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

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、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 Registrar11.1 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（Add Exception）] 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ます。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-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。

- **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。すべてのクライアントレート制限の属性については、次の表 1 : 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 *1*：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（*client-rate-limiting*）	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（*client-rate-limiting-qps*）	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（*client-rate-limiting-factor*）	*client-rate-limiting* 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（*client-report-max-count*）	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 2 : 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 *2:* 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（*domain-rate-limiting*）	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（*domain-rate-limiting-qps*）	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（*domain-rate-limiting-factor*）	*domain-rate-limiting* 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	*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指定します。 リストのエントリには次の属性があります。 • 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（*domain-report-max-count*）	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（Domein 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」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」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 Registrar11.1 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。

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。