtp-echo-domains-passed</i>	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。
<i>hhc-gtp-echo-rrs</i>	gtp-echo によるホストの正常性チェックで確認された RR の数を報告します。
<i>hhc-gtp-echo-rrs-passed</i>	gtp-echo によるホストの正常性チェックで合格した RR の数を報告します。
<i>hhc-gtp-echo-rrs-failed</i>	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 の数を報告します。

DNS ホストの正常性チェックの統計をサーバーにロギングすることもできます。それには、[ローカル DNS サーバーの編集 (Edit Local DNS Server)] ページの [アクティビティ サマリーの設定 (Activity Summary Settings)] セクションにある [host-health-check] オプションを有効にします。

CLI コマンド

ホストの正常性チェック合計統計を表示するには、**dns getStats dns-hhc total** を使用します。サンプルカウンタ統計を表示するには、**dns getStats dns-hhc sample** を使用します。



(注) DNS サーバーを再起動すると、設定の変更が適用されます。

SRV レコードのホストヘルスチェック

SRV レコードの DNS ホストヘルスチェックを有効にして、対応する A/AAAA レコードのヘルスチェックを自動的に行うことができます。同じ A/AAAA レコードを指す複数の SRV レコードに異なるホストヘルスチェック設定がある場合、サーバーは最初にクエリされたレコードに基づいてホストヘルスチェック設定を選択します。A/AAAA レコードがホストヘルスチェックに対してすでに有効になっている場合、A/AAAA の設定が使用され、SRV レコードの設定は無視されます。DNS サーバーがホストヘルスチェックが明示的に設定されていない A/AAAA を検索する場合、サーバーはハッシュをチェックして、SRV レコードを介して暗黙的に設定されているかどうかを確認します。SRV レコードでホストヘルスチェックが無効になっている場合、権威 DNS サーバーは、ホストヘルスチェックが明示的に設定されている A/AAAA レコードを引き続き監視します。すべての A/AAAA レコードがダウンしている場合、SRV ルックアップは、クライアントに応答するときに *hhc-failed-domain-response* を使用します。



第 8 章

DNS ファイアウォールの管理

- [DNS ファイアウォールの管理 \(163 ページ\)](#)

DNS ファイアウォールの管理

DNS ファイアウォールは、ネットワーク上で機能することが許可されているドメイン名、IP アドレス、およびネームサーバーを制御します。これにより、インターネット サービス プロバイダ (ISP)、企業、または組織は、FQDN、IP アドレス、サブネット、およびエンドノードのプレフィックスのリストを定義し、既知の不正ドメインまたは存在しないドメイン (NXDOMAIN) からの DNS 名の解決をリダイレクトすることでネットワークを保護するルールを設定できます。

キャッシュ DNS サーバーへのすべてのクエリは、プライオリティに従い DNS ファイアウォールルールのリストに照らして最初に確認されます。キャッシング DNS サーバーが存在しないドメインまたは既知の不正ドメインに対するクエリを確実にリダイレクトするように DNS ファイアウォールルールを作成できます。DNS ファイアウォールルールは、プライオリティ、ACL、アクション、およびドメインリストで構成され、例外とフォワードよりも優先されます。これらのクエリに対して、次のアクションを設定できます。

- **Drop** : リソースレコードクエリをドロップします。
- **Refuse** : データなしの [拒否 (REFUSED)] ステータスで応答します。
- **Redirect** : 指定された IP アドレスに A クエリまたは AAAA クエリをリダイレクトします。
- **Redirect-nxdomain** : 照会されたドメインが存在しない場合に、特定の A アドレスまたは AAAA アドレスにリダイレクトします。
- **RPZ** : RPZ ルールを使用します。

着信クエリが DNS ファイアウォールルールと一致する場合は、`redirect-nxdomain` のルールでない限り、指定されたアクションが実行されます。`redirect-nxdomain` ルールは、NXDOMAIN 応答を生じさせる着信クエリにのみ適用されます。



- (注) Drop、Refuse、Redirect、RPZ などのファイアウォールルールは、通常のクエリ処理の前に行われるため、フォワーダと例外よりも優先されます。その他のアクションとトリガーは、通常のクエリ処理中またはその後適用されます。

DNS RPZ ファイアウォールルール

Cisco Prime Network Registrar は RPZ をサポートしています。DNS ファイアウォールルールは、権威 DNS サーバー上の特別に指定されたゾーンに対して設定できます。RPZ と RR データを DNS リゾルバと組み合わせることにより、DNS サーバーの不正使用を防ぐ有効な DNS ファイアウォールを構成できます。RPZ ファイアウォールルールは、トリガー (query-name、ip-answers、ns-name、および ns-ip) と、対応するアクションで構成されます。

RPZ ファイアウォールルールは、権威 DNS サーバーとキャッシング DNS サーバーの両方を使用して RPZ 機能を提供します。権威 DNS サーバーは RPZ とルールのデータを保存します。キャッシュ DNS サーバーはクライアントクエリを受信してこれらのルールを適用します。

DNS RPZ

RPZ の権威 DNS サーバーで個別の正引きゾーンを作成することを推奨します。ゾーンはプライマリまたはセカンダリのいずれかになります。また、データは手動で入力するか、サードパーティ RPZ プロバイダから転送できます。ゾーンには **rpz** という名前を付けることができます。<customer-domain> という名前を付けることで、グローバル DNS 空間のドメイン名との重複を回避できます。ゾーンの [クエリ設定 (Query Settings)] セクションで rpz 属性を有効にすることで、そのゾーンは RPZ になります。



- (注) ゾーン転送で着信した RPZ は、送信元と同じ名前にする必要があります。商用 RPZ プロバイダを利用している場合、名前はプロバイダによって指定されます。

RPZ RR 名には、次の形式を使用できます。

表 50: RPZ トリガー

RPZ トリガー	RR 名	例	RR 名の例
クエリ対象ドメイン	<domain>.rpz. <customer-domain>	ドメイン www.baddomain.com	www.baddomain.com.rpz.cisco.com
照会する ネームサーバー	<ns-domain-name>.rpz- nsdname.rpz.<customer-domain>	ネームサーバー ns.baddomain.com	ns.baddomain.com.rpz-nsdname.rpz. cisco.com

照会する ネームサー バー IP	32.<reversed-ip>.rpz-nsip.rpz. <customer-domain>	ネームサーバー アド レス 192.168.2.10	32.10.2.168.192.rpz-nsip.rpz.cisco.com
照会する ネームサー バー IP	32.<reversed-ip>.rpz-nsip.rpz. customer-domain>	ネームサーバー アド レス 2001:db8:0:1::57	128.57.zz.1.0.db8.2001.rpz-nsip.rpz.cisco.com
応答の Answer セク ションの A レコード	32.<reversed-ip>.rpz-ip.rpz. <customer-domain>	A 応答レコード 192.168.2.10	32.10.2.168.192.rpz-ip.rpz.cisco.com
応答の Answer セク ションの A レコード	<subnet-mask>.<reversed-ip>. rpz-ip.rpz.<customer-domain>	サブネット 192.168.2.0/24 の A 応 答レコード	24.0.2.168.192.rpz-ip.rpz.cisco.com
応答の Answer セク ションの AAAA レ コード	128.<reversed-ip>.rpz-ip.rpz. <customer-domain>	AAAA 応答レコード 2001:db8:0:1::57	128.57.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com
応答の Answer セク ションの AAAA レ コード	<prefix-length>.<reversed-ip>. rpz-ip.rpz.customer-domain>	プレフィックス 2001:db8.0:1::/48 の AAAA 応答レコード	27.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com

このゾーンには、ブロックリストに登録されたクエリ名に関連するすべての RR が含まれています。IP アドレスと範囲のブロッキングは *rpz-ip* ラベル内（つまり *rpz-ip.rpz.cisco.com*）で行われる必要があります。同じロジックを *rpz-nsdname* と *rpz-nsip* ラベルを使用してネームサーバーのブロッキングに適用できます。



(注) *rpz-ip*、*rpz-nsdname*、および *rpz-nsip* は、異なるラベルであり、実際のサブドメインまたは別のゾーンではありません。このレベルには委任ポイントが存在しません。キャッシング DNS は参照先ゾーン内の全データの検索に依存します。



(注) *rpz-nsdname* と *rpz-nsip* を使用する場合は、対応するルールが元のクエリに適用されるため、応答セクションが変更されます。最後の応答が RPZ ルールから決定された場合は、*authority* セクションには RPZ の SOA が含まれます。

キャッシュ DNS サーバーが RPZ を使用するよう設定されている場合は、権威 DNS サーバーにクエリを送信して RPZ ルールをルックアップします。キャッシュ DNS サーバーは、正しいクエリ名を作成し、クエリ応答を RPZ ルールとして解釈し、クライアントクエリにそのルールを適用します。RPZ ルールに基づいてキャッシュ DNS サーバーがクライアント応答を書き換えると、このデータはキャッシュされて、その後のルックアップが速くなります。キャッシュ DNS サーバー RPZ 設定によって、使用する RPZ トリガーが決まります。RPZ ルールが見つからない場合は、クエリは正常に進行します。

さらに、キャッシュ DNS サーバーで RPZ オーバーライドを設定できます。これにより、キャッシュ DNS サーバーは権威 DNS サーバーから返された RPZ アクションをオーバーライドできるようになります。これは、データがサードパーティからプルされる場合と同様に、権威 DNS データの制御がない場合に役立ちます。キャッシュ DNS サーバーは、RPZ クエリの権威 DNS サーバーから一致を取得すると、RR データで指定されたルールアクションではなく、オーバーライドアクションを実行します。

DNS RPZ アクション

RPZ ルールは標準 DNS RR（大抵は CNAME RR）を使用して作成されます。ただし、リダイレクトの場合は、任意のタイプの RR を使用できます。RR 名は「[表 50: RPZ トリガー \(164 ページ\)](#)」の項で説明されている RPZ トリガーに基づく形式になります。rdata は、実行されるルールアクションを定義します。次の表で、RPZ アクションについて説明します。

表 51: RPZ アクション

RPZ ルール アクション	RPZ RR RData	RPZ RR の例
NXDOMAIN	CNAME .	www.baddomain.com.rpz.cisco.com. 300 CNAME .
NODATA	CNAME *.	www.baddomain.com.rpz.cisco.com. 300 CNAME *.
NO-OP (許可リスト)	CNAME rpz-passthru. CNAME FQDN	www.gooddomain.com.rpz.cisco.com. 300 CNAME rpz-passthru. www.gooddomain.com.rpz.cisco.com. 300 CNAME www.gooddomain.com.
DROP	CNAME rpz-drop.	www.baddomain.com.rpz.cisco.com. 300 CNAME rpz-drop.
Redirect	<any RR type> <redirect-data>	www.wrongdomain.com.rpz.cisco.com. 300 CNAME walledgarden.cisco.com. www.baddomain.com.rpz.cisco.com. 300 A 192.168.2.10 www.baddomain.com.rpz.cisco.com. 300 AAAA 2001:db8:0:1::57

DNS RPZ の要件とベスト プラクティス

- すべての RPZ で *rpz* 属性が有効になっている必要があります。変更を有効にするには、DNS のリロードが必要です。
- Cisco Prime Network Registrar 権威 DNS とキャッシング DNS の両方をエンドツーエンドの RPZ ソリューションに使用する必要があります。
- RPZ の *restrict-query-acl* にはキャッシュ DNS アドレスとローカルホストのみが含まれる必要があります。
- ゾーン転送 (*restrict-xfer-acl*) は完全に拒否されるか、または特定のサーバーセットに制限される必要があります。
- RPZ を親ゾーンから委任することはできません。これは非表示である必要があり、特別に設定されたキャッシュ DNS でのみ使用できます。
- RPZ ネームサーバーがキャッシュおよび保持されないように、ネームサーバーのアドレスレコードが存在しないようにする必要があります。
- ネームサーバー レコードは「localhost」を指している必要があります。
- キャッシング DNS サーバーの RPZ ファイアウォールルール数は、2～3 に制限されている必要があります。RPZ ファイアウォールルール数が増えるにつれて、クエリの処理時間は直線的に増加します。
- 手動で作成された RPZ のデフォルト TTL は、ゾーンデータの変化のペースを反映する必要があります。推奨されるペースは 5 分～2 時間です。
- キャッシング DNS サーバーは、信頼性の高い送信元からの情報がキャッシュされ、信頼できるように、*max-cache-ttl* 設定を変更する必要があります。この設定は、デフォルト TTL の 5 分～2 時間に即している必要があります。
- 権威 DNS サーバーは、分散 RPZ データのゾーン転送のために NOTIFY、IXFR、AXFR、および TSIG を有効にする必要があります。
- RPZ は、許可リストとブロックリストに登録されたドメインのデータを含むことができますが、2 つの異なるゾーンに分けることもできます。これは、重複するデータがある場合や、ブロックリストゾーンがサードパーティによって維持されている場合（つまり RPZ サブスクリプション）に役立ちます。

権威 DNS サーバーでの RPZ プライマリ ゾーンの設定

ローカル Web UI

ステップ 1 [デザイン (Design)] メニューの [認証 DNS (Auth DNS)] サブメニューの [転送ゾーン (Forward Zones)] を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)] ページを開きます。

ステップ 2 [正引きゾーン (Forward Zones)] ペインの [正引きゾーン追加 (Add Forward Zone)] アイコンをクリックして [ゾーンの追加 (Add Zone)] ダイアログボックスを開きます。

ステップ 3 ゾーンの名前(つまり、**rpz.zonename**)を入力します。ネームサーバーとして**localhost**を指定し、連絡先の電子メール、および開始シリアル番号を追加します。

ステップ 4 [ゾーンの編集 (Edit Zone)] ページで、次の変更を行います。

- a) [ゾーンのデフォルト TTL (Zone Default TTL)] を設定します (推奨設定は 5 分～2 時間)。
- b) [クエリ設定 (Query Settings)] セクションで **rpz** を **true** に設定し、**restrict-query-acl** 属性を使用してクエリを制限します。

(注) クエリは **localhost** とキャッシング DNS サーバーアドレス、**制限クエリー-acl = localhost、cdns アドレス**に制限されている必要があります。

- c) [ゾーン転送設定 (Zone Transfer Settings)] セクション でゾーン転送と通知を制限します。

(注) ゾーン転送と通知は他の RPZ セカンダリおよび **localhost** にのみ許可される必要があります。

ステップ 5 [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 [ローカル DNS サーバー (Local DNS Server)] ページを開きます。

ステップ 6 [サーバーの再起動 (Restart Server)] アイコンをクリックして、DNS サーバーをリロードし、RPZ をパブリッシュします。

CLI コマンド

次の CLI コマンドを使用します。

- RPZ を作成するには、そのゾーンが RPZ であることを名前で示す必要があります。たとえば、**rpz.example.com** です。

```
nrcmd> zone rpz.example.com. create primary localhost admin
```

- RPZ 属性 (**rpz**) を有効にします。

```
nrcmd> zone rpz.example.com. enable rpz
```

- キャッシング DNS とローカルホストからのクエリのみを許可するように、クエリを制限します。

```
nrcmd> zone rpz.example.com. set restrict-query-acl="localhost, cdns-server"
```

- 展開に応じてゾーン転送を制限または完全に拒否します。

```
nrcmd> zone rpz.example.com. set restrict-xfer-acl=none
```

- デフォルト TTL を 5 分～2 時間に設定します。

```
nrcmd> zone rpz.example.com. set defttl=5m
```

- 設定の変更を有効にするには、DNS サーバーをリロードして RPZ をパブリッシュします。

```
nrcmd> dns reload
```


DNS ファイアウォール ルールの設定

次の手順で DNS ファイアウォール ルールを追加または編集します。

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)]メニューで [DNS のキャッシュ (Cache DNS)]サブメニューの [DNS ファイアウォール (DNS Firewall)]を選択して [DNS ファイアウォールルールのリスト/追加 (List/Add DNS Firewall Rules)]ページを開きます。

ステップ 2 [DNS ファイアウォール (DNS Firewall)]ペインの [DNS ファイアウォールルールの追加 (Add DNS Firewall Rule)]アイコンをクリックすると、[DNS ファイアウォールの追加 (Add DNS Firewall)]ダイアログボックスが開きます。

ステップ 3 [ルール名 (Rule Name)]フィールドにルール名を入力し、アクション タイプを指定します。

(注) **drop** および **refuse** アクションは、指定されたドメインのすべてのクエリに適用されます。一方、**redirect** および **redirect-NXDOMAIN** ルールは、A レコードと AAAA レコードのクエリにのみ適用されます。

ステップ 4 [DNS ファイアウォールの追加 (Add DNS Firewall)]をクリックして、ファイアウォールルールを保存します。新しく追加されたファイアウォールルールが [DNS ファイアウォールルールのリスト表示/追加 (List/Add DNS Firewall Rules)]ページに表示されます。

(注) アクション **refuse** のルールには、ドメインまたは宛先 IP アドレスは使用されません。

ステップ 5 **drop** または **redirect** アクションを選択した場合 :

- ACL リストを入力し、[追加 (Add)]アイコンをクリックし、ドロップまたはリダイレクトをモニターする必要があるドメインを追加します。
- **redirect** アクションの場合は、IPv4 宛先または IPv6 宛先も入力する必要があります。

ステップ 6 **rpz** アクションを選択した場合 :

1. RPZ の名前と RPZ サーバー名を入力します。

(注) RPZ に **rpz.customer-domain** という推奨名を付けることで、グローバル DNS スペースのドメイン名との競合を回避します。

2. オプションおよび対応するオーバーライドアクションから RPZ トリガーを選択します。

ステップ 7 [保存 (Save)]をクリックして設定を保存するか、[元に戻す (Revert)]をクリックして変更をキャンセルします。

DNS ファイアウォールルールを削除するには、[DNS ファイアウォール (DNS Firewall)]ペインでルールを選択し、[削除 (Delete)]アイコンをクリックした後、削除を確認します。

CLI コマンド

DNS ファイアウォールルールをスペースで区切って追加するには、**cdns-firewall rule-name create** を使用します。

ドメインリダイレクトルールのドメインのリストを表示するには、**cdns-firewall list** を使用します。

ドメインリダイレクトルールを削除するには、**cdns-firewall rule-name delete** を使用します。

DNS ファイアウォール ルールの優先順位の変更

DNS ファイアウォールルールを作成するときに、ルールを適用する順位を指定できます。



- (注) 複数の DNS ファイアウォールルールを適用する場合は、ルールの処理順序を制御するためのルールプライオリティを設定することを推奨します。ゼロ以外の最も小さいプライオリティが最初に処理されます。プライオリティが 0 (デフォルト) の DNS ファイアウォールルールが最後に処理されます。

ローカル詳細およびリージョン詳細 [Web UI](#)

次の手順でプライオリティを設定するか、ルールの順序を変更します。

ステップ 1 [設計 (Design)]メニューで [DNS のキャッシュ (Cache DNS)]サブメニューの [DNS ファイアウォール (DNS Firewall)]を選択して [DNS ファイアウォールルールのリスト/追加 (List/Add DNS Firewall Rules)]ページを開きます。

ステップ 2 [DNS ファイアウォール (DNS Firewall)]ペインの [**DNS ファイアウォール ルールの順序変更 (Reorder DNS Firewall Rules)**]アイコンをクリックすると、[順序変更 (Reorder)]ダイアログボックスが開きます。

ステップ 3 次のいずれかの方法で、DNS ファイアウォールルールの優先順位を設定します。

- ルールを選択し、[上に移動 (Move up)]または[下に移動 (Move down)]アイコンをクリックして、ルールの順序を変更します。
- ルールを選択し、[移動先 (Move to)]ボタンをクリックして、ルールを移動する行番号を入力します。

ステップ 4 [保存 (Save)]をクリックして、順序を変更したリストを保存します。

CLI コマンド

cdns-firewall name set priority=value を使用して、他のルールに関連するルールの優先順位を指定します。

RPZ の TLS の有効化

Cisco Prime Network Registrar 11.0 以降では、キャッシング DNS のファイアウォール RPZ アクシオンは RPZ サーバーとの通信で TLS をサポートします。

ローカル詳細およびリージョン詳細 Web UI

RPZ サーバーの TLS を有効にするには、次の手順を実行します。

ステップ 1 [設計 (Design)] メニューで [DNS のキャッシュ (Cache DNS)] サブメニューの [DNS ファイアウォール (DNS Firewall)] を選択して [DNS ファイアウォールルールのリスト/追加 (List/Add DNS Firewall Rules)] ページを開きます。

ステップ 2 **enabled** オプションを選択して、*rpz-tls* 属性を有効にします。これを有効にする場合は、*tls-cert-bundle* を設定し、CA 証明書をロードする必要があります。そのようにしないと、接続を認証できません。

rpz-tls-auth-name 属性は、RPZ サーバーの認証名を定義します。TLS が有効になっている場合、キャッシング DNS サーバーは、RPZ サーバーから送信された名前の TLS 認証証明書をチェックします。

CLI コマンド

cdns-firewall name set rpz-tls=true を使用して、RPZ サーバーの TLS を有効にします。



第 9 章

ハイ アベイラビリティ DNS の管理

2 番目のプライマリ サーバーをメインのプライマリ サーバーの障害に備えるホット スタンバイ サーバーとして使用できます。この設定はハイ アベイラビリティ (HA) DNS と呼ばれます。Cisco Prime Network Registrar Web UI および CLI には、サーバー ペアの HA DNS に必要なプライマリ設定を複製できる機能があります。このサーバー ペアは通信障害などを検出します。HA DNS が設定されると、シャドウイングとエラー検出が自動的に行われます。Cisco Prime Network Registrar DHCP が Cisco Prime Network Registrar DNS を更新している Cisco Prime Network Registrar 展開では、障害の検出とフェールオーバーも自動的に行われます。



(注) HA を実行している場合は、サーバー上にプライマリゾーンだけを用意することを推奨します。

- [HA DNS 処理の概要 \(173 ページ\)](#)
- [ハイ アベイラビリティ DNS ペアの作成 \(175 ページ\)](#)
- [HA DNS ゾーンの同期 \(177 ページ\)](#)
- [HA DNS 情報のロギングの有効化 \(178 ページ\)](#)
- [HA DNS 統計の表示 \(178 ページ\)](#)

HA DNS 処理の概要

正常の状態では、メインサーバーとバックアッププライマリサーバーの両方が稼働しています。メインサーバーは、クライアントからのすべての DNS 更新を処理し、受け入れたすべての更新をホットスタンバイバックアップに送信します。メインサーバーは RR 更新をバックアップサーバーに転送します。DDNS クライアントからの更新は、バックアップサーバーで無視またはドロップされます。両方のサーバーがクエリとゾーン転送要求に応答できます。メインとバックアップはパートナーで、相手の可用性を検出するために通信を続けます。

メインがダウンした場合は、バックアップが短時間待ってから、通常ではメインが処理するクライアントからの DNS 更新の処理を開始し、アップデートを記録します。メインが復旧したら、HA ペアは通信中断の間に変更または削除された RR を同期して交換します。

新しいゾーンを追加する際は、プライマリサーバーとバックアップサーバーの両方をリロードして、HA バックアップと自動で同期されるようにする必要があります。

同期はゾーン単位で実行されます。これにより、特定のゾーンが同期されている間に、他のすべてのゾーンの更新が可能になります。

ホットスタンバイバックアップがダウンすると、メインは短時間待機してから、パートナーが確認応答しなかった更新を記録します。バックアップサーバーが復旧すると、メインは記録された更新をバックアップに送信します。

メインとバックアップの両方の状態は、次のように推移します。

- **Startup** : サーバーは通信を確立し、使用する HA バージョンに同意します。この状態では、サーバーは DNS 更新または RR 編集を受け入れず、スカベンジングが有効になっている場合はそれを延期します。
- **Negotiating** : 各サーバーは、他のサーバーが同期の準備が整うまで待機します。この状態では、DNS 更新と RR 編集は許可されません。
- **Normal** : 両方のサーバーが正常に稼働しており、DNS 更新とハートビートメッセージを交換しています。メインは DNS 更新と RR 編集を許可し、RR 更新メッセージをバックアップに送信します。バックアップは DNS 更新を無視し、RR 編集を拒否しますが、メインサーバーからの RR 更新メッセージは処理します。ゾーンが同期している間は、ゾーンでスカベンジングが一時停止されます。
- **Communication-Interrupted** : 通信タイムアウト (*ha-dns-comm-timeout*) 中にパートナーから応答または要求を受信しなかったサーバーにこの状態になります。サーバーは、パートナーからの通信のリスニングを続けて (両方とも、*ha-dns-poll-interval* で指定したハートビートメッセージを送信)、接続しようとします。その一方で、DNS 更新と RR 編集を許可し、スカベンジングを無効にします。
- **Partner-Down** : [通信の中断 (*communications-interrupted*)] と似ていますが、RR 変更の追跡は継続されません。パートナーが復旧すると、ゾーン全体がパートナーに送信されます。パートナーは再び稼働可能になったときにゾーンのコピーを受信するので、パフォーマンスが向上し、変更追跡に要するディスク容量が抑えられます。

DNS サーバーの起動後の動作は、次のとおりです。

1. 設定されている HADNS リスニングポートを開き、パートナーからの接続をリッスンします。
2. [ネゴシエーション (*Negotiating*)] 状態に移行します。[ネゴシエーション (*Negotiating*)] 状態では、RR 編集は許可されません。
3. [正常 (*Normal*)] 状態に移行したサーバーは、各プライマリゾーンへの変更の同期を開始します。メインは、ゾーン更新の許可と、バックアップへの更新情報の送信を開始します。

サーバーが正常な状態になると、ゾーンレベルの同期が開始されます。ゾーン同期は、常にメインの HA サーバーによって管理されます。ゾーンの状態は、次のように遷移します。

- **Sync-Pending State** : HA DNS サーバーが正常な状態になったとき、または手動同期が要求された場合に、ゾーンはこの状態になります。この状態では、ゾーンの RR 更新がメインサーバーで受け入れられ、バックアップサーバーに転送されます。
- **Synchronizing State** : ゾーンの RR 同期は、同期の状態で行われます。RR 更新は受け入れられず、通知は無効になります。

- **Sync-Complete State** リソース レコードの変更と HA DNS バックアップ上の対応するゾーンが正常に同期されると、ゾーンは同期の状態からこの状態に移行します。この状態で、HA DNS メイン サーバーのゾーンは、DNS の動的更新要求をすべて受け入れ、リソース レコード設定の変更を許可し、通知を再び有効にします。リソース レコードの変更は、バックアップ サーバーに転送されます。
- **Sync-Failed State** : 同期に失敗したゾーンは、同期の状態から `sync-failed` の状態に移行します。メイン サーバーのゾーンはリソース レコード更新を受け入れ、変更はバックアップに転送されます。サーバーは `ha-dns-zonesync-failed-timeout` の後にゾーンの同期を再試行します。手動同期要求またはサーバーの再起動によって、ゾーン同期も再び開始されます。

HA DNS は Cisco Prime Network Registrar DHCP サーバーと完全に統合され、ホストがネットワークに追加されると、パートナーが更新されます（『*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）。DHCP サーバーは、HA DNS の DHCP 側から DNS サーバー 1 台ごとに DNS 更新を送信します。

DHCP は、メインがダウンしていることを自動検出し、バックアップへの更新の送信を開始します。DHCP サーバーは、メイン DNS サーバーへの接続を 2 回試行します。両方の試行が失敗した場合は、バックアップパートナーへの接続を試行します。

メインサーバーがダウンしていることを検出したバックアップは、DDNS クライアントからの更新の受け入れを開始します。サーバーが復旧したら、HA 通信が自動的に確立されます。サーバーは正常の状態になり、ゾーン同期を実行して両方の RR が同じであることを確認します。

両方の DNS パートナーが通信している場合、バックアップサーバーは更新をドロップします。これにより、DHCP サーバーがタイムアウトし、メイン DNS サーバーへの接続を再試行します。両方のサーバーが到達不能または無応答の場合、DHCP サーバーは応答を受信するまで、各 DNS パートナーへの再試行を 4 秒ごとに続けます。

ローカルクラスタがメイン HA サーバーとして設定されている場合は、ゾーンレベルの同期用の詳細モードコマンドがローカルクラスタの [ゾーンコマンド (Zone Commands)] ページに追加されます。エキスパートモードでは、次の 2 つのオプションがあります。

- メインからバックアップへのすべての RR の同期 (Sync All RR's from Main to Backup)
- バックアップからメインへのすべての RR の同期 (Sync All RR's from Backup to Main)

HA DNS ステータスは、ゾーン同期ステータスを含むように変更されました。ステータスには、同期されたゾーンの数と割合、同期が保留されているゾーン、同期に失敗したゾーンが含まれます。

ゾーン ステータスが変更され、HA が設定されている場合は HA 同期ステータス (`ha-server-pending`、`sync-pending`、`sync-complete`、`synchronizing`、または `sync-failed`) も含まれるようになります。

ハイ アベイラビリティ DNS ペアの作成

HADNS サーバー ペアをメインサーバーから設定するために必要な属性は、次のとおりです。

- *ha-dns* : Enabled または disabled。プリセット値は enabled です。
- *main* : メインプライマリ DNS サーバーのクラスタ。
- *backup* : バックアッププライマリ DNS サーバーのクラスタ。

メインまたはバックアップの特定の IP アドレスが指定されるのは、クラスタ IP が管理に使用され、DNS が別のインターフェイスで動作する場合だけです。

ローカルおよびリージョンの詳細 Web UI

ステップ 1 バックアップ サーバーのクラスタを作成します。

ステップ 2 [展開 (**Deploy**)] メニューの [DNS] サブメニューで [HA ペア (**HA Pairs**)] を選択して [HA DNS サーバー ペアのリスト/追加 (List/Add HA DNS Server Pair)] ページを開きます。

