



## セットアップ Web UI の実行

Web UI の Cisco Prime Network Registrar セットアップ インタビューでは、連続する一連のページで基本設定を行うことができます。これらのページの基本ナビゲーションの詳細については、「[セットアップ Web UI の概要](#)」を参照してください。

この章の内容は、次のとおりです。

- [サービスのセットアップ \(1 ページ\)](#)

## サービスのセットアップ

ローカルの基本ユーザモードでメインメニューの [セットアップ (Setup)] アイコン (■) をクリックすると、[このサーバを設定 (Set up this Server)] ページが開きます。

このページでは、次の機能をイネーブルにするかディセーブルにするかを決定します。

- **管理者パスワードの変更**：セキュリティ上の理由から、Cisco Prime Network Registrar Web UI への最初のログイン時に設定した値から管理者パスワードを変更することができます。詳細については、[管理者パスワードの変更 \(2 ページ\)](#) を参照してください。
- **Dynamic Host Configuration Protocol (DHCP) サーバ**：DHCP には、Cisco Prime Network Registrar の重要な部分であるダイナミックアドレス割り当てのメカニズムが用意されています。DHCP をイネーブルにすると、DHCP セットアップの一連のページが表示されます。ディセーブルにすると、DHCP セットアップは省略されます。詳細については、[DHCP サービスの設定 \(2 ページ\)](#) を参照してください。
- **キャッシングドメインネームシステム (CDNS) サーバ**：CDNS には、ドメインネーム構造が用意されています。CDNS をイネーブルにすると、CDNS セットアップの一連のページが表示されます。ディセーブルにすると、CDNS セットアップは省略されます。詳細については、[CDNS サービスの設定 \(8 ページ\)](#) を参照してください。
- **権威ドメインネームシステム (DNS) サーバ**：DNS には、ドメインネーム構造が用意されています。DNS をイネーブルにすると、DNS セットアップの一連のページが表示されます。ディセーブルにすると、DNS セットアップは省略されます。詳細については、[DNS サービスの設定 \(10 ページ\)](#) を参照してください。
- **DNS 更新**：DNS 更新は、DHCP を使用したダイナミックアドレッシングの利点を永続的に固有の DNS ホスト名と組み合わせたものです。これにより、ネットワークアクセスの

ための DNS ホストを自動的に設定できます。DHCP サーバは DNS サーバがリソース レコード (RR) を最新の状態に維持できるように DNS サーバに通知します。DNS 更新をイネーブルにすると、DNS 更新セットアップの一連のページが表示されます。ディセーブルにすると、DNS 更新セットアップは省略されます。詳細については、[DNS 更新の設定 \(14 ページ\)](#) を参照してください。

- **Trivial File Transfer Protocol (TFTP) サーバ** : アドレスのプロビジョニング用ファイルをケーブル モデムに転送できるように、TFTP サーバをイネーブル化する必要があります。TFTP をイネーブルにするのにセットアップページでさらに設定を行う必要はありません ([セットアップインタビュー レポート \(16 ページ\)](#) を参照)。



(注) 選択内容はログインセッションを越えて保持されます。

選択内容に応じて次のページに移動するには[次へ (Next) ]をクリックし、セットアップを終了して[セットアップインタビューレポート (Setup Interview Report) ]ページに移動するには[終了 (Finish) ]をクリックします。

## 管理者パスワードの変更

セットアップインタビューの[このサーバを設定 (Set up this Server) ]ページで[パスワードの変更 (Change Password) ]の値を[はい (yes) ]に設定した場合は、[ユーザのパスワードを変更 (Change Password for User) ]ページが開きます。このページは、ナビゲーションバーで[パスワードの変更 (Change Password) ]をクリックした場合も開きます。

パスワードの変更後は、次回以降の管理者ログインで新しいパスワードを使用します。

パスワードを変更しない場合は、[いいえ (no) ]チェックボックスをオンにします。パスワードを変更するには、新しいパスワードを入力し、[検証 (Verify) ]フィールドにもう一度入力して確認します。[次へ (Next) ]または[終了 (Finish) ]をクリックすると、次のログインセッションのために変更が送信されます (変更がある場合)。

## DHCP サービスの設定

セットアップインタビューの[このサーバを設定 (Set up this Server) ]ページで [DHCPサーバを有効にする (Enable DHCP Server) ]の値を[はい (yes) ]に設定した場合は、適切な順序で [DHCPの設定 (Set up DHCP) ]ページが開きます。このページは、ナビゲーションバーで [DHCP] をクリックした場合も開きます。

DHCP サーバを設定するには、このページで [DHCPサーバを有効にする (Enable DHCP Server) ]の値が[はい (yes) ]に設定されていることを確認します。すでに Cisco Prime Network Registrar でメイン DHCP サーバを設定し、そのサーバと同期している場合は、セットアッププロセスによって、現在のホストがすでにバックアップサーバであるためこれ以上の DHCP 設定が必要ないことが示されます。

次の項に基づいて設定値を選択し、[次へ (Next)] をクリックします。セットアッププロセスによって設定がアクティブになり、その後はスコープ (アドレスプール) 管理用のページが表示されます。

### DHCP フェールオーバーの設定

DHCP フェールオーバーの設定では、メインサーバが何らかの理由でネットワークから切断された場合に処理を引き継ぐことができるバックアップ DHCP サーバを指定します。サーバは冗長ペアとして機能し、相互に通信してアドレスの重複割り当てを防ぎます。

