DNS 更新の管理

DNS 更新プロトコル (RFC 2136) は、DNS と DHCP を統合します。後者の 2 つのプロトコルは相互補完します。つまり、DHCP は、IP アドレス割り当てを集中化および自動化し、ダイナミック DNS 更新は、割り当てられたアドレスとホスト名の間のアソシエーションを自動的に記録します。DHCP を DNS 更新を使用する場合、ホストが IP ネットワークに接続するときに、必ずそのホストのネットワーク アクセスを自動的に設定します。固有の DNS ホスト名を使用してホストを検索し、ホストにリーチできます。たとえば、モバイルホストは、ユーザーや管理者の介入なしで、自由に移動できるようになります。

この章では、Cisco Primeネットワーク レジストラーサーバーで DNS アップデートを使用する方法と、Windows クライアント システムとの特別な関連性について説明します。

DNS 更新のプロセス

DNS 更新を構成するには、次の操作を行う必要があります。

1. 前方ゾーンまたは逆ゾーン、またはその両方に対して DNS 更新構成を作成します。DNS 更新設定の作成 （14 ページ）を参照してください。

2. 次の 2 つの方法のいずれかで、この DNS 更新の構成を使用します。
   - 名前付き、埋め込み、または既定の DHCP ポリシーで DNS 更新の構成を指定します。DHCP ポリシーの設定と適用を参照してください。
   - CISCO Prime Network レジストラー DHCP サーバーまたはフェールオーバー ペアと DNS サーバーまたは高可用性(HA)ペア間の単一 DNS アップデート 関係を自動設定する DNS アップデート マップを定義します。DNS 更新マップで更新の構成を指定します。DNS 更新マップの作成 （23 ページ）を参照してください。
3. 必要に応じて、DNS 更新のアクセス制御リスト (ACL) またはトランザクション署名 (TSIG) を定義します。アクセス コントロール リストとトランザクション セキュリティの設定 （6 ページ）を参照してください。
4. 必要に応じて、これらの ACL または TSIG に基づいて 1 つ以上の DNS 更新ポリシーを作成し、ゾーンに適用します。DNS 更新ポリシーの設定 （17ページ）を参照してください。
5. 必要に応じて、DHCPv4 の TXT RR から DHCID RR に移行するように DNS 更新を構成します。DHCPv4 の DHCID RR への移行 （26 ページ）を参照してください。
6. 必要に応じて、Windows クライアントの DNS 更新構成を調整します。たとえば、デュアル ゾーン更新の場合などです。Windows クライアントの DNS 更新の構成 （28 ページ）を参照してください。
7. ホスト名を提供するか、Cisco Prime ネットワークレジストラーがそれらを生成するように要求するように DHCP クライアントを設定します。
8. 必要に応じて、編集モードに基づいて DHCP サーバーと DNS サーバーを再ロードします。

特殊な DNS 更新に関する考慮事項

DNS 更新を構成する際には、次の 2 つの問題を考慮してください。

- セキュリティ上の理由から、Cisco Prime Network レジストラー DNS 更新プロセスでは、管理者が DNS データベースに手動で入力した名前は変更または削除されません。
- 大規模な展開で DNS 更新を有効にし、HA DNS を使用していない場合 (「高可用性 *DNS* ペアの展開」のCisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide 章を参照) は、プライマリ DNS サーバーと DHCP サーバーを複数のクラスターに分割します。DNS 更新は、サーバーに追加の負荷を生成します。

DHCPv6 の DNS 更新プログラム

Cisco プライムネットワーク レジストラーは現在、IPv4 および IPv6 経由の DHCPv6 DNS アップデートをサポートしています。DHCPv6 の場合、DNS 更新は非一時的なステートフル アドレスと委任されたプレフィックスに適用されます。

非一時ステートフル アドレスの DNS 更新

DHCPv6 の DNS 更新には、リース用の AAAA および PTR RR のマッピングが含まれます。Cisco Prime Network レジストラーでは、サーバーまたはエクステンションを使用した完全修飾ドメイン名と DHCPv6 クライアント*FQDN*オプション(39)がサポートされます。

Cisco Primeネットワーク レジストラーは RFC 4701、4703、および 4704 に準拠しているため、DHCID リソース レコード(RR)をサポートします。すべての RFC-4703 準拠のアップデータは、DHCID R を生成し、クライアント識別子 (DUID) と FQDN (RFC 4701 に従う) のハッシュであるデータを生成できます。ただし、更新ポリシー ルールで AAAA および DHCID の R を使用できます。

DHCPv6 の DNS 更新処理は、DHCPv4 の場合と似ていますが、1 つの FQDN が複数のリースを持つことができる点を除いて、1 つのクライアントに対して複数の AAAA および PTR R が発生します。複数の AAAA R は、同じ名前または異なる名前にすることができます。ただし、PTR の R は、リース アドレスに基づいて常に異なる名前で指定されます。RFC-4703 準拠のアップデータは、複数のクライアント間の競合を回避するために DHCID RR を使用します。

（注） DNS サーバーがダウンしていて、DHCP サーバーが DNS 更新を完了して DHCPv6 リースに追加された R を削除できない場合、リースは引き続き AVAILABLE 状態で存在します。同じクライアントのみがリースを再利用します。

委任されたプレフィックスの DNS 更新

委任されたプレフィックスの DNS 更新を有効にして、委任されたプレフィックス リースの AAAA および PTR マッピングを更新できます。ただし、この場合、委任されたプレフィックスの 0 アドレスの DNS のみが更新されます。たとえば、2001:db8:3333:3333:/64 のプレフィックスが委任されている場合、2001:db8:3333:3333::0 の PTR および/または AAAA のみが委任されます。は DNS で更新されます。この機能は、委任されたプレフィックスに対して DNS 委任を行う手段を提供しません。

委任されたプレフィックスの更新は、DNS 更新構成でプレフィックス委任更新属性が有効になっている場合にのみ有効になります。この属性はデフォルトでは無効になっています。委任されたプレフィックスの更新は、アドレス更新とは異なるゾーンに発生する可能性が高いため、新しい DNS 更新構成を作成して、対応するプレフィックスに関連付ける必要があります。

標準の名前生成規則が適用されるため、ヒントを含む FQDN オプションを含むクライアントは、結果の名前に影響を与える可能性があります(構成で許可されている場合)。クライアントは、FQDN オプションを要求した場合、プレフィックスの委任の更新に使用される名前を返されることはありません。

（注） この機能を使用する場合は、両方のフェールオーバー パートナーがこの機能をサポートするバージョンを実行していることを確認する必要があります。それ以外の場合、更新はアップグレードされたサーバーによってサービスを提供された場合にのみ実行されます。したがって、両方のパートナーがアップグレードされるまで、この機能を有効にしないでください。

DHCPv6 のアップグレードに関する考慮事項

Cisco Prime Network レジストラーの前に設定された、DHCPv6 処理用の DNSDHCPv6 ポリシー階層更新オブジェクトを参照するポリシーを使用する場合(を参照)、サーバーは、指定された DNS サーバーに対する DNS 更新のキューイングを開始します。これは、DNS 更新が DHCPv6 リースに対して自動的に (および予期せず) 開始する可能性があることを意味します。

注意 Cisco Prime Network レジストラーまたはその他の DNS サーバーの以前のバージョンを使用する場合、最近の DHCID RR 標準の変更により、ゾーン転送および DNS 更新の相互運用性の問題が発生する可能性があります。DHCPv6 DNS 更新をサポートするために、DNS サーバーをアップグレードする必要がある場合があります。

DHCPv4 と DHCPv6 での合成名の生成

クライアントがホスト名を指定しない場合、DHCPv4 および DHCPv6 には合成名生成プログラムが含まれます。DNS 更新構成の *v6* 合成名前生成属性を使用すると、次の内容に基づいて生成された名前を合成名のステムに追加できます。

- クライアント DHCP 一意識別子 (DUID) 値 (プリセット値) のハッシュ。
- 未加工のクライアント DUID 値 (区切り記号のない 16 進数のストリング)。
- *CableLabs* ケーブルラボ-*17*オプション*device-id*サブオプション値(区切り文字のない 16 進数文字列、または見つからない場合はクライアント DUID のハッシュ)。
- *CableLabs* ケーブルラボ-*17*オプション*cm-mac-address*サブオプション値 (区切り記号のない 16 進数の文字列として、または見つからない場合はクライアント DUID のハッシュ)。

注意 ドメインがインターネットからアクセス可能な場合、一部の生成方法によってプライバシーの問題が発生する可能性があります。

DNS 更新構成の*v4* 合成名前生成属性では、次の内容に基づいて生成された名前を合成名のステムに追加できます。

- **address**:クライアントの v4 アドレスを識別します。
- **クライアント ID**:要求で DHCPv4 クライアントによって指定されたクライアント ID または DUID (オプション 61)。

- **hashed-client-id**—SHA-256 ハッシュの右部分 64 ビットで形成された 13 文字のベース 32 でエンコードされた文字列である、ハッシュ化されたクライアント ID に、前方ゾーン名が付加されます。

合成DNS 更新設定の作成 （14 ページ）名の生成を使用して DNS 更新構成を作成する方法については、「」を参照してください。

CLI では、この設定の例を次に示します。

```
nrcmd> dhcp-dns-update example-update-config set v6-synthetic-name-generator=hashed-duid

nrcmd> dhcp-dns-update example-update-config set v4-synthetic-name-generator=client-id
```

DNS 更新のための逆引きゾーンの決定

DNS 更新構成では、指定された逆ゾーン プレフィックス長属性のプレフィックス長の値を使用して、ip6.arpa ドメインの逆ゾーンを生成します。ip6.arpa ドメインを使用して合成できるため、完全なリバースゾーンを指定する必要はありません。逆引き DNS 更新の構成に対してDNS 更新設定の作成 （14 ページ）この属性を設定します (「」を参照してください)。逆引きゾーンプレフィックス長に関する規則を次に示します。

- ip6.arpa ゾーンは 4 ビット境界上にあるため、値には 4 の倍数を使用します。4 の倍数でない場合、値は 4 の次の倍数に切り上げられます。
- 最大値は 124 で、128 を指定すると、ホスト名が含まれる可能性のないゾーン名が作成されます。
- 値 0 はゾーン名に使用されるビットが一切使用されないので、ip6.arpa が使用されます。
- DNS 更新構成から値を省略すると、サーバーはプレフィックスの値を使用するか、最後の手段としてプレフィックスのアドレス値から取得されるプレフィックス長を使用します (「」をプレフィックスとリンクの設定参照)。

逆ゾーン名を合成するには、DHCP サーバーに対して、ゾーンの逆引きのシンセを有効にしておく必要があります。したがって、逆ゾーン名が DHCPv6 に対して合成される順序は次のようになります。

1. 逆引き DNS 更新の構成で完全な逆ゾーン名を使用します。
2. 逆引き DNS 更新構成では、逆ゾーン プレフィックス長からの ip6.arpa ゾーンに基づいて設定します。
3. プレフィックス定義の逆ゾーンプレフィックス長から ip6.arpa ゾーンに基づいて設定します。
4. プレフィックス定義のアドレスのプレフィックス長から ip6.arpa ゾーンに基づいて設定します。

CLI では、リバース ゾーン プレフィックス長を設定する例を次に示します。

```
nrcmd> dhcp-dns-update example-update-config set reverse-zone-prefix-length=32
```

Web UI でプレフィックスの逆引きゾーンを作成するには、プレフィックスの一覧/追加ページ **Create Reverse Zone**に各プレフィックスのボタンが含まれています。（プレフィックスの作成と編集 を参照）。

CLI では、プレフィックス**prefix**のリバース**–range**ゾーンを作成する名前**createReverseZone**[ ] コマンドも提供します (アドレスまたは範囲の値から)。**prefix** 名前**deleteReverseZone**[ ]**–range** を使用して、逆引きゾーンを削除します。

逆ゾーンを直接構成するときにサブネットまたはプレフィックスの値を入力して、DHCPv4 サブネットまたは DHCPv6 プレフィックスからリバース ゾーンを作成することもできます。詳細については、以下の「プライマリ リバース ゾーンの構成」を Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide参照してください。

Client FQDN の使用

既存の DHCP サーバーの使用クライアント *fqdn*属性は、要求の DHCPv6 クライアント FQDN オプションにサーバーが注意を払うかどうかを制御します。クライアントに複数の名前が存在する場合に、サーバーが返す名前を決定するために使用する規則は、次の優先順位です。

1. クライアントを使用するサーバー FQDN は、(DNS 内に存在すると見なされない場合でも) リースに使用されている場合に、FQDN を要求しました。
2. DNS 内に最も長い有効期間を持つ FQDN が有効であると見なされます。
3. DNS 内にまだない有効期間が最長の FQDN。

アクセス コントロール リストとトランザクション セキュリティの設定

ACL は権限リストですが、トランザクション・シグニチャー (TSIG) は認証メカニズムです。

- ACL を使用すると、サーバーはパケットに定義された要求またはアクションを許可または禁止できます。
- TSIG は、DNS メッセージが信頼された送信元から送信され、改ざんされないようにします。

セキュリティで保護する DNS クエリ、更新、またはゾーン転送ごとに、アクセス許可を制御する ACL を設定する必要があります。TSIG 処理は、TSIG 情報を含むメッセージに対してのみ実行されます。この情報を含まない、またはこの情報が取り除かれるメッセージは、認証プロセスをバイパスします。

完全に安全なソリューションの場合、メッセージは同じ認証キーによって承認される必要があります。たとえば、DHCP サーバーが DNS アップデートに TSIG を使用するように設定されており、更新するゾーンの ACL に同じ TSIG キーが含まれている場合、TSIG 情報を含まないパケットは認証ステップに失敗します。これにより、更新トランザクションがセキュリティで保護され、ゾーンの変更を行う前にメッセージが認証され、承認されます。