ステップ 3 [HA ペア (**HA Pairs**)] ペインの [HA ペアの追加 (**Add HA Pair**)] アイコンをクリックして [HA DNS サーバーを追加 (Add HA DNS Server)] ダイアログを開きます。

ステップ 4 [名前 (**name**)] フィールドにサーバーペアの名前を入力します。これは、任意の識別テキスト文字列にすることができます。

ステップ 5 [メイン (**main**)] ドロップダウンリストからメイン DNS サーバーのクラスタ名を選択します。

- (注) ローカル ホスト マシンの IP アドレス (IPv4 または IPv6) を変更する場合は、[IPv4 アドレス (IPv4 Address)] フィールドまたは [IPv6 アドレス (IPv6 Address)] フィールドの IP アドレス (IPv4 または IPv6) を変更するために、([クラスタの編集 (**Edit Cluster**)] ページで localhost クラスタを変更する必要があります。値を 127.0.0.1 と ::1 に設定しないでください。

ステップ 6 [バックアップ (**backup**)] ドロップダウンリストからバックアップ DNS サーバーのクラスタ名を選択します。これをメインサーバー クラスタと同じにすることはできません。設定管理や更新要求で異なるインターフェイスを使用してサーバーが設定されている場合に限り、IPv4 の場合は属性 *ha-dns-main-address* と *ha-dns-backup-address*、IPv6 の場合は属性 *ha-dns-main-ip6address* と *ha-dns-backup-ip6address* を設定します (HA DNS プロトコルの設定には、サービス更新に使用されるインターフェイスのみを使用してください)。

ステップ 7 [HA DNSサーバーの追加 (**Add HA DNS Server**)] をクリックします。

ステップ 8 サーバー ペアが [HA DNS サーバー ペアのリスト表示/追加 (List/Add HA DNS Server Pair)] ページに表示された後の手順は、次のとおりです。

- [HA ペア (**HA Pairs**)] ペインで HA を選択し、[HA DNS サーバーペアの同期 (Sync HA DNS Server Pair)] タブをクリックします。
- 同期の方向 ([メインからバックアップ (**Main to Backup**)]、または[バックアップからメイン (**Backup to Main**)]) を選択します。
- 処理タイプ ([更新 (**Update**)]、[完全 (**Complete**)]、または[正確 (**Exact**)]) を選択します。各処理タイプの処理の詳細については、ページの表を参照してください。
- [レポート (**Report**)] ボタンをクリックすると、[HA DNS 同期レポートの表示 (View HA DNS Sync Report)] ページで今後の同期の変更が表示されます。
- [完全実行 (**Run Complete**)] をクリックして同期を完了します。
- [戻る (**Return**)] をクリックして [HA DNS サーバーペアのリスト/追加 (List/Add HA DNS Server Pair)] ページに戻ります。

ステップ9 両方の DNS サーバーをリロードして HA 通信を開始します。

CLI コマンド

HA DNS サーバー ペア (**ha-dns-pair name create main-cluster/address backup-cluster/address**) を作成します。*address* は IPv4 または IPv6 を使用できます。サーバーを同期するために、**ha-dns-pair name sync** を使用して、同期処理 (**update**、**complete**、または **exact**) と方向 (**main-to-backup** または **backup-to-main**) を指定します。両方の DNS サーバーをリロードしてください。次に例を示します。

```
nrcmd> ha-dns-pair example-ha-pair create localhost test-cluster
nrcmd> ha-dns-pair example-ha-pair sync exact main-to-backup
nrcmd> dns reload
```

シンタックス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 **ha-dns-pair** コマンドを参照してください。CLI には、Communication-Interrupted 状態のときのみ必要に応じて DNS サーバーを HA DNS パートナー ダウンに設定するための他のコマンドが用意されています。

```
nrcmd> dns setPartnerDown
```

パートナーダウンは、サーバーが保持するブックキーピングデータを制限することでパフォーマンスを最適化するので有益です。両方のサーバーが通信を再開すると、変更が個別に検出されるのではなく、すべてのゾーン RR が同期で送信されます。正常に動作していたパートナーが、停止したサーバーにすべての RR を送信します。

HA DNS ゾーンの同期

ローカルの詳細 Web UI

HA DNS ゾーンを手動で同期するには、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、[正引きゾーンのリスト/追加 (List/Add Forward Zones)] ページまたは [逆引きゾーンのリスト/追加 (List/Add Reverse Zones)] ページを開きます。
- ステップ2 [ゾーンの編集 (Edit Zone)] ページで、同期するゾーンの [コマンド (Commands)] ボタンをクリックします。
- ステップ3 [HAゾーンの同期 (Synchronize HA Zone)] の横にある [コマンド (Command)] アイコンをクリックして、HA DNS ゾーンを同期します。

HA DNS ゾーンを同期するたびに、プライマリ ゾーンに関連ビューと名前付き ACL が同期されます。

(注) エキスパート モードでは、同期のタイプを選択するオプションがあります。

CLI コマンド

zone name ha-sync-all-rrs を使用して、ゾーンの HA ゾーン同期を手動でスケジュールするか、ゾーンがすでに `sync-pending` 状態になっている場合は、プライオリティを上げます（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 **zone** コマンドを参照してください）。

HA DNS 情報のロギングの有効化

ログ設定、**ha** は、HA DNS 関連の情報のロギングを有効にします。

ローカル Web UI

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

HA DNS 関連情報のロギングを有効にするには、**dns set server-log-settings=ha** を使用します。

HA DNS 統計の表示

HA DNS 統計を表示できます。

ローカル Web UI

[DNS 権威サーバーの管理 (Manage DNS Authoritative Server)] ページの [統計 (Statistics)] タブをクリックして、[DNS サーバー統計 (DNS Server Statistics)] ページを開きます。統計は、[合計統計 (Total Statistics)] カテゴリと [サンプル統計 (Sample Statistics)] カテゴリの [HA 統計 (HA Statistics)] および [最大カウンタ統計 (Max Counter Statistics)] サブカテゴリに表示されます。

CLI コマンド

dns getStats ha [total] を使用して HA DNS 合計カウンタ統計を表示します。**dns getStats ha sample** を使用してサンプル カウンタ統計を表示します。



第 10 章

ゾーンの管理

DNS は、コンピュータネットワーク内のオブジェクトの分散データベースです。ネームサーバーアプローチでは、ネットワークは自律ドメインとゾーンの階層で構成されます。名前空間はツリーとして編成され、大抵そのツリーは管理境界に関する組織に似ています。プロトコルの概要については、「[ドメイン ネーム システムの概要 \(1 ページ\)](#)」を参照してください。

DNS ネームサーバーの基本的な機能は、クエリに応答することによってネットワークオブジェクトに関するデータを提供することです。Cisco Prime Network Registrar DNS サーバーおよびゾーンを設定するには、システムのデフォルトを受け入れるか変更します。

DNSは国際化ドメイン名 (IDN) の作成にも対応しています。Web UI、Web サービス (REST)、および Java SDK で DNS ドメインに名前を付ける際には、完全な Unicode 文字セットを使用できます。使用できるソートと検索の機能は限定されています。詳細については、*Cisco Prime Network Registrar 11.1* リリース ノートを参照してください。



- (注) Java SDK を使用する Java ツール (cnr_rules など) を実行している場合は、UNIX のロケールパラメータを en_US.UTF-8 に設定する必要があります。詳細については、*Cisco プライムネットワーク レジストラ 11.1 管理ガイド*の「*Running Data Consistency Rules*」の項を参照してください。

この章では、Cisco Prime Network Registrar DNS サーバーと、そのプライマリ ゾーンおよびセカンダリゾーンの設定の基本について説明します。「[リソースレコードの管理 \(221 ページ\)](#)」ではDNS リソースレコード (RR) とホストの管理方法について説明します。「[権威 DNS サーバーの管理 \(93 ページ\)](#)」ではゾーンと DNS サーバーの詳細プロパティを設定する方法について説明します。

- [プライマリ DNS サーバーの管理 \(180 ページ\)](#)
- [ゾーンテンプレートの作成と適用 \(180 ページ\)](#)
- [段階モードと同期モード \(183 ページ\)](#)
- [プライマリ正引きゾーンの設定 \(184 ページ\)](#)
- [プライマリ逆引きゾーンの設定 \(192 ページ\)](#)
- [サーバーのゾーンカウントの取得 \(195 ページ\)](#)
- [DNS 更新の有効化 \(195 ページ\)](#)

- [セカンダリ サーバーの管理 \(195 ページ\)](#)
- [サブゾーンの設定 \(198 ページ\)](#)
- [ゾーン分散の管理 \(201 ページ\)](#)
- [DNS ENUM ドメインの管理 \(206 ページ\)](#)

プライマリ DNS サーバーの管理

ゾーンを追加するには、ドメイン名を作成する必要があります。所有者を定義し、ゾーンテンプレートを使用することもできます。テンプレートを使用しない場合は、ゾーンの Start of Authority (SOA) およびネームサーバー (NS) プロパティも定義する必要があります。



(注) ローカルホストのループバックゾーンは、手動での作成は不要で、Cisco Prime Network Registrar で自動的に作成されます。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 を解決するために使用する逆引きゾーンであり、ネットワークトラフィックを自己に転送できます。ループバックゾーンは 127.in-addr.arpa であり、逆引きゾーンのリストに表示されます。

関連項目

- [プライマリ正引きゾーンの設定 \(184 ページ\)](#)
- [プライマリ逆引きゾーンの設定 \(192 ページ\)](#)
- [サーバーのゾーンカウントの取得 \(195 ページ\)](#)

ゾーンテンプレートの作成と適用

ゾーンテンプレートは、同じ属性の多くを共有するプライマリゾーンの定型を作成するのに便利な手段です。ゾーンテンプレートを任意のゾーンに適用し、そのゾーン属性をテンプレートの属性でオーバーライドできます。ゾーンテンプレートは、ローカルおよびリージョンクラスト Web UI と CLI で作成できます。



注意 既存のゾーンにテンプレートを適用する場合は注意してください。ゾーンの明示的に設定されたすべての属性（名前を除く）がテンプレートによって上書きされるため、ゾーンがネットワーク内にすでに設定されている場合は、重大な結果が生じる可能性があります。複数ゾーンの特定の属性をテンプレートを使用して変更するには、その属性のみを変更し、他の属性は未設定のまま、テンプレートをゾーンに適用してください。

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)] メニューの [権威 DNS (Auth DNS)] サブメニューで [ゾーンテンプレート (Zone Templates)] を選択して [ゾーンテンプレートのリスト/追加 (List/Add Zone Views)] ページを開きます。
- ステップ 2** ローカルおよびリージョンクラスタでゾーンテンプレートを追加できます。また、Web UI を使用してリージョンクラスタでゾーンテンプレートをプルおよびプッシュすることもできます。

- ローカルクラスタでゾーンテンプレートを追加する場合、またはリージョンクラスタでテンプレートを明示的に追加する場合は、[ゾーンテンプレート (Zone Templates)] ペインで [ゾーンテンプレートの追加 (Add Zone Templates)] アイコンをクリックします。[ゾーンテンプレートの追加 (Add Zone Template)] ダイアログボックスが開きますので、名前を入力して、[ゾーンテンプレートの追加 (Add Zone Template)] をクリックします。

ゾーンテンプレートを有効に活用するには、推奨シリアル番号、ネームサーバー、連絡先の電子メールアドレス、およびネームサーバーのリストを入力します。それらはゾーン自体に必要です。ゾーン所有者やゾーン分散を指定することもできます。これらの値をゾーンテンプレートに必ず追加しなければならないわけではありません。テンプレートからゾーンを作成した後に、そのゾーンに値を追加することもできます。ただし、テンプレート名とゾーンのデフォルト TTL は必須です。(最小限必要なゾーン属性の説明については、「[プライマリゾーンの作成 \(184 ページ\)](#)」を参照してください)。

これらの値を入力したら、ページの下部にある [保存 (Save)] をクリックします。

- リージョンクラスタで、1 つまたは複数のローカルクラスタからゾーンテンプレートをプルするには、[ゾーンテンプレート (Zone Templates)] ペインで [プル レプリカ (Pull Replica)] アイコンをクリックします。[プルするレプリカ ゾーンテンプレートデータの選択 (Select Replica Zone Template Data to Pull)] ダイアログボックスが開き、ローカルクラスタ ゾーンテンプレートのリージョンサーバーレプリカデータのツリービューが表示されます。ツリーには 2 つのレベルがあり、1 つはローカルクラスタ、もう 1 つは各クラスタのテンプレートです。クラスタから個々のテンプレートをプルすることも、すべてのテンプレートをプルすることもできます。
 - 個々のゾーンテンプレートをプルするには、クラスタのツリーを展開し、名前の横にあるプル基準を選択して、[プル ゾーンテンプレート (Pull Zone Template)] をクリックします。
 - クラスタからすべてのテンプレートをプルするには、プル基準を選択し、[すべてのゾーンテンプレートのプル (Pull All Zone Templates)] をクリックします。
 - クラスタのすべてのレプリカデータを更新するには、[プルレプリカ (Pull Replica)] アイコンをクリックします。

プル選択基準は、次のとおりです。

- [保証 (Ensure)]** : 各テンプレートがプルされます。ただし、その名前のテンプレートがリージョンクラスタにすでに存在する場合は除きます。その場合は、リージョンクラスタデータは上書きされません。
- [置換 (Replace)]** : 各テンプレートがプルされ、リージョンクラスタにすでに存在するテンプレートデータは上書きされます。リージョンクラスタの他のテンプレートに影響はありません。これはデフォルトの推奨設定です。
- [正確 (Exact)]** : 各テンプレートがプルされ、リージョンクラスタにすでに存在するテンプレートデータは上書きされます。リージョンクラスタの他のテンプレートが削除されます。

- リージョンクラスタで、1つまたは複数のローカルクラスタに1つのゾーンテンプレートをプッシュする方法:

- [ゾーンテンプレートのリスト/追加 (List/Add Zone Templates)] ページですべてのゾーンテンプレートをプッシュするには、[ゾーンテンプレート (Zone Templates)] ペインにある [すべてプッシュ (Push All)] アイコンをクリックします。
- [ゾーンテンプレートのリスト/追加 (List/Add Zone Templates)] ページで、個別のゾーンテンプレートをプッシュするには、[プッシュ (Push)] をクリックします。

どちらのアクションでも、[ローカルクラスタへのゾーンテンプレートデータのプッシュ (Push Zone Template Data to Local Clusters)] ページのバージョンが開きます。

このページでは、同期モードと宛先クラスタを選択できます。目的のクラスタを[選択可能 (Available)] フィールドから[選択済み (Selected)] フィールドに移動して、[データ同期モード (data synchronization mode)] オプション ボタンのいずれかをクリックします。

- [保証 (Ensure)]: 各テンプレートがプッシュされます。ただし、その名前のテンプレートがローカルクラスタにすでに存在する場合を除きます。その場合は、ローカルクラスタデータは上書きされません。これはデフォルトの推奨設定です。
- [置換 (Replace)]: 各テンプレートがプッシュされ、ローカルクラスタにすでに存在するテンプレートデータは上書きされます。ローカルクラスタの他のテンプレートに影響はありません。
- [正確 (Exact)]: [すべてプッシュ (Push All)] 操作のみで使用できます。各テンプレートがプッシュされ、ローカルクラスタにすでに存在するテンプレートデータは上書きされます。ローカルクラスタの他のテンプレートが削除されます。

選択後に[クラスタへのデータのプッシュ (Push Data to Clusters)] をクリックします。[ゾーンテンプレートデータのプッシュレポートの表示 (View Push Zone Template Data Report)] ページが開きますので、プッシュ操作の意図した結果を確認できます。[OK] をクリックしてプッシュ操作を実行します。

ステップ 3 テンプレートを新規または既存のゾーンに適用できます。

1. [新規ゾーン (New zone)]: 「[プライマリ正引きゾーンの設定 \(184ページ\)](#)」の説明に従って、ゾーンの作成時に [テンプレート (Template)] ドロップダウンリストからテンプレートを選択します。
2. [既存ゾーン (Existing zone)]: ゾーンを作成（「[プライマリ正引きゾーンの設定 \(184ページ\)](#)」を参照）したら、[ゾーンの編集 (Edit Zone)] ページでゾーンを編集するときにテンプレートを適用できます。[テンプレート (Template)] ドロップダウンリストでテンプレート名をクリックし、[テンプレートの適用 (Apply Template)] をクリックします。

CLI コマンド

zone-template name create を使用して、ゾーンテンプレートを作成します。（ゾーンにテンプレートを適用する方法については、[プライマリ正引きゾーンの設定 \(184ページ\)](#) を参照してください）。次に例を示します。

```
nrcmd> zone-template zone-template-1 create serial=1
```

ゾーンにテンプレートを適用するには、**zone-template name apply-to zone** を使用します。この構文では、1つまたは複数のゾーンをカンマで区切り、すべてのゾーンに対して **all** キーワー

ドを指定することもできます。 **zone-template clone-name create clone=template** を使用して、既存のテンプレートからテンプレートを複製し、そのコピーを調整することもできます。次に例を示します。

```
nrcmd> zone-template zone-template-1 apply-to example.com,boston.example.com
nrcmd> zone-template cloned-template create clone=zone-template-1 owner=owner-1
```

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。プッシュおよび再利用の場合は、クラスターのリストまたは「すべて」を指定できます。

```
zone-template <name | all> pull <ensure | replace | exact> cluster-name [-report-only | -report]
```

```
zone-template <name | all> push <ensure | replace | exact> cluster-list [-report-only | -report]
```

```
zone-template name reclaim cluster-list [-report-only | -report]
```

段階モードと同期モード

リージョンクラスターの2つのモードのいずれか（段階または同期）で、DNS ゾーン、RR、およびホストの追加や編集を行うことができます。

- **Staged (or CCM)** : ゾーン（およびそのホストと保護されたサーバー RR）に対する変更は、CCM データベースに書き込まれますが、同期が要求されるまで DNS サーバーにすぐに伝達されることはありません。
- **Synchronous (or DNS)** : CCM への変更をコミットした後に、ホストと保護された RR はただちに DNS サーバーに伝達されます。サーバーに到達できないために伝達が行われない場合は、次の同期の時に RR が伝達されます。

同期は、ゾーン別に発生するか、ゾーン分散の作成時に発生します。同期モードでは、ゾーンをネットワーク上で公開するためにサーバーのリロードが必要な場合でも、変更は DNS サーバーにすぐに書き込まれます。

このモードを選択するには、Web UI の上部にある [設定 (Settings)] ドロップダウンリストから **Session Settings** を選択します。



- (注) 同期モードは、ローカルクラスターレベルで唯一の DNS 編集モードです。ローカルクラスターで実行される RR の編集は、DNS を介してすぐに使用できます。

ローカルおよびリージョン Web UI

ステージングモードまたは同期ゾーンモードは、Web UI のメインページの [設定 (Settings)] ドロップダウンメニューにある [セッション設定 (Session Settings)] の [セッション編集モード (Session Edit Modes)] の設定に基づいて事前に設定されます。

- リージョン Web UI は、[staged] にプリセットされています。
- ローカル Web UI は、[synchronous] にプリセットされています。

CLI コマンド

`session dns-edit-mode` 属性を `staged` または `synchronous` に設定します。次に例を示します。

```
nrcmd> session set dns-edit-mode=sync
```

プライマリ正引きゾーンの設定

ここでは、プライマリ ネームサーバーにプライマリ正引きゾーンを設定する方法について説明します。この手順を完了したら、「[プライマリ逆引きゾーンの設定 \(192 ページ\)](#)」の手順に従い、使用する各ネットワークの逆引きゾーンを設定します。



ヒント 正引きゾーンの追加例については、『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「ゾーン インフラストラクチャの作成」の項を参照してください。

プライマリゾーンの作成

プライマリゾーンを作成するには、少なくともそのゾーンの特定のキー SOA 属性とネームサーバーを追加する必要があります。Web UI の基本モードの利点は、これらの多くが事前に設定されていることです。

ローカルの基本 Web UI

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、[正引きゾーンのリスト表示/追加 (List/Add Forward Zones)]ページを開きます。

ステップ 2 [正引きゾーン (Forward Zones)]ペインの[正引きゾーンの追加 (**Add Forward Zone**)]アイコンをクリックし、ゾーン名を (ドメイン名形式で) 入力します。

ステップ 3 ネームサーバー ホストの名前を入力します (例: **ns1**) 。

ステップ 4 連絡先の電子メール名を入力します (例: **hostadmin**) 。

ステップ 5 [DNSゾーン (**Add DNS Zone**)]をクリックします。基本モードでは、プリセット値を使用してゾーンが作成されます。

- [ゾーンのデフォルト TTL (Zone default TTL)] : **24h**
- [Start of Authority (SOA) シリアル番号 (Start of Authority (SOA) serial number)] : **1**
- [SOA セカンダリ更新時間 (SOA secondary refresh time)] : **3h**
- [SOA セカンダリ再試行時間 (SOA secondary retry time)] : **60m**
- [SOA セカンダリ有効期間 (SOA secondary expiration time)] : **1w**
- [SOA 最小 TTL (SOA minimum TTL)] : **10m**

ローカルの詳細 Web UI とリージョン Web UI

- 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、[正引きゾーンのリスト表示/追加 (List/Add Forward Zones)]ページを開きます。
- ステップ 2** [正引きゾーン (Forward Zones)]ペインの[正引きゾーンの追加 (Add Forward Zone)]アイコンをクリックし、ゾーン名を (ドメイン名形式で) 入力します。
- ステップ 3** ネームサーバー ホストの名前を入力します (例 : **ns1**) 。
- ステップ 4** 連絡先の電子メール名を入力します (例 : **hostadmin**) 。
- ステップ 5** シリアル番号を入力します。
- ステップ 6** [ゾーンの追加 (Add Zone)]をクリックします。
- ステップ 7** 必要に応じて、ドロップダウン リストから所有者またはリージョンを選択します。
- ステップ 8** 必要に応じて、既存のゾーンテンプレートを適用します (「[ゾーンテンプレートの作成と適用 \(180 ページ\)](#)」を参照) 。ドロップダウン リストで、設定したテンプレートの名前をクリックします。

注意 すでに運用されているゾーンにはテンプレートを慎重に適用してください。すでに定義されているゾーン属性は、テンプレートに明示的に定義されている属性に置き換えられます。

- ステップ 9** 必要に応じて、上位の属性を変更します。
- 所有者とリージョン
 - 事前設定済みゾーン分散 (「[ゾーン分散の管理 \(201 ページ\)](#)」を参照)
 - ゾーンのデフォルト TTL
- ステップ 10** SOA 属性で、次のように入力します。
- シリアル番号 (例 : **1**) 。

プライマリ DNS サーバーは、シリアル番号を使用してデータベースが変更されたことを示し、この番号の増分を使用してセカンダリ サーバーへのゾーン転送をトリガーします。ここで入力できるシリアル番号は提案でしかなく、DNS サーバーは常にそれを受け入れるわけではありません。シリアル番号を編集して、サーバーが保持している実際の番号より小さくすると、サーバーは警告メッセージをロギングし、提案されたシリアル番号を無視します。実際のシリアル番号は、提案された番号と同じか、それより大きな番号になります。(DNS サーバーが動作していない場合に) 実際のシリアル番号を取得するには、**zone name get serial** を使用します (サーバーが動作していない場合や、ゾーン属性が表示されない場合は、推奨するシリアル番号が常に返されます)。あるいは、ゾーンのシリアル番号属性の DNS サーバー値を更新します。ゾーンを作成するときは、この提案シリアル番号を明示的に入力する必要があります。

- ネームサーバー ホスト (例 : **ns1**) 。

ホスト名または完全修飾名 (例 : **ns1.example.com.**) を入力します。ただし、末尾にドットを付ける必要があります。プライマリ ネームサーバーが別のゾーンにある場合は、完全修飾名を使用します。プライマリ DNS サーバーは、ゾーン SOA レコードの **ns** 値になります。ゾーンには、1 つまたは複数の権威ネームサーバーも指定する必要があります。これらはゾーンのネームサーバー (NS) レコードになります。CLI では、プライマリ DNS サーバーが自動的に最初の NS レコードになり、**nameservers** 属性リストに最初のエン트리としても表示されます。

- 連絡先の電子メール名 (**hostadmin** など) 。

連絡先電子メールの完全修飾名は、電子メールアドレスのアットマーク (@) をドット (.) を置き換えて少し変えたバージョンになります。完全修飾値を使用している場合は、アドレスの末尾にドットを付けます（例：hostadmin@example.com の場合は **hostmaster.example.com** と入力します）。

ステップ 11 ページ下部にある [ネームサーバー (Nameservers)] に権威ネームサーバー名を入力し、[ネームサーバーの追加 (Add Nameserver)] をクリックします。

権威ネームサーバーはゾーン内のデータを検証します。プライマリサーバーとセカンダリサーバーの両方が権威になることができます。重要な違いは、ゾーンデータを取得する場所です。プライマリサーバーのデータソースは、管理者（サーバーコンフィギュレーションデータベースに保存）と、DNS更新（通常はDHCPサーバー）です。セカンダリサーバーは、指定プライマリサーバーからゾーン転送でゾーンデータを取得します。

ゾーンには少なくとも1つのネームサーバーを追加する必要があります。そうしないと、Cisco Prime Network Registrar ではゾーンデータが完全だとみなされません。入力するネームサーバーは、ドメイン外のユーザーがゾーン内の名前を解決しようとするときにクエリの送信先となるネームサーバーである必要があります。ゾーンのプライマリサーバーに加えて、権威ネームサーバーを追加する必要があります。ゾーンのプライマリDNSサーバーがゾーン内にある場合は、そのホストアドレスを作成する必要があります。

すべての DNS internal-to-zone ネームサーバーに対して、サーバードメイン名をIPアドレスに関連付けるアドレス (A) リソースレコード (RR) を作成する必要があります。

- a) [ホスト (**Host**)] をクリックして [ゾーンのリスト表示 (List Zones)] ページを開きます。
- b) ゾーン名をクリックして [ゾーンのリスト表示/追加 (Add Hosts for Zone)] ページを開きます。
- c) 権威サーバーのホスト名を入力します。
- d) そのIPアドレスを入力します。
- e) [ホストの追加 (**Add Host**)] をクリックします。サーバーのホスト名とアドレスがリストに表示されます。
- f) ホストを編集するには、その名前をクリックして [ホストの編集 (Edit Host)] ページを開きます。[変更 (**Modify**)] をクリックして、変更を行います。

ステップ 12 必要に応じて、追加の属性を設定します。

ステップ 13 [保存 (**Save**)] をクリックします。

CLI コマンド

プライマリゾーンを作成するには、**zone name create primary nameserver contact** を使用します。プライマリDNSサーバーを指定する必要があります。このサーバーは、最初の権威DNSネームサーバーになります。次に例を示します。

```
nrcmd> zone example.com create primary ns1 hostadmin
```

シリアル番号はデフォルトで1に設定されています。（DNSサーバーが動作していない場合に）実際のシリアル番号を取得するには、**zone name get serial** を使用します（サーバーが動作していない場合や、ゾーン属性がリスト表示または表示されない場合は、提案シリアル番号が常に返されます）。

ゾーンの権威ネームサーバーを追加するには、**zone name set nameservers=list** を使用して、完全修飾ドメイン名のカンマ区切りリストを入力します。入力された最初のサーバーだけがコマンドによって確認されることに注意してください。**zone name show** を使用して、すべてのサーバー名を表示します。

zone name addRR hostname A address を使用して、権威サーバーのホスト名とアドレスを追加します。ホストをリストに表示するには、**zone name listHosts** を使用します。ホストを削除するには、**zone name removeRR hostname A** を使用します。

ゾーンの作成時に既存のテンプレートを適用する場合は、*template* 属性を使用します。次に例を示します。

```
nrcmd> zone example.com create primary ns1 hostadmintemplate=zone-template-1
```



(注) この例では、構文の一部としてネームサーバーと連絡先を指定する必要がありますが、テンプレート定義が存在する場合は、指定したネームサーバーと連絡先は上書きされます。

ゾーンの作成後にテンプレートを適用するには、**zone name applyTemplate template** を使用します。次に例を示します。

```
nrcmd> zone example.com applyTemplate zone-template-1
```

プライマリ ゾーン編集

プライマリゾーンを編集してそのプロパティを変更したり、テンプレートを適用したり、ゾーン定義を使用してテンプレートを作成したりできます。

ローカルの詳細 Web UI とリージョン Web UI

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、[正引きゾーンのリスト表示/追加 (List/Add Forward Zones)] ページを開きます。

ステップ 2 [正引きゾーン (Forward Zones)] ペインでゾーンを選択し、[ゾーンの編集 (Edit Zone)] ページを開きます。

ステップ 3 必要に応じて、属性を変更します。

ステップ 4 ゾーンにテンプレートを適用するには、ページの下部にあるドロップダウンリストからテンプレート名を選択し、[テンプレートの適用 (Apply Template)] をクリックします。

注意 すでに運用されているゾーンにはテンプレートを慎重に適用してください。すでに定義されているゾーン属性は、テンプレートに明示的に定義されている属性に置き換えられます。

ステップ 5 ゾーンを変更する際に、ゾーン定義を使用してテンプレートを作成するには、[ゾーンの変更とテンプレートの保存 (Modify Zone and Save Template)] をクリックします。[新しいゾーンテンプレートの保存 (Save New Zone Template)] ページで、[値 (Value)] フィールドにテンプレート名を入力し、[ゾーンテンプレ

トの保存 (**Save Zone Template**)] をクリックします。[ゾーンのリスト表示/追加 (List/Add Zones)] ページに戻ります。