フェールオーバー サービスを提供するには、[DHCP フェールオーバーの設定 (Configure DHCP Failover)] の値を [はい (yes)] に設定します。セットアッププロセスで既存の複雑なフェールオーバー設定が検出された場合は、セットアップインタビューではフェールオーバーを設定できないことが通知されます。DHCP フェールオーバーがすでに拡張モードで設定され、次のいずれかの条件が満たされる場合、DHCP フェールオーバーを設定できません。

- 複数のフェールオーバー ペアが設定されている。
- 1 つのフェールオーバー ペアが存在し、main-server または backup-server が設定されている。

フェールオーバー設定の詳細については、[DHCP フェールオーバーの設定 \(4 ページ\)](#) を参照してください。

### DHCP サービス クラスの設定

サービスクラスは、DHCP クライアントにディファレンシエーテッド サービスを提供します。最も一般的なサービスは次のとおりです。

- アドレス リース
- IP アドレス範囲
- クライアントにサービスを提供する DNS サーバのアドレス
- ホスト名の割り当て
- アクセス コントロールによるサービス拒否

セットアップ ページで定義したサービス クラスによって最終的に次のものが定義されます。

- サービス クラスと同じ名前の DHCP クライアントクラス。
- サービス クラスと同じ名前の DHCP ポリシー。
- 選択タグがサービス クラスとして定義されている場合は DHCP スコープの割り当て。

サービス クラス設定の詳細については、[DHCP サービス クラスの設定 \(4 ページ\)](#) を参照してください。

### サーバ ロギング モード

DHCP サーバは、メッセージ出力のモードを設定できるログ メッセージを提供します。[サーバ ロギング モード (Server Logging Mode)] オプションには、特定のロギング設定に変換される 4 つの値を指定できます。

- **normal-operations** : 通常のロギングが行われます。

- **high-performance** : 高パフォーマンス ロギングが行われます。
- **debugging** : デバッグ ロギングが行われます。
- **customized** : 特定のログ設定を求めるメッセージを表示し、その設定のみを記録します。

### DHCP トラップのイネーブル化

DHCP サーバの SNMP トラップを設定すると、サーバが起動しているかどうか、パートナー通信のステータス、および特定の数の利用可能な下限フリーアドレスと上限フリーアドレスがあるかどうかを報告できます。DHCP トラップはデフォルトではイネーブルになっていないため、イネーブルにするにはこの値を [はい (yes)] に設定する必要があります。詳細については、[DHCP トラップの設定 \(7 ページ\)](#) を参照してください。

## DHCP フェールオーバーの設定

セットアップ インタビューの [DHCP の設定 (Set up DHCP)] ページで [DHCP フェールオーバーの設定 (Configure DHCP Failover)] の値を [はい (yes)] に設定した場合は、適切な順序で [DHCP フェールオーバーの設定 (Set up DHCP Failover)] ページが開きます。

[DHCP フェールオーバーの設定 (Configure DHCP Failover)] のプリセット値は [はい (yes)] で、[DHCP フェールオーバーロール (DHCP Failover Role)] は [メイン (main)] にプリセットされています。現在のマシンのロールを [バックアップ (backup)] に変更した場合は、このマシンに対するフェールオーバー設定をこれ以上行うことができません (メイン サーバマシンでフェールオーバー設定を実行し、フェールオーバー同期を実行するように指示するメッセージが表示されます)。

[フェールオーバー パートナー (Failover Partner)] の値によって、リモートバックアップサーバのアドレスとアクセス基準が決まります。そのサーバのクラスタがすでに存在する場合は、[既存のクラスタを選択 (Select existing cluster)] ドロップダウンリストからクラスタを選択できます。既存のクラスタがない場合は、バックアップサーバのクラスタを設定できます。

1. バックアップ DHCP サーバのホスト名または IP アドレスを入力します。
2. バックアップサーバのアクセス基準として、管理者の名前とパスワード、SCP ポート番号 (1234 にプリセット) を入力します。
3. [クラスタの追加 (Add Cluster)] をクリックしてクラスタを追加します。

フェールオーバー ペアをパートナー サーバ間のリース割り当てがサーバごとにアドレス プールの 50% であるロード バランシング関係にするかどうかを決定します。このロード バランシングを有効にする場合は、[ロード バランシング (Load Balancing)] の値を [はい (yes)] (プリセット値は [いいえ (no)]) に設定します。

設定値を選択するか入力し、[次へ (Next)] をクリックして設定をアクティブにすると、他の DHCP 設定を実行できます。

## DHCP サービス クラスの設定

セットアップ インタビューの [DHCP の設定 (Set up DHCP)] ページで [DHCP サービス クラスのイネーブル化 (Enable DHCP Classes of Service)] の値を [はい (yes)] に設定した場合は、適切な順序で [DHCP サービス クラスの設定 (Set up DHCP Classes of Service)] ページが開きます。

[DHCP サービスクラスのイネーブル化 (Enable DHCP Classes of Service)] のプリセット値は [はい (yes)] です。[サービスクラスの使用状況 (Class of Service Usage)] では、着信 DHCP パケットが着信パケットに基づいてサービスクラスを決定するか、このページで個別にクライアントを登録するかどうかを設定します。着信パケットによってサービスクラスを割り当てての場合は、*client-class-lookup-id* DHCP サーバ属性の式の設定など、拡張モードでいくつかの設定を行う必要があります。(着信パケットに基づくサービスクラスの割り当て (5 ページ) を参照)。