ACL と TSIG は、サーバーまたはゾーンの DNS 更新ポリシーを設定する役割をDNS 更新ポリシーの設定 （17 ページ）果たします。

DNS キャッシュ サーバーまたはゾーンでの ACL の割り当て

DNS キャッシュ サーバーまたはゾーン レベルで ACL を割り当てます。ACL には、次の 1 つ以上の要素を含めることができます。

- **IP** - ドット区切り 10**address**進表記法たとえば、192.168.1.2 とします。
- **Network** - ドット 10 進表記と**address**スラッシュ表記。たとえば、192.168.0.0/24 などです。この例では、そのネットワーク上のホストのみが DNS サーバーを更新できます。
- **Another** - 事前定義する**ACL**必要があります。埋め込みリレーションシップを削除するまでは、別の ACL に埋め込まれている ACL を削除できません。その ACL へのすべての参照が削除されるまで、ACL を削除しないでください。
- **Transaction- Signature**値は、キーワードの後にシークレット値が続く形式の値でなければなりません。 **(TSIG) key key key** スペース文字を格納するには、リスト全体を二重引用符で囲む必要があります。TSIG キーについては、トランザクションのセキュリティ （8 ページ）を参照してください。

各 ACL に一意の名前を割り当てます。ただし、次の ACL 名には特別な意味があり、通常の ACL 名には使用できません。

- **any**—誰でも特定のアクションを実行できます
- **none**-誰も特定のアクションを実行できません
- **localhost**- ローカル・ホスト・アドレスは、特定のアクションを実行できます。
- **localnets**- ローカル ネットワークは、特定のアクションを実行できます。

次の点に注意してください。

- ACL が設定されていない場合は**any**、この値が想定されます。
- ACL が設定されている場合、少なくとも 1 つの句でトラフィックを許可する必要があります。
- 否定演算子 (**!**) は、前のオブジェクトのトラフィックを禁止しますが、明示的に指定しない限り、本質的に他のトラフィックを許可しません。たとえば、IP アドレス 192.168.50.0 のトラフィックのみを禁止するには、を使用**!192.168.50.0, any**します。

ローカル アドバンスド Web UI

[**デザイン**] メニューの**ACLs**[**セキュリティ**] サブメニューの下で [リスト/ アクセスコントロールリストの追加] ページを開きます。[ACL] ペインの**[ACL の追加]** アイコンをクリックし、ACL 名と一致リストを入力して、**[ACL**の追加] をクリックします。**key** 値ペアは引用符で囲んではいりません。地域レベルでは、レプリカ ACL をプルしたり、ローカル クラスタに ACL をプッシュしたりできます。ACL を再利用することもできます。

CLI コマンド

名前**acl**と 1 つ以上の ACL 要素を受け取る名前**create** *match-list*を使用します。ACL リストはカンマで区切られ、スペース文字がある場合は二重引用符で囲まれます。CLI はプル/プッシュ機能を提供しません。

たとえば、次のコマンドは 3 つの ACL を作成します。1 つ目は値を持つキーで、2 つ目はネットワーク用で、3 つ目は最初の ACL を指します。値の前に感嘆符**!()** を含めると、その値を否定するので、一連の値で除外することができます。

```
nrcmd> acl sec-acl create "key h-a.h-b.example.com."

nrcmd> acl dyn-update-acl create "!192.168.2.13,192.168.2.0/24"

nrcmd> acl main-acl create sec-acl
```

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。

- <名前| **aclすべて**>**プル**<**確認**する |**置き換える**|**正確な**>クラスター名[**-レポートのみ**|**-レポート**]
- <名前|**aclすべて**>**プッシュ**<**確認**する |**置き換える**|**正確な**>クラスターリスト[**-レポートのみ**|**-レポート**]
- 名前再利用クラスタリスト [-レポートのみ | **acl -レポート**]

ACL のゾーンの設定

DNS サーバーまたはゾーンの ACL を構成するには、DNS 更新ポリシーを設定し、ゾーンに対してこの更新ポリシーDNS 更新ポリシーの設定 （17 ページ）を定義します (「」を参照)。

トランザクションのセキュリティ

トランザクション署名 (TSIG) の R を使用すると、DNS サーバーは、受信した各メッセージを、TSIG を含む認証を行います。サーバー間の通信は暗号化されませんが、認証されるため、データの信頼性とパケットの送信元を検証できます。

DNS アップデートに TSIG を使用するように Cisco Prime Network レジストラー DHCP サーバーを設定すると、サーバーはメッセージに TSIG RR を付加します。TSIG レコードの一部は、メッセージ認証コードです。

DNS サーバーは、メッセージを受信すると TSIG レコードを検索します。見つかった場合は、まず、そのキー名が認識されるキーの 1 つであることを確認します。その後、更新プログラムのタイム スタンプが妥当であることを確認します (トラフィックリプレイ攻撃との戦いを支援するため)。最後に、サーバーはパケットで送信されたキー共有シークレットを調べ、独自の認証コードを計算します。結果として計算された認証コードがパケットに含まれる認証コードと一致する場合、内容は本物であると見なされます。

TSIG キーの作成

ローカル アドバンスド Web UI

[**デザイン**] メニューの**Keys**[**セキュリティ**] サブメニューの下で [暗号化キーの一覧/追加] ページを開きます。

アルゴリズム、セキュリティタイプ、時間スキュー、キー ID、およびシークレットの各値の説明については、表 1 : cnr_keygen ユーティリティのオプション を参照してください。キーの管理に関する考慮事項 （11 ページ）も参照してください。

TSIG キーを編集するには、[暗号化キーの一覧/追加] ページでキー名をクリックし、[暗号化キーの編集] ページを開きます。

地域レベルでは、レプリカ キーをプルしたり、キーをローカル クラスターにプッシュしたりできます。

CLI コマンド

key 名前シークレットを **create**使用する: キーの名前 (ドメイン名形式、たとえば、hosta-hostb-example.com など) と、共有シークレットの最小値を base-64 でエンコードされた文字列として指定します (省略可能な time skew 属性の説明については表 1 : cnr_keygen ユーティリティのオプション を参照してください)。CLI の例は次のようになります。

```
nrcmd> key hosta-hostb-example.com.create secret-string
```

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。

- **キー**<名前|**すべて**>**プル**<**確認**する |**置き換える**|**正確な**>クラスター名[**-レポートのみ**|**-レポート**]
- **キー**<名前|**すべて**>**プッシュ**<**確認**する |**置き換える**|**正確な**>クラスターリスト[**-レポートのみ**|**-レポート**]
- **キー**名**再利用**クラスタリスト[**-レポートのみ**|**-レポート**]

キーの生成

TSIG キーを生成するには、Cisco Prime Network レジストラー **cnr_keygen**ユーティリティを使用して、追加するか、または**import keys**を使用してインポートすることをお勧めします。

DOS**cnr_keygen**Linux シェルからキー生成ユーティリティを実行します。このユーティリティは、インストールパス/usrbin ディレクトリにあります。

使用例を次に示します。

```
> /opt/nwreg2/local/usrbin/cnr_keygen -n a.b.example.com. -a hmac-md5 -t TSIG -b 16
-s 300

key "a.b.example.com." {
```

```
algorithm hmac-md5;
secret "xGVCsFZ0/6e0N97HGF50eg==";
# cnr-time-skew 300;
# cnr-security-type TSIG;
};
```

キー名だけが必要です。オプションを次の表に示します。

表 *1: cnr_keygen* ユーティリティのオプション

オプション	説明
–a hmac-md5	アルゴリズム。これはオプションです。現在、hmac-md5 のみがサポートされています。
–b *secret-size*	シークレットのバイト サイズ。これはオプションです。プリセット値は 16 バイトです。有効な範囲は 1 から 64 バイトです。
–s *time-skew*	キーの時間スキュー (秒単位)。これは、このキーで符号付きパケットとローカル システム時刻のタイムスタンプの最大差です。これはオプションです。プリセット値は 5 分です。範囲は 1 秒から 1 時間です。
–n *name*	キー名。必須。最大長は 255 バイトです。
–t TSIG	使用されるセキュリティの種類。これはオプションです。現在、TSIG のみがサポートされています。
–h	[ヘルプ（Help）]。これはオプションです。ユーティリティの構文とオプションが表示されます。
–v	[バージョン]。これはオプションです。ユーティリティのバージョンが表示されます。

結果のシークレットは、ランダムな文字列として base64 エンコードされます。

コマンド ラインの最後で右矢印 (>) または二重右矢印 (>>) を使用する場合は、出力をファイルにリダイレクトすることもできます。> は指定されたファイルを書き込むか、または上書きし、>> は既存のファイルに追加します。次に例を示します。

```
> /opt/nwreg2/local/usrbin/cnr_keygen -n example.com > keyfile.txt
```

```
> /opt/nwreg2/local/usrbin/cnr_keygen -n example.com >> addtokeyfile.txt
```

その後、CLI を使用してキー ファイルを Cisco Prime Network レジストラーにインポートし、ファイル内のキーを生成できます。キーのインポートでは、インポート ファイルで検出された数だけキーを生成できます。ファイルへのパスは完全修飾パスにする必要があります。次に例を示します。

```
nrcmd> import keys keydir/keyfile.txt
```

キーの管理に関する考慮事項

独自のキーを生成する場合は、base64 エンコード文字列として入力する必要があります(base64 エンコードの詳細については RFC 4648 を参照してください)。これは、許可される文字は base64 のアルファベット文字と、埋め込み文字としての等号(=)だけであることを意味します。base64 エンコードされていない文字列を入力すると、エラー メッセージが表示されます。

次に、他の推奨事項をいくつか示します。

- バッチ コマンドを使用してキーを追加または変更しないでください。
- 共有シークレットを頻繁に変更する。2ヶ月ごとにお勧めします。Cisco プライムネットワーク レジストラーでは、明示的にはこれを適用しないことに注意してください。
- 共有秘密の長さは、キー付きメッセージ ダイジェスト (HMAC-MD5 が 16 バイト) の長さ以上にする必要があります。Cisco Prime Network レジストラーでは、明示的に強制するものではなく、共有シークレットが有効な base64 でエンコードされた文字列であることを確認するだけですが、RFC 2845 で推奨されているポリシーです。

サポート TSIG 属性の追加

DNS 更新の構成に対して TSIGDNS 更新設定の作成 （14 ページ）サポートを追加するには (を参照) 次の属性を設定します。

- *server-key*
- *backup-server-key*

TSIG で GSS-TSIG セキュリティ アルゴリズムを使用するには、以下の属性を有効にします。

- 使用-*gss-tsig*

GSS-TSIG

RFC 3645 では、汎用セキュリティ サービス (GSS) の安全なキー交換を許可する TSIG の拡張を提案し、すべての GSS クライアントにキーを手動で配布する必要がなくなります。RFC 2743 で規定されている汎用セキュリティ サービス アプリケーション プログラム インターフェイス（GSS API）に基づく TSIG で使用するアルゴリズムを定義します。

GSS-TSIG は、Kerberos セキュリティ メカニズムを利用して、セキュア DDNS 更新とセキュア ゾーン転送を提供します。

クライアントとサーバーは、GSS API 呼び出しを使用して、認証、整合性、および機密性に関する制限された有効期間のセキュリティ コンテキストを確立します。セキュリティ コンテキストを確立するには、ネゴシエーションが完了するまで、クライアントとサーバーの間で不透明なトークンを渡す必要があります。TKEY リソース レコード [RFC 2930] は、クライアントとサーバー間でトークンを転送する手段として使用されます。セキュリティ コンテキストが確立されると、GSS API 呼び出しを使用して署名を生成および検証するために使用されます。これらの署名は、[RFC 2845] で説明されているように、クライアントとサーバーの間で送信され

るDNSメッセージで交換されるTSIGレコードの一部として、クライアントとサーバーによって交換されます。

このプロトコルを使用する前に、クライアントとサーバーはKerberosサーバーでローカルに認証される必要があります。一般に、初期TGT(チケットを取得するチケット)チケットは、システムログオンを通じてキャッシュで利用可能であるか、kinitのようなユーティリティを使用して取得されます。DHCP/DNSクライアントは、プリンシパル名(DNS/ホスト名)を使用してサービス チケット用の Kerberos サーバーを要求します。クライアントは、DNS サーバーと安全に対話する際に認証を証明するサービス チケットを提供します。サービス チケットは、同じサービス キーを使用してアプリケーション サーバーのみが暗号化解除できるサービス キーを使用して、Kerberos サーバーによって暗号化されます。

詳細については、DHCP サーバーGSS-TSIG の設定 （43 ページ）と DNS サーバーで必要な構成のを参照してください。

（注） デフォルトでは、Cisco プライムネットワーク レジストラーは HMAC-MD5 ベースのセキュア TSIG アップデートをサポートします。GSS ベースのセキュア更新を有効にするには、ユーザーは*tsig*処理属性でnoneオプションを選択して、DNSサーバーでHMAC-MD5設定をすべて無効にする必要があります。

DHCP サーバーとセカンダリ DNS サーバーの構成

KDC サーバー情報を /etc/krb5.conf で構成します。KDC から最初のチケットを取得するには、kinit ユーティリティを使用します。

（注） サーバー間の通信にKerberosサーバーを使用する場合は、/etc/krb5.confの最新の暗号化アルゴリズムを使用することをお勧めします。

DHCP サーバーとセカンダリ DNS サーバーの構成のトラブルシューティング

- 初期資格情報の取得中に発生する可能性のあるクライアント関連のエラー:
- クロックスキューエラー - Kerberosクライアントとサーバーを確認し、ntpと同期しない場合は時間内に同期します。
- KDC に到達できない - AD ホスト名が解決可能であることを確認します。
- kinit - 初期資格情報を取得中に Kerberos データベースにクライアントが見つかりません - ユーザーが AD に存在するかどうかを確認します。
- kinit - 初期資格情報を取得中に領域「DOMAIN.com」のKDCのサーバーを解決できません - REALMがADに存在するかどうかを確認します。

- kinit - 初期資格情報を取得中に事前認証に失敗しました - チケットを取得するために入力されたパスワードがADのユーザーに関連付けられたパスワードと同じかどうかを確認します。

GSS-TSIG 設定の作成

DNS/DHCP は、キー管理用の非永続的テーブルを維持します。

（注） DHCP および DNS サーバーで使用される既定の TKEY 管理値を変更するオプションがあります。GSS- TSIG 設定を作成し、DHCP/DNS サーバー ページで参照を提供する必要があります。