ゾーン ネームサーバー設定の確認

作成した RR を調べてゾーン NS RR の設定を確認します。

ローカルの詳細 Web UI とリージョン Web UI

[正引きゾーン (Forward Zones)] ペインからゾーンを選択し、[リソースレコード (**Resource Records**)] タブをクリックします。ゾーン内のネームサーバー ホストごとに A レコードが存在する必要があります。このページでこれらのレコードを編集または追加します。

[ゾーンへのリソースレコードの追加 \(222 ページ\)](#) を参照してください。

CLI コマンド

`zone name listRR` を使用して、追加した RR を確認します。

ゾーンの同期

手動によるゾーンの同期は、HA メインと HA バックアップの間に不整合があり、それがサーバーによって自動的に解決されない場合にのみ使用します。ゾーンを同期する必要がある場合は、次の手順を実行します。

地域の高度な Web UI

- ステップ 1** [デザイン (**Design**)] メニューの [認証DNS (**Auth DNS**)] サブメニューの [転送ゾーン (**Forward Zones**)] を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)] ページを開きます。
- ステップ 2** プライマリ正引き/逆引きゾーンに対して [ゾーンの同期 (**Zone Sync**)] タブを選択します。
- ステップ 3** [ゾーンの同期 : レポート (**Sync Zone - Report**)] ボタンをクリックして [ゾーンの同期 (**Synchronize Zone**)] ページを開きます。
- ステップ 4** エキスパートモードでは、[RR データからの CCM ホストの同期 : レポート (**Sync CCM Hosts from RR Data - Report**)] ボタンが表示されます。

CLI コマンド

`zone name sync <update | complete> [-report-only | -report]` コマンドは、リージョンクラスタに接続されている場合に使用できます。

ゾーンコマンド

[List/Add Zones (Forward/Reverse zone)] ページに **Commands** ボタンが表示されます。クリックすると、[コマンド (Commands)] ダイアログボックスが開きます。次のコマンドは、特定の目的で使用します。

- **Scavenge zone** : 『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。
- **Get scavenger start time** : 『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。
- **HA ゾーンの同期 (正引きゾーン)** : [HA DNS ゾーンの同期 \(177 ページ\)](#) を参照してください。



(注) **Synchronize HA Zone** コマンドは、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。

ゾーンデータのインポートおよびエクスポート

プライマリ ゾーンを作成する最も簡単かつ迅速な方法は、RFC 1035 で定義されている既存の BIND フォーマット ゾーン ファイルをインポートすることです。同じ種類のファイルを別のサーバーにエクスポートすることもできます。BIND 4.x.x は `named.boot` というブートファイルを使用して、サーバーをデータベース ファイルにポイントします。CLI で `import` コマンドを使用して、BIND 4.x.x コンフィギュレーションのすべてをインポートできます。BIND 8 と BIND 9 は、別の構文で `named.conf` というコンフィギュレーションファイルを使用します。

ゾーンデータのインポートとエクスポートは CLI でのみ可能です。

BIND ファイルに `$INCLUDE` ディレクティブが含まれている場合、BIND は `named.boot` ファイルでディレクトリ ディレクティブが示すディレクトリを対象にインクルードファイルを検索します。一方、`nrcmd` プログラムは、処理されているゾーン ファイルを含むディレクトリを対象にインクルードファイルを検索します。

この問題を回避するために、ゾーンファイル内のインクルードファイルを指定するときには、BIND コンフィギュレーションで絶対パスが使用されるようにしてください。インクルードファイルを指定する際の相対パスがゾーン ファイルに含まれていて、ゾーンファイルが存在するディレクトリが、`named.boot` ファイルでディレクトリディレクティブが示すディレクトリと同じではない場合は、コンフィギュレーションは適切にロードできません。BIND コンフィギュレーションを Cisco Prime Network Registrar にインポートできるように、ゾーンファイルに含まれている相対パスを絶対パスに変換する必要があります。ディレクトリ階層、コンフィギュレーションファイル、およびゾーン ファイルのコンフィギュレーションとパス変更方法の例を次に示します。

- ディレクトリ階層 :

```

/etc/named.conf
/etc/named.boot
/usr/local/domain/primary/db.example
/usr/local/domain/primary/db.include
/usr/local/domain/secondary

```

- コンフィギュレーション ファイル (/etc/named.conf) :

```

#BIND searches for zone files and include files relative to /usr/local/domain
option directory /usr/local/domain
#BIND finds zone file in /usr/local/domain/primary
zone example.com {
    type primary ;
    file primary/db.example ;
}
#end of /etc/named.conf

```

- コンフィギュレーション ファイル (/etc/named.boot) :

```

#BIND searches for zone files and include files relative to /usr/local/domain
directory /usr/local/domain
#BIND finds zone file in /usr/local/domain/primary
primary example.com primary/db.example
#end of /etc/named.boot

```

- 不適切なゾーン ファイル (/usr/local/domain/primary/db.example) :

```

#BIND searches for include file relative to /usr/local/domain
$INCLUDE primary/db.include
#end of /usr/local/domain/primary/db.example

```

コンフィギュレーションをロードできるようにするには、ファイル `db.example` の相対パス (`$INCLUDE primary/db.include`) を絶対パス (`$INCLUDE /usr/local/domain/primary/db.include`) に変更します。

次の表は、BIND 4 と BIND 9 でサポートされる `named.boot` および `named.conf` ファイル ディレクティブと、対応する Cisco Prime Network Registrar ユーザー インターフェイスの場所または構文 (存在する場合) を説明しています。

表 52: バインドから CLI へのコマンドのマッピング

BIND 4 コマンド	BIND 9 コマンド	ユーザー インターフェイスへのマッピング
—	<code>acl name { addr-match-list };</code>	Web UI : [アクセス制御リストの表示/追加 (List/Add Access Control Lists)] ページのフィールド (『Cisco Prime Network Registrar 11.1 DHCP ユーザ ガイド』の「DNS キャッシュ サーバーまたはゾーンでの ACL の割り当て」の項を参照)。 CLI: <code>acl name create value match-list=addr-match-list</code>
—	<code>key id { algorithm string ; secret string };</code>	Web UI : [暗号キーのリスト表示/追加 (List/Add Encryption Keys)] ページのフィールド。 CLI: <code>key name create secret algorithm=alg</code>

BIND 4 コマンド	BIND 9 コマンド	ユーザー インターフェイスへのマッピング
limit transfers-in num	options { transfers-in num };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで <i>xfer-client-concurrent-limit</i> を設定します。 CLI: session set visibility=3 dns set xfer-client-concurrent-limit=number
—	options { allow-query addr-match-list };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで、 <i>restrict-query-acl</i> を有効にします。 CLI : dns set restrict-query-acl
options listen-on port	options { listen-on port {addr-match-list} };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで [リスニングポート (Listening port)] を設定します。 CLI: dns set local-port-number=port
options max-cache-ttl num	options { max-cache-ttl num };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] で [最大 RR キャッシュ TTL (Max. RR caching TTL)] を設定します。 CLI: dns set max-cache-ttl=num
options no-fetch-glue	options { fetch-glue no };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで [欠落しているグルーレコードを取得しない (Don't fetch missing glue records)] を有効にします。 CLI : dns enable no-fetch-glue
options notify yes	options { notify yes };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで [ゾーン変更通知の送信 (NOTIFY) (Send zone change notification (NOTIFY))] を有効にします。 CLI : dns enable notify
<i>options rrsset-order order order ...</i>	options { rrsset-order order ; order ; ... };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで [ラウンドロビンの有効化 (Enable round-robin)] を有効にします。 CLI : dns enable round-robin
options support-ixfr yes	options { request-ixfr yes };	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで [要求の増分転送 (IXFR) (Request incremental transfers (IXFR))] を有効にします。 CLI : dns enable ixfr-enable

BIND 4 コマンド	BIND 9 コマンド	ユーザー インターフェイスへのマッピング
options transfer-format many-answers	options { transfer-format many-answers ;};	Web UI : [DNS サーバーの編集 (Edit DNS Server)] ページで [ゾーン転送でのマルチレコード形式の使用 (Use multirec format for zone transfers)]を有効に します。 CLI : dns enable axfr-multirec-default
primary <i>zonename</i> <i>file</i>	zone " <i>name</i> " { type primary; };	Web UI : [ゾーンの追加 (Add Zone)] ページの フィールド。 CLI : zone name create primary file=file
secondary <i>zonename</i> <i>addr list</i> [<i>backupfile</i>]	zone " <i>name</i> " { type secondary; };	Web UI : [セカンダリゾーンの追加 (Add Secondary Zone)] ページのフィールド。 CLI : zone name create secondary ip-addr [,ip-addr ...]
—	zone " <i>name</i> " { allow-query { <i>addr</i> ; ... }};	Web UI : [ゾーンの編集 (Edit Zone)] ページで <i>restrict-query-acl</i> を設定します。 CLI : zone name set restrict-query-acl=addr [,addr ...]
tcplist <i>addrlistxfernets</i> <i>addrlist</i>	zone " <i>name</i> " { allow-transfer { <i>addr</i> ; ... }};	Web UI : [ゾーンの編集 (Edit Zone)] ページで、 <i>restrict-xfer</i> を有効にして <i>restrict-xfer-acl</i> を設定しま す。 CLI : zone enable name restrict-xfer zone name , = addr [addr...] set restrict-xfer-acl

プライマリ逆引きゾーンの設定

正しい DNS 設定を行うには、使用するネットワークごとに逆引きゾーンを作成する必要があります。逆引きゾーンは、IP アドレスをホスト名に変換するために DNS クライアントが使用するプライマリゾーンであり、特別な `in-addr.arpa` ドメインに存在します。逆引きゾーンを手動で作成するか、バインドからインポートできます。サブネットから逆引きゾーンを作成することもできます（「[サブネットからの逆引きゾーンの追加 \(194 ページ\)](#)」を参照）。

ゾーンとしての逆引きゾーンの追加

逆引きゾーンをゾーンとして手動で追加できます。

ローカルおよびリージョン Web UI

[Design] メニューから [権威 DNS (Auth DNS)] サブメニューで [Reverse Zones] を選択して、[逆引きゾーンのリスト表示/追加 (List/Add Reverse Zones)] ページを開きます。このページは [正引きゾーンのリスト表示/追加 (List/Add Forward Zones)] ページとほぼ同じです。次に、

「[プライマリ正引きゾーンの設定 \(184ページ\)](#)」に説明されている正引きゾーンの追加と同じ方法で逆引きゾーンを追加します。ただし、ゾーン名として特別な `in-addr.arpa` ドメインに追加された正引きゾーンネットワーク番号を逆順に使用します。関連する正引きゾーンに使用したものと同一テンプレートまたは SOA と、ネームサーバー値を使用します。

[名前 (Name)] フィールドに DHCPv4 サブネットまたは DHCPv6 プレフィックス値を入力できます。これにより、サブネットまたはプレフィックスが適切な逆引きゾーン名に変換されます。

IPv4 サブネットまたは IPv6 プレフィックスを使用して逆引きゾーンを作成するには、次の手順を実行します。

-
- ステップ 1** [Design] メニューから [権威 DNS (Auth DNS)] サブメニューで [Reverse Zones] を選択して、[逆引きゾーンのリスト表示/追加 (List/Add Reverse Zones)] ページを開きます。
- ステップ 2** [逆引きゾーン (Reverse Zone)] ページで、[逆引きゾーンの追加 (Add Reverse Zone)] アイコンをクリックし、[名前 (Name)] フィールドに値を入力します。次に例を示します。
- **209.165.201.1/24** : IPv4 サブネットを使用して逆引きゾーンを作成します。
 - **2001:db8:ff80:ff80::/64** : IPv6 プレフィックスを使用して逆引きゾーンを作成します。
- ステップ 3** 逆引きゾーン作成の必須フィールドに次のように入力します。
- **Nameserver** : `ns1.example.com.` と入力します (末尾のドットを含む)。
 - **Contact E-Mail** : `hostadmin.example.com.` と入力します (末尾のドットを含む)。
 - **Serial Number** : `1` を入力します。
- ステップ 4** [逆引きゾーンの追加 (Add Reverse Zone)] をクリックします。[逆引きゾーンのリスト表示/追加 (List/Add Reverse Zones)] ページが表示されます。
-

ローカルおよびリージョン Web UI

IPv6 プレフィックスを使用して逆引きゾーンを作成するには、次の手順を実行します。

-
- ステップ 1** [設計 (Design)] メニューから、**DHCPv6** サブメニューの **Prefixes** 下にある を選択し、[DHCP v6 プレフィックスのリスト/追加 (List/Add DHCP v6 Prefixes)] ページを開きます。
- ステップ 2** [プレフィックス (Prefix)] ペインの [プレフィックスの追加 (Add Prefix)] アイコンをクリックして [IPv6 プレフィックスの追加 (Add IPv6 Prefix)] ダイアログボックスを開きます。
- ステップ 3** プレフィックス名 (たとえば、**prefix-1**) とアドレス (たとえば、**2001:db8:ff80:ff80::**) を入力します。
- ステップ 4** ドロップダウンリストからプレフィックス長 (たとえば、**64**) を選択します。
- ステップ 5** [Add IPv6 Prefix] をクリックします。プレフィックスが [DHCP v6 プレフィックスのリスト表示/追加 (List/Add DHCP v6 Prefixes)] ページに追加されます。
- プレフィックスから逆引きゾーンを作成するには、
- a) [Reverse Zone] タブをクリックします。

- b) ゾーンテンプレートを選択します。
- c) **[Report,]** をクリックしてから、**[Run]** をクリックします。

CLI コマンド

zone name create primary および **zone name addRR PTR** を使用して、サーバーのプライマリ逆引きゾーンとポインタ レコードを追加します。ゾーンテンプレートを適用することもできます。

逆引きゾーンの作成方法：

- IPv4 サブネットを使用する場合

たとえば、次のように入力できます。

```
nrcmd> zone 209.165.201.1/24 create primary ns1.example.com. hostadmin.example.com.
```

- IPv6 プレフィックスを使用する場合

たとえば、次のように入力できます。

```
nrcmd> zone 2001:db8::/64 create primary ns1.example.com. hostadmin.example.com.
```

- IPv6 プレフィックスの名前を使用する場合

たとえば、次のように入力できます。

```
nrcmd> prefix prefix-1 create 2001:db8:ff80:ff80::/64
nrcmd> zone prefix-1 create primary ns1.example.com. hostadmin.example.com.
```

サブネットからの逆引きゾーンの追加

逆引きゾーンを手動で作成する代わりに、既存のサブネットから作成することもできます。これは、Web UI でのみ実行できます。

ローカル詳細およびリージョン詳細 Web UI

- ステップ 1 **[Design]** メニューから **[DHCPv4]** サブメニューで **[Subnets]** を選択して、**[サブネットのリスト表示/追加 (List/Add Subnets)]** ページを開きます。
- ステップ 2 逆引きゾーンのサブネットを作成するか、既存のサブネットのいずれかを使用します。
- ステップ 3 **[Reverse Zone]** タブをクリックし、既存のゾーンテンプレートを選択します。
- ステップ 4 **[Report]** をクリックすると、作成のチェンジセットが表示されます。
- ステップ 5 **[Revert]** をクリックして **[サブネットのリスト表示/追加 (List/Add Subnets)]** ページに戻ります。
- ステップ 6 **[Run]** をクリックしてから **[Reverse Zones]** をクリックすると、**[逆引きゾーンのリスト表示/追加 (List/Add Reverse Zones)]** ページに新しく作成したゾーンが表示されます。

サーバーのゾーンカウントの取得

DNS サーバーに関連付けられている作成済みゾーンを表示して、Web UI でカウントを取得できます。

CLI で `dns getZoneCount [forward|reverse|primary|secondary|all]` を使用して、DNS サーバーの全ゾーンの正確なカウントを取得できます。オプションを指定しないと、パブリッシュされたゾーンの総数だけが返されます。

DNS 更新の有効化

DNS 更新 (RFC 2136) は、DNS と DHCP が連携できるように統合します。DNS 更新は、ホストと DHCP で割り当てられたアドレスの関連付けを自動的に記録します。DHCP と DNS 更新を使用することにより、ホストがネットワークに接続するときのホストのネットワークアクセスを自動的に設定できます。一意の DNS ホスト名を使用し、ホストを検索してそこにアクセスできます。

DNS 更新の詳細は、『*Cisco Prime Network Registrar 11.1 DHCP ユーザガイド*』の「Managing DNS Update」の章に記載されています。この章には、次の項があります。

- **Update policy (the Update Policies tab)** : 名前からアドレスへの関連付けが DHCP で変更されたときに更新する RR の種類を決定します。（『*Cisco Prime Network Registrar 11.1 DHCP ユーザガイド*』の「Configuring DNS Update Policies」の項を参照。）
- **Update map (the Update Maps tab)** : DNS サーバーまたは HA DNS ペアと、DHCP フェールオーバー ペア、DHCP ポリシー、クライアント クラス、またはアクセス制御リストの更新関係を定義します。（『*Cisco Prime Network Registrar 11.1 DHCP ユーザガイド*』の「DNS 更新マップの作成」の項を参照）。

セカンダリ サーバーの管理

ゾーンを設定する場合は、少なくとも 1 台のセカンダリ サーバーを選択します。ネームサーバーが 1 台しかなく、それを使用できなくなった場合は、名前を検索できなくなります。セカンダリサーバーは、負荷をプライマリと分けます。プライマリを使用できない場合には、セカンダリサーバーがすべての負荷を処理します。セカンダリサーバーが起動すると、プライマリサーバーに接続してゾーンデータをプルします。これはゾーン転送と呼ばれます。



(注) セキュアモードでのゾーン転送は、HMAC MD5 ベースの TSIG と GSS-TSIG の両方をサポートします。



ヒント セカンダリゾーンの権威サーバーも Cisco Prime Network Registrar 6.0 以降を実行している場合に、ゾーンの手動入力を回避する方法については、「[ゾーン分散の管理 \(201 ページ\)](#)」を参照してください。セカンダリサーバーが 1 台しかない場合は、プライマリサーバーから物理的に離します。セカンダリとプライマリを同じネットワークセグメント、スイッチ、またはルータに配置せずに、まったく別のクラスタに配置します。

セカンダリゾーンを受け持つようにセカンダリ DNS サーバーを設定することで、そのサーバーはそのゾーンに対してセカンダリになります。また、ゾーン転送を実行するプライマリサーバーのアドレスを指定する必要があります。Cisco Prime Network Registrar は、このプライマリサーバーについて認識する必要があります。

セカンダリ正引きゾーンの追加

ローカルクラスタでセカンダリ正引きゾーンを追加できます。

ローカル Web UI

ステップ 1 **Design** メニューから **Auth DNS** サブメニューで **[Secondary Zones]** を選択して、**[セカンダリゾーンのリスト表示/追加 (List/Add Secondary Zones)]** ページを開きます。

ステップ 2 **[セカンダリゾーン (Secondary Zones)]** ペインの **[Add Secondary Zone]** アイコンをクリックすると、**[セカンダリゾーンの追加 (Add Secondary Zone)]** ダイアログボックスが開きます。

セカンダリゾーンには、1 つの名前と 1 つ以上のプライマリサーバーのリストが必要です。ホストのセットへのゾーン転送の制限を有効にしてから、制限したホストのアクセスコントロールリスト (ACL) を `restrict-xfer-acl` フィールドに入力することもできます。必要に応じて、その他の属性値を入力します。

ステップ 3 **[Add Secondary Zone]** をクリックします。

[セカンダリゾーン (Secondary Zones)] ペインでセカンダリゾーン名をクリックして、**[セカンダリゾーンの編集 (Edit Secondary Zone)]** ページを開いて、そこでセカンダリゾーンを編集できます。このページで **[Save]** をクリックします。

セカンダリ正引きゾーンと同じ方法でセカンダリ逆引きゾーンを追加できますが、アドレスは逆引きゾーンアドレスである必要があります。

CLI コマンド

セカンダリゾーンを作成するには、`zone name create secondary address` を使用します。ゾーン転送を実行するには、プライマリ DNS サーバーの IP アドレスを指定する必要があります。

次に例を示します。

```
nrcmd> zone shark.zone. create secondary 172.18.123.177
```

HA DNS サーバー ペアを使用している場合は、IP アドレスをカンマで区切って指定する必要があります。HA DNS バックアップ サーバーは、プライマリ サーバーが使用できない場合に使用されます。

次に例を示します。

```
nrcmd> zone shark.zone. create secondary 172.18.123.177,172.18.123.45
```

ゾーン転送の有効化

セカンダリサーバーはプライマリサーバーに変更（ゾーン転送）を定期的に問い合わせます。この間隔はサーバー SOA レコードでセカンダリ更新時間として定義されます。プライマリサーバーで *restrict-xfer* 属性が **true**（プリセット値）に設定されている場合、ゾーン転送を制限できます。 *restrict-xfer-acl* を適宜設定する必要があります。



(注) ゾーン転送を制限する場合は、**ls** を実行する IP アドレスをゾーン *restrict-xfer-acl* リストに含めない限り、**nslookup utility ls** コマンドは完全ゾーン転送を実行しようとして失敗することがあります。

ローカルの詳細 Web UI とリージョン Web UI

ステップ 1 [正引きゾーン (Forward Zones)] ペインでプライマリ ゾーン名をクリックして、[ゾーンの編集 (Edit Zone)] ページを開きます。

ステップ 2 [ゾーン属性 (zone attributes)] エリアで、*restrict-xfer* 属性を **false**（プリセット値）に設定できます。この属性が **true**（プリセット値）に設定されている場合は、*restrict-xfer-acl* 属性を使用してゾーン転送を制限するサーバーのリストを指定することもできます。それには、IP アドレスをカンマで区切って指定します。

セカンダリ ゾーンでは、他のセカンダリ ゾーンからのゾーン転送を制限することもできます。*restrict-xfer* および *restrict-xfer-acl* 属性をセカンダリ ゾーン設定でも使用できます。

ステップ 3 [Save] をクリックします。

ステップ 4 DNS サーバーのゾーン転送は、次の 2 つの方法で強制できます。

- [セカンダリ ゾーン (Secondary Zones)] ペインで、[完全ゾーン転送 (Full Zone Transfer)] ボタンをクリックします。
- プライマリ サーバーからすべてのゾーン転送を強制するには、[DNS 権威サーバーの管理 (Manage DNS Authoritative Server)] ページで [コマンド (Commands)] ボタンをクリックして、すべてのゾーン転送を強制します。

CLI コマンド

CLI では、**zone namedisable restrict-xfer** を使用して有効にしない限り、ゾーン転送はデフォルトで制限されています。ゾーン転送を強制する場合は、**zone name forceXfer secondary** を使用します。

サブゾーンの設定

ゾーンが拡大するにつれて、サブゾーンと呼ばれる小さな部分に分割することが必要になる場合があります。サブゾーンに対する管理権限を委任して、サブゾーン内で管理させるか、個別サーバーで対応できます。このパーティション分割は、サブゾーン委任と呼ばれます。次のタスクを実行して、サブゾーンの委任を確立します。

1. サブゾーン名を選択します。
2. ネームサーバー名を指定します。
3. ネームサーバー アドレスを指定します。

サブゾーン名とサーバーの選択

ゾーンをサブゾーンに分割することを決定したら、それらの名前を指定する必要があります。サブゾーンの担当者と相談して名前を決定し、一貫した命名スキームを維持するようにします。

次の推奨事項は、サブゾーンの命名問題を回避するのに役立ちます。

- サブゾーンに組織名を付けないようにします。変化するビジネス環境では、組織がマージし、名前が変更されます。組織にちなんだ名前をサブゾーンに付けると、時間が経過するにつれて、名前の意味が失われる可能性があります。
- サブゾーンの場所を示す地理名を使わないようにします。地理名は、組織外の人には意味がありません。
- 不可解ではない明快な名前を使用します。
- 既存または予約済みのトップレベル ドメイン名をサブゾーンとして使用しないでください。既存の名前を使用すると、ルーティングの問題が発生する可能性があります。

サブゾーン名を選択したら、親ドメインネームサーバーがサブゾーンについて照会するときに使用するネームサーバーを指定します。サブゾーンが常に到達可能であるように、2つのネームサーバーを指定する必要があります。それらのネームサーバーはプライマリまたはセカンダリのいずれかとしてこのゾーンに対する権威である必要があります。

サブゾーン ネームサーバーの名前またはアドレスが変わるたびに、サブゾーンの管理者は親ゾーンに通知する必要があります。これにより、親ゾーンの管理者は、サブゾーンネームサーバーとグルーレコードを変更できます。グルーレコードは、サブゾーンの権威ネームサーバーのアドレスを持つ A レコードです。サブゾーン管理者が親への通知に失敗すると、グルーレコードは無効になります。一般的な現象としては、ホストが名前別ドメインのホストに到達できず、アドレスのみで到達できます。



- (注) NS レコードアドレスが一致せず、グルー A レコードが必要な場合に、Cisco Prime Network Registrarは親ゾーンに欠落しているサブゾーン NS レコードを報告することによって、不完全委任を検出します。

サブゾーンの作成と委任

親ゾーンでサブゾーンを作成して委任します。サブゾーンが委任されているネームサーバーごとに1つの NS レコードが存在する必要があります。各 NS レコードには、ネームサーバーが親ゾーンまたはサブゾーンの外側にある場合を除き、ネームサーバーのアドレスを記述した対応する A レコードが必要です。この A レコードは、グルー レコードと呼ばれます。親ゾーンの委任ポイントの NS RR および対応 A レコード (グルー レコード) を作成するゾーンは、親ありゾーンと呼ばれます。親ゾーンの委任ポイントの NS RR および対応 A レコード (グルー レコード) を作成しないゾーンは、親なしゾーンと呼ばれます。

ゾーン *example.com* には親ゾーン *.com* とサブゾーン *subdomain.example.com* があるとします。*example.com* が親ありゾーンの場合は、*example.com* の NS RR は *example.com* 内とその親ゾーン *.com* 内の2か所に作成されます。*example.com* 内のサブドメインまたは親ゾーンのいずれかの委任ポイントに、このゾーンのネームサーバーの権威レコードがあります。親ゾーン *.com* 内の委任ポイントには *example.com* の非権威 NS RR があり、*subdomain.example.com* 内の委任ポイントには *example.com* の非権威 NS RR があります。

サブゾーン名とサーバーの選択 (198 ページ) を参照してください。

ローカル Web UI

- ステップ 1** [正引きゾーンのリスト表示/追加 (List/Add Forward Zones)] ページで、親ドメインのサブドメインとしてゾーンを作成します。
- ゾーン テンプレートを適用する場合は、**ステップ 2** に進みます。
 - ゾーン テンプレートを適用しない場合は、[正引きゾーンのリスト表示/追加 (List/Add Forward Zones)] ページで **[Add Forward Zone]** アイコンをクリックし、そのアドレスを含む SOA レコードとネームサーバーを追加します。
- ステップ 2** Cisco Prime Network Registrar がサブゾーン名に基づいて親ゾーンを検出すると、[親ゾーンでのサブゾーンの作成 (Create Subzone in Parent Zone)] ページが表示されます。このページで **[Create as Subzone]** (またはサブゾーンにする必要がない場合は **[Create as Unparented Zone]**) をクリックします。
- [サブゾーンとして作成 (Create as Subzone)] により、親ゾーンの委任ポイントの NS RR および対応 A レコード (グルー レコード) が作成されます。
- ステップ 3** サブゾーンにネームサーバーを設定した場合は、それに対するグルー アドレス (A) レコードを作成する必要があります。表示されたフィールドに、ネームサーバーの IP アドレスを入力して、**[Specify Glue Records]** をクリックします。(複数のサブゾーンネームサーバーがある場合、グルー レコードに対して複数のフィールドがあります。)

- ステップ 4** **[Report]** をクリックすると、追加したレコードに対して意図したチェンジセットが表示されます。
- ステップ 5** 実装された実際のチェンジセットが表示されたら、**[Return]** をクリックします。
- ステップ 6** サブゾーンの追加レコードを確認するには、サブゾーンの **[RR]** 列で **[表示 (View)]** アイコンをクリックします。サブゾーン ネームサーバーのグルー A レコードが表示されます。**[Return to Zone List]** をクリックします。
- ステップ 7** 親ゾーンの追加レコードを確認するには、親ゾーンの **[RR]** 列で **[表示 (View)]** アイコンをクリックします。サブゾーン ネームサーバー (NS) レコードとグルー A レコードが表示されます。**[Return to Zone List]** をクリックします。

CLI コマンド

サブゾーンのプライマリ ネームサーバー マシンで、サブドメインを作成します。

```
nrcmd> zone boston.example.com. create primary bostonDNSserv1 hostadmin
```

親ゾーン ネームサーバーのマシンで、サブゾーン ネームサーバーの NS レコードを追加してから、サブゾーン ネームサーバーのグルー A レコードを作成します。

```
nrcmd> zone example.com. addRR boston NS bostonDNSserv1.boston.example.com.
nrcmd> zone example.com. addRR bostonDNSserv1.boston.example.com. A 192.168.40.1
```

サブゾーン委任の編集

サブゾーン RR を編集できます。

ローカルおよび地域 Web UI

- ステップ 1** 対応する **[ゾーンの編集 (Edit Zone)]** ページで、**[リソース レコード (Resource Records)]** タブをクリックし、レコードの横にある **[編集 (Edit)]** アイコンをクリックすると、**[ゾーンの RR の編集 (Edit RR in Zone)]** ページが開きますので、サブゾーンの NS RR を編集します。
- ステップ 2** NS レコード データを編集します。
- ステップ 3** **[リソース レコードの変更 (Modify Resource Record)]** をクリックします。
- ステップ 4** 前の手順と同じ方法で、サブゾーン サーバーのグルー A RR を編集します。