DHCP サービスクラスの値は、各サービスクラス名およびオプションで、サービスクラスを割り当てて DNS 正引きゾーンを設定するためのものです。追加するサービスクラスごとに [追加 (Add)] をクリックします。

設定値を選択するか入力し、[次へ (Next)] をクリックして設定をアクティブにすると、他の DHCP 設定を実行できます。[サービスクラスの使用状況 (Class of Service Usage)] の選択肢：

- [着信パケットに基づくサービスクラスの割り当て (Assign class of service based on incoming packet?)] : ページに特別なヘルプリンクが表示されます (着信パケットに基づくサービスクラスの割り当て (5 ページ) を参照)。
- [クライアントの個別登録 (Register clients individually?)] : [DHCP クライアントの一覧表示/追加 (List/Add DHCP Clients)] ページが開きます (クライアントの個別登録 (6 ページ) を参照)。

## 着信パケットに基づくサービスクラスの割り当て

[DHCP サービスクラスの設定 (Set up DHCP Classes of Service)] ページで [着信パケットに基づくサービスクラスの割り当て (Assign class of service based on incoming packet)] の [サービスクラスの使用状況 (Class of Service Usage)] 設定をイネーブルにした場合は、[DHCP サービスクラスの設定 (Set up DHCP Classes of Service)] ページが情報ページに変わります。

着信パケットに基づくサービスクラスの割り当ては、セットアップモードではクライアントの個別登録よりも使用頻度が低く、拡張モードでの設定を必要とします。このページで [次へ (Next)] をクリックして、DHCP の次のセットアップタスクに移動します。次のように続けます。

**ステップ 1** セットアップページを最後まで完了し、セットアップモードを終了します。

**ステップ 2** [拡張 (Advanced)] をクリックして拡張モードを開始します。

**ステップ 3** [導入 (Deploy)] メニューから、[DHCP] サブメニューの [DHCP サーバ (DHCP Server)] を選択して、[DHCP サーバの管理 (Manage DHCP Server)] ページを開きます。

**ステップ 4** [DHCP サーバ (DHCP Server)] ペインからサーバを選択します。

**ステップ 5** [DHCP サーバの編集 (Edit DHCP Server)] ページで、[クライアントクラス (Client-Class)] カテゴリの下にある *client-class-lookup-id* 属性の式の値を入力する (または、式を含むファイルへの参照を入力する) 必要があります。この属性を設定してクライアントを区別する例を次に示します。

- **voip クライアントクラスに Cisco IP 電話を入力** : *dhcp-parameter-request-list* オプション (55) のバイト値が 150 または 122 の着信パケットを検索します。見つかった場合、クライアントに **voip** クライアントクラスを割り当てます。

```
(or
  (if (search (byte 150) (request get-blob option 55)) "voip")
  (if (search (byte 122) (request get-blob option 55)) "voip")
  "<none>")
```

- クライアントクラスに **MAC アドレスの最初の 3 バイトを共有するクライアント** を入力 : MAC アドレスが 01:02:03 で始まる着信パケットを検索し、**red** クライアントクラスを割り当てます。また、04:05:06 で始まる MAC アドレスに **blue** クライアントクラスを割り当てます。

```
(or
  (if (starts-with (request get-blob chaddr) 01:02:03) "red")
  (if (starts-with (request get-blob chaddr) 04:05:06) "blue")
  "<none>")
```

- **msftclass** クライアントクラスに **Microsoft クライアント** を入力 : *dhcp-class-identifier* オプション (60) の値が MSFT で始まる着信パケットを検索し、クライアントに **msftclass** クライアントクラスを割り当てます。

```
(or
  (if (starts-with (request get-blob option 60) (as-blob "MSFT"))
    "msftclass")
  "<none>")
```

**ステップ 6** [保存 (Save) ] をクリックします。

**ステップ 7** [DHCP サーバの管理 (Manage DHCP Server) ] ページの [サーバの再起動 (Restart Server) ] ボタンをクリックしてサーバをリロードします。

## クライアントの個別登録

[DHCP サービスクラスの設定 (Set up DHCP Classes of Service) ] ページで [クライアントの個別登録 (Registering Clients Individually?) ] の [サービスクラスの使用状況 (Class of Service Usage) ] 設定をイネーブルにした場合は、[DHCP クライアントの一覧表示/追加 (List/Add DHCP Clients) ] ページが適切な順序で開きます ([DHCP クライアントの一覧表示/追加 (List/Add DHCP Clients) ] ページの例については、『Cisco Prime Network Registrar 11.0 DHCP ユーザガイド』の「Configuring Clients」の項を参照してください)。

このページでは、DHCP クライアントの名前を入力し、必要に応じて [クライアントクラス名 (Client-Class Name) ] ドロップダウンリストから設定済みのクライアントクラスを選択します。

- クライアントクラスも選択した場合は、それ以上設定を行わなくてもクライアントがリストの下に追加されます。
- クライアントクラスを選択しなかった場合は、[DHCP クライアントの追加 (Add DHCP Client) ] ページが開きます。
- このページで値を入力する方法については、『Cisco Prime Network Registrar 11.0 DHCP ユーザガイド』の「Configuring Clients」の項を参照してください。[DHCP クライアントの追加 (Add DHCP Client) ] ページでクライアントの名前をクリックすると、[DHCP クライアントの編集 (Edit DHCP Client) ] ページの基本モードバージョンが開きます (詳細につ