ローカルおよびリージョン Web UI

[設計] メニューから、[**セキュリティ**] サブメニューの下の**[GSS-TSIG]**を選択して、[GSS-TSIG 設定の一覧/追加]ページを開きます。左側の**GSS-TSIG ペインで[GSS-TSIG**の追加]アイコンをクリックします。名前を入力し、[**GSS-TSIG 設定の追加**] をクリックします。

GSS-TSIG 属性

- *tkey-max-exchanges* - 無限ループを防ぐために RFC 3645 からの勧告に従って、DNS サーバーは特定のキーをネゴシエートしようとして、TKEY 交換の最大数 (つまり、特定のクライアントから受け取った数の TKEY クエリ) を課すものとします。この属性は、この制限を指定する必要があります。TKEYテーブル レコードは、交換カウントを保持します。キー ネゴシエーション中に交換カウントが tkey-max 交換を超えた場合、DNS サーバーはキー ネゴシエーションを中止します。
- *tkey*-テーブル-最大サイズ- この属性は TKEY テーブルのサイズを制限します。
- *tkey* テーブル消去インターバル- TKEY テーブルから期限切れキーを削除する時間間隔。
- *tkey-session-time* - ユーザーが構成可能なキーの最大有効期間を指定します。キーの有効期間は、最初のキー ネゴシエーション中およびこの属性を使用して取得した Kerberos サーバーの有効期限時間によって制御されます。0に設定すると、この属性は無効になり、キーの有効期間は、指定された有効期限が指定されたKerberosによってのみ制御されます。この属性が値 > 0 で構成されている場合、Kerberos の有効期限の最小値とこの値がキーの最大有効期間として使用されます。

GSS-TSIG 設定を編集するには、[GSS-TSIG 設定の一覧/追加] ページで名前をクリックし、[GSS-TSIG 設定の編集] ページを開きます。

地域レベルでは、GSS-TSIG 設定をローカル クラスターにプルまたはプッシュすることもできます。

CLI コマンド

gss-tsig名**の作成**[属性=値..] を使用します。GSS-TSIG 設定オブジェクトの名前を指定します。次に例を示します。

```
nrcmd> gss-tsig gss create tkey-max-exchanges=6 tkey-table-max-size=500
tkey-table-purge-interval=90
```

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。

- **gss-tsig** <名前|**すべて**>**プル**<**確認**する |**置き換える**|**正確な**>クラスター名[**-レポートのみ**|**-レポート**]
- **gss-tsig**<名前|**すべて**>**プッシュ**<**確認**する |**置き換える**|**正確な**>クラスターリスト[**-レポートのみ**|**-レポート**]
- **gss-tsig** 名**再利用**クラスタリスト[**-レポートのみ**|**-レポート**]

DNS 更新設定の作成

DNS 更新の構成では、DNS サーバーまたは HA DNS サーバーのペアに対する DNS 更新用の DHCP サーバー フレームワークを定義します。これは、前方または逆ゾーンの DNS 更新 (またはその両方) を生成するかどうかを決定します。オプションで、トランザクションの TSIG キー、自動生成されたホスト名のスタイルを制御する属性、および更新する特定の前方または逆ゾーンを設定します。一意のサーバーリレーションシップごとに DNS 更新の構成を指定する必要があります。

たとえば、DHCP サーバーからのすべての更新が単一の DNS サーバーに送信される場合、サーバーの既定のポリシーで設定された単一の DNS 更新構成を作成できます。クライアント クラスのクライアントの各グループを対応する転送ゾーンに割り当てるには、より具体的なクライアント クラス ポリシーで、それぞれのクライアントの前方ゾーン名を設定します。

Cisco Prime Network Registrar 11.0 以降、より厳格なルールが DNS アップデート設定で指定する DNS サーバーに適用されます。DNS サーバーを複数のロールで使用するように設定できなくなります。つまり各サーバーは（アドレスに基づいて）スタンドアロン、HA メイン、または HA バックアップとしてのみ動作することができます。HA メインまたは HA バックアップは、単一の HA の関係でのみ存在できます。したがって、DNS サーバーを複数のロールで実行する必要がある場合は、ロールごとに個別の DNS サーバーのアドレスを使用する必要があります。

（注） DNS 更新設定で、複数のロールが DNS サーバーを使用していた場合、DHCP サーバーのリロード時にエラーが報告されます。報告されるエラーは、メッセージ 19696「DNS Update Configuration '*name1*' with *server-config-type* of *server(s)-address* conflicts with DNS Update Configuration '*name2*' with *server-config-type* of *server(s)-address* DNS Update Configuration '*name1*' will be set to disable DNS updates and thus will not configure server(s)」です。

ローカルアドバンスドおよびリージョン Web UI

ステップ 1 [**展開**] メニューの**DNSUpdateConfigsDNSUpdates**サブメニューの下で [DNS 更新の一覧/ 追加] ページを開きます。

ステップ 2 [DNS 更新構成] ウィンドウの**[DNS 更新構成の追加]** アイコンをクリックして、[DnsUpdateConfig の追加] ダイアログ ボックスを開きます。

ステップ 3 [名前属性] フィールドに、更新設定の名前を入力します。

ステップ 4 **Add DnsUpdateConfig** をクリックして、DNS 更新設定を追加します。

ステップ 5 更新構成の名前を選択して、[DNS 更新の構成の編集] ページを開きます。

ステップ 6 [更新設定] セクションで、適切な動的 *DNS*設定をクリックします。

- **update-none**- 前方ゾーンまたは逆方向ゾーンを更新しません。
- **update-all**- 前方ゾーンと逆方向のゾーンを更新します (デフォルト値)。
- **update-fwd-only**- 転送ゾーンのみを更新します。
- **update-reverse-only**- 逆ゾーンのみを更新します。

ステップ 7 更新設定ブロックの下で、適切な*DNS* クライアント *ID*設定をクリックします。

- **txt**—サーバーは DHCPv4 DNS 更新に TXT RR を使用し、DHCPv6 DNS アップデートには DHCID RR を使用します。
- **dhcid**—サーバーは DHCPv4 と DHCPv6 の両方の DNS 更新に DHCID RR を使用します。
- **移行から dhcid へ**—サーバーは、DNS サーバーの新しいレコードに対して DHCID RR を使用し、次の DNS 更新が行われたときに既存のエントリを更新して DHCID RR を使用します。
- **regress-to-txt**—サーバーは、DNS サーバーの新しいエントリに TXT RR を使用し、次の DNS 更新が行われるときに既存のエントリをアップグレードして TXT RR を使用します。

（注） *DNS* クライアント *ID*属性は、DHCP サーバー全体の設定の一部としても使用でき、個々の DNS 更新構成の属性が構成されていない場合に考慮されます。

ステップ 8 他の属性を適切に設定します。

- 必要に応じて、合成名を有効にし、合成名ステム値を設定します。

  クライアントがホスト名を提供しない場合は、合成名前-*stem*を使用して、デフォルトのホスト名のステムを使用するように設定できます。DHCPv4 の場合、合成名属性を有効にして、合成名ステムの値に基づいて DHCP サーバーがクライアントの一意の名前を合成するようにトリガーします。結果の名前は、名前の stem にハイフン付き IP アドレスが付加された名前になります。たとえば、example.comドメインのアドレス 192.168.50.1 に合成名のステム**host**を指定し、合成名属性を有効にすると、結果のホスト名はhost-192-168-50-1.example.comされます。合成名のステムのプリセット値は**dhcp**です。

  合成名ステムは次の必要があります。

- 末尾のドットを含まない相対名にします。
- 英数字の値とハイフン–( ) のみを含めます。スペース文字とアンダースコアはハイフンになり、他の文字は削除されます。
- 先頭または末尾のハイフンを含めずに使用します。
- DNS ホスト名は、ラベルあたり 63 文字以下、全体で 255 文字以内にしてください。このアルゴリズムは、構成された転送ゾーン名を使用して、ホスト名に使用できる文字の数を判別し、必要に応じて最後のラベルの末尾を切り捨てます。

DHCPv6 については、DHCPv4 と DHCPv6 での合成名の生成 （4 ページ）を参照してください。

- 転送ゾーンを更新する場合は、転送ゾーン名を転送ゾーンに設定します。ポリシーの転送ゾーン名は、DNS 更新構成の設定よりも優先されることに注意してください。

  DHCPv6 の場合、サーバーは、ポリシー階層で前方ゾーン名の値を検索するときに、クライアントおよびクライアント クラスのポリシーを無視します。前方ゾーン名の検索は、プレフィックス埋め込みポリシーで始まります。

- DHCPv4 の場合は、逆ゾーン名を、PTR および TXT レコードで更新する逆 (.addr.arpa) ゾーンに設定します。設定されていない状態で、DHCP サーバーの逆方向ゾーン属性が有効になっている場合、サーバーは、各リースのアドレス、スコープ サブネット番号、および DNS 更新の構成 (またはスコープ)の *DNS* ホスト バイト属性値に基づいて逆ゾーン名を合成します。

  *dns-host-bytes*値は、逆ゾーン名のホストとゾーンの部分の間の分割を制御します。この値は、ホスト名に使用するリース IP アドレスからのバイト数を設定します。残りのバイトは、in-addr.arpa ゾーン名に使用されます。値 1 は、ドメインのホスト部分に 1 バイトのみを使用し、残りの 3 バイトをドメイン名から使用する (逆)。値 4 は、アドレスのホスト部分に 4 バイトすべてを使用し、ドメインの in-addr.arpa 部分のみを使用します。設定されていない場合、サーバーはスコープサブネットのサイズに基づいて適切な値を合成するか、逆ゾーン名が定義されている場合は、この名前からホストバイトを計算します。

  one-a-rr-per-dns-name は、名前ごとに 1 つまたは複数の A RR を許可するように、DHCPv4 DNS 更新を制御します。8.2 より前のバージョンの Cisco Prime Network レジストラーでは、サーバーが Mac アドレス ベースの識別子を使用しているため、名前ごとに A (名前とアドレス マッピング エントリ) のみがサポートされました。Cisco Prime Network レジストラー 8.2 でDUID サポートと DHCID RR が導入されると、マルチ接続クライアントには複数の A RR が存在します。

  DHCPv6 の場合は、DNS 更新のための逆引きゾーンの決定 （5 ページ） を参照してください。

- サーバー アドイン/サーバー *ipv6addr*を、転送ゾーン (逆ゾーンのみ更新する場合は逆ゾーン) のプライマリ DNS サーバーの IPv4/IPv6 アドレスに設定します。

TSIG キーを使用してすべての DNS 更新を処理する場合は、サーバー キーとバックアップ サーバートランザクションのセキュリティ （8 ページ）キーを設定します (を参照)。

セキュリティで保護されたキー交換の汎用セキュリティ サービス (GSS) メソッドを使用している場合は、*use-gss-tsig*を true に設定します (を参照)。 GSS-TSIG の設定 （43 ページ）

- HA DNS が構成されている場合は、バックアップ サーバーの追加/バックアップ サーバー *ipv6addr*をバックアップ DNS サーバーの IPv4/IPv6 アドレスに設定します。
- 必要に応じて、*update-dns-for-bootp*（事前設定値は有効）を有効または無効にします。

ステップ 9 地域レベルでは、ローカル クラスターに更新の構成をプッシュしたり、[DNS 更新の一覧] ページまたは [DNS 更新の追加] ページでレプリカ データベースからそれらを取得したりすることもできます。

ステップ 10 **Save** をクリックします。

ステップ 11 ポリシーでこの DNS 更新の構成を指定するにはDHCP ポリシーの設定と適用、「」を参照してください。

CLI コマンド

dhcp-dns-update名前**create**を使用する [属性=値..] 次に例を示します。

```
dhcp-dns-update example-update-config create
```

*dynamic-dns*属性を適切な値 (更新なし、すべて更新、更新-fwd のみ、または更新 -逆のみ) に設定します。次に例を示します。

```
nrcmd> dhcp-dns-update example-update-config set dynamic-dns=update-all
```

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。

- **名前 |すべて>プル<確認**する |**置き換える**|**正確な**>クラスター名[-**レポートのみ**|-**レポート**]
- **名前 |すべて>プッシュ<確認**する |**置き換える**|**正確な**>クラスターリスト[-**レポートのみ**|-**レポート**]
- **dhcp-dns-update**名はクラスタリストを再利用する [-**レポートのみ**|-**レポート**]

関連項目

DNS 更新のプロセス （1 ページ）

特殊な DNS 更新に関する考慮事項 （2 ページ）

DHCPv6 の DNS 更新プログラム （2 ページ）

DNS 更新ポリシーの設定

DNS 更新ポリシーは、更新の承認を RR レベルで管理するためのメカニズムを提供します。更新ポリシーを使用すると、RR の名前と種類だけでなく、ACL に基づくルールに基づいて DNS 更新を許可または拒否できます。ACL については、「」DNS キャッシュ サーバーまたはゾーンでの ACL の割り当て （7 ページ）を参照してください。

Cisco プライムネットワーク レジストラーリリースとの互換性

Cisco Prime Network レジストラーリリースでは、管理者が入力した静的 R を使用しましたが、DNS 更新は変更できませんでした。静的な R と動的な R の区別はなくなりました。ここで、R を保護または保護解除としてマークできるようになりました (の「リソース レコード セットの保護」セクションを Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide 参照)。管理者が、R を作成または変更することで、R を保護するかどうかを指定できるようになりました。DNS 更新は、指定されたタイプの RR がセット内にまだ存在しない場合でも、保護された RR セットを変更できません。

（注） 以前のリリースでは、A、TXT、PTR、CNAME、および SRV レコードに対してのみ DNS 更新を許可しました。これは、保護されていない名前セット内の SOA レコードおよび NS レコード以外のすべてのレコードを更新できるように変更されました。以前のリリースとの互換性を維持するには、更新ポリシーを使用して RR 更新を制限します。

ポリシーの作成と編集

更新ポリシーの作成には、最初に名前の作成が含まれます。

ローカル アドバンスドおよびリージョン アドバンスド Web UI

ステップ 1 [**デザイン**] メニューの**Update Policies**[**セキュリティ**] サブメニューの下で [DNS 更新ポリシーの一覧/追加] ページを開きます。このオプションは、サーバーが権限のあるサービスで構成されている場合に使用できます。