CLI コマンド

zone name removeRR を使用して NS とグルー A レコードを削除してから、**zone name addRR** を使用して置換します。

サブゾーンの委任解除

サブゾーンの委任を解除する場合は、関連 NS とグルー A レコードを親ゾーンから削除する必要があります。



- (注) サブゾーンを削除すると、Cisco Prime Network Registrar が委任レコードを自動的にクリーンアップします。

ローカルおよびリージョン Web UI

対応する [ゾーンの編集 (Edit Zone)] ページで、[Resource Records] タブをクリックし、サブゾーンの NS レコードを削除してから、サブゾーン サーバー ホストのグルー A レコードを削除します。

CLI コマンド

`zone name removeRR NS` および `zone name removeRR A` を使用して、サブゾーン NS とグルー A レコードを削除します。

ゾーン分散の管理

ゾーン分散を作成することにより、同じセカンダリゾーン属性を共有する複数のゾーンを簡単に作成できます。これにより、プライマリからセカンダリへの共有や、DNSHA の場合のメインからバックアップへの共有など、ゾーン関係を共有する複数のクラスタのセットアップと管理が非常に簡単になります。

ゾーン分散では、1つ以上の定義済みセカンダリサーバーを追加する必要があります。ゾーン分散同期を実行すると、プライマリサーバーで管理される各プライマリゾーンに対して、セカンダリサーバーで管理されるセカンダリゾーンが追加されます。ゾーン分散を使用して、CCM データベースのゾーンデータをローカル DNS サーバーやリージョンおよびローカルクラスタゾーンデータに同期することもできます。ゾーンデータを同期するたびに、プライマリゾーンとセカンダリゾーンの両方の関連ビューと名前付き ACL が同期されます。

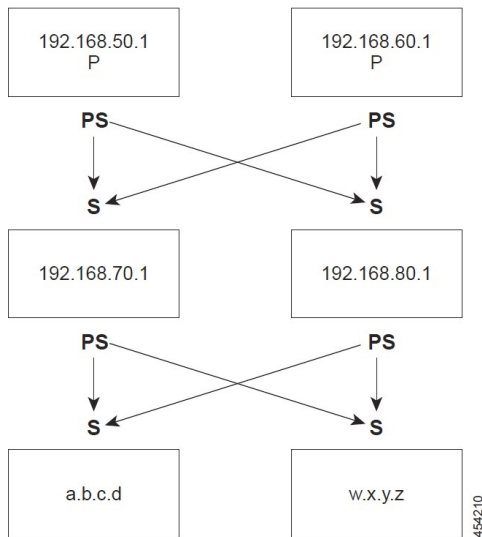
分散は1台のプライマリサーバーと複数のセカンダリサーバーで構成されるスタートポロジである必要があります。権威サーバーは、ゾーン分散のデフォルトが定義されているローカルプライマリサーバーにしかありません。ローカルクラスタで1つのゾーン分散を管理し、リージョナルクラスタで複数の分散を管理できます。

ゾーン分散マップの準備

ゾーン分散の作成を準備をするには、紙にゾーン分散マップの図を描きます。

- ステップ 1** マップに含めるすべてのゾーンについて、プライマリである HA DNS ペア（または HA でない場合はプライマリサーバー）を特定することから始めます。
- HA DNS ペアのサーバーごとにボックスを作成します。たとえば、シカゴクラスタのサーバーペアは、192.168.50.1 と 192.168.60.1 のサーバーで構成されます。
 - 各ボックスに各サーバーの IP アドレスを記入します。
 - 各ボックスの内側にプライマリを示す **P** を記入します（次の図を参照）。

図 17: ゾーン分散マップの図式化



- ステップ 2** 各サーバーの「セカンダリのプライマリサーバー (Primary Server of Secondary)」ロールを示す **PS** をボックスの下に記入します。この例の場合は、定義の上では、両方のプライマリサーバーがゾーン転送でゾーンのコピーを他のサーバーに送信するセカンダリのプライマリサーバーでもあります。それでも、後のステップを簡単にするために、ボックスの下に **PS** を記入してください。
- ステップ 3** これらのプライマリサーバー (PS) からゾーン転送を直接受信するすべてのセカンダリサーバーを特定します。ページのプライマリサーバーボックスの下に、各セカンダリ用のボックスを追加し、そのボックスの内側にセカンダリの IP アドレスを記入します。たとえば、192.168.70.1 と 192.168.80.1 のセカンダリサーバーは、シカゴクラスタプライマリサーバーからゾーン転送を受信します。
- ステップ 4** 各セカンダリサーバーボックスの上に **S** を記入します。
- ステップ 5** **PS** から各 **S** への矢印を書いて、ゾーン転送フローを表します (図を参照)。この HA DNS の例では、矢印は各プライマリサーバーから両方のセカンダリサーバーに移動します。
- ステップ 6** この図からわかるように、このボックスを増やすことで、元はセカンダリであったサーバーが別のサーバーセット (a.b.c.d と w.x.y.z) に対するプライマリサーバーになります。
- ステップ 7** ゾーン分散を作成するときには、下に **PS** が付いている各ボックスの IP アドレスをプライマリサーバーリストに入力します。

CLI では、たとえば次のように *primary-servers* 属性を IP アドレスリストに設定します。

```
nrcmd> zone-dist dist-1 create Chicago-cluster primary-servers=192.168.50.1,192.168.60.1
```

- ステップ 8** [ゾーン分散セカンダリサーバーの追加または編集 (Add or Edit Zone Distribution Secondary Server)] ページの [セカンダリサーバー (Secondary Servers)] ドロップダウンリストから、上に **S** が付いているボックスのセカンダリサーバー IP アドレスに関連付けられているクラスタを選択します。

CLI で、**zone-dist name addSecondary cluster** を使用します。例：

```
nrcmd> zone-dist dist-1 addSecondary Boston-cluster
```

ゾーン分散の作成



(注) ゾーンを別のゾーン分散に移動する場合は、最初のゾーン分散を同期し、ゾーンを移動してから、2 番目のゾーン分散を同期します。

ローカルおよびリージョン Web UI

- ステップ 1** Deployメニューの [DNS] サブメニューから、リージョナルクラスタの場合は **Zone Distributions**、ローカルクラスタの場合は **Zone Distribution** を選択します。サーバーが権威サービスを使用して設定されている場合は、このオプションを使用できます。リージョンの [ゾーン分散のリスト表示/追加 (List/Add Zone Distributions)] ページ、またはローカルの [ゾーン分散の表示 (View Zone Distribution)] ページが開きます。デフォルトのゾーン分散は両方のクラスタで事前に定義されていますが、デフォルトのクラスタを使用できるのはローカルクラスタのみであることに注意してください。
- ステップ 2** 新しいゾーン分散を追加するには、[**Add Zone Distribution**] アイコンをクリックして [ゾーン分散の追加 (Add Zone Distribution)] ダイアログボックスを開きます。既存のゾーン分散を編集するには、ゾーン分散名を選択して [ゾーン分散の編集 (Edit Zone Distribution)] ページを開きます。
- ステップ 3** [プライマリ サーバー (Primary Server)] フィールドに、プライマリ サーバーがあるクラスタ（または設定されている HA DNS ペア）を入力します。このプライマリ サーバーは、ページ下部で指定するゾーンに対する権威となります。この選択は引き算方式です。次のゾーン分散を作成すると、ここで選択肢の 1 つとして設定したクラスタはそのゾーン分散に含まれなくなります。
- ステップ 4** [プライマリサーバー (Primary Servers)] リストで、セカンダリの各プライマリサーバーの IP アドレス（およびオプションのキー）を追加します。通常は、このサーバーはプライマリサーバーです。ただし、セカンダリ関係ごとにプライマリサーバーを定義する必要がある場合は、プライマリとセカンダリの階層を設定することを推奨します。プライマリサーバーリストから HA DNS サーバーペアを決定することもできます。オプションの TSIG キーまたは GSS-TSIG キー（『Cisco Prime Network Registrar 11.1 DHCP ユーザーガイド』の「Transaction Security」の項または「GSS-TSIG」の項を参照）をプライマリサーバーアドレスに追加することもできます。それには、address-key の形式でエントリをハイフンでつなぎます。エントリごとに [**Add IP Key**] をクリックします。
- ステップ 5** 1 つのゾーン分散に少なくとも 1 つのセカンダリ サーバーを追加する必要があります。[ゾーン分散の編集 (Edit Zone Distribution)] ページの **Add Secondary Server** をクリックします。セカンダリサーバーのクラスタを選択します。セカンダリのプライマリサーバーがゾーン分散に対して指定されたプライマリサーバー以外の場合は、セカンダリのプライマリサーバーアドレスをカンマで区切って追加できます。[**Add Server**] をクリックすると、[編集 (Edit)] ページに戻ります。セカンダリサーバークラスタに接続するか、それを削除するか、それを編集してセカンダリのプライマリサーバーを変更することができます。
- ゾーン分散のセカンダリサーバーを管理するには、[サーバーの管理 (Manage Servers)] 列の [表示 (View)] アイコンをクリックして [セカンダリ サーバーのリスト (List Secondary Servers)] ページを開きます。[ゾーン分散セカンダリ サーバーの編集 (Edit Zone Distribution Secondary Server)] ページでセカンダリサーバーを編集することもできます。

- ステップ 6** ゾーン分散の正引きゾーンと逆引きゾーンを選択します。デフォルトのゾーン分散には、作成したすべての正引きゾーンと逆引きゾーンが含まれます。作成した他のすべてのゾーン分散では、ゾーンを [選択済み (Selected)] 列に移動する必要があります。
- ステップ 7** [Save] をクリックします。
- ステップ 8** ゾーン分散をローカル クラスタ DNS サーバーと同期します。同期は、次のように行われます。
- 段階ゾーン、RR、またはホストの編集は、[保証 (Ensure)]、[置換 (Replace)]、または [正確 (Exact)] モードではプライマリ サーバー クラスタまたはリージョン クラスタの HA DNS ペアにプッシュされ、[正確 (Exact)] モードではローカル クラスタからプッシュされます。
 - セカンダリ サーバーのセカンダリ ゾーンを [正確 (Exact)] モードで作成します。
- ステップ 9** [Synchronize Zone Distribution] タブをクリックして、同期モードを選択します。
- **Update** : 新しいゾーン、RR セット、およびホストが追加されます。競合がある場合は、既存のホストが置き換えられます。新しいセカンダリ ゾーンが作成されます。
 - **Complete** : [保証 (Ensure)] モードと似ていますが、既存の RR セットとホストが常に置換され、既存のセカンダリゾーンのプライマリサーバーリストが変更される点が異なります。
 - **Exact** : [完全 (Complete)] モードと似ていますが、プライマリに存在しなくなった余分なゾーン、RR セット、ホスト、およびセカンダリ ゾーンが削除される点が異なります。
- ステップ 10** [ゾーン分散の同期 (Synchronize Zone Distribution)] タブで **Report** をクリックします (または、リージョン クラスタのページの [すべてのゾーン分散の同期 (Synchronize All Zone Distributions)] 領域で同じアイコンをクリックします) 。[ゾーン分散の同期 (Sync Zone Distribution)] ページが開き、同期されたデータのプレビューが表示されます。

CLI コマンド

ゾーン分散を作成するには、**zone-dist name create primary-cluster** を使用します (プライマリ クラスタも HA DNS ペアになることができます) 。次に例を示します。

```
nrcmd> zone-dist dist-2 create Chicago-cluster
```

セカンダリのプライマリサーバーを設定するには、**zone-dist name set primary-servers=addresses** を使用して、アドレスをカンマで区切ります。次に例を示します。

```
nrcmd> zone-dist zone-dist-2 set primary-servers=192.168.50.1,192.168.60.1
```

セカンダリ サーバーを追加するには、**zone-dist name addSecondary secondary-cluster** を使用します。次に例を示します。

```
nrcmd> zone-dist zone-dist-2 AddSecondary Boston-cluster
```

ゾーン分散をゾーンまたはゾーン テンプレートに直接関連付ける必要があります。**zone name set dist-map=zone-dist-list** または **zone-template name set dist-map=zone-dist-list** を使用して、ゾーン分散エントリをカンマで区切ります。次に例を示します。

```
nrcmd> zone example.com set dist-map=zone-dist-2
nrcmd> zone-template zone-template-1 set dist-map=zone-dist-2
```

ゾーン分散を同期するには、**zone-dist name sync** を使用します。同期を **update**、**complete**、または **exact** モードで行い、RR とセカンダリ ゾーンを除外できます。

- ローカルクラスタでは、段階編集が DNS サーバーに同期され、プライマリ ゾーンがセカンダリに同期されます。同期モードに関係なく、権威ゾーンの正確なリストが常に同期されます。
- リージョンクラスタでは、プライマリ ゾーンがローカルクラスタに同期され、プライマリがセカンダリに同期されます。これにより、**Update** モードと **Complete** モードではローカルクラスタのプライマリゾーンが置き換えられ、**Exact** モードではローカルクラスタの余分なプライマリ ゾーンが削除されます。
- セカンダリ ゾーンでは、同じ同期ロジックがローカルクラスタとリージョンクラスタで生じます。**Update** モードでは、これにより、対応するセカンダリ ゾーンがサーバーに存在するようになります。**Complete** モードでは、ゾーン分散マップで指定されたプライマリサーバーリスト（セカンダリのプライマリサーバー）を使用するように既存のゾーンが更新されます。**Exact** モードでは、分散マップに一致しないゾーンは削除されます。

次に例を示します。

```
nrcmd> zone-dist zone-dist-1 sync exact no-rrs no-secondaries
```

レプリカ データからのゾーン分散のプル

ゾーンの分散を明示的に作成するのではなくローカル レプリカ データからプルできます。



ヒント ゾーン分散を作成するためにローカルゾーンデータをプルする例については、『Cisco プライムネットワークレジストラ 11.1 管理ガイド』の「ゾーンデータのプルとゾーン分布の作成」の項を参照してください。

リージョン Web UI

- ステップ 1** **Deploy** メニューの [DNS] サブメニューから **Zone Distribution** を選択して、[ゾーン分散のリスト/追加 (List/Add Zone Distribution)] ページを開きます。
- ステップ 2** [ゾーン分散のリスト/追加 (List/Add Zone Distribution)] ページで、[ゾーン分散の同期 (Synchronize Zone Distribution)] タブをクリックします。
- ステップ 3** ゾーン同期モード (**Update**、**Complete**、または **Exact**) を選択します。これらのモードについては、そのページの表に説明されています。
- ステップ 4** ダイアログボックス上部で [**Report**] をクリックします。
- ステップ 5** [**実行 (Run)**] をクリックします。

DNS ENUM ドメインの管理

別個の ENUM ドメインを作成することで、Naming Authority Pointer (NAPTR) 電子番号 (ENUM) の管理が簡素化されます。それによって、E.164 番号のセットアップと管理や、利用可能なサービスが E.164 番号に接続する方法が大幅に簡素化されます。ENUM ゾーンを作成して、対応する E.164 番号を追加すると、Cisco Prime Network Registrar が正引きゾーンと各 NAPTR リソース レコードを自動的に作成します。

DNS ENUM デフォルトの管理

デフォルトの ENUM 設定を構成するには、次の手順を実行します。

ローカル Web UI

- ステップ 1** [設計 (Design)]メニューの [DNS ENUM] サブメニューで [デフォルト (Defaults)] を選択して [DNS ENUM デフォルトの管理 (Manage DNS ENUM Defaults)] ページを開きます。
- ステップ 2** トップレベル ドメインを入力します。
- ステップ 3** ローカルプレフィックスを入力します (例 : +46) 。
- ステップ 4** デフォルトサービスの値を入力します。これを行うには、[サービス (Services)] セクションの [追加 (Add)] ボタンをクリックし、サービスタイプを選択して URI を入力し、[追加 (Add)] をクリックします。
- ステップ 5** ドロップダウンリストから [ゾーンテンプレート (Zone Template)] を選択します。
- ステップ 6** [保存 (Save)] をクリックします。

CLI コマンド

dns-enum-config set [number-prefix prefix | zone-template name] を使用して、デフォルトの ENUM ドメイン、デフォルトのトップレベルドメイン、ローカルプレフィックス、サービス、およびゾーンテンプレートを設定します。

dns-enum-config addService type subtype URI [order [preference]] を使用して、デフォルトのサービスを追加します。

dns-enum-config removeService type subtype URI を使用して、デフォルトのサービスユーザーを削除します。

DNS ENUM ドメインの追加

ENUM ドメインを追加するには、ドメイン名を作成する必要があります。所有者を定義し、ゾーンテンプレートを使用することもできます。

ENUM ゾーンを作成する際、Cisco Prime Network Registrar は自動で正引きゾーンを作成します。たとえば、E.164 番号プレフィックス 100 の ENUM ドメインを作成し、デフォルトの最上

位ドメインが `e164enum.net` に設定されている場合は、正引きゾーン `0.0.1.e164enum.net.` が自動的に作成され、正引きゾーンのリストに表示されます。

ENUM ドメインを構成するには、次の手順を実行します。

ローカルおよび地域 Web UI

- ステップ 1** [設計 (Design)]メニューの [DNS ENUM] サブメニューで [ドメイン (Domains)]を選択して [DNS ENUM ドメインのリスト/追加 (List/Add DNS ENUM Domains)] ページを開きます。
- ステップ 2** [ドメイン (Domains)] ペインの [ドメインの追加 (Add Domains)] アイコンをクリックして [ENUM ドメインの追加 (Add ENUM Domain)] ダイアログボックスが開きます。
- ステップ 3** ドメインの E.164 番号プレフィックス (897 など) を入力します。
- ステップ 4** ネームサーバー ホスト名 (ns1 など) を入力します。
- ステップ 5** たとえば、hostadmin などの連絡先の電子メール名を入力します。
- ステップ 6** [ENUM ドメインの追加 (Add ENUM Domain)] をクリックします。ドメインは、デフォルトのローカルプレフィックス (+4689 など) を使用して作成されます。基本モードでは、次のプリセット値を使用してゾーンが作成されます。
 - [ゾーンのデフォルト TTL (Zone default TTL)] : 24 時間
 - [Start of Authority (SOA) シリアル番号 (Start of Authority (SOA) serial number)] : 1
 - [SOA セカンダリ更新時間 (SOA secondary refresh time)] : 3 時間
 - [SOA セカンダリ再試行時間 (SOA secondary retry time)] : 60 分
 - [SOA セカンダリ有効期間 (SOA secondary expiration time)] : 1 週間
 - [SOA 最小 TTL (SOA minimum TTL)] : 10 分

CLI コマンド

dns-enum-domain name create [zone-template=name] [nameservers [person]] を使用して ENUM ドメインを作成します。

dns-enum-domain name delete を使用して ENUM ドメインを削除します。

リージョン クラスタに接続されているときには、次のコマンド pull、push、および reclaim を使用できます。

dns-enum-domain <name | all > pull < ensure | replace | exact > cluster-name [-report-only | -report]

dns-enum-domain <name | all > push < ensure | replace | exact > cluster-list [-report-only | -report]

dns-enum-domain name reclaim cluster-list [-report-only | -report]

DNS ENUM 番号の追加

Cisco Prime Network Registrar は、NAPTR RR をサポートしています。これらのレコードは、特定の名前空間の名前解決に役立つとともに、解決サービスに到達するために処理されます。

NAPTR リソース レコードを追加するオプションに加えて、E.164 番号を直接追加し、対応するサービスを番号に関連付けることができるようになりました。DNS ENUM 番号を追加する場合は、親ドメインまたはゾーンテンプレートの E.164 番号プレフィックスのいずれかを指定する必要があり、E.164 番号に対する NAPTR リソース レコードが作成されます。このアプローチでは、逆順の E.164 番号を使用し、すべての桁を DNS 名前階層のノードとして扱います。たとえば、E.164 アドレス +4689761234 の場合は、+46 E.164 プレフィックス ドメインの NAPTR RR 4.3.2.1.6.7.9.8 が作成されます。

NAPTR リソース レコードの詳細については、「[NAPTR リソース レコードを使用した名前空間の名前解決 \(229 ページ\)](#)」を参照してください。

ローカルおよび地域 Web UI

- ステップ 1 [設計 (Design)] メニューの [DNS ENUM] サブメニューで [番号 (Numbers)] を選択して、[DNS ENUM 番号のリスト/追加 (List/Add DNS ENUM Numbers)] ページを開きます。
- ステップ 2 [番号 (Numbers)] ペインの [番号の追加 (Add Numbers)] アイコンをクリックすると、[ENUM 番号の追加 (Add ENUM Number)] ダイアログボックスが開きます。
- ステップ 3 E.164 番号プレフィックスとともに E.164 番号を入力します (1234 など)。
- ステップ 4 [サービス (Services)] セクションの [追加 (Add)] ボタンをクリックし、サービスタイプを選択して URI を入力し、[追加 (Add)] をクリックします。
- ステップ 5 親ドメインの E.164 番号プレフィックスを入力します。
- ステップ 6 E.164 プレフィックスを指定していない場合は、ゾーン テンプレートを選択します。
- ステップ 7 [移植 (Ported)] オプションを選択し、移植ネームサーバー FQDN を入力します。
- ステップ 8 [ENUM 番号の追加 (Add ENUM Number)] をクリックします。この番号は作成されてドメイン +4689 の下に追加されます。

CLI コマンド

dns-enum-number number create type subtype URI [zone-template=name] [domain-prefix] を使用して、ENUM 番号を作成します。

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。プッシュおよび再利用の場合は、クラスターのリストまたは「すべて」を指定できます。

dns-enum-number <name | all> pull <ensure | replace | exact> cluster-name [-report-only | -report]

dns-enum-number <name | all> push <ensure | replace | exact> cluster-list [-report-only | -report]

dns-enum-number name reclaim cluster-list [-report-only | -report]

ENUM ドメインのプルとプッシュ

リージョン クラスタ Web UI の [DNS ENUM ドメインのリスト表示/追加 (List/Add DNS ENUM Domains)] ページで、ローカル クラスタに ENUM ドメインをプッシュしたり、ローカル クラスタから ENUM ドメインをプルしたりすることができます。

ローカルクラスタへの ENUM ドメインのプッシュ

ENUM ドメインをローカルクラスタにプッシュするには、次の手順を実行します。

地域の Web UI

- ステップ 1** [設計 (Design)]メニューの [DNS ENUM] サブメニューで [ドメイン (Domains)] を選択してリージョナル Web UI に [DNS ENUM ドメインのリスト/追加 (List/Add DNS ENUM Domains)] ページを表示します。
- ステップ 2** [ドメイン (Domains)] ペインの [すべてプッシュ (Push All)] アイコンをクリックして、ページに一覧表示されているすべての ENUM ドメインをプッシュするか、または [ドメイン (Domains)] ペインで ENUM ドメインを選択して [プッシュ (Push)] アイコンをクリックし、 [ENUM ドメインのプッシュ (Push ENUM Domain)] ページを開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)] ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。

- すべての ENUM ドメインをプッシュする場合は、 [保証 (Ensure)]、 [置換 (Replace)]、または [正確 (Exact)] モードを選択できます。
- 1 つの ENUM ドメインをプッシュする場合は、 [保証 (Ensure)] または [置換 (Replace)] を選択できます。

いずれの場合も、 [保証 (Ensure)] がデフォルトのモードです。

ローカルクラスタで ENUM ドメインデータを置換する場合にのみ、 [置換 (Replace)] を選択します。ローカルクラスタに ENUM ドメインデータの正確なコピーを作成し、リージョン クラスタに定義されていない ENUM ドメインデータをすべて削除する場合にのみ、 [正確 (Exact)] を選択します。

- ステップ 4** [クラスタへのデータのプッシュ (Push Data to Clusters)] をクリックします。

CLI コマンド

リージョナルクラスタに接続されている場合は、 `dns-enum-domain <name | all> push <ensure | replace | exact> cluster-list [-report-only] -report` を使用できます。

レプリカ データベースからの ENUM ドメインのプル

レプリカ データベースから ENUM ドメインをプルするには、次の手順を実行します。

地域の Web UI

- ステップ 1** [設計 (Design)]メニューの [DNS ENUM] サブメニューで [ドメイン (Domains)] を選択してリージョナル Web UI に [DNS ENUM ドメインのリスト/追加 (List/Add DNS ENUM Domains)] ページを表示します。
- ステップ 2** [ドメイン (Domains)] ペインで [レプリカのプル (Pull Replica)] アイコンをクリックします。
- ステップ 3** クラスタの [レプリカデータの更新 (Update Replica Data)] 列で [レプリカ (Replica)] アイコンをクリックします。(自動レプリケーション間隔については、『Cisco プライムネットワーク レジストラ 11.1 管理ガイド』の「Replicating Local Cluster Data」の項を参照してください)。
- ステップ 4** [モード (Mode)] ラジオ ボタンのいずれかを使用して、複製モードを選択します。

- ステップ 5** ローカルクラスタの既存の ENUM ドメインデータを保持するには、[保証 (Ensure)] を選択しますが、それ以外の場合は、デフォルトの [置換 (Replace)] モードを有効のままにします。
- ステップ 6** [すべての ENUM ドメインのプル (Pull all ENUM Domains)] ボタンをクリックしてプルの詳細を表示し、[実行 (Run)] をクリックします。

CLI コマンド

リージョンクラスタに接続されている場合は、`dns-enum-domain <name | all> pull <ensure | replace | exact> cluster-name [-report-only| -report]` を使用できます。

ENUM 番号のプルとプッシュ

リージョンクラスタ Web UI の [DNS ENUM 番号のリスト表示/追加 (List/Add DNS ENUM Numbers)] ページで、ローカルクラスタに ENUM 番号をプッシュしたり、ローカルクラスタから ENUM 番号をプルしたりすることができます。

ローカルクラスタへの ENUM 番号のプッシュ

ENUM 番号をローカルクラスタにプッシュするには、次の手順を実行します。

リージョン Web UI

- ステップ 1** [設計 (Design)] メニューから [DNS ENUM] サブメニューで [番号 (Numbers)] を選択してリージョナル Web UI に [DNS ENUM 番号のリスト/追加 (List/Add DNS ENUM Numbers)] ページを表示します。
- ステップ 2** [番号 (Numbers)] ペインの [すべてプッシュ (Push All)] アイコンをクリックして、ページのリストに表示されているすべての ENUM 番号をプッシュするか、または [番号 (Numbers)] ペインの ENUM 番号を選択し、[プッシュ (Push)] アイコンをクリックして [ENUM 番号のプッシュ (Push ENUM Number)] ページを開きます。
- ステップ 3** [データ同期モード (Data Synchronization Mode)] ラジオ ボタンのいずれかを使用して、プッシュモードを選択します。
- すべての ENUM 番号をプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [正確 (Exact)] モードを選択できます。
 - 1 つの ENUM 番号をプッシュする場合は、[保証 (Ensure)] または [置換 (Replace)] を選択できません。
- いずれの場合も、[保証 (Ensure)] がデフォルトのモードです。
- ローカルクラスタで ENUM 番号データを置換する場合にのみ、[置換 (Replace)] を選択します。ローカルクラスタに ENUM 番号データの正確なコピーを作成し、リージョンクラスタに定義されていない ENUM 番号データをすべて削除する場合にのみ、[正確 (Exact)] を選択します。
- ステップ 4** [クラスタへのデータのプッシュ (Push Data to Clusters)] をクリックします。

CLI コマンド

リージョナルクラスタを接続する場合は、**dns-enum-number** <name | all> **push** <ensure | replace | exact> *cluster-list* [-report-only | -report] を使用できます。

レプリカ データベースからの ENUM 番号のプル

レプリカデータベースから ENUM 番号をプルするには、次の手順を実行します。

リージョン Web UI

-
- ステップ 1** [設計 (Design)]メニューから [DNS ENUM] サブメニューで [番号 (Numbers)]を選択してリージョナル Web UI に [DNS ENUM 番号のリスト/追加 (List/Add DNS ENUM Number)]ページを表示します。
 - ステップ 2** [番号 (Numbers)]ペインで [レプリカのプル (Pull Replica)]アイコンをクリックします。
 - ステップ 3** クラスタの [レプリカデータの更新 (Update Replica Data)]列で [レプリカ (Replica)]アイコンをクリックします。(自動複製の間隔については、の「*Replicating Local Cluster Data*」の項を参照してくださいCisco プライムネットワーク レジストラ 11.1 管理ガイド)。
 - ステップ 4** [モード (Mode)]ラジオ ボタンのいずれかを使用して、複製モードを選択します。
 - ステップ 5** ローカルクラスタの既存の ENUM 番号データを保持するには、[保証 (Ensure)]を選択しますが、それ以外の場合は、デフォルトの [置換 (Replace)]モードのままにします。
 - ステップ 6** [すべての ENUM 番号のプル (Pull all ENUM Numbers)]ボタンをクリックしてプルの詳細を表示し、[実行 (Run)]をクリックします。
-

CLI コマンド

リージョンクラスタに接続されている場合は、**dns-enum-number** <name | all> **pull** <ensure | replace | exact> *cluster-name* [-report-only | -report] を使用できます。



第 11 章

DNS ビューの管理

DNS ビューで、1つのネームサーバーを使用してゾーンデータの代替バージョンをさまざまなクライアントコミュニティに表示できます。たとえば、`example.com` の DNS サーバーは、ゾーンの2つのビューを維持できます。内部で照会できる `example.com` のビューには、外部ビューに存在しない多数のホストが含まれています。各ゾーンビューは、ゾーンの独立したコピーとして扱われます。DNS サーバーは、ゾーンに関するクエリに応答するときに、各ビューで定義されている一致基準を使用して、クライアントの一致ゾーンを見つけます。クエリは、そのゾーンの内容に基づいて応答されます。ゾーンコンテンツがビュー間でわずかに異なる場合があります。

- [DNS ビューの処理 \(213 ページ\)](#)
- [DNS ビューで作業する際に覚えておくべき重要事項 \(214 ページ\)](#)
- [DNS ビューの管理 \(215 ページ\)](#)
- [DNS ビューの順序変更 \(216 ページ\)](#)
- [DNS ビューの同期 \(217 ページ\)](#)
- [DNS ビューのプッシュとプル \(217 ページ\)](#)