いては、『Cisco Prime Network Registrar 11.0 DHCP ユーザガイド』の「*Editing Clients and Their Embedded Policies*」の項を参照してください。

## DHCPv4 サブネットの管理

DHCPv4 サービスをイネーブルにし、セットアップ インタビューで DHCP フェールオーバーの設定を完了すると、[スコープテンプレートおよびサブネット (Scope Templates and Subnets)] ページが開きます。これらのサブネットとスコープテンプレートは、設定をローカル DHCP サーバにプッシュするために必要となります。

スコープテンプレートを定義するには、[名前 (Name)] フィールドに名前を入力してから、[スコープ名の式 (Scope Name Expression)] フィールドにその式を入力します。

[スコープテンプレートの追加 (Add Scope Templates)] をクリックしてスコープテンプレートを追加し、[次へ (Next)] をクリックして [サブネット (Subnets)] ページに移動します。[サブネットの追加 (Add subnet)] アイコンをクリックして、サブネットアドレスを入力します。次に、フェールオーバー ペア/クラスタとスコープテンプレートを選択して、プッシュします。

## DHCPv6 プレフィックスの管理

DHCPv6 サービスをイネーブルにし、セットアップ インタビューで DHCP フェールオーバーの設定を完了すると、[プレフィックステンプレート (Prefix Template)] ページが開きます。これらのプレフィックスおよびプレフィックステンプレートは、設定をローカル DHCP サーバにプッシュするために必要となります。

プレフィックステンプレートを定義するには、[名前 (Name)] フィールドに名前を入力してから、[プレフィックス名の式 (Prefix Name Expression)] フィールドにその式を入力します。

[プレフィックステンプレートの追加 (Add Prefix Templates)] をクリックしてプレフィックステンプレートを追加し、[次へ (Next)] をクリックして [プレフィックス (Prefix)] ページに移動します。[プレフィックスの追加 (Add Prefix)] アイコンをクリックして、プレフィックスアドレスを入力します。次に、フェールオーバー/クラスタとプレフィックステンプレートを選択して、プッシュします。

## DHCP トラップの設定

セットアップ インタビューの [DHCP の設定 (Set up DHCP)] ページで [DHCP トラップのイネーブル化 (Enable DHCP Traps)] の値を [いいえ (no)] に設定した場合は、適切な順序で [DHCP トラップの設定 (Set up DHCP Traps)] ページが開きます。

[DHCP トラップのイネーブル化 (Enable DHCP Traps)] のプリセット値は [いいえ (no)] です。設定するトラップとトラップの設定方法を決定する必要があります。設定するトラップの種類は、[DHCP トラップの選択 (Select DHCP Traps)] の値によって決まります。すべてのトラップを設定するか、次の項目を報告するトラップを選択して設定できます。

- サーバの起動と終了 (server-start と server-stop)。
- フリーアドレスの検出日時 (free-address-low と free-address-high)。
- DNS キューのサイズ (dns-queue-size)。

- パートナー サーバがダウンしているかアップしているか（other-server-down と other-server-up）。
- 検出された重複アドレス（duplicate-address）、アドレス競合（address-conflict）、またはフェールオーバー設定エラー（failover-config-error）。

フリーアドレスの検出トラップを設定した場合は、その設定も指定する必要があります。

- フリーアドレス設定の名前（display-only の値：**global**）
- フリーアドレスの決定方法：**scope**、**network**、または **scope-selection タグ**（プリセット値：**scope**）
- フリーアドレスの何パーセントが検出されたら low-threshold トラップを生成して高しきい値を再度イネーブルにするか（プリセット値：**20%**）
- フリーアドレスの何パーセントが検出されたら high-threshold トラップを生成して低しきい値を再度イネーブルにするか（プリセット値：**25%**）

設定値を選択するか入力し、[次へ (Next)] をクリックして設定をアクティブにすると、DHCP アドレスのスコープを設定できます。

## DHCP スコープの管理

セットアップ インタビューで DHCP サービスをイネーブルにし、DHCP フェールオーバー、サービスクラス、またはトラップの最後の設定ページを完了すると、[スコープの管理 (Manage Scopes)] ページが開きます。スコープは、一般的なリース設定を指定するアドレス プールです。これらのスコープは、DHCP に必要です。

スコープを定義するには、[名前 (Name)] フィールドにスコープ名を入力してから、そのサブネットアドレス (192.168.50/24 など) を [サブネット (Subnet)] フィールドに入力します。[DHCP サービス クラスの設定 \(4 ページ\)](#) でサービス クラスを設定した場合は、[サービス クラス (Class of Service)] ドロップダウン リストからサービス クラスをスコープに関連付けることもできます。

[スコープの追加 (Add Scope)] をクリックしてスコープを追加してから、[次へ (Next)] をクリックして設定をアクティブにし、次の設定手順に進みます。たとえば、DHCP トラップを設定する場合は、次にトラップの受信側 ([トラップの受信側の設定 \(15 ページ\)](#)) を参照) を設定できます。DNS サーバをイネーブルにした場合は、DNS サーバの設定ページに移動します ([DNS サービスの設定 \(10 ページ\)](#) を参照)。