ステップ 2 [更新ポリシー] ウィンドウの [**更新ポリシーの追加**] アイコンをクリックして、[DNS 更新ポリシーの追加] ダイアログ ボックスを開きます。

ステップ 3 更新ポリシーの名前を入力します。

ステップ 4 [DNS更新ポリシーの追加（Add DNS Update Policy）] をクリックします。

ステップ 5 更新ポリシーのルールの定義と適用 （19 ページ）に進みます。

CLI コマンド

update-policy *name* **create** を使用します。次に例を示します。

```
nrcmd> update-policy policy1 create
```

更新ポリシーのルールの定義と適用

DNS 更新ポリシーは、ACL に基づいて特定の R の更新を許可または拒否するルールを定義する場合にのみ有効です。ルールが満たされない場合、デフォルトの (最後の暗黙的な) ルールは**"deny any wildcard * *"**、すべての更新を拒否する ( )。

名前付き更新ポリシーのルールの定義

名前付き更新ポリシーのルールを定義するには、一連の Grant ステートメントと Deny ステートメントが必要です。

ローカル アドバンスドおよびリージョン アドバンスド Web UI

ステップ 1 ポリシーの作成と編集 （18 ページ） の説明に従い更新ポリシーを作成するか、編集します。

ステップ 2 [DNS 更新ポリシーの一覧/追加] ページまたは [DNS 更新ポリシーの編集] ページで、次の手順を実行します。

a) [インデックス] フィールドにオプションの値を入力します。

b) **[許可]**を有効にしてルールを許可するか、[**拒否**] を有効にしてルールを拒否します。

c) [ACL リスト]フィールドにアクセス制御リストを入力します。

d) [**キーワード**] ドロップダウン リストからキーワードを選択します。

e) [値] フィールドにキーワードに基づいて値を入力します。これは、RR またはサブドメイン名、またはキーワードが**wildcard**使用されている場合は、ワイルドカードを含めることができます (下の表を参照してください)。

ネットワークが IPv4 から IPv6 アドレスへの移行を行うため、多くのネットワーク デバイスは IPv4 アドレスと IPv6 アドレスの両方を使用します。これらのデバイスは、同じホスト上の複数のインターフェイスを使用している場合や、異なるネットワークを使用している場合や、異なる DHCP バージョンを使用している場合があります。これらのデバイスは、DHCP サーバーに関して一貫して識別する必要があり、それに応じて DHCP サーバーは DNS サーバーを更新します。

Cisco プライム ネットワーク レジストラー 8.1 以前、DHCPv4 は TXT R を使用し、DHCPv6 は DHCID R を使用して DNS を更新します。クライアントが要求した名前の競合を避けるために、デュアルスタック クライアントは単一の前方 FQDN を使用できません。これらの競合は、主にクライアントが要求した名前に適用され、生成される名前には適用されません。これらの競合を避けるために、DHCPv4 と DHCPv6 の名前に異なるゾーンが使用されました。

Cisco プライムネットワーク レジストラー 8.2 以降では、DHCPv4 は TXT RR または DHCID RR を使用し、DHCPv6 は DNS アップデートに DHCID RR を使用します。DHCP サーバー全体の設定属性 dnsクライアント *ID*の既定値は txt であり、属性は個々の DNS 更新構成オブジェクトに対して構成されていません。DNS 更新は、次のいずれかの方法で設定できます。

- DHCPv4 の TXT RR と DHCPv6 の DHCID:この構成を有効にするには、dns クライアント ID を txt に設定します。サーバーは、DHCPv4 DNS 更新で TXT RR を使用し、DHCPv6 DNS 更新には DHCID RR を使用します。 この設定は、DHCPv4 で TXT RR の使用のみをサポートする Cisco Prime Network Registrar 8.1 以前のバージョンで下位互換性を得るために使用されます。 この設定は、Cisco Prime

Network レジストラー 8.1 以前のクラスタがゾーンに対する DNS 更新に関与している場合に使用する必要があります。

- DHCPv4 と DHCPv6 の両方の DHCID RR:この構成を有効にするには、dns クライアント ID を dhcid に設定します。サーバーは、DHCPv4 および DHCPv6 DNS 更新の両方に DHCID RR を使用します。この設定は、デュアル スタック クライアントをサポートするために使用する必要があり、この構成をサポートするゾーンに対して DNS 更新を行うすべての DHCP サーバーが DHCID RR を使用するように構成されている場合にのみ使用できます。
- DHCID RR への移行:この構成を有効にするには、*dns* クライアント *ID*を dhcid への移行に設定します。強制*DNS* 更新属性を true に設定します。サーバーをリロードします。アップグレードする必要があるゾーンについては、*dns* クライアント *ID*属性を dhcid に設定し、サーバーで最長のリース時間が設定された後で、*force-dns-update*属性を以前の値に復元します。

（注） すべての DHCPv4 リソース・レコードが DHCID RR に更新されるまで、*dhcid* への移行属性を設定する必要があります。詳細については、DHCPv4 の DHCID RR への移行 （26 ページ）を参照してください。

- TXT RR への後退:この設定を有効にするには、*dns* クライアント *ID*をリグレッションから txt に設定します。強制*DNS* 更新属性を true に設定します。サーバーをリロードします。アップグレードする必要があるゾーンについては、*dns* クライアント *ID*属性を txt に設定し、サーバーで最長のリース時間が設定された後で、*force-dns-update*属性を以前の値に復元します。

表 *2:* 更新ポリシー ルールのワイルドカード値

ワイルドカード	説明
*****	0 個以上の文字と一致します。たとえば、パターン**example***は、例で始まるすべての文字列に一**example**–致します。
?	1 つの文字のみと一致します。たとえば、パターン**example?.com**は と **example1.comexample2.com**一致します**example.com**が、 は一致しません。
/[/]	(エスケープされた) 角かっこ内の任意の文字に一致します。たとえば、**/[abc/]**などです。各角かっこはスラッシュ ( )/を使用してエスケープする必要があります。文字は範囲内に含めることができます。など、**/[0–9/]**と**/[a–z/]**。パターンにハイフンを含める場合は、ハイフンを最初の文字にします。たとえば、**example/[–a–z/]**などです。

f) 1 つ以上の RR タイプをカンマで区切って[RR タイプ]フィールド*****に入力するか、「すべての RR」に使用します。否定された値は、感嘆符の接頭辞が付いた値で使用できます。たとえば、**!PTR**などです。

g) **Save** をクリックします。

ステップ 3 地域レベルでは、ローカルクラスターに更新ポリシーをプッシュしたり、[DNS 更新ポリシーの一覧/追加]ページでレプリカ データベースからポリシーをプルすることもできます。

ステップ 4 更新ポリシーを編集するには、[リスト/DNS 更新ポリシーの追加]ページで更新ポリシーの名前をクリックし、[DNS 更新ポリシーの編集] ページを開き、**Save**フィールドを変更して をクリックします。

CLI コマンド

更新ポリシーを作成または編集するポリシーの作成と編集 （18 ページ）(「」を**update-policy** 参照) ルールをルールにして名前**rulesadd**ルールを使用します。(ルールのワイルドカード値については、上の表を参照してください。次に例を示します。

```
nrcmd> update-policy policy1 rules add "grant 192.168.50.101 name host1 A,TXT" 0
```

ルールは引用符で囲まれます。例のルール構文を解析するには、次の手順を実行します。

- **grant**- サーバーが実行するアクションまたは. **grantdeny**
- **192.168.50.101**— ACL (この場合は IP アドレス)。ACL は次のいずれかになります。
  - 名前: 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 （7 ページ）説明に従って、名前で作成された ACL。
  - 例のように IP アドレス。
  - マスクを含むネットワークアドレス。たとえば、**192.168.50.0/24**などです。
  - TSIG キー: トランザクション署名キー **key=**(フォームキー)トランザクションのセキュリティ （8 ページ）で 、(説明を参照)。
  - 予約語の 1 つ:

    any—任意の ACL

    none—ACL なし

    localhost：任意のローカル ホスト アドレス

    localnets：任意のローカル ネットワーク アドレス

ACL 値の前に感嘆符 ()**!**を付けて、ACL 値を否定できます。

- **name**- RR で実行するキーワード、またはチェックのタイプは、次のいずれかです。
  - **name**- RR の名前(名前の値を必要とする)
  - **subdomain**RR または RR のいずれか 1 つの RR を持つサブドメインの名前(名前またはサブドメインの値を必要とする)
  - **wildcard**— ワイルドカード値を使用した RR の名前 (上の表を参照)。
- **host1**— キーワードに基づく値(この場合は、host1 という名前のRR)。サブドメイン名を指定することも、キーワードが**wildcard**使用されている場合はワイルドカードを使用することもできます (上の表を参照)。
- **A,TXT**RR タイプ(それぞれカンマで区切られた)。これは、感嘆符 ( )**!**を前に付けて、各レコードの種類の値を否定する「リソース レコード」でCisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide説明されている RR の種類の一覧にすることができます。
- この規則または割り当てられた規則が満たされない場合、デフォルトではすべての RR 更新が拒否されることに注意してください。

引用符の外側のルールの末尾に取り付け、インデックス番号、例では、**.0**です。インデックス番号は0から始まります。更新ポリシーに複数のルールがある場合、インデックスは、より低

い番号付きインデックスがリスト内で優先されるような特定の順序でルールを追加するのに役立ちます。ルールにインデックスが含まれていない場合は、リストの末尾に配置されます。したがって、ルールは、明示的に定義されているかどうかにかかわらず、常にインデックスを持っています。ルールを削除する必要がある場合に備えて、インデックス番号も指定します。

ルールを置き換えるには**update-policy**、*name* **delete**を使用してから、更新ポリシーを再作成します。ルールを編集するには、**update-policy** 名前 **rules remove** インデックスを使用します (インデックスは明示的に定義されたインデックス番号またはシステム定義のインデックス番号です)、ルールを再作成します。前の例の 2 番目のルールを削除するには、次のように入力します。

```
nrcmd> update-policy policy1 rules remove 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。

- **更新ポリシー**<名前|**すべて**>**プル**<**確認**する|**置き換える**|**正確な**>クラスター名[**-レポートのみ**|**-レポート**]
- **更新ポリシー**<名前|**すべて**>**プッシュ**<**確認**する|**置き換える**|**正確な**>クラスターリスト[**-レポートのみ**|**-レポート**]
- **更新ポリシー**名再**請求**クラスタリスト[**-レポートのみ**|**-レポート**]

ゾーンへの更新ポリシーの適用

更新ポリシーを作成した後、権限のあるサービスを使用してDNSサーバーを構成した場合は、更新ポリシーをゾーン (順方向および逆方向) またはゾーン テンプレートに適用できます。

ローカル アドバンスドおよびリージョン アドバンスド Web UI

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

ステップ 2 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。

ヒント また、ゾーン テンプレートの編集ページでゾーン テンプレート、プライマリ リバース ゾーンの編集ページでプライマリ リバース ゾーンに対してもこの機能を実行できます(の「ゾーンの管理」の章Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guideを参照してください)。

ステップ 3 [DNS 更新設定] セクションの [更新ポリシーリストの属性] フィールドに、1 つ以上の既存の名前付き更新ポリシーの名前または名前 (コンマ区切り) を入力します。

（注） サーバーは更新ポリシーリストを処理する前に、更新acl を処理します。

ステップ 4 [保存（Save）] をクリックします。

CLI コマンド

zone名前ポリシーの作成と編集 （18 ページ）を使用し、update-policy-list 属性とコンマ区切りの更新ポリシーの引用符付きリストを使用します。 **set update-policy-list** 次に例を示します。

```
nrcmd> zone example.com set update-policy-list="policy1,policy2"
```

DNS 更新マップの作成

DNS 更新マップを使用すると、更新の構成に基づいて、更新のプロパティが HA DNS サーバーペアまたは DHCP フェールオーバー サーバー ペア間で同期されるように DNS 更新を構成しやすくなるので、冗長なデータエントリを減らすことができます。更新マップは、DNS ペアサービスのすべてのプライマリ ゾーン、または DHCP がサービスをペアにするすべてのスコープに適用されます。更新マップのポリシーを指定する必要があります。この機能を使用するには、管理者に DNS 管理または中央 DNS 管理ロールのサーバー管理サブロール、および dhcp 管理ロール (更新の構成用) が割り当てられている必要があります。

ローカルおよびリージョンの詳細 Web UI

ステップ 1 メニューから**Deploy**[DNS **UpdateMaps**更新]サブメニューの下で選択し、**[DNS**アップデート マップの一覧/追加]ページを開きます。オプションは、サーバーが権限を持つサービスで設定されている場合に選択できます。

ステップ 2 [マップ**AddDNSUpdate**の**Map**更新] ウィンドウのアイコンをクリックして、[DNS 更新マップの追加] ダイアログ ボックスを開きます。

ステップ 3 [名前（Name）] フィールドに更新マップ名を入力します。

ステップ 4 この設定に関連付けられた DNS サーバーまたは HA ペアを選択します。

ステップ 5 この構成に関連付けられている DHCP サーバーまたは DHCP フェールオーバー ペアを選択します。

ステップ 6 *dns-config*フィールドに、前のセクションの DNS 更新の構成を入力します。

ステップ 7 *dhcp* ポリシー セレクタ属性に対して、ポリシー選択の種類を設定します。次の選択項目があります。

- **use-named-policy**: *dhcp* 名前付きポリシー属性(プリセット値)に対して、名前付きポリシー セットを使用します。
- **use-client-class-embedded-policy**: *dhcp-client*クラス属性に対して、クライアント クラス セットの組み込みポリシーを使用します。
- **use-scope-embedded-policy**- スコープの埋め込みポリシーを使用します。

ステップ 8 更新 ACL (を参照アクセス コントロール リストとトランザクション セキュリティの設定 （6 ページ）) または DNS 更新DNS 更新ポリシーの設定 （17 ページ） ポリシー (を参照) を使用する場合は、*dns-update-acl*属性または DNS 更新ポリシー リスト属性を設定します。いずれの値も、コンマで区切られた 1 つ以上のアドレスにすることができます。*dns* 更新*-acl*は、*dns* 更新ポリシーリストよりも優先されます。

両方の値を省略すると、単純な更新の ACL が構築され、指定された DHCP サーバーまたはフェールオーバー ペアのみが更新を実行でき、*dns-config*属性に指定された更新構成で設定されたサーバー キー値も設定されます。

ステップ 9 **Add DNS Update Map** をクリックします。

ステップ 10 地域レベルでは、更新マップをローカル クラスターにプッシュするか、[DNS 更新マップの一覧/追加] ページのレプリカ データベースからプルできます。

CLI コマンド

名前、DHCP**dns-update-map**サーバーと DNS サーバーのクラスタ (または DHCP フェールオーバーまたは HA DNS サーバーペア) と、名前*dhcp-cluster dns-config*を使用して更新マップを作成するときに DNS 更新の構成を**create**指定します。次に例を示します。