DNS ビューの処理

DNS ビューでネームサーバーはデータを分離し、そのデータにアクセスするクライアントに基づいてデータの別のビューを提供できます。DNS が DNS 要求を受信すると、その要求は DNS ビューに関連付けられて処理されます。関連付けは、クライアントの送信元アドレスまたは宛先アドレス、あるいはその両方をビューで設定された送信元と宛先の ACL と照合することによって実行されます。ビューは優先順位に従って照合され、ゼロ以外の優先順位が最初に照合されます。要求が DNS ビューに一致すると、そのビューのデータのみが要求で使用可能になります。ゾーンとビューの間には1対1のマッピングがあります。ゾーンは1つのビューにのみ存在できます。ゾーンが複数のビューに存在する必要がある場合は、ゾーンをコピーし、別のビューに関連付けます。

間隔ビューと外部ビューがある場合、一般的な設定では、内部ビューの優先順位を1に設定し、内部クライアントの基準に一致するように ACL (通常は、`acl-match-clients`) を設定します。外部ビューの場合、デフォルトの優先順位と ACL をそのままにしておくと、内部ビューと一致しないすべての要求が外部ビューと一致するようになります。



(注) DNS ビューが設定されているときに NOTAUTH rcode 応答を取得することは、通常、要求がゾーンが存在しないビューと一致したことを示します。



(注) 自動ビュー検出は、Cisco Prime Network Registrar サーバーにのみ適用されます。

キャッシング DNS、セカンダリ DNS、通知のプライマリ、DHCP などの DNS クライアントサーバーのビューは、最小限の設定で簡単に定義されます。

Cisco Prime Network Registrar 10.1 以降では、ゾーンに関連付けられていない DNS ビューは自動で無視されます。ただし、以前のバージョンでは引き続き処理され、クライアントと空のビューが関連付けられる可能性があります。

DNS ビューで作業する際に覚えておくべき重要事項

DNS ビューで作業する際に知っておく必要があるキーポイントまたは属性は、次のとおりです。

- **ビューの ID** : DNS ビューの作成時に CCM サーバーまたはユーザーによって割り当てられたビューの一意の整数識別子を定義します。
- **ビューの優先順位 (*priority* 属性)** : 各 DNS ビューには、ビューの処理順序を決定する一位の優先順位が割り当てられます。ゼロ以外の最も低い優先順位が最初に処理され、2 番目に低い優先順位がその次に処理されます。ゼロの優先順位は、常に最後に処理されるデフォルトビュー用に予約されています。Web UI には、明示的に優先順位を設定せずにビューの順序を変更するメカニズムがあります。
- **デフォルトビュー** : デフォルトビューを作成するには、*view-id=0*、*priority=0*、およびクライアントと宛先 ACL を *any* に設定します。名前付きビューに一致しない要求は、常にデフォルトビューに分類されます。デフォルトでは、ゾーンは *view-id=0* で作成され、デフォルトビューに自動的に配置されます。デフォルトビューは変更または削除できません。
- ***acl-match-clients* 属性** : クライアント送信元アドレスに基づいて、クライアントをビューにマッピングする ACL を指定します。デフォルトは *any* ですが、クライアントを適切なビューに関連付けるために変更する必要があります。
- ***acl-match-destinations* (エキスパートモード属性)** : クライアント宛先アドレスに基づいてクライアントをビューにマッピングする ACL を指定します。デフォルトは *any* ですが、DNS サーバーがビューごとに異なるネットワークインターフェイスを使用している場合のみ変更する必要があります。
- ***ignore-unused-views* 属性** : DNS サーバーが、設定されたゾーンのいずれにも関連付けられていない設定済み DNS ビューを使用するかどうかを制御します。

- **代替ビュー** : Cisco Prime Network Registrar 11.0 以降では、ゾーンをコピーせずに複数のビューからゾーンを参照できます。

これは、ゾーンのサブセットが複数のビューで共通である表示構成で役立ちます。ゾーンを他のビューで表示できるようにするには、ゾーンの *alternate-view-ids* 属性を設定し、DNS サーバーをリロードします。共通ゾーンの *view-id* をデフォルトビューに設定することをお勧めします。UI セッションの DNS ビューを変更すると、一致する *view-id* を持つゾーンのみが表示されます。

- Cisco Prime Network Registrar キャッシング DNS サーバーは、権威 DNS サーバーの代わりに、クライアント要求を適切なビューに関連付けることができます。これを行うには、キャッシング DNS サーバーで DNS ビューを設定し、[例外の一覧/追加] ページの *uses-views* 属性を **true** に設定します。キャッシング DNS サーバーはクライアントを適切なビューにマッピングし、権威 DNS サーバーに転送されたクエリに適切なビューをタグ付けします。したがって、このような場合、ビューマッピングはキャッシング DNS サーバーによって実行されます。



- (注) キャッシング DNS サーバーはクライアントを *acl-match-clients* にのみマッピングします。*acl-match-destinations* 属性は無視されません。

DNS ビューと例外の設定は、ゾーン ディストリビューションによって自動的に同期/設定されます。

DNS ビューの管理

ローカルクラスタまたはリージョンクラスタから DNS ビューを作成、編集、および削除できます。[保証 (Ensure)]、[置換 (Replace)]、および [正確 (Exact)] モードで、リージョン CCM サーバーを相手にビューと ACL をプッシュまたはプルすることもできます。



- (注) 最大 100 個のビューを作成できます。

ローカルおよび地域 Web UI

DNS ビューを作成するには、次の手順を実行します。

- ステップ 1 Design** メニューの **Auth DNS** サブメニュー（または **Cache DNS**（ローカル Web UI））にある **Views** を選択します。
- ステップ 2** [ビュー (Views)] ペインで [ビューの追加 (Add View)] アイコンをクリックします。
- ステップ 3** DNS ビューの名前を指定します。

- ステップ 4** ビュー ID を指定します（詳細モード）。ビュー ID を指定しなかった場合は、アプリケーションがビュー ID をビューに自動的に割り当てます。
- ステップ 5** クライアントをこのビューにマッピングする ACL を `[acl-match-clients]` フィールドに指定できます。
- ステップ 6** `[DnsView の追加 (Add DnsView)]` ボタンをクリックします。
- ステップ 7** DNS ビューを編集するには、左側の `[ビュー (Views)]` ペインでビューの名前をクリックし、必要に応じて属性を編集します。

CLI コマンド

view コマンドは、DNS サーバーの DNS ビューを制御および管理するために使用されます。次に例を示します。

```
nrcmd> view MyView create
```

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。プッシュおよび再利用の場合は、クラスターのリストまたは「すべて」を指定できます。

```
view <name | all> pull <ensure | replace | exact> cluster-name [-report-only | -report]
```

```
view <name | all> push <ensure | replace | exact> cluster-list [-report-only | -report]
```

```
view name reclaim cluster-list [-report-only | -report]
```

DNS ビューの順序変更

一連の DNS ビューを作成するときに、プライオリティの順序を指定できます。プライオリティ順序を指定するには、次の手順を実行します。

- ステップ 1** `[設計 (Design)]` メニューの `[権威 DNS (Auth DNS)]` サブメニューで `[表示 (View)]` を選択して、`[ゾーンビューのリスト/追加 (List/Add Zone Views)]` ページを開きます。
- ステップ 2** `[ビュー (Views)]` ペインの `[ビューの順序変更 (Reorder Views)]` アイコンをクリックすると、`[Reorder (順序変更)]` ダイアログボックスが開きます。
- ステップ 3** 次のいずれかの方法で、DNS ビュー ルールのプライオリティを設定します。
- ビューを選択し、`[上に移動 (Move up)]` または `[下に移動 (Move down)]` アイコンをクリックして、ルールの順序を変更します。
 - ビューを選択して、`[移動先 (Move to)]` ボタンをクリックし、行番号を入力してビューを移動します。
- ステップ 4** `[保存 (Save)]` をクリックして、順序を変更したリストを保存します。
- ビューを削除する場合は、すべてのゾーンを削除するための選択肢が表示されます。

CLI コマンド

`dns-view name create` を使用して DNS ビューを追加します（構文と属性の説明については、`install-path/docs` ディレクトリにある `CLIGuide.html` の `dns-view` コマンドを参照してください）。

DNS ビューの同期

ゾーン分散同期、シングルゾーン同期、および HA DNS ゾーン同期では、プライマリゾーンとセカンダリゾーンの関連ビューおよび名前付き ACL が常に同期されます。ゾーン分散同期または HADNS 同期の実行時には、異なる同期モードが適用されます。次のモードが適用されます。

- **ゾーン分散同期** : すべてのゾーン分散同期タイプ（[更新 (Update)]、[完全 (Complete)]、および [正確 (Exact)]）で、ビューの同期には [置換 (Replace)] モードが適用され、ACL には [保証 (Ensure)] モードが適用されます。キャッシング DNS サーバーがゾーン分散に含まれている場合、関連ビューと名前付き ACL はこれらのサーバーに同期され、プライマリサーバーリストは分散におけるドメイン名の一意セットの例外として設定されます。ユーザーは、セカンダリサーバーまたはキャッシュサーバーを除外する必要があります。
- **HA DNS 同期** : [更新 (Update)] 同期と [完全 (Complete)] 同期でのビューの同期には [置換 (Replace)] モードが適用され、[正確 (Exact)] 同期でのビューの同期では [正確 (Exact)] モードが適用されます。

DNS ビューのプッシュとプル

[保証 (Ensure)]、[置換 (Replace)]、および [正確 (Exact)] モードで、リージョンクラスタを相手にビューと ACL をプッシュおよびプルすることもできます。

ローカルクラスタへの DNS ビューのプッシュ

作成したビューをリージョンクラスタから任意のローカルクラスタにプッシュできます。

リージョン Web UI

ステップ 1 Design メニューから、**Views** サブメニューの **Auth DNS** を選択して [ゾーンビューのリスト/追加 (List/Add Zone Views)] ページを開きます。

ステップ 2 [ビュー (Views)] ペインの左ペインにある **Push All** アイコンをクリックするか、または [DNS ビュー (DNS View)] を選択して [ゾーンビューの編集 (Edit Zone View)] ページの上部にある **Push** をクリックします。[ローカルクラスタへのデータのプッシュ (Push Data to Local Clusters)] または [ゾーンビューのプッシュ (Push Zone View)] ページが開きます。

ステップ 3 [データ同期モード (Data Synchronization Mode)] ラジオ ボタンのいずれかを使用して、プッシュ モードを選択します。

- すべての DNS ビューをプッシュする場合は、[保証 (Ensure)]、[置換 (Replace)]、または [正確 (Exact)] モードを選択できます。
- 1 つの DNS ビューをプッシュする場合は、[保証 (Ensure)] または [置換 (Replace)] を選択できません。

上記のいずれの場合も、[保証 (Ensure)] がデフォルトのモードです。

ローカル クラスタの既存の DNS ビュー データを置き換える場合のみ、[置換 (Replace)] を選択します。ローカル クラスタの DNS ビューの正確なコピーを作成することで、リージョン クラスタに定義されていないすべての DNS ビューをすべて削除する場合に限り、[正確 (Exact)] を選択します。

ステップ 4 デスティネーション クラスタの [使用可能 (Available)] フィールドで 1 つ以上のローカル クラスタを選択し、それらを [選択済み (Selected)] フィールドに移動します。

ステップ 5 **Push Data to Clusters** をクリックします。

CLI コマンド

リージョン クラスタに接続されているときには、**view <name | all> push <ensure | replace | exact> cluster-list [-report-only | -report]** を使用できます。

ローカル クラスタからの DNS ビューのプル

ビューを明示的に作成する代わりに、ローカル クラスタからプルできます。リージョン Web UI では、クラスタ名の横にある [レプリカ (Replica)] アイコンをクリックして、ビュー レプリカ データを更新しておいてください。

リージョン Web UI

ステップ 1 **Design** メニューから、**Views** サブメニューの **Auth DNS** を選択して [ゾーンビューのリスト/追加 (List/Add Zone Views)] ページを開きます。

ステップ 2 [ビュー (Views)] ペインで [レプリカのプル (Pull Replica)] アイコンをクリックします。

ステップ 3 データ同期モード (**Update**、**Complete**、または **Exact**) を選択します。これらのモードについては、そのページの表に説明されています。

ステップ 4 ダイアログボックス下部でをクリック **Report** します。

ステップ 5 [実行 (**Run**)] をクリックします。

CLI コマンド

リージョンクラスタに接続されているときには、**view** <name | all> **pull** <ensure | replace | exact> *cluster-name* [-report-only | -report] を使用できます。



第 12 章

リソース レコードの管理

この章では、Cisco Prime Network Registrar の Web UI と CLI を使用して、DNS ゾーンとサーバーのより高度なパラメータを設定する方法について説明します。この章のコンセプトに進む前に、プライマリおよびセカンダリ DNS サーバーとその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 \(179 ページ\)](#)」を参照してください。

- [ゾーンのリソース レコードの管理 \(221 ページ\)](#)
- [ゾーンへのリソース レコードの追加 \(222 ページ\)](#)
- [リソース レコードの編集 \(223 ページ\)](#)
- [ゾーンからのリソース レコードの削除 \(223 ページ\)](#)
- [ホストのリソース レコードの管理 \(224 ページ\)](#)
- [リソース レコードセットの保護 \(224 ページ\)](#)
- [サーバー全体でのレコードとアドレスの検索 \(226 ページ\)](#)
- [リソース レコードのフィルタリング \(227 ページ\)](#)
- [サービスロケーション \(SRV\) レコードを使用したネットワークへのサービスのアドバタイジング \(228 ページ\)](#)
- [NAPTR リソース レコードを使用した名前空間の名前解決 \(229 ページ\)](#)
- [DNS 認証局認証 \(CAA\) リソースレコード \(230 ページ\)](#)
- [Uniform Resource Identifier \(URI\) リソースレコード \(232 ページ\)](#)

ゾーンのリソース レコードの管理

リソース レコード (RR) は、DNS ゾーン内のデータを構成します。1つのゾーンが所有できる RR の数に一定の制限はありませんが、通常では1つのゾーンが特定のタイプの RR を1つまたは複数所有できます (ゾーンには常に Start of Authority、SOA レコードがあります)。関連するタイプによっては、いくつかの例外があります。すべての RR には、次の表に記載されているエン트리があります。

表 53: リソース レコードの共通エン트리

RR エン트리	説明
名前	ゾーンやホスト名など、レコードの所有者。

RR エントリ	説明
Class (すべての形式に必要なということではありません)	Cisco Prime Network Registrar は IN (インターネット) クラスのみをサポートします。
TTL (存続可能時間)	レコードをキャッシュに保存する時間 (秒単位)。TTL が指定されていない場合は、Cisco Prime Network Registrar はゾーン属性として定義されたゾーンのデフォルト TTL を使用します。
タイプ	A (IPv6 の場合は AAAA)、NS、SOA、MX などのレコードのタイプ。さまざまな RFC で多くのタイプが定義されていますが、一般的に使用されているタイプの数は 10 未満です。
レコード データ	データ型の形式と意味はレコードタイプによって異なります。

ゾーンへのリソース レコードの追加

RR を追加または変更する前に、段階と同期という 2 つの dns 編集モードを設定して使用できることを覚えておいてください (『Cisco Prime Network Registrar 11.1 DHCP ユーザガイド』の「段階モードと同期モード」の項を参照)。

RR 管理に必要な管理者ロールは、ローカル クラスタでは dns-admin ロール、リージョン クラスタでは central-dns-admin ロールです。ローカル クラスタの host-admin ロールと、リージョン クラスタの central-host-admin ロールでは、ホスト レコードのみを表示できます。

ローカルおよび地域 Web UI

ステップ 1 [デザイン (Design)] メニューの [認証 DNS (Auth DNS)] サブメニューの [転送ゾーン (Forward Zones)] を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)] ページを開きます。

ステップ 2 [正引きゾーン (Forward Zones)] ペインでゾーン名をクリックして [ゾーンの編集 (Edit Zone)] ページを開きます。リソースレコードの編集は CCM と DNS によって共同で管理されるため、システムロックを使用して DNS と CCM によるリソース レコード データベースへの同時アクセスを防ぎます。

ヒント レコードは、それぞれの RFC で指定されている形式でリスト表示され、セット内の最初のレコードだけに名前ラベルが付いて、DNSSEC 順序で示されます。テーブルの項目数を増減させるには、ページの下部にあるページサイズの値を変更してから、[Change Page Size] をクリックします。

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 デフォルトでは RR は保護されます。つまり DNS 更新で RR を上書きすることはできません（「[リソースレコードセットの保護（224 ページ）](#)」を参照）。RR の保護を解除するには、レコード名の左側にある [ロック済み (Locked)] アイコンをクリックすると、そのアイコンが [ロック解除済み (Unlocked)] アイコンに変わります。同様に、レコードを保護するには [ロック解除済み (Unlocked)] アイコンをクリックして [ロック済み (Locked)] アイコンに変えます。

ステップ 6 [Add Resource Record] をクリックします。

CLI コマンド

`zone name addRR` を使用して、特定タイプの保護ありの RR を追加します。相対名（所有者が同じドメイン内に存在する場合）、絶対名（FQDN を指定）、またはゾーン名と同じ名前（[@] 記号を使用）を指定できます。

次に例を示します。

```
nrcmd> zone example.com addRR -sync host101 A 192.168.50.101
```

`zone name addDNSRR type data` を使用して、保護なしの RR を追加します。

リソースレコードの編集

RR を個々のレコードまたは RR セットとして編集できます。

- **Individual RRs** : レコード名の横にある [編集 (Edit)] アイコンをクリックすると、[ゾーンでの RR の編集 (Edit RR in Zone)] ページが開きます。
- **RR sets** : レコード名をクリックすると、[ゾーンでの RR セットの編集 (Edit RR Set in Zone)] ページが開きます。

データを入力するフィールドの説明については、「[ゾーンへのリソースレコードの追加（222 ページ）](#)」を参照してください。

ゾーンからのリソースレコードの削除

ゾーンから RR を削除できます。

ローカルおよび地域 Web UI

[ゾーン (Zone)] ページの [リソースレコード (Resource Records)] タブでは、次の手順を実行します。

- レコード名セット全体を削除するには、リストのレコードセット名の横にある [削除 (Delete)] アイコンをクリックして、削除を確認します。
- セットから個々のレコードを削除するには、レコードセットの名前をクリックして [編集 (edit)] ページを開き、リスト内の個々のレコードの横にある [削除 (Delete)] アイコンをクリックして削除を確認します。

CLI コマンド

CLI には、削除する RR のタイプに応じて、次の 2 つの削除コマンドがあります。

- RR を削除するには **zone name removeRR** を使用します。所有者を指定する必要があります。データを省略すると、Cisco Prime Network Registrar は、指定所有者の指定タイプのレコードをすべて削除します。同様に、タイプを省略すると、Cisco Prime Network Registrar は、指定所有者のすべてのレコードを削除します。
- 保護されていない RR のみを削除するには、**zone name removeDNSRR** を使用します。

ホストのリソース レコードの管理

個々の RR ではなくホスト レコードを設定することによって、ホストの RR を管理できます。ホストを定義しておくことで、DNS サーバーは IPv4 用のアドレス (A) RR または IPv6 用の AAAA RR を自動的に作成します。ホストの逆引きゾーンが存在する場合、サーバーは関連ポインタ (PTR) RR を作成することもできます。

詳細については、[ホストの管理 \(235 ページ\)](#) を参照してください。

リソース レコード セットの保護

RR が保護されている場合に、DNS 更新でレコードを変更することはできません。管理上作成されたほとんどの RR は保護されています。ただし、DNS 更新で作成された RR は、サーバーによる変更が可能になるように保護を解除する必要があります。[ゾーンの DNS サーバー RR のリスト表示/追加 (List/Add DNS Server RR for Zone)] ページで、各 RR セットに対してこの保護ステータスを設定できます。

プライマリ DNS サーバーのみがこの保護ステータスを認識できることに注意してください。セカンダリ サーバーは RR の保護ステータスを認識しません。



注意 保護されていない RR はゾーンのスカベンジングで削除できます。詳細については、『*Cisco Prime Network Registrar 11.1 DHCP ユーザーガイド*』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。

ローカルおよび地域 Web UI

既存の RR を保護するには、次の手順を実行します。

ステップ 1 [デザイン (Design)] メニューの [認証 DNS (Auth DNS)] サブメニューの [転送ゾーン (Forward Zones)] を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)] ページを開きます。

ステップ 2 [正引きゾーン (Forward Zones)] ペインでゾーン名をクリックして [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 [リソース レコード (Resource Records)] タブで、リソース レコードのリストにあるリソース レコード名をクリックして、リソース レコードを編集します。

ステップ5 [Protect Set] ボタンをクリックすると、選択した RR セットの保護が解除されます。

ステップ6 [保存 (Save)] をクリックして、リソース レコード属性の変更を保存します。

リソース レコード セットの保護解除

RR の保護を解除することもできます。追加中に RR の保護を解除するには、[リソース レコード名 (Resource Record name)] フィールドの横にある [ロック済み (Locked)] アイコンをクリックします。そのアイコンが [ロック解除済み] アイコンに変わります。

ローカルおよび地域 Web UI

既存の RR の保護を解除するには、次の手順を実行します。

ステップ1 [デザイン (Design)] メニューの [認証DNS (Auth DNS)] サブメニューの [転送ゾーン (Forward Zones)] を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)] ページを開きます。

ステップ2 [正引きゾーン (Forward Zones)] ペインでゾーン名をクリックして [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 [リソース レコード (Resource Records)] タブで、リソース レコードのリストにあるリソース レコード名をクリックして、リソース レコードを編集します。

ステップ5 [Unprotect Set] ボタンをクリックすると、選択した RR セットの保護が解除されます。

ステップ6 [保存 (Save)] をクリックして、リソース レコード属性の変更を保存します。

(注) RR セット名の左側にあるアイコンは、リソース レコードのステータス (保護あり/保護なし) を示します。

CLI コマンド

RR セットを保護するには、**zone name protect-name rrset-name** を使用します。ゾーンの保護を解除するには、**unprotect-namerrset-name** を使用します。次に例を示します。

```
nrcmd> zone example.com protect-name boston
100 Ok
protected boston
```

```
nrcmd> zone example.com unprotect-name boston
100 Ok
unprotected boston
```

サーバー全体でのレコードとアドレスの検索

Cisco Prime Network Registrar を使用すると、サーバー全体で RR と IP アドレスを検索できます。検索はフィルタメカニズムであり、RR 属性とアドレス属性の組み合わせを指定して、ネットワークに設定された 1 つ以上の RR またはアドレスをターゲットにすることができます。検索機能は、ローカルクラスタでのみ使用できます。

次の方法で RR を検索できます。

- IP アドレス
- 保護状態
- 名前のプレフィックス
- タイプ
- ゾーン

ローカルの詳細 Web UI

IP アドレスでリソースレコードを検索するには、次の手順を実行します。

ステップ 1 [操作 (Operate)] メニューの [レポート (Reports)] サブメニューで [IP アドレスごとの DNS RR (DNS RRs By IP Address)] を選択し、[IP アドレスの検索 (IP Address Search)] ページを開きます。

ステップ 2 IP アドレスで検索するには、IP アドレスを入力して、[Search] をクリックします。

(注) IP アドレス検索では、[データ (data)] フィールドに指定されたアドレスを含む RR を DNS サーバーがすべての正引きゾーン内で検索するわけではありません。代わりに、DNS サーバーは一致する PTR レコードを逆引きゾーン内で検索し、正引きゾーン内で該当するすべての RR を返します。

ローカルの詳細 Web UI

リソースレコードを検索するには、次の手順を実行します。

ステップ 1 [操作 (Operate)] メニューのサブメニューから **DNS Resource Records Reports** を選択して [DNS リソースレコードの検索 (DNS Resource Record Search)] ページを開きます。

ステップ 2 ドロップダウンリストからフィルタ属性を選択します。

ステップ 3 選択したフィルタ属性に応じて、ドロップダウンリストからフィルタタイプを選択します。

- **RR Protection State** : RR 保護ステータス ([ロック済み (locked)] または [ロック解除 (unlocked)])。
- **RR Name Prefix** : RR 名のプレフィックス。
- **RR Type** : RR タイプ。
- **Zone** : ゾーンリスト、正規表現、またはゾーンフラグ

- ステップ 4** 選択したタイプに基づいて、値を入力または選択します。フィルタをクリアするには、[Clear Filter] をクリックします。
- ステップ 5** 要素をフィルタ要素リストに追加するには、[Add Element] をクリックします。フィルタ要素の見出しが変わり、フィルタに使用されるフィルタ属性と値を識別します。複数の要素を追加すると、見出しは要素の論理積を識別します。たとえば、ユーザーの名前プレフィックス検索するための要素を追加してから、A レコードの RR タイプを検索するために別の要素を追加すると、フィルタ要素の見出しは検索を ****RRName Prefix = user AND RR Type = A** と識別します。
- ステップ 6** 必要な数の要素を追加できます（検索結果はフィルタ要素の共通部分です）。プラス記号 (+) をクリックして、フィルタ要素のリストを表示します。
- ステップ 7** [Search] をクリックします。
- ステップ 8** 検索結果として生成された RR のテーブルを確認します。各 RR のゾーン、ホスト名、TTL、タイプ、および関連データが表示されます。必要に応じて、一度に表示されるエントリの数が増えるようにページサイズを変更します（それでもページ間の移動が必要な場合があります）。RR は DNSSEC 順序でソートされます。

ヒント フィルタ要素の論理積を求めたために、検索結果が予想よりも少ない場合は、フィルタリストの中で検索を妨げている可能性のある要素を調べて、その要素の横にある [削除 (Delete)] アイコンをクリックして削除してから、検索をやり直します。

CLI コマンド

`dns findRR` を使用して、ゾーン全体で RR を検索します。コマンド構文は 2 種類あります。

```
nrcmd> dns findRR -name fqdn | domainaddr
```

```
nrcmd> dns findRR [-namePrefix nameprefix] [--rrTypes RRtypelist] [--protected| -unprotected]
[-zoneType
forward| reverse| primary|secondary| ALL]
```

ドメインまたはそのアドレスで検索したり、RR 名の先頭文字（名前プレフィックス）を入力したりすることができます。RR 名プレフィックスで検索する場合は、RR タイプ、保護ステータス、またはゾーンタイプのリストを使用して検索を絞り込むことができます。見つかった各エントリのゾーンは出力に明確に示されます。次に例を示します。

```
nrcmd> dns findRR -namePrefix user -rrTypes A

userhost101.example.com IN A 192.168.50.101
userhost102.example.com IN A 192.169.50.102
userhost103.boston.example.com IN A 192.168.50.103
```

リソース レコードのフィルタリング

A（または IPv6 AAAA）や PTR レコードなど、1 つのタイプのレコードのみを表示するようにレコードをフィルタリングすることができます。（「[サーバー全体でのレコードとアドレスの検索（226 ページ）](#)」も参照してください）。

ローカルおよびリージョン Web UI

[ゾーン編集 (Edit Zone)] ページから直接 RR のフィルタ処理ができます。[Add Resource Record] ボタンのすぐ下にある [名前 (Name)] フィールドと [タイプ (Type)] フィールドを探します。

デフォルトでは、RR は名前のアルファベット順にソートされます。最初はゾーン最上位のレコード (@ マーク付き) で、次にタイプ順にソートされ、その後にデータが続きます。次の方法でソートすることもできます。

- **Protected state** : [すべて (All)]、[保護なし (Unprotected)]、または [保護あり (Protected)] をクリックできます。
- **Name prefix** : 名前の先頭文字。* 文字はワイルドカードではないことに注意してください。たとえば、**al** を入力すると、**alberta**、**allen.wrench**、および **allie** が返されます。**al*** を入力すると、**al*** と **al*ert** が返されます。
- **RR type** : ドロップダウンリストから A (または IPv6 AAAA) や TXT など、RR タイプのいずれかをクリックします、

選択したら [Filter List] をクリックします。フィルタ処理されたエントリだけがフィールドの下のテーブルに返されます。フィルタ処理されていない完全なリストに戻るには、[Clear Filter] をクリックします。

CLI コマンド

zone zonename findRR を使用して RR 名プレフィックス、RR タイプ、または保護ステータスを検索します。

```
nrcmd> zone zonename findRR [-namePrefix nameprefix] [-rrTypes RRtypelist] [-protected|
-unprotected]
```

サービス ロケーション (SRV) レコードを使用したネットワークへのサービスのアドバタイジング

サービス ロケーション (SRV) RR は、サービスをネットワークにアドバタイズするために使用されます。この RR は RFC 2782 : A DNS RR for specifying the location of services (DNS SRV) に定義されています。SRV には A レコードまたは AAAA レコードが関連付けられていることがあります。Windows ドメインコントローラは、SRV レコードを使用するサービスです。

RFC では、SRV レコード (DNS タイプ コード 33) の形式が次のように定義されています。

```
_service._protocol.name ttl class SRV priority weight port target
```

クライアントがサービスをホストに解決できるように、SRV レコードターゲットに関連付けられた A レコードが必ず必要です。SRV レコードの Microsoft Windows 実装では、レコードは次のようになります。

```
myserver.example.com A 201.165.201.1
_ldap._tcp.example.com SRV 0 0 389 myserver.example.com
_kdc._tcp.example.com SRV 0 0 88 myserver.example.com
_ldap._tcp.dc._msdcs.example.com SRV 0 0 88 myserver.example.com
```