## CDNS サービスの設定

セットアップ インタビューの [このサービスを設定 (Set up this Server)] ページで [CDNS サーバのイネーブル化 (Enable CDNS Server)] の値を [はい (yes)] に設定した場合、および [DNS サーバの役割 (DNS Server role)] を [プライマリ (primary)] に設定した場合は、適切な順序で [CDNS の設定 (Set up CDNS)] ページが開きます。このページは、ナビゲーション バーで [CDNS] をクリックした場合も開きます。

次の項の情報に基づいて設定値を選択し、[次へ (Next)] をクリックして設定をアクティブにします。その後、アクセスコントロールとトラップの設定用のセットアップ ページが表示されます。



### CDNS サーバ ロール :

DNS サーバはキャッシング サーバにすることができます。

- **Caching** : ゾーンに対して権威を持たず、ゾーン情報のデータベースを保持しませんが、キャッシュおよび権威ネーム サーバへの照会によってクエリーに応答します。

### サーバ ロギング モード

キャッシング DNS サーバはログ メッセージを提供し、ユーザがメッセージ出力のモードを設定できます。[サーバロギングモード (Server Logging Mode)] オプションには、特定のロギング設定に変換される 4 つの値を指定できます。

- **normal-operations** : 通常のロギングが行われます。
- **high-performance** : 高パフォーマンス ロギングが行われます。
- **debugging** : デバッグ ロギングが行われます。
- **customized** : 特定のログ設定を求めるメッセージを表示し、その設定のみを記録します。

### CDNS トラップのイネーブル化

CDNS サーバの SNMP トラップを設定すると、サーバが起動しているかどうかを報告する手段が提供されます。CDNS トラップはデフォルトではイネーブルになっていないため、イネーブルにするにはこの値を [はい (yes)] に設定する必要があります。詳細については、[CDNS トラップの設定 \(10 ページ\)](#) を参照してください。

## CDNS アクセスコントロールの設定

セットアップ インタビューの [CDNS の設定 (Set up CDNS)] ページで CDNS サーバを設定した場合は、適切な順序で [CDNS アクセスコントロールの設定 (Set up CDNS Access Control)] ページが開きます。

このページで、アクセスコントロールリスト (ACL) に基づいてクエリーとゾーン転送を制限できます。

- **dns-restrict-query-acl** : DNS サーバが受け入れるデバイス クエリーを制限するために使用されるグローバル ACL を提供します。クエリー クライアントは、ホスト IP アドレス、ネットワーク アドレス、およびその他の ACL に基づいて制限できます。プリセット値では、任意のクライアントによるクエリーの実行を許可します。複数の ACL 値はカンマで区切ります。
- **CDNS Forwarders** : キャッシング DNS サーバのフォワーダを設定する場合は、名前と IP アドレスを指定し、[フォワーダの追加 (Add Forwarder)] をクリックします。
- **CDNS Resolution Exceptions** : CDNS サーバでドメイン外の特定の名前をルートネームサーバに照会する通常の方法を使用しない場合は、解決例外を使用してルートネームサーバをバイパスし、特定のサーバを対象にして名前解決を処理します。ネームサーバ名とそのカンマで区切られたアドレスを入力し、[例外の追加 (Add Exception)] をクリックします。

[次へ (Next)] をクリックして設定をアクティブにし、CDNS サーバ設定を続行 (または完了) します。

## CDNS トラップの設定

セットアップ インタビューの [CDNSの設定 (Set up CDNS)] ページで [CDNSトラップのイネーブル化 (Enable CDNS Traps)] の値を [はい (yes)] に設定した場合は、適切な順序で [CDNSトラップの設定 (Set up CDNS Traps)] ページが開きます。

[CDNSトラップのイネーブル化 (Enable CDNS Traps)] のプリセット値は [はい (yes)] です。設定するトラップとトラップの設定方法を決定する必要があります。設定するトラップの種類は、[CDNSトラップの選択 (Select CDNS Traps)] の値によって決まります。[CDNSトラップの選択 (Select CDNS Traps)] のプリセット値は [なし (none)] です。すべてのトラップを設定するか、サーバの起動と終了 (server-start と server-stop) などを報告するトラップを選択して設定することもできます。

設定値を選択します。次に、[次へ (Next)] をクリックして設定をアクティブにし、CDNS 設定を完了します。

## DNS サービスの設定

セットアップ インタビューの [このサーバを設定 (Set up this Server)] ページで [DNS サーバを有効にする (Enable DNS Server)] の値を [はい (yes)] に設定した場合は、適切な順序で [DNS の設定 (Set up DNS)] ページが開きます。このページは、ナビゲーションバーで [DNS] をクリックした場合も開きます。

DNS サーバを設定するには、[DNS サーバを有効にする (Enable DNS Server)] の値が [はい (yes)] に設定されていることを確認します。すでに他の場所でプライマリ DNS サーバを設定し、そのサーバと同期している場合は、セットアッププロセスによって、現在の Cisco Prime Network Registrar ホストがすでにセカンダリ サーバまたはキャッシングサーバとして設定されているためこれ以上の DNS 設定が必要ないことが示されます。

次の項の情報に基づいて設定値を選択し、[次へ (Next)] をクリックして設定をアクティブにします。その後、正引きおよび逆引き DNS ゾーン (High-Availability DNS サーバ用など)、ゾーン配信、およびアクセス コントロールの設定用のセットアップ ページが表示されます。