```
nrcmd> dns-update-map example-update-map create Example-cluster Boston-cluster
example-update-config
```

dhcpポリシー セレクタ属性値を、名前付きポリシー、use-client クラス埋め込みポリシー、または use スコープ埋め込みポリシーに設定します。名前付きポリシーの使用値を使用する場合は、*dhcp* 名前付きポリシー属性値も設定します。次に例を示します。

```
nrcmd> dns-update-map example-update-map set dhcp-policy-selector=use-named-policy

nrcmd> dns-update-map example-update-map set dhcp-named-policy=example-policy
```

地域クラスターに接続する場合は、**dns-update-map** 名 **プッシュ**を使用できます [**-report-only** |-**レポート**]コマンド。

動的レコードの確認

Cisco プライムネットワーク レジストラー DHCP サーバーは、保留中のすべての DNS アップデート データをディスクに保存します。DHCP サーバーが DNS サーバーと通信できない場合は、定期的に通信の再確立をテストし、保留中のすべての更新を送信します。このテストは通常 40 秒ごとに行われます。

ローカルおよび地域 Web UI

[**デザイン**] メニュー**Forward Zones**のサブメニュー**Auth DNS**の下で選択し、[転送ゾーンのリスト/追加] ページを開きます。左側のペインで必要なゾーンを選択し、[ゾーンの編集] ページの [**リソース レコード**] タブをクリックします。

CLI コマンド

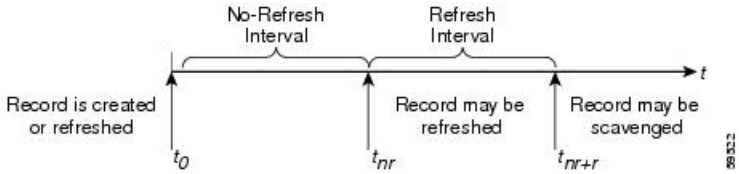
zone *name* **listRR dns** を使用します。

動的レコードのスカベンジング

DHCP リースを取得する Microsoft Windows DNS クライアントは、アドレス (A) レコードを DNS サーバーに直接更新 (更新) できます。これらのクライアントの多くは、永続的に接続されていないモバイル ラップトップであるため、一部の A レコードは時間の経過とともに古くなっている可能性があります。Windows DNS サーバーは、これらのプライマリ ゾーン レコードを定期的に清掃および削除します。Cisco Prime Network レジストラーは、古いレコードを定期的に削除するために使用できる同様の機能を提供します。

清掃は通常、既定では無効になっていますが、Windows クライアントのみを含むゾーンでは有効にする必要があります。ゾーンは、更新なしおよび更新間隔で構成されます。レコードは、最初の作成日とこれら2つの間隔を超えて経過すると期限切れになります。下の図は、清掃のタイム ラインの間隔を示しています。

図 *1:* アドレス レコードの清掃タイム ライン間隔



Cisco プライムネットワーク レジストラープロセスは次のとおりです。

1. クライアントが新しい A レコードで DNS サーバーを更新すると、このレコードはタイムスタンプを取得するか、クライアントがその A レコードを更新すると、タイムスタンプが更新される場合があります (「レコードが作成または更新されました」)。
2. 更新なし間隔 (既定値の 7 日) の間に、クライアントがアドレス変更なしで同じレコードを送信し続ける場合、レコードのタイムスタンプは更新されません。
3. レコードが非更新間隔を過ぎると、更新間隔 (7 日間の既定値) が入力され、その間に DNS 更新はタイムスタンプを更新し、レコードを更新しない間隔に戻します。
4. 更新間隔を過ぎたレコードは、清掃間隔に達したときに清掃に使用できます。

（注） 保護されていない R のみが清掃されます。R が清掃されないようにするには、それらを保護に設定します。ただし、ゾーンの最上位の (@) R は、保護されていない場合でも清掃されません。

次の DNS サーバー属性は、清掃に影響します。

- *scvg-interval*：DNS サーバーがゾーン内の古いレコードを確認する期間。値の範囲は 1 時間から 365 日です。また、サーバーに対して設定することもできます (既定値は 1 週間です) が、ゾーンの設定によって上書きされます。
- *scvg-no-refresh-interval*：動的または前提条件のみの DNS 更新などのアクションがレコードのタイムスタンプを更新しない間隔。この値は 365 日の範囲になります。ゾーンの設定は、サーバーの設定を上書きします (既定値は 1 週間です)。

- *scvg-refresh-interval*：DNS の更新がレコードのタイムスタンプを増分する間隔。更新なしと更新の間隔の両方が期限切れになると、レコードは清掃の候補になります。この値は 365 日の範囲になります。ゾーンの設定は、サーバーの設定を上書きします (既定値は 1 週間です)。
- *scvg-ignore-restart-interval*：サーバーを再起動するたびにサーバーがスカベンジング時間をリセットしないようにします。この間隔内で、Cisco Prime Network レジストラーはサーバー ダウン インスタンスと再起動の間の時間を無視します。

  値の範囲は 2 時間から 1 日です。この設定値より長い値を使用すると、Cisco Prime Network レジストラーは清掃期間を再計算し、サーバーの停止中に発生できないレコード更新を許可します。ゾーンの設定は、サーバーの設定を上書きします (既定値は 2 時間です)。

Cisco Prime Network レジストラー DNS サーバーが Windows クライアント(または自動定期的な DNS 更新を行うことがわかっているもの)から更新を受信するゾーンに対してのみ清掃を有効にします。上記の属性を設定します。Cisco プライムネットワーク レジストラー清掃マネージャは、サーバーの起動時に起動します。変更セットデータベースに対して清掃によって消去されたレコードがレポートされます。Cisco Prime Network レジストラーは、プライマリ ゾーンから清掃されたレコードのゾーン転送を通じてセカンダリ ゾーンに通知します。清掃が無効になっているゾーンを作成し(レコードにタイムスタンプがない)、その後有効にした場合、Cisco Prime Network レジストラーは各レコードのデフォルト タイムスタンプとしてプロキシ タイムスタンプを使用します。

1 つ以上のログ設定の清掃、清掃の詳細、ddns の更新、および ddns 更新の詳細を使用して清掃アクティビティを監視できます。

ローカル詳細 Web UI

[DNS サーバーの管理] ページで、[コマンド] をクリックして [DNS**コマンド**] ダイアログ ボックスを開きます。[すべてのゾーンを清掃する] の横にある [**実行**] アイコンをクリックします。

特定の前方ゾーンまたは逆ゾーンのみをスキャベンジするには、[ゾーンのゾーン コマンド] ページに移動します。 [スキャベンジ ゾーン] の横にある [**実行**] アイコンをクリックします。次に清掃がゾーンにスケジュールされている時刻を確認するには、[清掃開始時刻を取得] の横にある [**実行**] アイコンをクリックします。

CLI コマンド

清掃**dns scavenge**が有効になっているすべてのゾーンに使用します。ゾーンで**getScavengeStartTime**のアクションを使用して、清掃が次回開始される予定の時刻を確認します。

DHCPv4 の DHCID RR への移行

ネットワークが IPv4 から IPv6 アドレスへの移行を行うため、多くのネットワーク デバイスは IPv4 アドレスと IPv6 アドレスの両方を使用します。これらのデバイスは、同じホスト上の複

数のインターフェイスを使用している場合や、異なるネットワークを使用している場合や、異なる DHCP バージョンを使用している場合があります。これらのデバイスは、DHCP サーバーに関して一貫して識別する必要があり、それに応じて DHCP サーバーは DNS サーバーを更新します。

Cisco プライム ネットワーク レジストラー 8.1 以前では、DHCPv4 は TXT R を使用し、DHCPv6 は DHCID R を使用して DNS 更新を行います。クライアントが要求した名前の競合を避けるために、デュアルスタック クライアントは単一の前方 FQDN を使用できません。これらの競合は、主にクライアントが要求した名前に適用され、生成される名前には適用されません。これらの競合を避けるために、DHCPv4 と DHCPv6 の名前に異なるゾーンが使用されました。

Cisco プライムネットワーク レジストラー 8.2 以降では、DHCPv4 は TXT RR または DHCID RR を使用し、DHCPv6 は DNS アップデートに DHCID RR を使用します。DHCP サーバー全体の設定属性 dnsクライアント *ID*の既定値は txt であり、属性は個々の DNS 更新構成オブジェクトに対して構成されていません。DNS 更新は、次のいずれかの方法で設定できます。

- **DHCPv4 の TXT RR と DHCPv6 の DHCID**:この構成セットの *dns* クライアント *ID*を txt に有効にします。サーバーは、DHCPv4 DNS 更新で TXT RR を使用し、DHCPv6 DNS 更新には DHCID RR を使用します。この設定は、旧バージョンとの互換性のために使用されます。これは、Cisco Prime Network Registrar 8.1 以前では、DHCPv4 に TXT RR の使用のみをサポートしているためです。この設定は、Cisco Prime Network レジストラー 8.1 以前のクラスタがゾーンに対する DNS 更新に関与している場合に使用する必要があります。
- **DHCPv4 と DHCPv6 の両方の DHCID RR**—この構成を有効にするには、*dns* クライアント *ID*を dhcid に設定します。サーバーは、DHCPv4 および DHCPv6 DNS 更新の両方に DHCID RR を使用します。この設定は、デュアル スタック クライアントをサポートするために使用する必要があり、この構成をサポートするゾーンに対して DNS 更新を行うすべての DHCP サーバーが DHCID RR を使用するように構成されている場合にのみ使用できます。
- **DHCID RR への移行**— この構成を有効にするには、*dns* クライアント *ID*を dhcid への移行に設定します。強制*DNS* 更新属性を true に設定します。サーバーをリロードします。アップグレードする必要があるゾーンについては、*dns-client-identity* 属性を dhcid に設定し、サーバーに設定されている最長のリース時間が経過した後で *force-dns-update* 属性を以前の値に復元します。

（注） すべての DHCPv4 リソース・レコードが DHCID RR に更新されるまで、*dhcid* への移行属性を設定する必要があります。詳細については、DHCPv4 の DHCID RR への移行 （26 ページ）を参照してください。

- **[TXT RR への後退]**: この構成を有効にするには、*dns* クライアント *ID*をリグレスから txt に設定します。強制*DNS* 更新属性を true に設定します。サーバーをリロードします。アップグレードする必要があるゾーンについては、*dns* クライアント *ID*属性を txt に設定し、サーバーで最長のリース時間が設定された後で、*force-dns-update*属性を以前の値に復元します。

ローカルアドバンスドおよびリージョン Web UI

ステップ 1 [**展開**] メニューの**[DNS 更新**] サブメニューの**[DNS 更新**構成] を選択して、[DNS 更新の一覧/ DNS 更新の構成の追加] ページを開きます。

ステップ 2 更新構成の名前を選択して、**[DNS 更新の構成の編集**] ページを開きます。

ステップ 3 DNS 更新の設定で、DNS 更新設定で、移行から *dhcid* を *DNS* クライアント *ID* として設定します。

ステップ 4 必要に応じて、強制 *DNS* 更新を true に設定します。この設定を使用すると、TXT RR から DHCID RR への移行プロセスが迅速に行われます。

ステップ 5 前方ゾーンまたは反転ゾーンの清掃設定属性を次の値に設定します。

- *scvg* 有効に設定して true にします。

ステップ 6 DNS サーバーの清掃設定属性を次の値に設定します。

- *scvg-interval*を最長リース時間に設定します。
- *scvg-refresh-interval*を最長リース時間に設定します。
- *scvg-no-refresh-interval* を0 に設定します。

ステップ 7 すべての TXT R がゾーンの DR の DHCID R に変換されていることを確認します。すべての DHCPv4 リソース レコードが dhcid RR に更新されるまで、*transition-to-dhcid* 属性を設定する必要があります。一部の TXT RR エントリが DHCID RR に移行しない場合は、Cisco Prime Networkレジストラーの単一レコードの動的 RR 削除機能を使用して、これらの DNS エントリを手動で削除する必要があります。

ステップ 8 [保存（Save）] をクリックします。

Windows クライアントの DNS 更新の構成

Windows オペレーティング システムは DNS と、より少ない程度では DHCP に大きく依存しています。この依存性には、大規模な Windows 展開を行う前に、ネットワーク管理者側で慎重に準備する必要があります。Windows クライアントは、アドレス (A) レコードを使用して転送ゾーンを直接更新することで、自身のエントリを DNS に追加できます。逆ゾーンは、ポインター (PTR) レコードで更新できません。

クライアント DNS の更新

クライアントが DNS を直接更新することを許可することはお勧めしません。

Windows クライアントがアドレス レコードの更新を DNS サーバーに送信するには、次の 2 つの条件が適用される必要があります。

- Windows クライアントの [TCP/IP コントロール パネル**Register this connection's addresses in DNS**] 設定の**DNS**タブでチェック ボックスをオンにする必要があります。

- DHCP ポリシーは直接更新を有効にする必要があります(Cisco Prime Network レジストラーポリシーはデフォルトで有効にします)。

Windows クライアントは、*DHCPREQUEST*パケットでクライアント FQDN DHCP オプション (81) を送信して、DNS サーバーに A レコードを更新する意図を DHCP サーバーに通知します。完全修飾ドメイン名 (FQDN) を示すことによって、このオプションは、ドメイン名前空間内のクライアントの場所を明確に示します。FQDN 自体と共に、クライアントまたはサーバーは、クライアント *FQDN*オプションで次のいずれかのフラグを送信できます。

- **0**クライアントは、その A レコードを DNS サーバーに直接登録し、DHCP サーバーは PTR レコードを登録します (有効になっているポリシーのクライアントレコード更新を許可する属性を使用して行われます)。
- **1**:クライアントは、DHCP サーバーに対して、その A レコードと PTR レコードを DNS サーバーに登録するように要求します。
- **3**DHCP サーバーは、クライアント要求に関係なく、A および PTR レコードを DNS サーバーに登録します(ポリシーの*[*クライアントのレコード更新を許可]属性を使用して行われる場合は、デフォルト値です)。このフラグを設定できるのは DHCP サーバーだけです。

DHCP サーバーは、DNS 更新が有効になっているかどうかに基づいて、DHCPACK 内のクライアントに対して、独自のクライアント *FQDN*応答を返します。ただし、0 フラグが設定されている場合(ポリシーでクライアントのレコード更新を許可する属性が有効になっている)、DNS 更新を有効または無効にすることは、クライアントが DNS サーバーに更新を送信できるため、無関係です。さまざまなプロパティの設定方法に基づいて実行されるアクションについては、次の表を参照してください。

表 *3 : Windows* クライアント *DNS* 更新オプション

DHCP クライアント アクション	DNS 更新	DHCP サーバーの操作
クライアント **Registerthisconnection'saddressesinDNS** *FQDN*をチェックして送信します。DHCP サーバーは、クライアント・ア・レコード更新を許可する	有効または無効	クライアントが A レコードを更新することを許可するクライアント *fqdn* (フラグ 0 を設定) で応答しますが、DHCP サーバーは引き続き PTR レコードを更新します。
を**Register**チェックします。クライアント*FQDN*を送信します。DHCP は、クライアントのレコード更新を許可することを無効にします。	[有効（Enabled）]	クライアントが DNS サーバーを直接更新することを許可しないことをクライアント *fqdn*で応答し (フラグ 3 を設定)、A および PTR レコードを更新します。
	無効	クライアント *fqdn*で応答せず、DNS サーバーも更新されません。

DHCP クライアント アクション	DNS 更新	DHCP サーバーの操作
チェック**Register**を解除..クライアント*FQDN*を送信します	[有効（Enabled）]	A レコードと PTR レコードを更新していることをクライアント *FQDN*で返します。
	無効	クライアント *fqdn*で応答せず、DNS サーバーも更新されません。
クライアント*FQDN*を送信しません。	[有効（Enabled）]	クライアント *fqdn*で応答しませんが、A レコードと PTR レコードを更新します。
	無効	クライアント *fqdn*で応答せず、DNS サーバーも更新されません。

DHCP サーバーは、クライアント要求を無視する *client-fqdn* オプションを設定できます。Cisco Prime Network レジストラーでこの動作を有効にするには、Windows クライアント用のポリシーを作成し、このポリシーのクライアントのレコード更新許可属性を無効にします。

Cisco プライムネットワーク レジストラーでは、次の属性がデフォルトで有効になっています。

- Server *use-client-fqdn*：サーバーは着信パケットで *client-fqdn* 値を使用しますが、*host-name* は確認しません。DHCP サーバーは、ドメイン名の値の最初のドットの後のすべての文字を無視します。クライアント名が予期しない文字を送信している可能性があるために、サーバーがクライアント名をクライアント *fqdn*から判別しないようにする場合にのみ、*use-client-fqdn*を無効にします。
- Server *use-client-fqdn-first*：サーバーは *host-name* オプション (12) を確認する前に、クライアントからの着信パケットで *client-fqdn* を確認します。クライアント *fqdn*にホスト名が含まれている場合、サーバーはそれを使用します。サーバーがオプションを見つけられない場合は、*host-name*値を使用します。*use-client-fqdn-first*が無効になっている場合、サーバーはクライアント *fqdn*よりもホスト名の値を優先します。
- Server *use-client-fqdn-if-asked*：クライアントが要求した場合、サーバーは発信パケットの *client-fqdn* 値を返します。たとえば、クライアントは DNS アクティビティの状態を知りたい場合、DHCP サーバーがクライアント *fqdn*値を提示するように要求します。
- Policy *allow-client-a-record-update*：クライアントが *client-fqdn* フラグを 0 に設定（直接の更新を要求）している限り、クライアントは DNS サーバーで直接 A レコードを更新できます。それ以外の場合、サーバーは、他の構成プロパティに基づいて A レコードを更新します。

クライアント要求に返されるホスト名は、これらの設定によって異なります(下の表を参照)。

表 *4:* クライアント要求パラメータに基づいて返されるホスト名

クライアントによるリクエスト	サーバー/ポリシー設定を使用する	結果のホスト名
host-name（オプション 12）を含む	使用ホスト名=真の使用クライアント*-fqdn* =false (または使用クライアント*-fqdn-first* =false)トリム ホスト名=true	最初のドットでトリムされたホスト名。例:ホスト名host1.bob が返されるホスト 1。
	(同じ以外)トリム ホスト名=false	*host-name*。例:ホスト名host1.bob が返されるホスト 1.bob。
クライアント*FQDN*を含む (オプション 81)	使用クライアント*-fqdn*=真の使用ホスト名=false (または使用クライアント*-fqdn-first* =true)	クライアント*FQDN*は最初のドットでトリムされます。例:クライアント *fqdn* host1.bob が返される例は、host1 です。
ホスト名(オプション 12) およびクライアント *FQDN* (オプション 81) を省略します。	または:使用ホスト名=偽の使用クライアント*-fqdn* =偽	クライアント/ポリシー階層別に設定します。