アンダースコア () はサービス名とプロトコル名の前に必ず付きます。この例では、_kdc がキー発行局です。プライオリティと重みは、同じサービスを提供するターゲットサーバーをクライアントが選択するのに役立ちます（優先度が同じサーバーを差別化する重み）。プライオリティと重みがすべてゼロに設定されている場合は、クライアントはサーバーの順位をランダムに決めます。



- (注) DNS サーバーおよび DHCP サーバーと Windows クライアントとの相互運用方法（動的 RR のスカベンジングを含む）の説明については、『Cisco Prime Network Registrar 11.1 DHCP ユーザーガイド』の「WINDOWS クライアントの DNS 更新の設定」の項を参照してください。

NAPTR リソース レコードを使用した名前空間の名前解決

Cisco Prime Network Registrar は、Naming Authority Pointer (NAPTR) RR をサポートしています。これらのレコードは、特定の名前空間の名前解決に役立つとともに、解決サービスに到達するために処理されます。NAPTR レコードは標準化への提唱 RFC 3403 であるため、Cisco Prime Network Registrar はそれらのレコードの数値レコードフィールドのみ検証します。ただし、標準化への提唱によると、null ("") の場合やプリセット値がない場合でも、各フィールドには値が必要です。

NAPTR レコードを使用してセッション開始プロトコル (SIP) プロキシを検索する場合は、標準化への提唱 RFC 2916 または RFC 3263 を参照してください。RFC 2916 では、Internet Engineering Task Force の ENUM 作業グループが、E.164 アドレスを Universal Resource Identifier (URI) にマッピングするために NAPTR レコードを使用することを規定しています。NAPTR レコードを使用すると、E.164 国際公衆電気通信番号の名前空間の名前は URI に解決され、リゾルバとして使用するサービスの名前は示されません。この目的のために、U フラグが NAPTR レコードに追加されました。

たとえば、電話番号+4689761234 の SIP プロキシを指定するには、次の内容を使用して、名前 4.3.2.1.6.7.9.8.6.4.e164.arpa. で NAPTR レコードを追加します。

```
100 10 "u" "sip+E2U" "/^.*$/sip:info@example.com/" .
```

これにより、NAPTR レコードの次のフィールドが設定されます。

```
order = 100
preference = 10
flags = "u"
service = "sip+E2U"
regexp = "/^.*$/sip:info@example.com/"
replacement = .
```

これらのフィールドを設定すると、電話番号+4689761234 を処理する DNS クライアントは、その番号を sip:info@tele2.se に置き換えて、SIP サービスの URI を得ることができるようになります。E.164 ゾーンでの NAPTR レコードの主な用途は、入力電話番号の大規模な交換です。RFC 2916 のセクション 3.2.3 には、数字を保持する Lightweight Directory Access Protocol (LDAP) クエリへの変換の例が含まれています。人間にとって読みやすい SIP URL を (@) 記号の左側

に取得するために、E.164 ゾーンはサービス ロケーション (SRV) レコードにマッピングされません。

ローカルおよび地域 Web UI

ステップ 1 [デザイン (Design)] メニューの [認証DNS (Auth DNS)] サブメニューの [転送ゾーン (Forward Zones)] を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)] ページを開きます。

ステップ 2 [リソース レコード (Resource Records)] タブをクリックします。

ステップ 3 [名前 (Name)] フィールドにレコードの所有者を入力します。

ステップ 4 TTL を入力します (必要な場合)。

ステップ 5 [タイプ (Type)] ドロップダウンリストから、[NAPTR] を選択します。

ステップ 6 データを引用符で囲まれた文字列として入力して、スペースで区切ります。

- a) [順序 (Order)]
- b) [優先順位 (Preference)]
- c) [フラグ (Flags)]
- d) [サービス (Service)]
- e) [正規表現 (Regular expression)]
- f) [置換文字列 (Replacement string)]

例 :

```
"100 10 u sip+E2U /^.*$/sip:info@tele2.se/ ."
```

ステップ 7 **Add Resource Record** をクリックします。

CLI コマンド

Use `zone name addRR` を使用して、保護されたリソース レコードをゾーンに追加します。

DNS 認証局認証 (CAA) リソースレコード

DNS 認証局認証 (CAA) は、ドメイン所有者がドメインの証明書の発行を許可されている認証局を宣言できるインターネットセキュリティポリシーメカニズムです。CAA は、Web ドメインのセキュリティをさらに強化する標準規格です。DNS CAA レコードは RFC 6844 で指定されています。

CAA レコード (DNS タイプコード 257) は、次の要素で構成されます。

- **フラグ** : 0 ~ 255 の符号なし整数。
- **タグ** : RFC は現在、次の 3 つの使用可能なタグを定義しています。

- **issue** : 単一の認証局がホスト名の証明書 (任意のタイプ) を発行することを明示的に許可します。
 - **issuewild** : 単一の認証局がホスト名のワイルドカード証明書 (およびワイルドカードのみ) を発行することを明示的に許可します。
 - **iodef** : 認証局がポリシー違反を報告する URL を指定します。
- 値 : 文字列。



(注) CAA レコードは、フラグバイトと「プロパティ」と呼ばれるタグと値のペアで構成されます。複数のプロパティを同じドメイン名に関連付けるには、そのドメイン名で複数の CAARR を公開します。

CAA レコードの例 :

```
example.com. CAA 0 issue "letsencrypt.org"  
example.com. CAA 0 issuewild "comodoca.com"
```

Cisco Prime Network Registrar では、Web UI および CLI コマンドを使用して、CAA RR タイプを追加、維持、および照会できます。ドメインで使用する予定の各認証局 (CA) の CAADNS レコードを追加します。

CAA の rdata 部分はフラグタグ値です。

値は次のとおりです。

- **flag** : バイトサイズ。現在、ビット 0 とビット 7 が使用され、その他のビットは将来の使用のために予約されています (サポートされる値 : 0、1、および 128) 。
- **tag** : US-ASCII 文字と数字のゼロ以外のシーケンス。タグの長さは 1 以上 15 以下である必要があります。
- **value** : 文字列。

ローカルおよび地域 Web UI

DNS サーバーに CAA RR タイプを追加するには、次の手順を実行します。

- ステップ 1** [デザイン (Design)]メニューの [認証DNS (Auth DNS)]サブメニューの [転送ゾーン (Forward Zones)]を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)]ページを開きます。
- ステップ 2** [リソース レコード (Resource Records)]タブをクリックします。
- ステップ 3** [名前 (Name)]フィールドにレコードの所有者を入力します。
- ステップ 4** TTL を入力します。
- ステップ 5** [タイプ (Type)]ドロップダウンリストから、CAA を選択します。
- ステップ 6** 正しいシンタックスに従って、[データ (Data)]フィールドに文字列としてデータを入力します。

例 :

```
0 issue "letsencrypt.org"
```

ステップ7 [リソースの追加 (Add Resource)]をクリックします。

CLI コマンド

CAA レコードを追加、削除、および変更するには、**addRR**、**removeRR** および **modifyRR** コマンドを使用します。次に例を示します。

```
nrcmd> zone example.com addRR test1 CAA 0 issue comodoca.com
nrcmd> zone example.com removeRR test1
nrcmd> zone example.com modifyRR test1 CAA 0 issue comodoca.com rdata="0 issue
new-comodoca.com" ttl=86400
```

Uniform Resource Identifier (URI) リソースレコード

Cisco Prime Network Registrar は、Uniform Resource Identifier (URI) リソースレコードをサポートしています。URI とは、ロケーションまたは名前、あるいはその両方によってインターネットのリソースを特定するために使用される文字列です。統一性を保証するために、すべての URI は事前に定義されたシンタックスルール式に従いますが、個別に定義された階層型命名スキーム (たとえば、`http://`) によって拡張性も維持しています。DNS では、URI レコード (RFC 7553) は、ホスト名から URI へのマッピングを公開するための手段です。クライアントは、使用する関連プロトコル/サービスがわかっているアプリケーションの URI レコードを使用します。

Cisco Prime Network Registrar では、Web UI と CLI コマンドを使用して、URI RR タイプの追加、維持、およびクエリを実行できます。これは、プロトコル/サービスとドメイン名を入力として提供することで、確立される実際の接続の明示的な URI を取得するのに役立ちます。また、ゾーンを URI RR と HA パートナーと同期してから、いずれかのパートナーに URI RR を照会することもできます。

URI RR のクエリは、NAPTR RR のクエリを置き換えるものではありません。代わりに、URI RR タイプは、どのサービスフィールドが対象であるかがすでに分かっている場合に使用される補完的なメカニズムを提供します。これを使用すると、NAPTR RR を照会するときに戻される大きな RRSets の特定のサブセットを直接照会できます。

URI レコード (DNS タイプ コード 256) は、次の形式で表されます。

```
_service._proto.name. TTL class URI priority weight target
```

値は次のとおりです。

- *service* : 目的のサービスのシンボリック名。
- *proto* : 目的のサービスのトランスポートプロトコル。これは通常、TCP または UDP です。
- *name* : ドットで終わる、このレコードが有効なドメイン名。
- *TTL* : 標準 DNS 存続可能時間フィールド。
- *class* : 標準 DNS クラス フィールド (常に IN) 。

- *priority* : この RR のターゲット URI の優先順位。範囲は、0 ~ 65535 です。値が小さいほど優先順位が高くなります。
- *weight* : 同じ優先順位を持つレコードの相対的な重み。範囲は、0 ~ 65535 です。値が大きいほど、優先順位が高くなります。
- *target* : 二重引用符で囲まれたターゲットの URI。このフィールドの長さは、ゼロより大きくする必要があります。

URI レコードの例 :

```
_ftp._tcp IN URI 10 1 "ftp://ftp1.example.com/public"
```

ローカルおよび地域 Web UI

権威 DNS サーバーに URI RR タイプを追加するには、次の手順を実行します。

- ステップ 1 [デザイン (Design)]メニューの [認証DNS (Auth DNS)]サブメニューの [転送ゾーン (Forward Zones)]を選択して、[転送ゾーンの一覧/追加 (List/Add Forward Zones)]ページを開きます。
- ステップ 2 [リソース レコード (Resource Records)]タブをクリックします。
- ステップ 3 [名前 (Name)]フィールドにレコードの所有者を入力します。
- ステップ 4 TTL を入力します。
- ステップ 5 [タイプ (Type)]ドロップダウンリストから、[URI] を選択します。
- ステップ 6 正しいシンタックスに従って、[データ (Data)]フィールドに文字列としてデータを入力します。

例 :

```
10 1 "ftp://ftp1.example.com/public"
```

- ステップ 7 [リソースの追加 (Add Resource)]をクリックします。

CLI コマンド

addRR、**removeRR**、および **modifyRR** コマンドを使用して、URI レコードを追加、削除および修正します。次に例を示します。

```
nrcmd> zone example.com addRR _ftp._tcp URI 10 1 "ftp://ftp1.example.com/public"  
nrcmd> zone example.com removeRR _ftp._tcp URI 10 1 "ftp://ftp1.example.com/public"  
nrcmd> zone example.com modifyRR _ftp._tcp URI 10 1 "ftp://ftp1.example.com/public"  
rdata="11 1 ftp://ftp1.example.com/public"
```




第 13 章

ホストの管理

この章では、DNSゾーンでホストを設定する方法について説明します。この章のコンセプトに進む前に、プライマリおよびセカンダリ DNS サーバーとその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 \(179 ページ\)](#)」を参照してください。

- [ゾーンのホストの追加 \(235 ページ\)](#)
- [ホストの RR の追加 \(236 ページ\)](#)
- [ホストの編集 \(237 ページ\)](#)
- [ホストの削除 \(237 ページ\)](#)

ゾーンのホストの追加

個々の RR ではなく、ホストを設定することによって、ホストのリソースレコードを管理できます。ホストを定義すると、DNS サーバーは、指定したアドレスごとに、IPv4 の場合はアドレス (A) RR、IPv6 の場合は AAAA RR を自動的に作成します。ホストに 1 つ以上のエイリアスを指定すると、サーバーは各エイリアスの正規名 (CNAME) RR も作成します。逆引きゾーンが存在する場合は、サーバーにホストの逆引きゾーンにあるホストのポインタ (PTR) RR を作成させることもできます。

ローカル Web UI

ステップ 1 **Design** メニューの **Auth DNS** サブメニューで **Hosts** を選択して、[ゾーンのホストのリスト/追加 (List/Add Hosts for Zone)] ページを開きます。

ヒント [ゾーンのホストのリスト表示/追加 (List/Add Host for Zone)] ページで、対応する列の見出しをクリックして、ホスト名、IP アドレス、IPv6 アドレス (該当する場合)、またはエイリアスを基準にソートできます。ただし、多数の (5 万を超える) ホストがあるゾーンの場合は、ソートの基準をホスト名に限定してください。IP アドレスまたはエイリアスを基準とするソートは、非常に長い時間を要することがあり、CCM サーバーのメモリ容量を超えた場合には失敗する可能性があります。

ステップ 2 ホストの名前とその IPv4 アドレス、IPv6 アドレス、またはカンマで区切ったアドレスを入力します。

- ステップ 3** ホストにエイリアス名がある場合は、カンマ区切りのリストを入力します。
- ステップ 4** ホストに対応するポインタ (PTR) RR を作成する際に、そのホストの逆引きゾーンが存在することが分かっている場合は、[PTR レコードを作成しますか (Create PTR Records?)] チェックボックスをオンにします。
- ステップ 5** [Add Host] をクリックします。
- ステップ 6** 確認するには、**Design** メニューの **Auth DNS Forward Zones** サブメニューにある を選択して、[正引きゾーンのリスト/追加 (List/Add Forward Zones)] ページを開きます。
- ステップ 7** **Resource Records** タブをクリックし、選択したゾーンの RR を表示します。
- (注) 特定のゾーンのホストのリストを表示するには、[Hosts] タブをクリックします。

CLI コマンド

既存の逆引きゾーンの RR、エイリアス RR、および PTR RR を 1 回の操作で作成するには、各ホストに **zone name addHost hostname address alias** を使用します。作成されたゾーンのリストを表示するには、**zone name listHosts** を使用します。

ホストの RR の追加

選択した dns 編集モード (段階または同期) に基づいて、ホストに RR を追加します。詳細については、「[ゾーンへのリソースレコードの追加 \(222 ページ\)](#)」を参照してください。

これらの RR がアクティブなサーバー RR になるようにするには、DNS サーバーをリロードします。

ローカル Web UI

たとえば、CNAME RR を追加するには、[正引きゾーンのリスト表示/追加 (List/Add Forward Zones)] ページの [リソースレコード (Resource Records)] タブにある [名前 (Name)] フィールドにエイリアスホスト名を追加し、[タイプ (Type)] ドロップダウンリストから [CNAME] を選択して、[データ (Data)] フィールドにホストの正規名を追加してから、[Add Resource Record] をクリックします。この DNS の仕様では、別の RR と同じ名前の CNAME RR は使用できないことに注意してください。

MXRR の場合は、[名前 (Name)] フィールドに元のホスト名を追加します。[タイプ (Type)] ドロップダウンリストから [MX] を選択します。[データ (Data)] フィールドに、整数プリファレンス値、スペース、および元のホストのメールエクスチェンジャのドメイン名を追加して、[Add Resource Record] をクリックします。これらのエントリはページ下部のリストに表示されます。

CLI コマンド

CNAME レコードを作成するには、保護された RR の場合は **zone name addRR alias CNAME canonical** を使用し、保護されていない RR の場合は **zone name addDNSRR alias CNAME canonical** を使用します。

MX レコードを作成するには、保護された RR の場合は **zone name addRR hostname MX preference mxname** を使用し、保護されていない RR の場合は **zone name addDNSRR hostname MX preference mxname** を使用します。

ホストの編集

ホストの編集には、次の作業が含まれます。

- アドレスまたはエイリアスの追加
- リソースレコード (RR) の変更。

ローカル Web UI

ステップ 1 **Design** メニューの **Hosts Auth DNS** サブメニューで を選択して [ゾーンのホストのリスト/追加 (List/Add Hosts for Zone)] ページを開きます。

複数のゾーンが設定されている場合は、左側の [ホスト (Hosts)] ペインのゾーン リストからゾーンを選択します。

ステップ 2 ホスト名をクリックして、追加の IP アドレスまたはエイリアスを追加し、[**Save**] をクリックします。

ステップ 3 RR を変更するには、[**RR の編集 (Edit RR)**] ボタンをクリックして [RR リスト表示の編集 (Edit View RR List)] ページを開きます。

CLI コマンド

ホストを編集するには、**zone name removeRR name type data** または **zone name removeDNSRR name type data** を使用して RR を削除してから、**zone name addRR name ttl class type data** または **zone name addDNSRR name ttl type data** を使用して RR を再入力する必要があります。

ホストの削除

ホストを削除すると、そのホストのすべての A、CNAME、および PTR RR が削除されます。

ローカル Web UI

[ゾーン (Zone)] ページの [ホストのリスト表示/追加 (List/Add Hosts)] で (そこへのアクセス方法については、「[ホストの編集 \(237 ページ\)](#)」を参照)、削除するホストの横にある [削除 (Delete)] アイコンをクリックし、削除を確認します。

CLI コマンド

zone name removeHost を使用してホストを削除してから、**zone name addHost** を使用してホストを再び追加します。



第 14 章

権威 DNS のメトリック

ダッシュボードでは、次の権威 DNS メトリック要素を使用できます。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 11.1 管理ガイドの付録「*Server Statistics*」の「*DHCP Statistics*」の項を参照してください。

- [DNS の一般的なインジケータ \(239 ページ\)](#)
- [DNS インバウンドゾーン転送 \(240 ページ\)](#)
- [DNS ネットワーク エラー \(240 ページ\)](#)
- [DNS アウトバウンドゾーン転送 \(241 ページ\)](#)
- [1 秒あたりの DNS クエリ数 \(242 ページ\)](#)
- [DNS 関連サーバーエラー \(242 ページ\)](#)

DNS の一般的なインジケータ

テーブルとしてレンダリングされるダッシュボード要素 [DNS の一般的なインジケータ (DNS General Indicators)] は、サーバーの状態、最終起動時のリロード時間、サーバー 1 台あたりのゾーン数、およびリソースレコード (RR) の合計数を示します。この表は、[チャートの選択 (Chart Selections)] ページで [DNS Metrics: DNS General Indicators] を選択すると表示されます。

結果の表は、次の情報を示しています。

- **Server State** : (統計が使用可能かどうかに基づく) アップまたはダウンと、サーバーがこの状態である期間。
- **Last Reload** : 最後のサーバー リロードからの経過時間。
- **Total Zones** : 設定されているゾーンの数。
- **Total RRs** : リソース レコードの数。

データの解釈方法

このチャートのデータは、サーバー全般の正常性と稼働時間を示しています。目的はサーバーに関する決定を行うことです。たとえば、リロードのタイミングは、設定されているゾーンの数に応じて判断される場合があります。

結果に基づくトラブルシューティング

サーバーの状態が Down の場合は、すべての DNS チャート インジケータに赤色のステータスボックスが表示され、データは使用できません。サーバーがダウンしている場合は、サーバーを再起動します。表示されるゾーンの数によっては、評価と再設定が必要になる場合があります。

DNS インバウンド ゾーン転送

面グラフとしてレンダリングされる [DNS インバウンドゾーンの転送 (DNS Inbound Zone Transfers)] ダッシュボードの要素は、完全および増分のインバウンドゾーン転送の応答が変化するレートと関連エラーを追跡します。チャートは、[チャートの選択 (Chart Selections)] ページで [DNS Metrics: DNS Inbound Zone Transfers] を選択した場合に使用できます。

結果の面グラフには、次の傾向が表示されます。

- **Full Response** : 完全インバウンド ゾーン転送の数 (AXFRs in)。
- **Incremental Responses** : 増分インバウンド ゾーン転送の数 (IXFRs in)。
- **Authorization Errors** : 拒否された応答の数 (xfer-in-auth-errors)。
- **Failed Attempts** : 拒否ではない失敗の数 (xfer-failed-attempts)。
- **Exceed Max Transfers In** : 同時インバウンド転送が上限に達する回数。

データの解釈方法

このグラフでは、セカンダリ DNS サーバーへのインバウンド ゾーン転送が予測どおりに実行されているかどうかを確認したり、そのプロセスで許可や転送試行の失敗が発生したかどうかを確認したりできます。最も重要なインジケータは、権限不足、そのゾーンに対する不許可、またはその他の理由で拒否されたインバウンドゾーン転送の数のトレンドです。

結果に基づくトラブルシューティング

インバウンドゾーン転送でエラーまたは制限超過が発生した場合は、プライマリ サーバーとセカンダリ サーバーの設定を確認します。

DNS ネットワーク エラー

面グラフとしてレンダリングされる [DNS ネットワークエラー (DNS Network Errors)] ダッシュボードの要素は、DNS サーバーネットワークエラーが変化するペースをトラックします。チャートは、[チャートの選択 (Chart Selections)] ページで [DNS Metrics: DNS Network Errors] を選択した場合に使用できます。

結果の面グラフには、次の傾向が表示されます。

- **Query Error Packets/Query Responses** : 応答数に対するクエリ エラー パケット数の割合。
応答とは、次のとおりです。
 - 権威あり

- 権威あり no-such-name
 - 権威あり no-such-data
 - 権威なし
 - 権威なし no-such-data
 - 拒否された要求
- **Non Error Dropped Packets/Query Responses** : 応答数に対する、エラーではないドロップされたパケット数（ドロップされたクエリ数）の割合。
 - **Update Errors/Updates** : 更新の合計数に対する DNS 更新エラー数の割合。

データの解釈方法

このグラフはサーバーの正常性を示すクエリおよび応答のエラーを表します。

結果に基づくトラブルシューティング

エラーが増加している場合は、DNS サーバーのネットワーク構成を確認します。

DNS アウトバウンド ゾーン転送

面グラフとしてレンダリングされる [DNS アウトバウンドゾーン転送 (DNS Outbound Zone Transfers)] ダッシュボードの要素は、完全および増分アウトバウンドゾーン転送応答が変化するレートと関連エラーとして追跡します。チャートは、[チャートの選択 (Chart Selections)] ページで [DNS Metrics: DNS Outbound Zone Transfers] を選択した場合に使用できます。

結果の面グラフには、次の傾向が表示されます。

- **Full Responses** : 完全アウトバウンド ゾーン転送の数 (AXFRs out) 。
- **Incremental Responses** : 増分アウトバウンド ゾーン転送の数 (IXFRs out) 。
- **Authorization Errors** : 不許可 (拒否された) ゾーン転送要求の数。
- **Exceed Max Transfers Out** : 上限を超えたアウトバウンド転送の失敗の数。
- **Other Errors** : 許可エラーではない他のアウトバウンド転送エラーの数。

データの解釈方法

このグラフでは、セカンダリ DNS サーバーへのアウトバウンドゾーン転送が予測どおりに実行されているかどうかを確認したり、そのプロセスで許可や転送試行の失敗が発生したかどうかを確認したりできます。最も重要なインジケータは、権限不足やそのゾーンに対する不許可が理由で拒否されたアウトバウンドゾーン転送の数のトレンドです。

結果に基づくトラブルシューティング

アウトバウンドゾーン転送でエラーまたは制限超過が発生した場合は、プライマリ サーバーとセカンダリ サーバーの設定を確認します。

1 秒あたりの DNS クエリ数

[1 秒あたりの DNS クエリ数 (DNS Queries Per Second)] ダッシュボードの要素は面グラフとしてレンダリングされ、権威 DNS サーバーの 1 秒あたりのクエリ数を表示します。このチャートは、[チャートの選択 (Chart Selections)] ページで [DNS Metrics: DNS Queries Per Second] を選択した場合に使用できます。

DNS 関連サーバー エラー

[DNS 関連サーバーエラー (DNS Related Servers Errors)] ダッシュボードの要素は、DNS 関連エラーの変化のレートを追跡する面グラフとしてレンダリングされます。チャートは、[チャートの選択 (Chart Selections)] ページで [DNS Metrics: DNS Related Servers Errors] を選択した場合に使用できます。

結果の面グラフには、次の傾向が表示されます。

- **Referral Timeouts/Referrals**— 参照数に対する参照タイムアウト数の割合。
- **Failed Responses/Total Incoming Zone Transfer Requests**— 着信ゾーン転送要求数に対する失敗応答数の割合。
- **TSIG Errors/TSIG Attempts**— TSIG 試行の合計数 (正常に受信されたパケット数) に対する、トランザクションシグニチャ (TSIG) エラー数 (無効な時間、キー、またはシグニチャ) の割合。

データの解釈方法

このグラフは、関連 DNS サーバーとの接続およびデータ転送の正常性を示します。3つのグラフ線にはすべて診断上の意味があります。

結果に基づくトラブルシューティング

エラーが増加している場合は、HA DNS 関係における関連サーバーの設定と接続を確認します。



付録 **A**

リソース レコード

この章では、Cisco Prime Network Registrar でサポートされているすべてのリソースレコードタイプを示します。

- [リソース レコード \(243 ページ\)](#)

リソース レコード

リソース レコードは、DNS ゾーン内のデータを構成します。ゾーンが所有できるリソース レコードの数に一定の制限はありません。一般に、特定タイプのリソース レコードは 0 件、1 件、または複数存在します。ただし、ゾーンに存在できる特定タイプのレコードの数は制限されています。

すべてのリソース レコードには、次の必須エントリがあります。

- **Name** : example.com など、レコードを所有する名前 (ホスト)。
- **Class** (すべてのフォーマットには必要ありません) : DNS はレコードの IN (インターネット) クラスのみをサポートします。
- **TTL** : レコードをキャッシュに保存する時間 (秒単位)。TTL が指定されていない場合は、Cisco Prime Network Registrar は SOA リソース レコードで定義されたゾーンのデフォルト TTL を使用します。
- **Type** : レコードのタイプ (A、NS、SOA、MX など)。さまざまな RFC で多くのタイプが定義されていますが、一般的に使用されているタイプの数は 10 以下です。
- **Record data** : データ型 (形式と意味はレコードタイプによって異なる)。

次の表は、Cisco Prime Network Registrar でサポートされているすべてのリソース レコードタイプのリストです。フィールドの構文、フィールドの説明、および Cisco Prime Network Registrar GUI でのフィールドの表示について説明します。

表 54: リソース レコード

レコー ド	番号	名前	構文と説明	RFC
A	1	Host Address : ゾーンの名称 からアドレス へのマッピン グ	<p><i>name ttl class A address</i></p> <p>Web UI : [ゾーンのホスト追加または編集 (Add or Edit Host for Zone)] ページ : ホスト名、IP アドレス、または [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Name)]、[データ (Name)]</p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host123 3600 IN A 192.168.40.123</pre>	1035
A6	38	IPv6 Address : (廃止。代わり に AAAA レ コードを使 用)	<p><i>name ttl class A address</i></p> <p>データでは、サフィックスアドレスは、ネットワーク順序 (上位のオクテットが最初) でエンコードされる IPv6 アドレスです。128 からプレフィクス長を差し引いた値に相当するビット数に完全に十分であるオクテットがこのフィールドには必要です。0 ~ 7 の先頭パッドビットを使用して、このフィールドを整数のオクテットにする必要があります。パッドビットが存在する場合は、ゾーンファイルをロードするときに、パッドビットをゼロに設定し、受信時に無視する必要があります。次に例を示します。</p> <p>2001:0:734c:c0::</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)] = A6、[データ (Data)] = <i>prefixlength suffixaddr prefixname</i>、次の形式のデータ :</p> <p>CLI コマンド :</p> <pre>0 2345:00c1:ca11:0001:1234:5678:9abc:def0</pre> <pre>nrcmd> zone example.com addRR host456 A6 0 1345:c1:ca11:1:1234:5678:9abc:def0</pre>	6563

レコード	番号	名前	構文と説明	RFC
AAAA	28	IPv6 アドレス (IPv6 Address)	<p><i>name ttl class AAAA address</i></p> <p>データは、4 桁の 16 進数 8 セットがコロンで区切られる IPv6 アドレス形式です。4 桁の最初のセットは、アドレスの上位 16 ビットです。セットの先行ゼロを省略し、セットの値がゼロの場合はそのセット値を省略できます。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = AAAA、[データ (Data)] = <i>address</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host456 AAAA 1345:c1:ca11:1:1234:5678:9abc:def0</pre>	3596
AFSDB	18	Andrew File System (AFS) データベース (Andrew File System (AFS) Data Base)	<p><i>name ttl class AFSDB subtype hostname</i></p> <p>subtype は 1 (AFS セルデータベース サーバー) または 2 (DCE 認証ネームサーバー) のいずれかです。hostname は、所有者が名前を付けたセルのサーバーのホスト ドメイン名です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = AFSDB、[データ (Data)] = <i>subtype hostname</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host4 AFSDB 1 AFSDBhost.example.com.</pre>	1183
AXFR	252	Authoritative Zone Transfer	<p>プライマリネームサーバーからセカンダリネームサーバーにゾーンファイル全体を転送します。AXFR レコードは、通常のゾーン ファイルでは使用されません。プライマリ DNS サーバーからゾーンファイルを複製するため、セカンダリ DNS サーバーで使用されます。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = AXFR、[データ (Data)] = <i>Auth Zone Transfer</i></p>	1995