### DNS サーバの役割

DNS サーバはプライマリまたはセカンダリ サーバにすることができます。

- **プライマリ** (プリセット値) : ゾーンに対して権威があり、このゾーン情報をデータベースに保持します。
- **セカンダリ** : プライマリ サーバのゾーン情報のコピーをロードします。プライマリは、セカンダリにゾーン情報の変更を通知し、セカンダリへのゾーン転送を実行します。

サーバがプライマリの場合は、そのサーバを High-Availability (HA) DNS サーバ設定に含めるかどうかを指定することもできます ([高可用性 DNS の設定 \(11 ページ\)](#) の項を参照)。サーバがセカンダリの場合は、そのサーバ専用のアクセス コントロールを設定できます。

## 高可用性 DNS の設定

高可用性 (HA) DNS サーバは、サーバがダウンしたときにフェールオーバーを提供します。この関係では、2つ目のプライマリサーバがメインプライマリサーバをシャドウイングするホットスタンバイになることができます。

HA DNS サービスを提供するには、[高可用性 DNS の設定 (Configure High-Availability DNS)] の値を [はい (yes)] に設定します。セットアッププロセスで既存の複雑な HA DNS 設定が検出された場合、セットアップインタビューでは HA DNS を設定できないことが通知されます。HA DNS がすでに拡張モードで設定され、次のいずれかの条件が満たされる場合、セットアップ ページでは HA DNS を設定できません。

- 複数の HA DNS サーバ ペアが設定されている。
- 1 つの HA DNS ペアが存在し、main-server または backup-server の値が設定されている。

HA DNS 設定の詳細については、[高可用性 DNS の設定 \(11 ページ\)](#) を参照してください。

## サーバ ロギング モード

DNS サーバはログ メッセージを提供し、ユーザがメッセージ出力のモードを設定できます。[サーバロギングモード (Server Logging Mode)] オプションには、特定のロギング設定に変換される 4 つの値を指定できます。

- **normal-operations** : 通常のロギングが行われます。
- **high-performance** : 高パフォーマンス ロギングが行われます。
- **debugging** : デバッグ ロギングが行われます。
- **customized** : 特定のログ設定を求めるメッセージを表示し、その設定のみを記録します。

## DNS トラップのイネーブル化

DNS サーバの SNMP トラップを設定すると、サーバが起動しているかどうか、パートナー通信のステータス、パートナー設定、プライマリ通信、およびセカンダリゾーンステータスを報告できます。DNS トラップはデフォルトではイネーブルになっていないため、イネーブルにするにはこの値を [はい (yes)] に設定する必要があります。詳細については、[DNS トラップの設定 \(13 ページ\)](#) を参照してください。

## 高可用性 DNS の設定

セットアップインタビューの [DNS サーバの設定 (Set up DNS Server)] ページで [高可用性 DNS の設定 (Configure High-Availability DNS)] の値を [はい (yes)] に設定した場合、および [DNS サーバの役割 (DNS Server Role)] を [プライマリ (primary)] に設定した場合は、適切な順序で [高可用性 DNS の設定 (Set up High-Availability DNS)] ページが開きます。

[高可用性 DNS の設定 (Configure High-Availability DNS)] のプリセット値は [はい (yes)] で、[HA DNS ロール (HA DNS Role)] のプリセット値は [メイン (main)] です。[DNS ロール (DNS Role)] は、この特定のマシンで実行するロールです。現在のマシンのロールを [バックアップ (backup)] に変更した場合は、このマシンに対するフェールオーバー設定をこれ以上行うことができません (メインサーバマシンでフェールオーバー設定を実行し、HA DNS 同期を実行するように指示するメッセージが表示されます)。同様に、Cisco Prime Network

Registrar が複雑な HA DNS 設定を検出すると、警告が表示され、HA DNS 設定のセットアップを実行する必要があります。

[HA パートナー (HA Partner)] の値によって、リモートバックアップサーバのアドレスとアクセス基準が決まります。そのサーバのクラスタがすでに存在する場合は、[既存のクラスタを選択 (Select existing cluster)] ドロップダウンリストからクラスタを選択できます。既存のクラスタがない場合は、バックアップサーバのクラスタを設定できます。

1. バックアップ DNS サーバのホスト名または IP アドレスを入力します。
2. バックアップサーバのアクセス基準として、管理者の名前とパスワード、SCP ポート番号 (プリセット値は **1234**) を入力します。
3. [クラスタの追加 (Add Cluster)] をクリックしてクラスタを追加します。

設定値を選択するか入力し、[次へ (Next)] をクリックして設定をアクティブにすると、DNS ゾーン分散を設定できます。

## DNS ゾーン配信の設定

セットアップインタビューの [DNS の設定 (Set up DNS)] ページで DNS サーバをプライマリとして設定した場合は、適切な順序で [DNS ゾーン分散の設定 (Set up DNS Zone Distribution)] ページが開きます。

[DNS セカンダリサーバ (DNS Secondary Server(s))] の値によって、現在の DNS プライマリのバックアップセカンダリとなるサーバが決まります。セカンダリサーバが存在する既存のクラスタをドロップダウンリストから選択するか、新しいクラスタを追加できます。新しいクラスタを作成するには、次の手順を実行します。