	(上記の場合と同じですが、次の場合は次の点を除き、ホスト名はクライアント/ポリシー階層で定義されず、合成名=true	合成規則に従って合成され、指定された合成名ステムの後にホストのハイフンで区切られた IP アドレスを追加します。
	(上記の場合と同じですが、次の場合は次の点を除き、合成名=偽	未定義。

Windows クライアント用デュアル ゾーンの更新

Windows DHCP クライアントは、2 つの DNS ゾーンに A レコードを持つ DHCP 展開の一部である場合があります。この場合、DHCP サーバーはクライアントがデュアル ゾーン更新を要求できるように、クライアント *fqdn*を返します。デュアル ゾーン更新を有効にするには、ポリシー属性の許可デュアル ゾーン *DNS* 更新を有効にします。

DHCP クライアントは、クライアント *fqdn*に 0 フラグを送信し、クライアントがメイン ゾーンの A レコードを使用して DNS サーバーを更新できるように、0 フラグを返します。ただし、DHCP サーバーは、クライアントの代わりにクライアントのセカンダリ ゾーンに基づいて A レコードの更新も直接送信します。クライアントのレコード更新と、デュアル ゾーンDNS の許可の両方が有効になっている場合、デュアルゾーン更新が優先され、サーバーがセカンダリ ゾーン A レコードを更新できるようになります。

Windows クライアントの DNS 更新設定

Windows クライアントは、クライアント *fqdn*オプションの送信を有効にする詳細プロパティを設定できます。

ステップ 1 Windows クライアントで、コントロールパネルに移動し、[TCP/IP 設定] ダイアログ ボックスを開きます。

ステップ 2 [**Advanced**] タブをクリックします。

ステップ 3 [**DNS**] タブをクリックします。

ステップ 4 クライアントがクライアントの要求でクライアント *fqdn*オプションを送信するようにするには、**Register this connection's addresses in DNS**チェック ボックスをオンのままにします。これは、クライアントが A レコードの更新を実行することを示します。

DHCP サーバーの Windows クライアント設定

Windows クライアントを含むスコープに関連するポリシーを適用し、そのスコープの DNS 更新を有効にできます。

ステップ 1 Windows クライアントを含むスコープのポリシーを作成します。次に例を示します。

a) ポリシー win2k を作成します。ポリシーを作成する際には、前方または逆方向のゾーン名、メインおよびバックアップ サーバーの IP アドレスを指定する必要があります。

b) サブネット 192.168.1.0/24 と policywin2k をポリシーとして win2k スコープを作成します。アドレス範囲を 192.168.1.10 から 192.168.1.100 まで追加します。

ステップ 2 のDNS 更新設定の作成 （14 ページ）説明に従って、ゾーン名、サーバー アドレス (A レコードの場合)、逆引きゾーン名、および逆サーバー アドレス (PTR レコードの場合) を設定します。

ステップ 3 クライアントが DNS サーバーで A レコードを更新する場合は、ポリシー属性の*[*クライアント-レコードの更新を許可] を有効にします (これは事前設定値です)。これにはいくつかの注意点があります。

- クライアントのレコード更新を許可するが有効になっている場合、クライアントが更新ビットを有効にしてクライアント *FQDN*を送信すると、クライアントに返されるホスト名とクライアント *FQDN*はクライアントのクライアント *fqdn*に一致します。(ただし、サーバーでクライアント名の上書き *fqdn*も有効になっている場合、クライアントに返されるホスト名と FQDN は、構成されたホスト名とポリシー ドメイン名によって生成されます。
- その代わりに、クライアントが更新ビットを有効にしてクライアント *fqdn*を送信しない場合、サーバーは A レコードの更新を行い、クライアントに返されたホスト名とクライアント *FQDN* (要求された場合) は DNS 更新に使用された名前と一致します。
- クライアントのレコード更新を許可するが無効になっている場合、サーバーは A レコードの更新を行い、クライアントに返されるホスト名とクライアント *FQDN* (更新ビットが無効な) の値は、DNS 更新に使用された名前と一致します。
- 二重ゾーン *DNS* 更新が有効になっている場合、DHCP サーバーは常に A レコードの更新を行います。（Windows クライアント用デュアル ゾーンの更新 （31 ページ） を参照）。
- DHCP サーバーまたは DNS 更新の構成で *use-dns-update-prereqs* が有効（事前設定値）の場合、クライアントに返されるホスト名と *client-fqdn* は、DNS の更新と一致する保証はありません。ただし、リース データは新しい名前で更新されます。

RFC 2136 に従って、更新の前提条件により、プライマリ DNS サーバーが RR セットまたは名前のレコードが存在する必要があるかどうかに基づいて実行するアクションを決定します。まれな状況でのみ使用 *dns* 更新前の前提条件を無効にします。

ステップ 4 DHCP サーバーをリロードします。

SRV レコードと DNS 更新

Windows は、ネットワークへの広告サービスの DNS プロトコルに大きく依存しています。次の表は、Windows がサービスロケーション (SRV) DNS R および DNS 更新を処理する方法を示しています。

Cisco Prime Networkレジストラー DNS サーバーを設定して、Windows ドメイン コントローラがサービスを DNS に動的に登録し、それによってネットワークにアドバタイズできるようにすることができます。このプロセスは RFC 準拠の DNS アップデートによって行われるため、Cisco Prime Network レジストラーでは通常の方法で何もする必要はありません。

表 *5 : Windows SRV* レコードおよび *DNS* 更新

機能	説明

SRV レコード	Windows ドメイン コントローラは SRV RR を使用してネットワークにサービスをアドバタイズします。この RR は、RFC 2782 の「サービスの場所を指定するための DNS RR（DNS SRV）」で定義されています。RFC は SRV レコードの形式を定義します (DNS タイプ コード 33) は、次のように定義します。
	`_ service ._ protocol . name ttl class SRV priority weight port target`
	クライアントがホストにサービスを解決できるように、SRV レコードのターゲットに関連付けられた A レコードが常に必要です。SRV レコードの Windows 実装では、レコードは次のようになります。
	`myserver.example.com A 10.100.200.11`
	`_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`
	アンダースコアは常にサービス名とプロトコル名の前に置きます。この例では、キー配布センター_kdcです。優先順位と重みにより、同じサービスを提供するターゲット・サーバー(優先順位が等しいサーバーを区別する重み)を選択できます。優先順位と重みがゼロの場合、リストされている順序によって優先順位が決まります。Windows ドメイン コントローラは、これらの SRV レコードを自動的に DNS に配置します。

SRV レコードの使用方法	Windows クライアントは、起動すると、ネットワーク ログイン プロセスを開始して、その Windows ドメイン コントローラに対して認証を試みます。クライアントは、まずドメイン コントローラの場所を検出し、動的に生成された SRV レコードを使用して検出する必要があります。net-login プロセスを起動する前に、クライアントはサービス名を使用して DNS を照会します。たとえば、_ldap._tcp.dc_msdcs.example.com です。たとえば、DNS サーバーの SRV レコード ターゲットは my-domain-controller.example.com。Windows クライアントは、ホスト名を使用して DNS にクエリを実行 my-domain-controller.example.com。DNS はホスト アドレスを返し、クライアントはこのアドレスを使用してドメイン コントローラを検索します。ネットログインプロセスは、これらの SRV レコードなしで失敗します。
DNS 更新	Windows サーバーをドメイン コントローラとして構成すると、Active Directory 管理コンソールを使用して、管理するドメインの名前を静的に構成することになります。この Windows ドメインには、対応する DNS ゾーンが関連付けられている必要があります。また、ドメイン コントローラのコントロール パネルの [TCP/IP プロパティ] で、一連の DNS リゾルバを構成する必要があります。Windows ドメイン コントローラは、起動時に次の手順を実行して、自身を DNS に登録し、そのサービスをネットワークにアドバタイズします。 **1.** 主に Windows ドメインを密封している DNS ドメインの権限 (SOA) レコードの開始を求めるクエリを実行します。 **2.** 主に Windows ドメイン名を密封している DNS ゾーン (SOA レコードから) のプライマリ DNS サーバーを識別します。 **3.** RFC 2136 DNS 更新プロトコルを使用して、このゾーンに一連の SRV レコードを作成します。

サーバーブートプロセスログファイルの例	通常の動作条件では、Cisco Prime Network レジストラープライマリ DNS サーバーは、Windows ドメイン コントローラが起動して SRV レコードを作成するときに、これらのログ エントリを書き込みます。
	`data time name/dns/1 Activity Protocol 0 Added type 33 record to name "_ldap._tcp.w2k.example.com", zone "w2k.example.com"`
	`data time name/dns/1 Activity Protocol 0 Update of zone "w2k.example.com" from address [10.100.200.2] succeeded.`
	このログには、1 つの SRV レコードに対して 1 つの DNS 更新のみが表示されます。Windows ドメイン コントローラは、通常、起動時にこれらの SRV レコードのうち 17 個を登録します。

Windows 環境に関連する問題

次の表では、Windows および Cisco Prime Network Registrar 間の接続相互運用性に関する問題について説明します。この表の情報は、現場で発生する可能性のある問題を事前に通知することを目的としています。Windows の相互運用性に関してよく寄せられる質問Windows の統合に関するよく寄せられる質問 （40 ページ）については、を参照してください。

表 *6 : Windows* および *Cisco* プライムネットワーク レジストラー相互運用性に関する問題

問題	説明

非表示動的に作成された R	Cisco プライムネットワーク レジストラーは、正しく設定されていれば、DHCP サーバーと Windows サーバーの両方から DNS アップデートを受け入れます。CLI を使用して、レコードの表示と削除のために DNS ゾーンの動的部分にアクセスできます。指定したゾーンのすべての DNS R を表示するには、次のコマンドを入力します。
	`nrcmd> zone myzone listRR dynamic myfile`
	これにより、出力が myfile ファイルにリダイレクトされます (次の例: 非表示の動的に作成された *RRs* セクションを示す出力を参照)。動的に生成されたレコードは、次のコマンドを入力して削除できます。
	`nrcmd> zone myzone removeDynRR myname [ type ]`
	nslookupを使用して、nslookup が存在するかどうかを確認したり、バージョン 5 を使用することもできます。動的 SRV レコードを表示する場合は、*x* (Windows に同梱されています)。このバージョンでは、**セット type=SRV**を使用して SRV レコードの表示を有効にします。

ドメイン コントローラ登録	Windows ドメイン コントローラは、DNS 更新を使用して自身を DNS に登録する必要があります。DNS RFC では、ゾーン データの編集を受け付けることができるのは、特定のゾーンのプライマリ DNS サーバーだけです。したがって、Windows ドメイン コントローラは、Windows ドメイン名を含むゾーンのプライマリ DNS サーバーを検出する必要があります。 ドメイン コントローラは、リゾルバー リスト (TCP/IP プロパティ コントロール パネルで構成) の最初の DNS サーバーに対してクエリを実行して、この問題を検出します。最初のクエリは、ドメイン コントローラの Windows ドメインを含むゾーンの SOA レコードを対象にしています。SOA レコードには、ゾーンのプライマリ サーバーの名前が含まれます。ドメイン名のゾーンが存在しない場合、ドメイン コントローラはドメイン名の左端のラベルを削除し続け、そのドメインに含まれるプライマリ サーバーを持つ SOA レコードが見つかるまでクエリを送信します。ドメイン コントローラは、そのドメインのプライマリ DNS サーバーの名前を持つと、DNS 更新を送信して必要な SRV レコードを作成します。 ゾーンのプライマリ DNS サーバーの名前が SOA レコードに含まれているかどうかを確認します。
レコード DNS 更新の失敗	Windows ドメイン コントローラがネットワークに対して自身をアドバタイズしようとすると、ドメインのレコードの DNS サーバーに複数の DNS 更新要求が送信されます。これらの更新要求のほとんどは SRV レコードに対する要求です。ただし、ドメイン コントローラは、Windows ドメインと同じ名前の単一の A レコードの更新も要求します。 Cisco Prime Network レジストラー DNS サーバーもこの Windows ドメインと同一のゾーンに対して権限を持っている場合、DNS A レコードの更新が静的 SOA および NS レコードと競合するため、A レコードの登録は拒否されます。これは、動的ホストが自分自身を登録し、サイトへの Web トラフィックを偽装するなど、セキュリティ侵害の可能性を防ぐためです。 たとえば、ドメイン コントローラは、Windows ゾーン w2k.example.comを制御できます。Cisco Prime Network レジストラー DNS サーバーに同じ名前のゾーンが存在する場合、これらの R はそのゾーンの一部である可能性があります。(例は以下の通りです。 `w2k.example.com. 43200 SOA nameserver.example.com. hostadmin.example.com. ( 98011312 ;serial 3600 ;refresh 3600 ;retry 3600000 ;expire 43200 ) ;minim w2k.example.com.86400 NS nameserver.example.com`

	ドメイン コントローラは、レコードを追加しようとします。例えば：
	`w2k.example.com. 86400 A 192.168.2.1`
	Cisco Prime Network レジストラーでは、DNS の更新がゾーン内の静的に設定された名前と競合することはありません。上記の例では、名前に関連付けられた A レコードを追加しようとすると、SOA レコードと NS レコードw2k.example.com競合します。
	ドメイン コントローラが起動すると、次のような DNS ログ ファイル エントリが表示されます。
	`0 8/10/2000 16:35:33 name/dns/1 Info Protocol 0 Error - REFUSED -`
	`Update of static name "w2k.example.com", from address [10.100.200.2]`
	Cisco プライムネットワーク レジストラーが静的 DNS データの DNS アップデートに応答する方法は、次のようになります。さらに、この DNS 更新の失敗を無視できます。Windows クライアントはこの A レコードを使用しません。ドメイン コントローラの割り当ては、SRV レコードを通じて行われます。マイクロソフトは、SRV レコードをサポートしない従来の NT クライアントに対応するために A レコードを追加しました。
	コントローラ A レコードの登録に失敗すると、ドメイン コントローラのブートアップ プロセスが遅くなり、ワーカー クライアントの全体的なログインに影響することに注意してください。前述のように、Windows ドメインを権限のあるゾーンのサブドメインとして定義するか、DNS サーバーのゾーントップ *dynupdate* 属性をシミュレートする方法を使用します。これが不可能な場合は、シスコ テクニカル アシスタンス センターに問い合わせてください。

RC1 DHCP クライアントを使用します。	マイクロソフトは、壊れた DHCP クライアントを使用して Windows ビルド 2072 (RC1) をリリースしました。このクライアントは、Cisco Prime ネットワークレジストラーが解析できない、不正な形式のパケットを送信します。Cisco Prime Network レジストラーはパケットを廃棄し、クライアントにサービスを提供できません。
	`08/10/2000 14:56:23 name/dhcp/1 Activity Protocol 0 10.0.0.15 Lease offered to Host:'My-Computer' CID: 01:00:a0:24:1a:b0:d8 packet'R15' until True, 10 Aug 2000 14:58:23 -0400. 301 ms.`
	`08/10/2000 14:56:23 name/dhcp/1 Warning Protocol 0 Unable to find necessary Client information in packet from MAC address:'1,6,00:d0:ba:d3:bd:3b'. Packet dropped!`
	Cisco Prime Network レジストラーには、この不適切に構築された FQDN オプションなどのエラーに対処するために特別に設計されたエラーチェックが含まれています。ただし、この問題が発生した場合は、DHCP クライアントの RC1 クライアントにマイクロソフトの修正プログラムをインストールします。この修正プログラムは、マイクロソフトから入手する必要があります。

Windows プラグ アンド プレイ ネットワーク インターフェイス カード (NIC) の構成	DHCP を使用するように構成されている場合、Windows システムは起動時に DHCP リースを取得しようとします。DHCP サーバーが利用できない場合、Windows は、プラグ アンド プレイ IP アドレスを使用してコンピュータ インターフェイスを自動的に構成することがあります。このアドレスは、ネットワーク管理者または DHCP サーバーが構成または選択したアドレスではありません。 これらのプラグアンドプレイアドレスは、169.254.0.0/16の範囲内にあります。ネットワーク上にこのアドレス範囲のデバイスが表示される場合は、DHCP サーバーからリースを取得できないため、Windows がインターフェイスを自動構成したことを意味します。 これにより、ネットワークやトラブルシューティングに関する重大な問題が発生する可能性があります。Windows システムは、DHCP クライアントがリースを取得できなかったことをユーザーに通知しなくなりました。すべてが正常に機能しているように見えますが、クライアントはローカル サブネットからパケットをルーティングできません。さらに、DHCP クライアントが 169.254.0.0/16 ネットワークからのアドレスを使用してネットワーク上で動作しようとしているのを見ることができます。これにより、Cisco Primeネットワーク レジストラー DHCP サーバーが壊れ、間違ったアドレスを配っていると考える場合があります。
	この問題が発生した場合、次のステップを実行します。 **1.** DHCP クライアントにアクティブなネットワーク ポートと正しく構成された NIC があることを確認します。 **2.** クライアントと DHCP サーバー間のネットワークが正しく構成されていることを確認します。すべてのルータ インターフェイスが正しい IPHelper アドレスで設定されていることを確認します。 **3.** DHCP クライアントを再起動します。 **4.** 必要に応じて、DHCP ログ ファイルを確認します。DHCP クライアントがパケットをサーバーに正常にルーティングできる場合、Cisco Prime Network レジストラーがパケットに応答しない場合でも、DHCPDISCOVER がログに記録されます。 ネットワークが正しく設定され、DHCP クライアントが破損していない場合、Cisco Prime Network レジストラーはパケットを受信してログに記録する必要があります。パケット受信のログ エントリがない場合は、ネットワークのどこか別の場所で問題が発生します。

Windows クライアント アドレス レコードの清掃	Windows クライアントは、動的レコード登録が無期限に残る可能性があり、自分自身の後にクリーンアップされません。これにより、古いアドレス レコードが DNS サーバーに残ります。これらの古いレコードが定期的に削除されるようにするには、ゾーンの清掃を有効にする必要があります (を参照 動的レコードのスカベンジング（25 ページ）)。

例: 非表示の動的に作成された R を示す出力