レコー ド	番号	名前	構文と説明	RFC
CAA	257	Certification Authority Authorization	<p><i>name ttl class CAA flag tag value</i></p> <p>データには、<i>flag</i>、<i>tag</i>、および <i>value</i> が含まれます。ここで、</p> <ul style="list-style-type: none"> • <i>flag</i> : バイトサイズ。現在、ビット0とビット7が使用され、その他のビットは将来の使用のために予約されています（サポートされる値：0、1、および128）。 • <i>tag</i> : US-ASCII 文字と数字のゼロ以外のシーケンス。タグの長さは1以上15以下である必要があります。 • <i>value</i> : 文字列。 <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)]=CAA、[データ (Data)]=<i>flag tag value</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR test1 CAA 0 issue comodoca.com</pre>	6844
CNAME	5	Canonical Name : エイリアス または ニックネーム	<p><i>alias ttl class CNAME canonicalname</i></p> <p>他のリソース レコードが CNAME に関連付けられていないようにしてください。エイリアスは、外部向けに簡単に覚えられる単一名が必要なときに役立ちます。ホスト名が変わるときにエイリアスを使用することもできます。この場合は、ユーザーが元の名前を使用するときに、それを新しい名前に解決できるように、CNAME ポインタが必要です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]=<i>alias</i>、[TTL]、[タイプ (Type)]=CNAME、[タイプ (Type)]、[データ (Data)]=<i>canonicalname</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host456 CNAME host1234</pre>	1035

レコード	番号	名前	構文と説明	RFC
DHCID	49	Dynamic Host Configuration Identifier : (RFC 4701)	<p><i>name ttl class DHCID data</i></p> <p>DNS サーバーはこの RR を使用して、DHCP クライアントとサーバーが DNS を自動的に更新できるようにします。ユーザーはこの RR を設定できません。データは、クライアントメッセージとドメイン名の一方方向ハッシュ計算の結果です。IPv6 アドレスのサンプル RR 出力 :</p> <pre>chi6.example.com IN DHCID (AAIBY2/AuCccgoJbaxcQc9TUapptP691OjxfNuVAA2kjEA=)</pre>	4701
HINFO	13	Host Info : ホストのハードウェアおよびソフトウェア情報	<p><i>name ttl class HINFO cpu os</i></p> <p>データは、ハードウェア (CPU) とオペレーティングシステムです。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)] = HINFO、[データ (Data)] = <i>cpu os</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host5 HINFO CPU1 OS2</pre>	1035

レコード	番号	名前	構文と説明	RFC
HTTPS	65	HTTPS のバインド	<p><i>name ttl class HTTPS SvcPriority TargetName SvcParams</i></p> <ul style="list-style-type: none"> • <i>SvcPriority</i> : このレコードの優先順位 (他のレコードと比較して、低い値が優先されます)。値 0 は <i>AliasMode</i> を示します。 • <i>TargetName</i> : エイリアスターゲット (<i>AliasMode</i> の場合) または代替エンドポイント (<i>ServiceMode</i> の場合) のいずれかのドメイン名。 • <i>SvcParams</i> (オプション) : <i>TargetName</i> の代替エンドポイントを説明する key=value ペアのリスト。 <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = HTTPS、[データ (Data)] = <i>SvcPriority TargetName SvcParams</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR cdn1 HTTPS 1 h3pool alpn=h</pre> <p>注 : 「ech」 サービスパラメータはサポートされていません。</p>	
ISDN	20	統合サービス デジタル網 (ISDN) アドレス (Integrated Services Digital Network (ISDN) Address)	<p><i>name ttl class ISDN ISDNnumber [subaddr]</i></p> <p>データは、所有者の ISDN 番号、直通ダイヤル (存在する場合) 、およびオプションの ISDN サブアドレス文字列です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = ISDN、[データ (Data)] = <i>ISDNnumber [subaddr]</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host6 ISDN ISDN88888</pre>	1183

レコード	番号	名前	構文と説明	RFC
IXFR	251	増分ゾーン転送	<p>増分転送 (IXFR) は、ゾーン内の変更を IXFR サーバーから IXFR クライアントに転送する効率的な手段です。ゾーンの変更部分だけを転送するので、提案どおりより効率的なメカニズムです。これらのメカニズムの目的は、一連の DNS ネームサーバーが特定のゾーンに対して一貫した権威を維持できるようにすることです。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)] = IXFR</p>	1995
MB	7	メールボックスドメイン名 (Mailbox Domain Name)	<p><i>name ttl class MB mbox</i></p> <p>データは、指定されたメールボックスがあるホストのドメイン名です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)] = MB、[データ (Data)] = <i>mbox</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host7 MB mailbox.example.com.</pre>	1035
MD	3	メールの宛先 (Mail Destination) : (廃止。代わりに MX を使用)	メール宛先 (廃止 : MX を使用)	1035
MF	4	メールフォワーダ (Mail Forwarder) : (廃止。代わりに MX を使用)	メールフォワーダ (廃止 : MX を使用)	1035

レコード	番号	名前	構文と説明	RFC
MG	8	メールグループメンバー (Mail Group Member)	<p><i>name ttl class MG mgroup</i></p> <p>データは、メールボックス グループ (メーリングリスト) のドメイン名です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = MG、[データ (Data)] = <i>mgroup</i></p> <p>CLI コマンド :</p>	1035
MINFO	14	メールボックス情報 (Mailbox Info)	<p><i>name ttl class MINFO respmbx errormsg</i></p> <p>データは、メーリングリストのためのメールボックス、およびエラー メッセージを受信するためのメールボックスです。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = MINFO、[データ (Data)] = <i>respmbx errormsg</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host7 MINFO resp.example.com. error.example.com.</pre>	1035
MR	9	メール名の変更 (Mail Rename)	<p><i>name ttl class MR newmbx</i></p> <p>データは、所有者のメールボックス名を変更するメールボックス名です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)] = MR、[データ (Data)] = <i>newmbx</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host7 MR renamemb.example.com.</pre>	1035

レコード	番号	名前	構文と説明	RFC
MX	15	MailExchanger : ドメイン名の メール配信先	<p><i>name ttl class MX pref mxname</i></p> <p>データは、プリファレンス値（レコードの優先順位を決める 16 ビット整数で、小さい値の方が優先される）、および所有者のメールエクスチェンジャーのドメイン名です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)]=MX、[データ (Data)] = <i>pref mxname</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host8 MX 10 exchanger.example.com.</pre>	1035

レコード	番号	名前	構文と説明	RFC
NAPTR	35	Naming Authority Pointer : 新しいドメインラベルまたは Universal Resource Identifier (URI) を生成します。その後、DNS を使用して、ドメイン名の構文にない多くのリソース名のサービスを検索できます。	<p><i>name ttl class NAPTR order pref flags serv regexp replace</i></p> <ul style="list-style-type: none"> • <i>order</i> : ルールの正しい順序に応じた NAPTR レコードの処理順序を示す 16ビットの整数。小さい値が大きい値より前に処理されます。 • <i>pref</i> : <i>order</i> 値が等しい NAPTR レコードの処理順序を示す 16ビットの符号なし整数。小さい値が大きい値より前に処理されます。 • <i>flags</i> : フィールドの書き換えと解釈を制御するフラグを含む文字列。セット [A-Z0-9] (大文字と小文字を区別しない) からの単一文字。S、A、およびUのフラグは端末ルックアップを表し、Pフラグはアプリケーション側のアルゴリズムの残りの部分がプロトコル別に行われる必要があることを示します。 • <i>serv</i> : 有効なプロトコルまたはサービス。 • <i>regexp</i> : 検索する次のドメイン名を構成するためにクライアントが保持する元の文字列に適用される代入式を含む文字列。(一般的な正規表現の使用については、『Cisco プライム ネットワーク レジストラ 11.1 管理ガイド』の「一般的な正規表現の値」の表を参照してください)。 • <i>replace</i> : [フラグ (<i>flags</i>)] フィールドの値に応じて NAPTR、SRV、またはアドレスレコードを照会する次の FQDN。 <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[状態 (State)]、[TTL]、[タイプ (Type)] = NAPTR、[データ (Data)] = <i>order pref flags service regexp replace</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone 8.6.4.e164.arpa addRR 4.3.2.1.6.7.9 naptr 100 10 u sip+E2U /^.*\$/sip:info@tele2.se/ .</pre>	2915

レコード	番号	名前	構文と説明	RFC
NS	2	Name Server : ゾーンの権威 サーバー	<p><i>name ttl class NS nameserver</i></p> <p>ネーム サービスを提供するマシンは、所有者ドメインに存在してはなりません。ドメインごとに、少なくとも1つのNSレコードが必要です。ドメインのNSレコードは、ドメインの委任先ゾーンとドメイン自体の両方に存在する必要があります。NSレコード名には同等のAレコードが必要です（NSレコード名がエイリアスを指すことはできません）。</p> <p>Web UI : [ゾーンの追加または編集（Add or Edit Zone）] ページのネームサーバー : [NS TTL]、[ネームサーバーの追加（Add Nameserver）]</p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR @ NS DNSserv2.example.com.</pre>	1035
NSAP	22	ネットワーク サービス アク セス ポイント (NSAP) アド レス (Network Service Access Point (NSAP) Address)	<p>名前 <i>ttl</i> クラス <i>NASP Nsapaddr</i></p> <p>データはNSAPAddrです。これは、割り当て権威によって割り当てられるオクテット値で、TXTおよびHINFOレコードで使用されるタイプの文字列です（RFC 1706を参照）。</p> <p>Web UI : [ゾーンのリソースレコード（Resource Records for Zone）] ページ : [名前（Name）]、[TTL]、[タイプ（Type）]=NSAP、[データ（Data）]=NSAPAddr</p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host10 NSAP 39840f80005a0000000001e13708002010726e00</pre>	1706
NSEC	47	Next Secure record	<p>DNSSECの一部：名前が存在しないことの証明に使用されます。（廃止）NXTレコードと同じ形式を使用します。</p> <p>Web UI : [ゾーンのリソースレコード（Resource Records for Zone）] ページ : [名前（Name）]、[TTL]、[タイプ（Type）]=NSEC、[データ（Data）]=Next Secure record</p>	

レコード	番号	名前	構文と説明	RFC
OPT	41	DNS EDNS(0) Options	<p>これは、EDNS をサポートするために必要な「疑似 DNS レコードタイプ」です。OPT 疑似 RR（別名「メタ RR」）を要求の追加データセクションに追加できます。受信した要求に OPT レコードが存在する場合、対応する応答側は各応答に OPT レコードを含める必要があります。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)] = OPT</p>	
PTR	12	Pointer : 逆マッピング	<p><i>name ttl class PTR dname</i></p> <p>データは、所有者によって示されたリバースレコードがあるホストのドメイン名です。PTR レコードは、アドレスを名前に変換するために、特に in-addr.arpa ゾーンでの逆マッピングに使用されます。PTR はエイリアスでなく正式名を使用します。PTR レコード内の名前は、リバース名のローカル IP アドレス部分です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[状態 (State)]、[TTL]、[Type (タイプ)] = PTR、[Data (データ)] = <i>dname</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR 45.40.168.192.in-addr.arpa. PTR host1234</pre>	1035
RP	17	担当者 (Responsible Person)	<p><i>name ttl class RP mbox txt host</i></p> <p>データは、担当者のメールボックスのドメイン名、および TXT レコードが存在するホストのドメイン名です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)] = RP、[データ (Data)] = <i>mbox txt host</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host7 RP resp.example.com. text.example.com.</pre>	1183

レコード	番号	名前	構文と説明	RFC
RT	21	経由ルート (Route Through)	<p><i>name ttl class RT pref intermediatehost</i></p> <p>データは、<i>pref</i> (このレコードを同じ所有者の他のレコードより優先することを示す 16 ビットの整数)、および <i>intermediatehost</i> (所有者に到達するための中継ホストのドメイン名) です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)]=RT、[データ (Data)]=<i>pref intermediatehost</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host7 RT 10 routthru.example.com.</pre>	1183
SOA	6	Start of Authority : すべてのゾーンに 1 つの SOA レコードが必要です。	<p><i>name ttl class SOA primeserver hostadmin (serial refresh retry expire minimum)</i></p> <p>Web UI : [ゾーンの追加または編集 (Add or Edit Zone)] ページの SOA 属性 : [シリアル番号 (Serial Number)]、[SOA TTL]、[ネームサーバー (Nameserver)]、[連絡先の電子メール (Contact E-Mail)]、[セカンダリ更新 (Secondary Refresh)]、[セカンダリの再試行 (Secondary Retry)]、[セカンダリの有効期限 (Secondary Expire)]、[最小 TTL (Minimum TTL)]</p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR @ 172800 IN SOA ns hostadmin 1 10800 3600 604800 86400</pre>	1035
SPF	99	Sender Policy Framework	<p>Sender Policy Framework (SPF) レコードはドメインネーム サービス (DNS) TXT レコードの一種であり、ドメインに代わって電子メールを送信することが許可されているメールサーバーを識別します。SPF レコードの目的は、ドメインの送信元アドレスを偽装して送られるスパム メッセージを検出して阻止することです。</p> <p>SPF レコードは、1 つのテキスト文字列として定義されます。</p>	7208

レコード	番号	名前	構文と説明	RFC
SRV	33	Service Location	<p><i>name ttl class SRV priority weight port target</i></p> <ul style="list-style-type: none"> • <i>priority</i> : 所有者の SRV レコードのうち優先するレコードを指定する 16ビットのプライオリティ。 • <i>weight</i> : 同じプライオリティ レベルのレコードに重みを与える 16ビット。 • <i>port</i> : サービスを実行するポートを示す 16ビット。 • <i>target</i> : 指定されたポートで実行されるホストのドメイン名。 <p>管理者は、1つのドメインに対して複数のサーバーを使用したり、ホスト間でサービスを簡単に移動したりすることができます。一部のホストをサービスのプライマリ サーバーとして指定し、他のホストをバックアップとして指定することもできます。クライアントはドメインに対する特定のサービスまたはプロトコルを問い合わせ、利用可能なサーバーの名前を得られます。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)]=SRV、[データ (Data)] = <i>priority weight port target</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host2 SRV 10 1 60 host7.example.com.</pre>	2782

レコード	番号	名前	構文と説明	RFC
SVCB	64	サービスのバインド	<p><i>name ttl class SVCB SvcPriority TargetName SvcParams</i></p> <ul style="list-style-type: none"> • <i>SvcPriority</i> : このレコードの優先順位（他のレコードと比較して、低い値が優先されます）。値 0 は <i>AliasMode</i> を示します。 • <i>TargetName</i> : エイリアスターゲット（<i>AliasMode</i> の場合）または代替エンドポイント（<i>ServiceMode</i> の場合）のいずれかのドメイン名。 • <i>SvcParams</i>（オプション） : <i>TargetName</i> の代替エンドポイントを説明する key=value ペアのリスト。 <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)]=SVCB、[データ (Data)] = <i>SvcPriority TargetName SvcParams</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com svc4 SVCB 3 svc4.example.net alpn="bar" port="8004"</pre> <p>注 : 「ech」 サービスパラメータはサポートされていません。</p>	
TSIG	250	Transaction Signature	<p>キー名。これは、クライアントとサーバーで一意である必要があります。承認されたクライアントからの動的更新、または承認された再帰ネームサーバーからの応答を DNSSEC と同様に認証するために使用できます。</p>	2854
TXT	16	テキスト	<p><i>name ttl class TXT textstring</i></p> <p>データは、任意のタイプの情報を含むことができる 1 つ以上のテキスト文字文字列です。</p> <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)], [TTL]、[タイプ (Type)]=TXT、[データ (Data)] = <i>textstring</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host2 TXT "this message"</pre>	1035

レコード	番号	名前	構文と説明	RFC
URI	256	Uniform Resource Identifier; ユニフォーム リソース識別子	<p><i>name ttl class URI priority weight target</i></p> <p>データには、<i>priority</i>、<i>weight</i> および <i>target</i> が含まれます。ここで、</p> <ul style="list-style-type: none"> • <i>priority</i> : この RR のターゲット URI の優先順位。範囲は、0～65535 です。値が小さいほど優先順位が高くなります。 • <i>weight</i> : 同じ優先順位を持つレコードの相対的な重み。範囲は、0～65535 です。値が大きいほど、優先順位が高くなります。 • <i>target</i> : 二重引用符で囲まれたターゲットの URI。このフィールドの長さは、ゼロより大きくする必要があります。 <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)]=URI、[データ (Data)] = <i>priority weight target</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR _ftp._tcp URI 10 1 "ftp://ftp1.example.com/public"</pre>	7553
WKS	11	既知のサービス (Well Known Services)	<p><i>name ttl class WKS addr protocol servicelist</i></p> <ul style="list-style-type: none"> • <i>addr</i> : 32 ビット IP アドレス。 • <i>protocol</i> : TCP または UDP の 8 ビット IP プロトコル番号。 • <i>servicelist</i> : サービスの 8 ビットの倍数での可変長ビットマップ (TIME、TELNET、FTP、または SMTP) 。 <p>Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、[TTL]、[タイプ (Type)]=WKS、[データ (Data)] = <i>addr protocol servicelist</i></p> <p>CLI コマンド :</p> <pre>nrcmd> zone example.com addRR host8 WKS 192.168.40.56 TCP TELNET</pre>	1035

レコード	番号	名前	構文と説明	RFC
X25	19	X.25 アドレス (X.25 Address)	<i>name ttl class X25 PSDNaddr</i> データは、所有者に関連付けられている X.121 番号計画のパブリックスイッチデータネットワーク (PSDN) アドレスの文字列です。 Web UI : [ゾーンのリソースレコード (Resource Records for Zone)] ページ : [名前 (Name)]、 [TTL]、[タイプ (Type)]=X25、[データ (Data)]= <i>PSDNaddr</i> CLI コマンド : <pre>nrcmd> zone example.com addRR host9 IN X25 311061700956</pre>	1183



付録 **B**

Cisco Prime Network Registrar を使用した DNS エニーキャスト

エニーキャストは、同じサービスを提供する多くのサーバーに1つのクライアントからパケットを送信できるようにするネットワークとルーティングのメカニズムです。エニーキャストグループ内のすべてのサーバーは同じエニーキャスト IP アドレスを使用して設定されます。パケットはルーティングアルゴリズムに基づいて判断されたベストパスでクライアントから最も近いサーバーにルーティングされます。エニーキャストルーティングで複数のサーバーを1つのサービスとしてグループ化することにより、シームレスな冗長性、ロードバランシング、水平スケーリングといった重要な機能を利用できます。エニーキャスト DNS は DNS サービスのエニーキャストの実装です。エニーキャストは、サービスの可用性を隣接ルータにアドバタイズするために BGP (Border Gateway Protocol) などのルーティングプロトコルと併用されます。これにより、エニーキャスト DNS が有効に機能します。

この章では、エニーキャストを使用して Cisco Prime Network Registrar DNS サービスを設定するための情報とツールについて説明します。

- [DNS エニーキャストの基本要件 \(261 ページ\)](#)
- [エニーキャストルーティング \(262 ページ\)](#)
- [Script \(263 ページ\)](#)
- [ルータ設定 \(264 ページ\)](#)
- [BGP を使用したエニーキャスト設定の例 \(264 ページ\)](#)
- [ネットワーク ルータ設定 \(265 ページ\)](#)
- [DNS サーバーでの FRRouting の設定 \(266 ページ\)](#)
- [DNS サーバーでの Quagga の設定 \(268 ページ\)](#)
- [ルータでの診断の実行 \(269 ページ\)](#)
- [BGP トラフィック ログのモニター \(270 ページ\)](#)
- [DNS ゾーンの設定 \(271 ページ\)](#)

DNS エニーキャストの基本要件

次のリストは、エニーキャスト DNS をサポートするための要件と推奨事項です。

- キャッシング DNS サーバーのエニーキャストアドレスを介して DNS クエリを解決するようにクライアントを設定する必要があります。
- ネームサーバーは、NS と A RR でエニーキャストアドレスをアドバタイズする必要があります。
- ネームサーバーは、エニーキャスト IP アドレスの DNS クエリをリッスンする必要があります。
- ループバック インターフェイスの少なくとも 1 つのエニーキャスト IP アドレスを使用してネームサーバーを設定する必要があります。
- また、管理 IP（物理または追加のループバック インターフェイスのいずれか）を使用してサーバーを設定する必要があります。
- ルーティング情報の交換と、エニーキャスト IP アドレスへのルートが存在しない場合のシステムアクセスとメンテナンスのために、DNS サーバーに少なくとも 1 つの物理 IP を定義する必要があります。
- ゾーン転送、ゾーン更新、または query-source に物理 IP または管理 IP のアドレスを使用し、意図したサーバーに更新が送信されるように、ネームサーバーを設定する必要があります。
- ネームサーバーは、RIP、OSPF、BGP などのルーティングプロトコルを使用して、ルーテッドネットワークにエニーキャスト IP アドレスを挿入する必要があります。

エニーキャストルーティング

エニーキャストは手動で設定できますが、エニーキャスト宛先アドレスをゲートウェイルータに通知する BGP や OSPF などのルーティングプロトコルを使用して設定することを推奨します。ルーティングプロトコルを使用して DNS サービスの可用性を通知することにより、サービスが停止した場合にルータが DNS クエリをブラックホールに送信しないようにします。Cisco Prime Network Registrar DNS アプリケーションにはルーティング機能がないため、DNS アプリケーションの外部にあるコードを DNS 環境（物理サーバーまたは仮想マシン）に追加する必要があります。主要なオープンソース製品は、RHEL/CentOS 8.x 用の FRRouting（FRR）と RHEL/CentOS 7.x 用の Quagga です。

FRRouting



（注） RHEL/CentOS 8.x では、FRR を使用します。

FRR は、Linux および Unix プラットフォーム用の IP ルーティングプロトコルスイートで、BGP、IS-IS、LDP、OSPF、PIM、および RIP のプロトコルデーモンが含まれています。

FRR は、Linux 用の別のルーティングプロトコルスイートである Quagga から分岐されます。FRR には、Quagga を広く普及させた基本的な機能と、その基盤を大幅に改善した多くの拡張機能が含まれています。

FRR は、Cisco Prime Network Registrar に同梱されていません。FRR の詳細については、FRR のマニュアルを参照してください。

Quagga



(注) RHEL/CentOS 7.x では、Quagga を使用します。

Quagga はルーティングソフトウェアスイートであり、Unix プラットフォーム、Linux、Solaris、および NetBSD 用の OSPFv2、OSPFv3、RIP v1 および v2、RIPng、ならびに BGP-4 が実装されます。この章では、BGP を使用してこのソリューションを説明します。

Quagga アーキテクチャにはコアデーモンとして zebra が含まれています。zebra は基盤となる Linux カーネルの抽象化レイヤとして機能し、Unix または TCP ストリームを介した Quagga クライアントへの Zserv API を提供します。これらの Zserv クライアントは、通常ではルーティングプロトコルを実装し、zebra デーモンにルーティングの更新を伝達します。

Quagga デーモンは、ネットワークアクセス可能な CLI (**vty** という) を使用して設定できます。CLI は、他のルーティングソフトウェアと同様のスタイルに従います。Quagga には **vttysh** と呼ばれる別のツールがあります。vttysh はすべてのデーモンに対する単一の統合されたフロントエンドとして機能するため、さまざまな Quagga デーモンのほぼすべての側面を 1 か所で管理できます。

Quagga は、Cisco Prime Network Registrar に同梱されていません。Quagga の詳細については、Quagga のマニュアルを参照してください。

Script

サンプルの Python スクリプトは Cisco Prime Network Registrar のインストールに含まれており、次の場所にあります。

- FRR
`/opt/nwreg2/local/examples/dns/python/dns_anycast_bgp_frr.py`
- Quagga
`/opt/nwreg2/local/examples/dns/python/dns_anycast_bgp.py`

スクリプトは FRR/Quagga を開始および停止し、DNS クエリを送信して動作を確認します。FRR/Quagga が開始されると、FRR/Quagga デーモンが接続ルータにエニーキャストのアドバタイズメントを送信し、エニーキャストアドレスによる DNS サービスが使用可能になります。DNS サーバーがスクリプトからのクエリに回答しない場合、スクリプトは FRR/Quagga デーモンを停止します。FRR/Quagga の停止によって TCP 接続が切断され、ルータは BGP キープア

ライブメッセージの受信を停止します。その後で、ルータはそのエニーキャストグループから DNS サービスを削除し、次に最も近い、使用可能な DNS サービスへの DNS クエリの送信を開始します。DNS サーバーがスクリプトからのクエリに応答すると、スクリプトは FRR/Quagga デーモンが実行されているかどうかを確認します。デーモンが実行されていない場合、スクリプトはデーモンを開始します。

サンプルスクリプトを別の場所にコピーし、定期的にスクリプトを実行して DNS サーバーのステータスを確認するように cron ジョブを設定し（推奨は5分間隔）、設定に応じて BGP デーモンを開始または停止することをお勧めします。cron ジョブの例は、このソリューションの範囲外です。

ルータ設定

設定はネットワーク要件やアドレス方式のバリエーションによって異なる可能性があります。

BGP を使用したエニーキャスト設定の例

この項では、シスコのルータと FRR/Quagga ホストベースのルーティングソフトウェアで BGP を使用したエニーキャストの基本的なセットアップと設定について説明します。この章の目的は、ルータと BGP の設定について管理者に手順を示すことではなく、Cisco Prime Network Registrar ラボで正常にテストされた設定を示すことです。ネットワーク要件は異なる場合がありますので注意してください。

BGP は、インターネットの自律システム (AS) 間でルーティング情報と到達可能性情報を交換することを目的として標準化された外部ゲートウェイプロトコルです。この設定は単一の AS を使用します。この方法は、自律システム全体に展開されるソリューションではありません。

次の手順をホスト DNS-1 と DNS-2 で実行する必要があります。

FRR

FRR ルーティングソフトウェアのインストール

Cisco Prime Network Registrar を実行している同じシステムに FRR をインストールします。これにより、次のような FRR パッケージがインストールされます。

```
fr-7.0-5.el8.x86_64
```

Quagga

Quagga ルーティングソフトウェアのインストール

Cisco Prime Network Registrar を実行している同じシステムに Quagga をインストールします。これにより、次のような Quagga パッケージがインストールされます。

```
quagga-0.99.15-7.el6_3.2.x86_64
```

ループバック インターフェイスの作成

システムでループバック インターフェイスのエイリアスを作成します。このループバック インターフェイスのエニーキャスト IP アドレスを設定します。

RHEL の場合、インターフェイス コンフィギュレーション ファイルは、`/etc/sysconfig/network-scripts` にあります。 `ifcfg-lo:0` という名前のディレクトリに次の内容のファイルを作成します。

```
DEVICE=lo:0
IPADDR=10.10.10.1
NETMASK=255.255.255.255
BOOTPROTO=none
ONBOOT=yes
```

Ifup lo: 0 コマンドを使用して、新しいループバックインターフェイスを起動します。

ネットワーク ルータ設定

このルータ設定は、この DNS エニーキャストソリューションの検証で使用されます。これは、DNS エニーキャスト ソリューションの開発を補助するための参考資料として提供されています。この特定のソリューションの完全な設定ですが、ソリューション開発のための参考用ではありません。

```
csr1000v# sh run
Building configuration...
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet1
 ip address 10.78.29.77 255.255.255.0 (Router)
 negotiation auto
!
interface GigabitEthernet2
 ip address 10.0.2.1 255.255.255.0 (Client)
 negotiation auto
!
interface GigabitEthernet4 (DNS-2)
 platform ring rx 256
 ip address 10.0.3.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet5 (DNS-3)
 platform ring rx 256
 ip address 10.0.5.1 255.255.255.0
 negotiation auto
!
router ospf 1
 router-id 2.2.2.2(is the loopback IP address)
 redistribute bgp 65500 subnets
 network 2.2.2.2 0.0.0.0 area 1
 network 10.0.6.0 0.0.0.255 area 1
 network 10.0.0.0 0.0.255.255 area 1
!
router bgp 65500
 bgp log-neighbor-changes
 neighbor IBGP peer-group
 neighbor IBGP update-source Loopback0
 neighbor ANY peer-group
 neighbor 192.0.2.1 remote-as 65500
```

```

neighbor 192.0.2.1 peer-group IBGP
neighbor 192.0.2.1 update-source Loopback0
neighbor 10.0.3.2 remote-as65500
!(This should be the bgp AS in Quagga for DNS-2)
neighbor 10.0.3.2 peer-group ANY
neighbor 10.0.5.2 remote-as 65500
!(This should be the bgp AS in Quagga for DNS-3)
neighbor 10.0.5.2 peer-group ANY
!
address-family ipv4
redistribute ospf 1
neighbor IBGP next-hop-self
neighbor ANY next-hop-self
neighbor 192.0.2.1 activate
neighbor 10.0.3.2 activate
neighbor 10.0.5.2 activate
exit-address-family
!
virtual-service csr_mgmt
ip shared host-interface GigabitEthernet1
activate
!
ip default-gateway 10.78.28.1
ip forward-protocol nd
!
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.78.28.1
ip route 10.78.28.0 255.255.254.0 GigabitEthernet1 10.78.28.1
!
ip prefix-list anycast-ip seq 5 permit 10.10.10.1/32
!
control-plane
!
line con 0
  stopbits 1
line vty 0 4
  login local
!
!
end

```

DNS サーバーでの FRRouting の設定

両方のサーバーで FRR 構成ファイルを設定します。次は DNS-1 の例です。DNS-2 も同様に設定する必要があります。構成ファイルは `/etc/frr` にあります。

`/etc/frr` には構成ファイルの例が複数あります。（FRR がサポートする各ルーティングプロトコル用と、メインプロセスである `zebra` 用）。BGP を使用してエニーキャストを有効にするには、`zebra.conf`、`bgpd.conf`、`daemons` ファイルを設定する必要があります。

デーモンファイルで `zebra` と `bgpd` を有効にする

```

# cat /etc/frr/daemons
# This file tells the frr package which daemons to start.
watchfrr_enable=yes
watchfrr_options="-r '/usr/lib/frr/frr restart %s' -s '/usr/lib/frr/frr start %s' -k '/usr/lib/frr/frr stop %s'"

```

```
#
zebra=yes
bgpd=yes
ospfd=no
```

FRR Zebra 設定

```
# cat /etc/frr/zebra.conf
hostname DNS-1
!
password zebra
enable password zebra
!
interface eth0
 ip address 10.0.3.2/24
!
interface lo
 ip address 10.10.10.1/32
!
line vty
!
```