1. バックアップ DNS サーバのホスト名または IP アドレスを入力します。
2. バックアップサーバのアクセス基準として、管理者の名前とパスワード、SCP ポート番号 (プリセット値は **1234**) を入力します。
3. [クラスタの追加 (Add Cluster)] をクリックしてクラスタを追加します。

設定値を選択するか入力し、[次へ (Next)] をクリックして設定をアクティブにすると、DNS サーバのゾーンを設定できます。

## 正引きゾーンの管理

セットアップインタビューの [DNS の設定 (Set up DNS)] ページで DNS サーバをプライマリとして設定した場合は、適切な順序で [正引きゾーンの管理 (Manage Forward Zones)] ページが開きます。

追加の正引きゾーンを定義するには、[名前 (Name)] フィールドにゾーン名を、[ネームサーバ (Nameserver)] フィールドにネームサーバドメイン名 (ns1.example.com. など) を、[連絡先電子メール (Contact E-Mail)] フィールドにホスト管理者名 (hostmaster.example.com. など、ゾーンの担当者のメールボックスを指定するドメイン名) を入力します。

正引きゾーンデータを追加してから、[正引きゾーンの管理 (Manage Forward Zones)] ページの [ゾーンの追加 (Add Zone)] をクリックして、正引きゾーンを追加します (『Cisco PrimeNetwork Registrar 11.0 権限のあるキャッシュ DNS ユーザガイド』の「Configuring Primary

Forward Zones」の項を参照)。[次へ (Next)] をクリックして設定をアクティブにすると、DNS サーバの逆引きゾーンを追加できます。

## 逆引きゾーンの管理

[DNSの設定 (Set up DNS)] ページで DNS サーバをプライマリとして設定し、セットアップ インタビューで正引きゾーンを設定した場合は、適切な順序で [逆引きゾーンの管理 (Manage Reverse Zones)] ページが開きます。

Cisco Prime Network Registrar によってループバック逆引きゾーン (127.in-addr.arpa.) が自動的に作成されます。追加の逆引きゾーンを定義するには、[名前 (Name)] フィールドにゾーン名を、[ネームサーバ (Nameserver)] フィールドにネームサーバドメイン名 (ns1.example.com. など) を、[連絡先電子メール (Contact E-Mail)] フィールドにホスト管理者名 (hostmaster.example.com. など、ゾーンの担当者のメールアドレスを指定するドメイン名) を入力します (名前には最後のドットも含めた完全修飾名を使用してください)。

逆引きゾーンデータを追加し、[逆引きゾーンの管理 (Manage Reverse Zones)] ページで [ゾーンの追加 (Add zone)] をクリックして、逆引きゾーンを追加します (『Cisco PrimeNetwork Registrar 11.0 権限のあるキャッシュ DNS ユーザガイド』の「Adding Reverse Zones as Zones」の項を参照)。[次へ (Next)] をクリックして設定をアクティブにすると、DNS サーバのアクセスコントロールを追加できます。

## DNS アクセスコントロールの設定

セットアップ インタビューの [DNSの設定 (Set up DNS)] ページで DNS サーバをプライマリまたはセカンダリとして設定した場合は、適切な順序で [DNS アクセスコントロールの設定 (Set up DNS Access Control)] ページが開きます。

このページで、アクセスコントロールリスト (ACL) に基づいてクエリーとゾーン転送を制限できます。

- **dns-restrict-xfer-acl** : ゾーン転送を受け入れることができるユーザを指定するデフォルトの ACL。ゾーンに *restrict-xfer-acl* 属性を設定すると、この設定が上書きされます。この設定は、キャッシングサーバには適用されません。プリセット値は [なし (none)] です。複数の ACL 値はカンマで区切ります。

[次へ (Next)] をクリックして設定をアクティブにし、DNS サーバ設定を続行 (または完了) します。

## DNS トラップの設定

セットアップ インタビューの [DNS の設定 (Set up DNS)] ページで [DNS トラップのイネーブル化 (Enable DNS Traps)] の値を [はい (yes)] に設定した場合は、適切な順序で [DNS トラップの設定 (Set up DNS Traps)] ページが開きます。

[DNS トラップのイネーブル化 (Enable CDNS Traps)] のプリセット値は [はい (yes)] です。設定するトラップとトラップの設定方法を決定する必要があります。設定するトラップの種類は、[DNS トラップの選択 (Select DNS Traps)] の値によって決まります。[DNS トラップの選

択 (Select DNS Traps) ] のプリセット値は [なし (none) ] です。すべてのトラップを設定するか、次の項目を報告するトラップを選択して設定することもできます。

- サーバの起動と終了 (server-start と server-stop) 。
- HA DNS パートナーのアップ/ダウン状態 (ha-dns-partner-up/ha-dns-partner-down) および設定エラー (ha-dns-config-error) 。
- プライマリサーバが応答しているか (primary-responding) 、応答していないか (primary-not-responding) 。
- セカンダリゾーンが期限切れになっているかどうか (secondary-zone-expired) 。

設定値を選択します。次に、[次へ (Next) ] をクリックして設定をアクティブにし、DNS 設定を完了します。

## DNS 更新の設定

セットアップインタビューの [このサーバを設定 (Set up this Server) ] ページで [DHCP サーバを有効にする (Enable DHCP Server) ] の値を [はい (yes) ] に設定し、[DHCP の更新を有効にする (Enable DHCP Update) ] の値を [はい (yes) ] に設定した場合は、適切な順序で [DNS 更新の設定 (Set up DNS Update) ] ページが開きます。更新にローカルサーバを使用する場合は、[DNS サーバを有効にする (Enable DNS Server) ] も [はい (yes) ] に設定しておく必要があります。前の基準が満たされている場合、このページはナビゲーションバーで [DNS の更新 (DNS Update) ] をクリックしても開きます。