```
 Dynamic Resource Records _ldap._tcp.test-lab._sites 600 IN SRV 0
100 389 CNR-MKT-1.w2k.example.com. _ldap._tcp.test-lab._sites.gc._msdcs 600 IN
SRV 0 100 3268 CNR-MKT-1.w2k.example.com.
_kerberos._tcp.test-lab._sites.dc._msdcs 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _ldap._tcp.test-lab._sites.dc._msdcs 600 IN SRV 0
100 389 CNR-MKT-1.w2k.example.com. _ldap._tcp 600 IN SRV 0 100 389
CNR-MKT-1.w2k.example.com. _kerberos._tcp.test-lab._sites 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _ldap._tcp.pdc._msdcs 600 IN SRV 0 100 389
CNR-MKT-1.w2k.example.com. _ldap._tcp.gc._msdcs 600 IN SRV 0 100 3268
CNR-MKT-1.w2k.example.com.
_ldap._tcp.1ca176bc-86bf-46f1-8a0f-235ab891bcd2.domains._msdcs 600 IN SRV 0 100
389 CNR-MKT-1.w2k.example.com. e5b0e667-27c8-44f7-bd76-6b8385c74bd7._msdcs 600
IN CNAME CNR-MKT-1.w2k.example.com. _kerberos._tcp.dc._msdcs 600 IN SRV 0 100
88 CNR-MKT-1.w2k.example.com. _ldap._tcp.dc._msdcs 600 IN SRV 0 100 389
CNR-MKT-1.w2k.example.com. _kerberos._tcp 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _gc._tcp 600 IN SRV 0 100 3268
CNR-MKT-1.w2k.example.com. _kerberos._udp 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _kpasswd._tcp 600 IN SRV 0 100 464
CNR-MKT-1.w2k.example.com. _kpasswd._udp 600 IN SRV 0 100 464
CNR-MKT-1.w2k.example.com. gc._msdcs 600 IN A 10.100.200.2
_gc._tcp.test-lab._sites 600 IN SRV 0 100 3268 CNR-MKT-1.w2k.example.com.
```

Windows の統合に関するよく寄せられる質問

Cisco Primeネットワーク レジストラー DNS サービスと Windows の統合について、次の質問がよく寄せられます。

Windows クライアントと DHCP サーバーの両方が同じゾーンを更新できる場合の動作これにより、古い DNS レコードがゾーンに残される可能性が生まれますか。もしそうなら、それについて何ができますか?

Windows クライアントがゾーンを更新することを許可しないことをお勧めします。代わりに、DHCP サーバーはすべてのクライアントの動的 RR レコードを管理する必要があります。DNS 更新を実行するように構成されている場合、DHCP サーバーはリースを提供したクライアントに関連付けられたすべての DR を正確に管理します。これに対し、Windows クライアント マシンは、毎日の DNS 更新をサーバーに盲目的に送信し、ネットワークから削除された場合は、古い DNS エントリを残します。

DNS 更新クライアントによって更新されるゾーンでは、一時的な Windows クライアントが残す古い R の長寿を短縮するために DNS の清掃機能を有効にする必要があります。DHCP サーバーと Windows クライアントの両方が同じゾーンを更新している場合、Cisco Prime Network レジストラーでは次の 3 つのことが必要です。

1. ゾーンの清掃を有効にします。

2. 各クライアントがリースを更新するたびに、DHCP サーバーが DNS 更新エントリを更新するように構成します。デフォルトでは、Cisco Primeネットワーク レジストラーは、作成から最終削除までの間に DNS レコードを再度更新しません。Cisco プライムネットワーク レジストラーがリースの開始からリースの期限が切れるまで、ライフを作成する DNS 更新レコード。この動作は、DHCP サーバー (または DNS 更新構成) 属性 (強制 *DNS* 更新) を使用して変更できます。次に例を示します。

```
nrcmd> dhcp enable force-dns-updates

100 Ok
force-dns-updates=true
```

3. 特定のゾーンで清掃が有効になっている場合、DHCP サーバーが代わりにそのゾーンを更新するクライアントに関連付けられているリース時間は、更新なし間隔および更新間隔の清掃設定の合計より小さくなければなりません。これらの設定は両方とも 7 日間に設定されています。これらのデフォルト値を変更しない場合は、リース期間を 14 日以下に設定できます。

重複する DNS ドメインと Windows ドメインを持たないと判断した場合に Windows ドメインを既存の DNS ドメインの命名構造と統合するのに必要な手順たとえば、example.com という既存の DNS ドメインがあり、w2k.example.comという Windows ドメインが作成されている場合、Windows ドメインを DNS ドメインに統合するには何をする必要がありますか。

この例では、Windows ドメイン フォレストのツリーにルートの w2k.example.com があります。example.comという名前の DNS ドメインが存在します。この DNS ドメインは、example.comという名前のゾーンで表されます。このゾーンに表される追加の DNS サブドメインが存在する可能性がありますが、このゾーンからそのゾーンに委任されるサブドメインはありません。すべてのサブドメインは常にexample.comに存在します。ゾーン。

この場合、ドメイン コントローラからの DNS 更新はどのように処理されますか。

Windows ドメイン コントローラからの SRV レコードの更新を処理するには、DNS の更新をexample.comに制限します。ゾーンは IP アドレスによってのみドメイン コントローラに接続されます。(後で、DHCP サーバーの IP アドレスも一覧に追加します)。ゾーンの清掃を有効にします。コントローラは、example.com ゾーン内のw2k.example.com サブドメインの SRV レコードと A レコードを更新します。w2k.example.comの A レコードは、EXAMPLE.COM ゾーン内の SOA、NS、またはその他の静的レコードと競合しないため、各ドメイン コントローラからの A レコードの更新を処理するために特別な構成は必要ありません。

example.comゾーンには、次のレコードが含まれる場合があります。