(注) このグループに属する他のエニーキャスト サーバーに対して、この手順を繰り返します。

FRR BGP 設定

```
# cat /etc/frr/bgpd.conf
! -- bgp --
!
! BGPd sample configuration file
!
!
hostname DNS-1
password zebra
log stdout
!
router bgp 65500
 bgp router-id 10.78.29.79
 bgp log-neighbor-changes
 network 10.10.10.1/32
 timers bgp 4 16
 neighbor 10.0.3.1 remote-as 65500
 neighbor 10.0.3.1 next-hop-self
 neighbor 10.0.3.1 prefix-list DEFAULT in
 neighbor 10.0.3.1 prefix-list ANYCAST out
!
 address-family ipv4
  network 10.0.3.1/24
  neighbor 10.0.3.1 activate
 exit-address-family
!
 ip prefix-list ANYCAST seq 5 permit 10.10.10.1/32
 ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
 line vty
!
```

FRR サービスの開始

次のコマンドを使用して、FRR サービスを開始します。

```
systemctl start frr.service
```

ループバックインターフェイスで追加の IP アドレス を作成する

FRR を使用してエニーキャスト用のループバック インターフェイスに追加の IP アドレスを作成するには、Red Hat のマニュアルを参照してください。

FRR サービスの再起動

次のコマンドを使用して、FRR サービスを再起動します。

```
systemctl restart frr.service
```

DNS サーバーでの Quagga の設定

両方のサーバーで Quagga コンフィギュレーションファイルを設定します。次は DNS-1 の例です。DNS-2 も同様に設定する必要があります。コンフィギュレーションファイルは `/etc/Quagga` にあります。

`/etc/Quagga` にはコンフィギュレーションファイルの例が複数あります (Quagga がサポートする各ルーティングプロトコル用と、メインプロセスである `zebra` 用)。BGP を使用してエニーキャストを有効にするには、`zebra.conf` と `bgpd.conf` を設定する必要があります。

Quagga Zebra の設定

```
# cat /etc/quagga/zebra.conf
hostname DNS-1
!
password zebra
enable password zebra
!
interface eth0
  ip address 10.0.3.2/24
!
interface lo
!
line vty
!
```



(注) このグループに属する他のエニーキャストサーバーに対して、この手順を繰り返します。

Quagga BGP の設定

```
# cat /etc/quagga/bgpd.conf
! *- bgp *-
!
! BGPd sample configuration file
!
!
hostname DNS-1
password zebra
log stdout
!
router bgp 65500
bgp router-id 10.78.29.79
bgp log-neighbor-changes
network 10.10.10.1/32
timers bgp 4 16
neighbor 10.0.3.1 remote-as 65500
neighbor 10.0.3.1 next-hop-self
neighbor 10.0.3.1 prefix-list DEFAULT in
neighbor 10.0.3.1 prefix-list ANYCAST out
!
address-family ipv4
network 10.0.3.1/24
neighbor 10.0.3.1 activate
exit-address-family
!
ip prefix-list ANYCAST seq 5 permit 10.10.10.1/32
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
line vty
!
```

BGP デーモンの開始

次のコマンドを使用して、BGP デーモンを開始します。

```
systemctl start bgpd
```

ルータでの診断の実行

ルータで診断を実行して、エニーキャストが正しく設定されていることを確認します。

sh ip bgp summary コマンドの出力は、router-1 が 2 つのネイバーとの BGP セッションを開始したことを示します。**State/PfxRcd** の値は、TCP セッションがアップしており、ルータとホストがルートを交換していることを示します。このフィールドは、リモートネイバーから受信したルートプレフィックスの数を示す数値である必要があります。値の例は 1 です。この時点で、DNS サーバーとの BGP 接続が確立された状態になります。

sh ip bgp summary の概要 :

```
BGP router identifier 2.2.2.2, local AS number 65500
BGP table version is 86, main routing table version 86
1 network entries using 248 bytes of memory
2 path entries using 240 bytes of memory
1/1 BGP path/bestpath attribute entries using 248 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
BGP using 736 total bytes of memory
BGP activity 16/15 prefixes, 61/59 paths, scan interval 60 secs
```

ネイバー	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.0.2.1	4	65500	0	0	1	0	0	4w0d	Idle
10.0.3.2	4	65500	137919	129519	86	0	0	1w0d	1
10.0.5.2	4	65500	137923	129519	86	0	0	1w0d	1

show ip bgp neighbors コマンドは、ネイバーに関する情報を詳細に示します。

show ip route コマンドには、エニーキャストアドレスと現在ルーティングされているホストのエントリが含まれている必要があります。

```
#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
B 10.10.10.1/32 [200/0] via 10.0.3.2, 00:00:10
```

BGP トラフィック ログのモニター

ホスト DNS-1 と DNS-2 の BGP トラフィックログをモニターするには、**telnet localhost bgpd** コマンドを使用します。

FRR

```
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is FRRouting (version 7.0).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
dns-anycast-1> enable
dns-anycast-1# terminal monitor
dns-anycast-1# conf t
dns-anycast-1(config)# debug bgp keepalives
dns-anycast-1(config)# 2020/10/27 02:56:22 BGP: : 10.0.3.1 KEEPALIVE rcvd

dns-anycast-1(config)# 2020/10/27 02:56:23 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:27 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:28 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:32 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:33 BGP: : 10.0.3.1 sending KEEPALIVE
```

```
2020/10/27 02:56:37 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:38 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:42 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:43 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:47 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:48 BGP: : 10.0.3.1 sending KEEPALIVE
```

Quagga

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Hello, this is Quagga (version 0.99.15).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
User Access Verification
Password:
DNS-1> enable
DNS-1# terminal monitor
DNS-1# 2016/07/13 15:49:20 BGP: 10.0.5.1 send message type 4, length (incl. header) 19
2016/07/13 15:49:21 BGP: 10.0.5.1 rcv message type 4, length (excl. header) 0
2016/07/13 15:49:25 BGP: 10.0.5.1 send message type 4, length (incl. header) 19
2016/07/13 15:49:27 BGP: 10.0.5.1 rcv message type 4, length (excl. header) 0
```

DNS ゾーンの設定

これでエニーキャスト機能の設定は終わりますが、管理者は DNS サーバーの設定を完了する必要があります。 [ゾーンの管理 \(179 ページ\)](#) を参照してください。

詳細については、次のリンクを参照してください。

- <http://www.pacnog.org/pacnog6/IXP/Anycast-v10.pdf>
- <http://www.nongnu.org/Quagga>
- <https://frrouting.org/>
- <https://cumulusnetworks.com/learn/frrouting/>
- <https://bgpgeek.com/installing-frr/>
- <https://access.redhat.com/solutions/4967711>
- <https://access.redhat.com/solutions/4538371>
- <http://www.linuxjournal.com/magazine/ipv4-anycast-linux-and-Quagga>
- <http://ddiguru.com/blog/125-anycast-dns-part-5-using-bgp>



(注) 上記のリンクは外部 Web サイトを参照しており、シスコはそれらを最新の状態に保つ責任を負いません。これらは参照のためだけに提供されています。コンテンツが古い場合やリンクにアクセスできない場合は、Web サイトの所有者に連絡して最新情報を入手してください。



付録 C

DNS のセキュリティと攻撃の防止

DNS 攻撃は、ネットワークの DNS サービスの可用性または安定性を標的とする攻撃です。DNS キャッシュポイズニング、DDoS、DNS スプーフィングなど、さまざまな方法で DNS を攻撃できます。この章では、Cisco Prime Network Registrar で使用可能であり、DNS のセキュリティ関連の脅威と攻撃の防止に役立つ機能について説明します。

- [Cisco Prime Network Registrar での DNS 攻撃の防止 \(273 ページ\)](#)

Cisco Prime Network Registrar での DNS 攻撃の防止

Cisco Prime Network Registrar の次の機能は、DNS セキュリティ関連の脅威と攻撃を防止するのに役立ちます。

キャッシュポイズニング

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。キャッシュポイズニング攻撃の処理の詳細については、[DNS キャッシュポイズニングの検出と防止 \(66 ページ\)](#) を参照してください。

- **UDP ポートのダイナミックな割り当て**

キャッシング DNS のサーバーは多くの UDP ポート番号を使用します。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。詳細については、[UDP ポートの動的割り当て \(61 ページ\)](#) を参照してください。

- **DNS トランザクション ID のランダム化**

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。

- **ランダム化されたクエリ名**

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。

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。詳細については、[リゾルバ設定の指定 \(62 ページ\)](#) を参照してください。

DDoS 攻撃

分散型サービス妨害攻撃 (DDoS 攻撃) では、ターゲットサーバー、サービス、またはネットワークにフラディングする着信トラフィックが、さまざまな送信元から発信されます。そのため、単一の送信元をブロックするだけでは攻撃を阻止することができません。

• レート制限

レート制限によって、少数のクライアントで DNS サーバーが過負荷になるのを防ぐことができます。また、権威 DNS サーバーに対するアップストリームクエリ攻撃からも保護します。この機能によって、一部の DDoS 攻撃を軽減し、サーバーが少数のクライアントによって過負荷になるのを防ぐことができます。これにより、悪意のあるトラフィックを制限することができます。詳細については、[レート制限のキャッシュ管理 \(78 ページ\)](#) を参照してください。

• スマートキャッシュ

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期限切れのデータを更新します。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。詳細については、[スマートキャッシュの有効化 \(58 ページ\)](#) を参照してください。

• DNS アンプ攻撃の防止

DNS アンプ攻撃は、パブリックアクセスが可能なオープン DNS サーバーを使用してターゲットシステムを DNS 応答トラフィックでフラディングさせる、一般的な形式の DDoS 攻撃です。主な手法は、攻撃者が DNS 名のルックアップ要求をオープン DNS サーバーに送信し、送信元アドレスをスプーフィングしてターゲットのアドレスにします。DNS サーバーが DNS レコード応答を送信すると、代わりにターゲットに送信されます。攻撃者は通常、アンプ効果を最大化するために、できるだけ多くのゾーン情報の要求を送信します。このタイプのほとんどの攻撃は、攻撃者が送信するスプーフィングされたクエリのタイプは単一の要求で DNS ゾーンに関するすべての既知の情報を返す「ANY」です。応答のサイズは要求よりもかなり大きいため、攻撃者はターゲットに向けられるトラフィックの量を増やすことができます。

キャッシュ DNS サーバーのセキュリティイベント設定の詳細については、[セキュリティイベントのロギング \(44 ページ\)](#) を参照してください。

権威 DNS サーバーのセキュリティイベント設定の詳細については、[セキュリティイベントの設定 \(127 ページ\)](#) を参照してください。

- **Allow ANY Query ACL**

Cisco Prime Network Registrar では、[サーバーの管理 (Manage Servers)] ページの *allow-any-query-acl* 属性が応答のサイズを最小化するのに役立ちます。この属性は、権威 DNS サーバーページとキャッシング DNS サーバーページの両方に存在し、デフォルト値は「none」です。

- **最小限の応答**

Cisco Prime Network Registrar は、権限と追加のセクションが応答で省略される *minimal-responses* をサポートしています。これによりクエリの応答サイズが小さくなるため、サービス拒否をある程度遅らせることができます。Cisco Prime Network Registrar 11.0 以降、*minimal-responses* はキャッシュ DNS サーバーでデフォルトで有効になり、権威 DNS サーバーではデフォルトで無効になっています。

データの認証と許可

- **DNSSEC**

DNSSECにより、データ出元の認証、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。Cisco Prime Network Registrar は、権威 DNS サーバーとキャッシング DNS サーバーの両方で DNSSEC をサポートしています。

権威 DNS サーバーでの DNSSEC サポートの詳細については、[権威 DNSSEC の管理 \(141 ページ\)](#) を参照してください。

キャッシング DNS サーバーでの DNSSEC サポートの詳細については、[DNSSEC の管理 \(77 ページ\)](#) を参照してください。

- **DNS ファイアウォール**

キャッシング DNS ファイアウォールは、ネットワーク上で機能することが許可されているドメイン名、IP アドレス、およびネームサーバーを制御します。また、DNS ファイアウォールルールは、RPZ を使用して権威 DNS サーバー上の特別に指定されたゾーンに対しても設定できます。RPZ と RR データを DNS リゾルバと組み合わせることにより、DNS サーバーの不正使用を防ぐ有効な DNS ファイアウォールを構成できます。詳細については、[DNS ファイアウォールの管理 \(163 ページ\)](#) を参照してください。

- **Cisco Umbrella**

Cisco Umbrella は、フィッシングやマルウェアなどのインターネット上の脅威に対する防御の最前線となります。Umbrella を解決に使用するようにキャッシング DNS を設定することにより、シスコの Umbrella のクラウドサービスで、要求されたドメイン/ホストに関

する最新の応答を提供することが可能になります。詳細については、[Umbrella を使用するためのキャッシュ DNS の設定 \(83 ページ\)](#) を参照してください。

• ACL を使用したセキュアな DNS サーバーアクティビティ

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。

- ゾーンクエリの制限：権威 DNS サーバーの属性 *restrict-query-acl* は、サーバーが受け入れる必要があるデバイスクエリを制限します。キャッシング DNS サーバーの属性 *acl-query* と *acl-do-not-query* では、それぞれ、照会される IP アドレスと照会されないサブネットを指定します。
- ゾーン転送要求の制限：*restrict-xfer-acl* 属性を使用して、既知のセカンダリサーバーへのゾーン転送要求をフィルタリングします。
- DDNS 更新の制限：*update-acl* 属性を使用して、既知の DHCP サーバーからの DDNS パケットをフィルタリングします。
- 悪意のあるクライアントのブロック：*acl-blocklist* 属性は、アクセスコントロールリストに登録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 または GSS-TSIG を使用したセキュアゾーン転送と DNS の更新

セキュアモードでのゾーン転送は、HMAC MD5 ベースの TSIG と GSS-TSIG の両方をサポートします。オプションの TSIG キーまたは GSS-TSIG キー（『*Cisco Prime Network Registrar 11.1 DHCP ユーザーガイド*』の「Transaction Security」の項または「GSS-TSIG」の項を参照）をプライマリサーバーアドレスに追加することができます。それには、*address-key* の形式でエントリをハイフンでつなぎます。

• DoT によるセキュアなクエリ

DNS over TLS (DoT) は、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。

権威 DNS サーバーの TLS 設定の詳細については、「権威 DNS サーバーの管理」の章の、「[TLS 設定の指定](#)」の項を参照してください。

キャッシング DNS サーバーの TLS 設定の詳細については、「キャッシング DNS サーバーの管理」の章の、「[TLS 設定の指定](#)」の項を参照してください。



索引

- A**
- A レコード [223, 243](#)
 - 追加 [223](#)
 - リソース レコード [243](#)
 - A6 レコード [243](#)
 - AAAA レコード [243](#)
 - AFSDBレコード [243](#)
- B**
- BIND ファイル [189](#)
 - 形式 [189](#)
 - zones [189](#)
 - インポート [189](#)
- C**
- CAA [230](#)
 - CAA レコード [230, 243](#)
 - cdns コマンド (CLI) [26, 61–62, 75](#)
 - addException [75](#)
 - addRootHint [61](#)
 - listExceptions [75](#)
 - removeException [75](#)
 - set [62](#)
 - msg-cache-size [62](#)
 - neg-cache-size [62](#)
 - rrset-cache-size [62](#)
 - show [26](#)
 - CDNS ドメイン リダイレクト [169](#)
 - 概要 [169](#)
 - cdns [49, 71](#)
 - セキュリティログ [49](#)
 - フォワーダの追加 [71](#)
 - フォワーダのリスト [71](#)
 - CDNS [27, 58, 76](#)
 - DNS64 [76](#)
 - スマートキャッシュ [58](#)
 - パケットロギング [27](#)
 - cdns64 コマンド (CLI) [77](#)
 - イネーブル化 [77](#)
 - cdns64 コマンド (CLI) (続き)
 - create [77](#)
 - cdns コマンド [68](#)
 - CNAME レコード [243](#)
- D**
- DHCID レコード [243](#)
 - dns [131](#)
 - セキュリティログ [131](#)
 - DNS ENUM domain コマンド (CLI) [207](#)
 - delete [207](#)
 - create [207](#)
 - DNS ENUM number コマンド (CLI) [208](#)
 - 追加 [208](#)
 - DNS ENUM コマンド (CLI) [206](#)
 - remove [206](#)
 - 追加 [206](#)
 - デフォルトの設定 [206](#)
 - DNS ENUM ドメイン [206, 209](#)
 - pull [209](#)
 - push [209](#)
 - 追加 [206](#)
 - DNS ENUM 番号 [207, 210–211](#)
 - pull [211](#)
 - push [210](#)
 - 追加 [207](#)
 - DNS ENUM [206](#)
 - 概要 [206](#)
 - デフォルトの管理 [206](#)
 - DNS over HTTPS [54](#)
 - dns コマンド (CLI) [65, 73, 94, 135, 137, 139, 146, 150, 153, 195, 227](#)
 - addForwarder [73](#)
 - findRR [227](#)
 - get [65, 135](#)
 - round-robin [65, 135](#)
 - getZoneCount [195](#)
 - listForwarders [73](#)
 - removeForwarder [73](#)
 - set [150, 153](#)
 - mem-cache-size [150](#)
 - notify-min-interval [150](#)
 - notify-send-stagger [150](#)

dns コマンド (CLI) (続き)

set (続き)

- notify-wait [150](#)
- アクティビティの概要 - 間隔 [153](#)
- log-settings [153](#)

show [94, 146](#)

- イネーブル化 [65, 135, 137, 139](#)
- ixfr-enable [137](#)
- notify [139](#)
- round-robin [65, 135](#)

DNS サーバーの設定 [138, 180](#)

- NOTIFY [138](#)
- 有効化 [138](#)
- ループバックゾーン [180](#)

DNS サーバーの転送 [71, 73](#)

- リスト [73](#)

DNS ビュー コマンド (CLI) [217](#)

- 順序変更 [217](#)

DNS ビュー [213–218](#)

- pull [218](#)
- push [217](#)
- 管理 [215](#)
- キー ポイント [214](#)
- 順序変更 [216](#)
- 設定 [213](#)
- 同期 [217](#)

DNS [2, 4–5, 57, 61, 65, 68–69, 73, 93, 126, 140–141, 149, 153, 196, 198, 200, 239–243](#)

- dns コマンド (CLI) [153](#)
- set [153](#)
- log-settings [153](#)

DNS キャッシュのフラッシュ [65](#)

- localhost [153](#)
- アドレス形式 [2](#)
- オプション [61, 149](#)
- 最大メモリキャッシュサイズ [61](#)

外部ポート [149](#)キャッシュ、フラッシュ [65](#)キャッシュ専用サーバー、キャッシュ専用サーバーを参照 [5](#)グルー レコード [198, 200](#)

- 削除 [200](#)
- 無効なグルーレコード [198](#)

サーバ [68–69, 93, 140–141](#)

- コマンド [68, 140](#)
- ネットワーク インターフェイス、設定 [69, 141](#)

サーバー ロギング [153](#)最大 [57](#)

- キャッシュ TTL プロパティ [57](#)

セカンダリサーバー、セカンダリネームサーバーを参照 [4](#)zones [196](#)

DNS (続き)

ダッシュボード [239–242](#)

- アウトバウンドゾーン転送チャート [241](#)
- 一般的なインジケータ チャート [239](#)
- インバウンドゾーン転送チャート [240](#)
- 関連サーバー エラー チャート [242](#)
- ネットワーク エラー チャート [240](#)

トップネーム [126](#)ドメイン名 [2](#)

- 空間 [2](#)

トラブルシューティング [153](#)名前からアドレスへの解決 [243](#)ポート [149](#)ルートネームサーバー [61](#)例外処理 [73](#)DNS64 [76](#)

- 管理 [76](#)

DNSSEC [77](#)

- 管理 [77](#)

DNS コマンド [140](#)dns コマンド CLI [178](#)

- getStats [178](#)
- ha [178](#)

DoH [54](#)DoH 設定 [54](#)

E

EDNS0 について [7](#)

H

HA DNS [175, 177](#)

- dns コマンド (CLI) [177](#)
- セットパートナーダウン [177](#)
- ha-dns-pair コマンド (CLI) [177](#)
- create [177](#)
- サーバー ペアの同期 [177](#)
- バックアップサーバー、設定 [175](#)
- メインサーバー、設定 [175](#)
- 有効化 [175](#)

ha-dns-pair コマンド (CLI) [175, 177](#)

- set [175](#)
- ha-dns-backup-server [175](#)
- ha-dns-main-server [175](#)
- sync [177](#)

HTTPS レコード [243](#)

I

in-addr.arpa ドメイン [6](#)

IP アドレス [1](#)
 アドレスを参照、IP [1](#)
 ISDN レコード [243](#)

L

LDAP [229](#)
 localhost [180](#)

M

MB レコード [243](#)
 MG レコード [243](#)
 MINFO レコード [243](#)
 MR レコード [243](#)
 MX レコード [243](#)

N

Naming Authority Pointer レコード [243](#)
 NAPTR レコードを参照 [243](#)
 NAPTR レコード [229, 243](#)
 NOTIFY [153](#)
 トランザクションのロギング [153](#)
 NSAP レコード [243](#)
 nslookup コーティリティ [153](#)
 NS レコード [243](#)

R

remote-dns コマンド (CLI) [150](#)
 create [150](#)
 RFC [137–138, 189, 195, 228–230, 232, 243](#)
 1035 [189](#)
 1995 [137](#)
 1996 [138](#)
 2136 [195](#)
 2782 [228, 243](#)
 2915 [243](#)
 2916 [229](#)
 3263 [229](#)
 3403 [229](#)
 4701 [243](#)
 6844 [230](#)
 7553 [232](#)
 RP レコード [243](#)
 RT レコード [243](#)

S

SOA レコード [147, 185, 243](#)
 TTL プロパティ [147](#)
 ゾーン [147](#)
 定義済みの [185](#)
 SRV レコード [243](#)
 SVCB レコード [243](#)

T

TLS 設定 [51, 133](#)
 TTL プロパティ [57, 61, 147–148, 243](#)
 DNS [57](#)
 最大 [57](#)
 キャッシュ TTL プロパティ [57](#)
 最大 DNS オプション [61](#)
 default [147–148](#)
 応答 [147](#)
 TXT レコード [243](#)

U

URI [232](#)
 URI レコード [232, 243](#)

W

WKS レコード [243](#)

Z

zone-dist コマンド (CLI) [204](#)
 sync [204](#)
 zone-template コマンド (CLI) [182, 204](#)
 apply-to [182](#)
 set [204](#)
 dist-map [204](#)
 create [182](#)
 clone [182](#)

あ

悪意のある DNS クライアントと応答しないネームサーバーの
 処理 [150](#)

い

インポート コマンド (CLI) [189](#)

え

面グラフ 16

お

折れ線グラフ 16

か

解決例外 73

き

既知のサービス レコード 243

WKS レコードを参照 243

逆引き 6, 192, 243

zones 6, 192

設定 192

ドメイン 6

マッピングレコード 243

キャッシュ 65

キャッシュ、フラッシュ 65

キャッシュ専用サーバー 5

け

権威 DNS 96

パケットロギング 96

権威ネームサーバー 4

こ

公開キー 50, 132

さ

サブゾーン 198–200

委任 199

削除 200

追加 198

ネームサーバー 198

命名 198

散布図 16

し

証明書の設定 50, 132

公開キーファイル 50, 132

秘密キーファイル 50, 132

す

スマートキャッシュ 58

せ

secondary 5, 148–149, 196–197

DNS 196

zones 196

SOA レコード 148–149

更新時間 197

再試行時間 149

zones 196

ゾーン 148

タイムゾーン 149

ネームサーバー、DNS 5

定義済みの 5

有効期間 149

セキュリティログ 49, 131

セッション・コマンド (CLI) 184

set 184

dns-edit-mode 184

セッション開始プロトコル (SIP) プロキシ 229

絶対ドメイン名 222

そ

相対ドメイン名 223

増分ゾーン転送 137

有効化 137

zones 4–6, 147, 184–185, 187, 189, 195, 197, 200, 204, 222–224, 227, 235, 237

DNS 更新 195

dns コマンド (CLI) 195

getZoneCount 195

DNS 更新の有効化 195

TTL プロパティ、設定 147

委任ポイント 4

インポート 189

逆引き、逆引きゾーンを参照 6

権威ネームサーバー 185

追加 185

削除 200

サブゾーン 200

削除 200

編集 200

シリアル番号 185

ゾーン・コマンド (CLI) 204

set 204

dist-map 204

ゾーン転送、定義済み 5

zones (続き)

- ゾーン転送、有効化 197
- 追加 222
- 定義済みの 4
- 転送、ゾーン転送を参照 5
- テンプレートからの追加 187
 - ドメイン 4, 222
 - ゾーンとの違い 4
- 名前、作成 184
- ホスト 235, 237
 - 削除 237
- ホストテーブル、編集 237
- リソース レコード 222–224, 227
 - フィルタリング 227
 - 保護 224
- リソース レコードの削除 223
- ゾーン 182, 184
 - テンプレート 182
 - zone-template コマンド (CLI) 182
 - create 182
 - コピー 182
 - 編集モード、設定 184
- ゾーン・コマンド (CLI) 139, 148–149, 185–186, 188, 198, 223–224, 228, 236–238
 - addDNSRR 223, 237
 - addHost 236
 - addRR 186, 223, 237
 - staged または -sync 223
 - A 186
 - applyTemplate 186
 - findRR 228
 - forceXfer 198
 - get 185–186
 - serial 185–186
 - listHosts 186, 236
 - リストRR 188
 - removeDNSRR 224, 237
 - removeHost 238
 - removeRR 224, 237
 - restrict-xfer 198
 - set 139, 148–149, 186
 - defttl 148
 - expire 149
 - nameservers 186
 - notify-set 139
 - refresh 148
 - retry 149
 - show 186
 - イネーブル化 139
 - notify 139
 - create 186
 - primary 186
 - テンプレート、使用 186

- ゾーン転送 197
 - 強制実行 197
 - すべて強制 197
 - 有効化 197
- ゾーンテンプレート 180, 182, 204
 - 作成 180
 - ゾーン分散、関連付け 204
 - ゾーンへの適用 182
- ゾーン分散 201, 204
 - zone-dist コマンド (CLI) 204
 - addSecondary 204
 - create 204
 - 管理 201
 - 同期 204
- 存続可能時間のプロパティ 147
 - TTL プロパティを参照 147

た

- ダッシュボード 85–88, 239–242
 - DNS クエリ応答チャート 87
 - DNS 239–242
 - ダッシュボード 239–242
 - アウトバウンドゾーン転送チャート 241
 - 一般的なインジケータチャート 239
 - インバウンドゾーン転送チャート 240
 - 関連サーバーエラーチャート 242
 - ネットワークエラーチャート 240
 - DNS キャッシングサーバーの再帰レート制限チャート 86
 - DNS キャッシング アクティビティチャート 86
 - DNS クエリタイプのチャート 88
 - DNS 再帰クエリタイムチャート 88
 - DNS 着信クエリチャート 87
 - キャッシング DNS の一般的なインジケータチャート 85
- 段階モードと同期モード 183

て

- テキスト レコード 243
 - TXT レコード 243
- テンプレート 180
 - ゾーン 180

と

- 同期 183
 - DNS 編集モード 183
 - ステーjing DNS 編集モード 183
 - 編集 183

ドメイン **3**
 登録 **3**
 ドメイン名 **2**
 空間 **2**
 ツリー構造 **2**

な

名前からアドレスへの解決 **243**

ね

ネームサーバー **5**
 DNS クライアント/サーバーモデル **5**
 DNSプライマリサーバー、プライマリネームサーバーを参照 **5**
 名前からアドレスへの解決 **5**
 ネームサーバー **4-5**
 secondary **4**
 ネームサーバー、DNS **4**
 タイプ **5**
 ドメイン **5**
 プライマリ、プライマリネームサーバーを参照 **4**
 ネームサーバー レコード **243**
 NS レコードを参照 **243**
 ネットワーク インターフェイス **69, 141**
 DNS サーバー **69, 141**
 ネットワーク番号 **3**

は

パケットロギング **27, 96**

ひ

秘密キー **50, 132**

ふ

プライマリネームサーバー **4, 180, 185, 243**
 SOA レコード **243**
 設定 **180**
 zones **185**
 プライマリサーバー、設定 **185**
 分散 **201**
 ゾーン **201**

ほ

ポインタ (逆マッピング) レコード **243**
 PTR レコードを参照 **243**
 棒グラフ **16**
 ホスト **195, 235, 237**
 ゾーンへの追加 **235**
 動的 **195**
 編集 **237**
 ホスト情報レコード **243**
 HINFO レコードを参照 **243**

ら

round-robin **135**
 有効化 **135**

り

リソースレコード **200, 221, 223-224, 230, 232, 243**
 A **243**
 A6 **243**
 AAAA **243**
 AFSDB **243**
 CAA **230, 243**
 CLIでの追加 **223**
 CNAME **243**
 DHCID **243**
 HINFO **243**
 HTTPS **243**
 ISDN **243**
 MB **243**
 MG **243**
 MINFO **243**
 MR **243**
 MX **243**
 NAPTR **243**
 NS **243**
 NSAP **243**
 PTR **243**
 RP **243**
 RT **243**
 SOA **243**
 SRV **243**
 SVCB **243**
 TXT **243**
 URI **232, 243**
 WKS **243**
 設定 **221**
 タイプ **243**
 編集 **200, 221**
 サブゾーン情報 **200**
 保護 **224**

れ

例外 [73](#)
解決の例外を参照 [73](#)

ろ

ロギング [153](#)
NOTIFY [153](#)
トランザクションのロギング [153](#)

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。