このページでは、DNS 更新を有効にするために DNS サーバと DHCP サーバの関係を設定する必要があります。

- **DNS サーバまたは HA ペア (DNS Server or HA Pair)** : DNS 更新用に 1 つの DNS サーバまたは HA DNS サーバペアを設定できます。1 つのサーバの場合、値は **localhost** にプリセットされます。HA DNS ペアが定義されている場合、その設定名をドロップダウンリストから選択できます。新しいクラスタを定義するには、ホスト名、IP アドレス、管理者名、パスワード、および SCP ポート値 (プリセット値 : 1234) をそれぞれのフィールドに入力し、[クラスタの追加 (Add Cluster) ] をクリックします。
- **DHCP サーバまたはフェールオーバー ペア (DHCP Server or Failover Pair)** : DNS 更新用に 1 つの DHCP サーバまたは DHCP フェールオーバー サーバペアを設定できます。1 つのサーバの場合、値は **localhost** にプリセットされます。フェールオーバー パートナーシップが定義されている場合、その設定名をドロップダウンリストから選択できます。新しいクラスタを定義するには、ホスト名、IP アドレス、管理者名、パスワード、および SCP ポート値 (プリセット値 : 1234) をそれぞれのフィールドに入力し、[クラスタの追加 (Add Cluster) ] をクリックします。
- **正引きゾーンの名前 (Forward Zone Name)** : DNS 更新を受信する正引きゾーンを定義する必要があります。ゾーンは DNS サーバまたは HA DNS ペアに定義されている必要があります。このフィールドにゾーン名を入力します。サービスクラスのゾーンを区別する場合は、複数のゾーンをカンマで区切ったリストを入力することもできます。それ以外の場合は、[example.com] または [なし (none) ] を [正引きゾーンの名前 (Forward Zone Name) ]

ドロップダウンリストから選択できます。正引きゾーンに対して逆引きゾーンがすでに定義されている場合は、このページを完了すると、ポインタ (PTR) レコードが適切な逆引きゾーンにも書き込まれます。

- **DNS更新のセキュリティ (Secure DNS Updates?)** : トランザクション署名 (TSIG) を使用して DNS 更新をセキュリティ保護する場合は、この値を [はい (yes)] に設定します (プリセット値は [いいえ (no)] )。この値をイネーブルにすると、DNS サーバは *dns-update-server-key* 属性に指定されている TSIG キーを使用するか、次の [サーバキー (Server Key)] フィールドに定義されているキーを使用します。
- **サーバキー (Server Key)** : [DNS更新のセキュリティ (Secure DNS Updates)] をイネーブルにし、TSIG キーが存在する場合は、ドロップダウンリストからキーを選択できます。キーが存在しない場合は、作成できます。[名前 (Name)] フィールドにキー名を入力し、[キーの生成 (Generate Key)] をクリックします (この処理では Cisco Prime Network Registrar **cnr-keygen** ツールが使用されます)。キーを生成すると、その名前が [既存のキーを選択 (Select existing key)] ドロップダウンリストに表示されます。

設定値を選択するか入力します。次に、[次へ (Next)] をクリックして設定をアクティブにし、DNS の更新設定を完了します。

## トラップの受信側の設定

[このサーバを設定 (Setup this Server)] ページで DHCP または DNS サーバをイネーブルにし、セットアップインタビューの DHCP または DNS サーバのセットアップ ページでトラップをイネーブルにした場合は、適切な順序で [トラップの受信側の設定 (Set up Trap Recipients)] ページが開きます。前の基準が満たされている場合、このページはナビゲーションバーで [トラップ (Traps)] をクリックしても開きます。

トラップを有効にするには、トラップ受信側 (トラップ通知を受け取るホスト) を指定する必要があります。受信側ホストの識別名と IP アドレスを入力し、[トラップの受信側を追加 (Add Trap Recipient)] をクリックします。[次へ (Next)] をクリックして設定をアクティブにし、[セットアップインタビュー タスク (Setup Interview Tasks)] ページに移動します。

## セットアップ インタビュー タスク

[セットアップインタビュー タスク (Setup Interview Tasks)] ページは、セットアップインタビューで設定に基づいて実行するタスクがある場合に開きます。たとえば、スコープを作成するには、DHCP サーバのリロードが必要になることがあります。このページには、タスク名、ID、およびタスクの最終実行日時が示されます。[アクション (Action)] カラムには、タスクを選択するためのチェックボックスがあります。1つ以上のタスクを実行するには、[選択したタスクの実行 (Run Selected Tasks)] をクリックします。クリックすると確認ページが開きます。このページで [レポートと終了 (Report and Exit)] を実行すると、[セットアップインタビュー レポート (Setup Interview Report)] ページに移動します。

## セットアップインタビューレポート

[セットアップインタビューレポート (Setup Interview Report)] ページは、セットアップインタビューで最後に開くページです。このページには、インタビューページで実行したアクションの要約およびセッション時間と完了ステータスが表示されます。

[セットアップの終了 (Exit Setup)] をクリックするとメインメニューページに戻ります。