```
example.com. 43200 SOA ns.example.com. hostadmin.example.com. (
98011312 ;serial
3600 ;refresh
3600 ;retry
3600000 ;expire
43200 ) ;minimum
example.com.86400 NS ns.example.com
ns.example.com. 86400 A 10.0.0.10
_ldap._tcp.w2k.example.com. IN SRV 0 0 389 dc1.w2k.example.com
w2k.example.com 86400 A 10.0.0.25
...
```

この場合、個々の Windows クライアント マシンからのゾーン更新はどのように処理されますか。

このシナリオでは、クライアントは、example.comを更新しようとする可能性があります。w2k.example.com ドメインの更新を含むゾーン。これを回避する方法は、信頼できるソースからのゾーンを更新プログラムに閉じる方法です。Cisco Prime Network レジストラーでは、DHCP サーバーとexample.com ゾーンのプライマリ DNS サーバーの間でトランザクション シグニチャ(TSIG)を使用できます。

DHCP サーバーを構成して、example.com ゾーンに対して DNS 更新を行い、各クライアントに対して適切な逆ゾーンを使用し、オプション 81 を使用してクライアントが DNS 更新を実行できないようにします。

この場合、セキュリティは対処されていますか?

信頼された IP アドレスからの更新のみを受け入れるように、前方ゾーンと逆方向のゾーンを構成すると、ネットワーク上の他のデバイスからの更新プログラムに対してゾーンを閉じます。IP によるセキュリティは、なりすまし IP アドレス ソースからの悪意のある攻撃を防ぐことができないので、最も理想的なソリューションではありません。DHCP サーバーと DNS サーバーの間で TSIG を構成することで、DHCP サーバーからの更新をセキュリティで保護できます。

この場合、清掃は必要ですか?

いいえ。更新は、ドメイン コントローラと DHCP サーバーからのみ受け付けられます。DHCP サーバーは、追加するレコードのライフ サイクルを正確に維持し、清掃を必要としません。Cisco Prime Network レジストラーの単一レコード動的 RR 削除機能を使用して、ドメイン コントローラのダイナミック エントリを手動で管理できます。

名前空間を DNS ドメインと共有する Windows ドメインを統合するのに必要な手順たとえば、example.comという既存の DNS ゾーンがあり、example.comという Windows Active Directory ドメインを展開する必要がある場合、どうすればいいでしょうか。

この例では、Windows ドメイン フォレストのツリーにルート example.comが含まれます。example.comという名前のゾーンで表されるexample.comという名前の既存のドメインもあります。

この場合、個々の *Windows* クライアント マシンからの *DNS* 更新はどのように処理されますか。

SRV レコードの更新を処理するには、次のサブゾーンを作成します。

```
_tcp.example.com.
_sites.example.com.
_msdcs.example.com.
_msdcs.example.com.
_udp.example.com.
```

DNS の更新をこれらのゾーンに対して、IP アドレスのみでドメイン コントローラに制限します。これらのゾーンで清掃を有効にします。

各ドメイン コントローラからの A レコードの更新を処理するには、DNS サーバー属性であるゾーン トップ *dynupdate*をシミュレートする属性を有効にします。

```
nrcmd> dns enable simulate-zone-top-dynupdate
```

必須ではありませんが、必要に応じて、ドメインコントローラのAレコードを手動でexample.comゾーンに追加します。

この場合、個々の Windows クライアント マシンからのゾーン更新はどのように処理されますか。

このシナリオでは、クライアントがexample.comゾーンを更新しようとする可能性があります。これを回避する方法は、信頼できるソースからのゾーンを更新プログラムに閉じる方法です。Cisco Prime Network レジストラーでは、DHCP サーバーとexample.com ゾーンのプライマリ DNS サーバーの間でトランザクション シグニチャ(TSIG)を使用できます。

DHCP サーバーを構成して、example.com ゾーンに対して DNS 更新を行い、各クライアントに対して適切な逆ゾーンを使用し、オプション 81 を使用してクライアントが DNS 更新を実行できないようにします。

この場合、セキュリティは対処されていますか?

信頼された IP アドレスからの更新のみを受け入れるように、前方ゾーンと逆方向のゾーンを構成すると、ネットワーク上の他のデバイスからの更新プログラムに対してゾーンを閉じます。IPによるセキュリティは、なりすましソースからの悪意のある攻撃を防ぐことができないので、最も理想的なソリューションではありません。DHCP サーバーと DNS サーバーの間で TSIG が構成されている場合、DHCP サーバーからの更新の方が安全です。

この場合、清掃は対処されていますか?

はい。サブゾーン _tcp.example.com、_sites.example.com、_msdcs.example.com、_msdcs_msdcs.example.com、および _udp.example.com ゾーンは、ドメイン コントローラーからのみ更新を受け入れ、これらのゾーンに対して清掃が有効になっています。example.com ゾーンは、DHCP サーバーからのみ DNS 更新を受け付けます。

GSS-TSIG の設定

AD と統合するための Cisco プライムネットワーク レジストラー DNS 設定

AD を Cisco プライムネットワーク レジストラー DNS 設定と統合するには、次の手順を実行します。

ステップ 1 Cisco プライムネットワーク レジストラー DNS をワークグループ マシンにインストールします。

ステップ 2 ゾーンを作成します (AD のドメインと同じです)。

DCpromo.exe を使用して WINDOWS サーバーに AD をインストールし、Cisco Prime Network Registrar DNS と統合します。

ステップ 3 Cisco プライムネットワーク レジストラー DNS に SRV レコードが追加されていることを確認します。

```
DCHOSTNAME. DOMAIN.COM A AD-IP-ADDRESS
_ldap._tcp.DOMAIN.COM. SRV 0 0 389 DCHOSTNAME.DOMAIN.COM.
_kerberos._tcp.DOMAIN.COM. SRV 0 0 88 DCHOSTNAME.DOMAIN.COM.
_ldap._tcp.dc._msdcs.DOMAIN.COM. SRV 0 0 389 DCHOSTNAME.DOMAIN.COM.
_kerberos._tcp.dc._msdcs.DOMAIN.COM. SRV 0 0 88 DCHOSTNAME.DOMAIN.COM.
```

（注） **DCHOSTNAME**は AD ホスト名を参照し、**DOMAIN.COM**は AD に存在するドメインです。

（注） サーバー間の通信に Kerberos サーバーを使用する場合は常に、/etc/krb5.conf にある最新の暗号化アルゴリズムを使用することを推奨しています。

Cisco Prime Network Registrar および AD を、Windows 環境の同じドメインの下に置きます。

ステップ 1 ドメインを変更し、**コンピューター > プロパティ > コンピューター名 >**ドメインのメンバーを変更します (AD のドメインと同じ)。

ステップ 2 コントロール パネル > ネットワークとインターネット > ネットワークと共有センター > ローカル エリア接続 > プロパティ > TCP/IPV4 > 優先 DNS (Cisco Cisco プライムネットワーク レジストラー DNS 実行 IP)。

ステップ 3 コンピューターを再起動し、AD に存在するユーザーでログインします。

ステップ 4 AD にログインし、次の操作を行います。

- DNS アクティブ ホスト名が追加されていることを確認する、**AD サーバー マネージャー > コンピューター**

```
setspn -s DNS/ <hostname of the DNS server> <Computer Name>
```

DNS サーバーを AD-KDC に統合する

プライマリ DNS サーバーは AD-KDC に統合されています。

ステップ 1 SRV レコードを持つ /etc/krb5.conf または DNS サーバーが、必要な AD に到達するように構成されていることを確認します。

```
krb5.conf cofiguration
[libdefaults]
ticket_lifetime = 24h
default_realm = <AD REALM>
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
dns_lookup_realm = true
dns_lookup_kdc = false
forwardable = true
<AD REALM> = {
  kdc =< AD-HOSTNAME>:88
```

```
  admin_server = =< AD-HOSTNAME:749
  default_domain = <AD REALM>
}
```

（注） AD-HOSTNAME が解決可能であることを確認します。

（注） サーバー間の通信に Kerberos サーバーを使用する場合は常に、/etc/krb5.conf にある最新の暗号化アルゴリズムを使用することを推奨しています。

ステップ 2 Windows Server Active Directory にサービス アカウントを作成します。

1. Active Directory Users and Computers 管理ツールを使用して、新しいユーザー アカウントを作成します。
   - ユーザー名をスペースなしでアカウントに割り当てます。
   - アカウントにパスワードを割り当てます。

     （注） パスワードの有効期限が切れたり変更された場合は、**キータブ**ファイルを新しい関連付け *kvno*で生成する必要があります。

2. SETSPN を使用するアカウントにサービス プリンシパル名 (SPN) を割り当てます。Exe。SPN は、デプロイメントに応じてサービス名/ホスト名/ドメインです。1 つのアカウントに複数の SPN を割り当てることができます。

   たとえば、<service-name> と <hostname> を指定します。

   ```
   setspn -s DNS/<DNS running Computer Name> <Service Name>
   ```

3. *kvno*の詳細を取得します。

   ```
   ldifde -f <Filename> -d "DC=<DOMAIN>,DC=com" -l *,msDS-KeyVersionNumber -r
   "(serviceprincipalname=<service-principal name>)" -p subtree OR kvno.exe <service-principal
   name>@<REALM>
   ```

4. ktpass.exe コマンドを使用してキータブ ファイルをジェネタレします。

   ```
   ktpass -out<filename>  -princ <Principal name> -pass <password associated with the user> -crypto
    all -ptype KRB5_NT_PRINCIPAL -kvno <Kvno details>
   ```

   キータブファイルを Linux マシンに転送し、Kutil を実行して、Keytab 項目を既存のキータブファイルに追加します。

   ```
   > ktutil
    ktutil:  rkt <keytab file name>
    ktutil:  wkt /etc/krb5.keytab
    ktutil:  q
   ```

ステップ 3 以下を使用して、キー・タブ項目を表示します。

```
klist -k -t -e /etc/krb5.keytab
```

Linux 上のプライマリ DNS サーバー MIT-KDC に統合

サービス プリンシパル名を MIT KDC に関連付けるには、次の手順を実行します。

ステップ 1 Linux DNS サーバーにログインし、kadmin ユーティリティを使用して、MIT-KDC にプリンシパル名を追加します。

```
>kadmin
Authenticating as principal <MIT-KDC USER@REALM> with password.
Password for <MIT-KDC USER@REALM.COM > : <Enter the associated Password>
kadmin:  addprinc -randkey DNS/<hostname of the DNS server>
WARNING: no policy specified for DNS/<hostname of the DNS server>@REALM; defaulting to no policy
add_principal: Principal or policy already exists while creating " DNS/<hostname of the DNS
server>@REALM".
kadmin:  ktadd -randkey DNS/<hostname of the DNS server>
kadmin: Principal -randkey does not exist.
Entry for principal DNS/<hostname of the DNS server> with kvno x, encryption type AES-256 CTS mode
 with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal DNS/<hostname of the DNS server>with kvno x, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal DNS/<hostname of the DNS server>with kvno x, encryption type Triple DES cbc mode
 with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal DNS/<hostname of the DNS server>with kvno x, encryption type ArcFour with HMAC/md5
 added to keytab WRFILE:/etc/krb5.keytab.
kadmin:  quit
```

ステップ 2 次を使用して、keytab のエントリを表示します。

```
klist -k -t -e /etc/krb5.keytab
```

ステップ 3 Linux サーバーを実行している MIT-KDC にログインし、追加されたプリンシパル名に上記と同じ kvno が関連付けられているかどうかを確認します。

```
Kvno DNS/<hostname of the DNS server>
```

GSS-TSIG 設定のトラブルシューティング

GSS/SSPI の障害およびメジャー/マイナーステータスの詳細を取得するには、DNS サーバーで DEBUG オプションを有効にし、値 g=3 を設定します。

- "キー テーブルのプリンシパルのキー バージョン番号が正しくありません。

  KVno から返される, klist -k -t -e /etc/krb5.keytab DNS 実行中のマシンで kvno は KDC で同じ kvno でなければなりません。

  AD-KDCにおけるknvoの検証:

  ```
  ldifde -f c:\spn1_out.txt -d "DC=TIG,DC=com" -l *,msDS-KeyVersionNumber -r
  "(serviceprincipalname=DNS/WIN-CPNUV*)" -p subtree
  ```

  kvno の検証は、MIT- KDC です。

  ```
  Kvno <principal name>
  ```

- "間違ったプリンシパル名"

  GSS クライアントとサーバーが、サービス チケットの暗号化と復号化に使用されるのと同じサービス キーを使用していることを確認します。

DNS 更新のトラブルシューティング

などの**dig**標準 DNS ツールを使用**nslookup**して、サーバーに対してラールを照会できます。このツールは、動的に生成された RR が存在するかどうかを判断する際に役立ちます。次に例を示します。

```
$ nslookup
default Server: server2.example.com
Address: 192.168.1.2

> leasehost1.example.com
Server: server2.example.com
Address: 192.168.1.100

> set type=ptr
> 192.168.1.100
Server: server2.example.com
Address: 192.168.1.100
100.40.168.192.in-addr.arpa name = leasehost1.example.com
40.168,192.in-addr.arpa nameserver = server2.example.com
```

ログ設定属性を*ddns*に設定して DNS サーバーの DNS 更新を監視したり、dns-details に設定して詳細を表示したりできます。

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