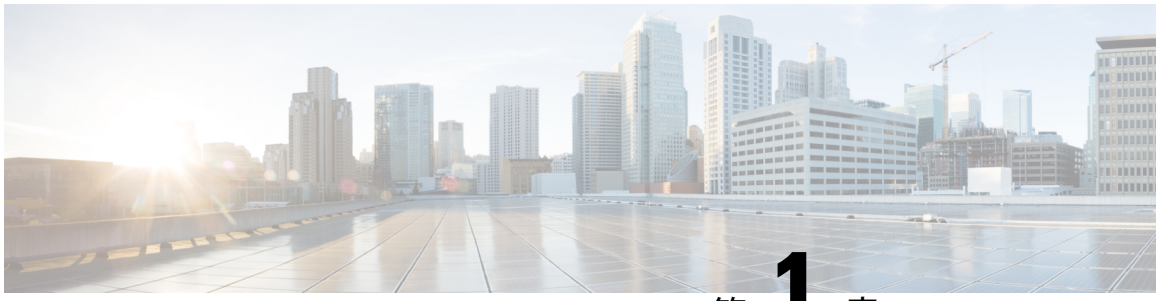
Cisco Prime Network Registrar 10.1 クイック スタート ガイド

初版：2019 年 12 月 16 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

セットアップ Web UI の概要

Cisco Prime Network Registrar Web UI のリージョン クラスタおよびローカル クラスタは、基本ユーザ モードでセットアップ環境を指定します。セットアップはウィザードによく似た一連のインタビュー ページの形式で、ユーザの選択にのみ基づきます。

ライセンス管理は、Cisco Prime Network Registrar がインストールされるときに、リージョン クラスタから実行されます。まず、リージョン サーバをインストールしてから、リージョン サーバにすべてのライセンスをロードする必要があります。ローカル クラスタをインストールすると、リージョンを登録してライセンスを取得します。詳細については、「*Cisco Prime Network Registrar 10.1* インストール ガイド」を参照してください。

この章は、次の項で構成されています。

リージョンのセットアップ機能

セットアップ ページには次の機能が用意されています。

- ダイナミック ホスト コンフィギュレーション：
  - ダイナミック ホスト コンフィギュレーション（DHCP）サービスのイネーブル化
  - 2 つのサーバ間における DHCP フェールオーバーの設定
  - サブネット、スコープ テンプレート、プレフィックス、およびプレフィックス テンプレートの設定
- BYOD：
  - キャッシング DNS 設定
  - ポリシーの作成（BYOD_unregistered）
  - クライアント クラス（BYOD_registered、BYOD_unregistered）
  - BYOD のスコープ/プレフィックス分割が未登録
  - BYOD Web サーバの HTTPS 設定
  - クラスタのリロード

- セキュリティ：
  - 外部認証の設定

ローカルのセットアップ機能

セットアップ ページには、次の機能が用意されています。

- ユーザ パスワードの変更
- ダイナミック ホスト コンフィギュレーション：
  - ダイナミック ホスト コンフィギュレーション（DHCP）サービスのイネーブル化
  - 2 つのサーバ間における DHCP フェールオーバーの設定
  - サービス クラスの設定
  - サーバ ロギング モードの選択
  - 簡易ネットワーク管理プロトコル（SNMP）トラップのイネーブル化
- キャッシング DNS 設定：
  - キャッシング ドメイン ネーム システム（CDNS）サービスのイネーブル化
  - CDNS アクセス コントロールの設定
  - CDNS トラップの設定
- 権威 DNS 設定：
  - 権威 DNS サービスのイネーブル化
  - 高可用性（HA）DNS サーバの設定
  - ゾーン配信の設定によるプライマリ サーバとセカンダリ サーバの調整
  - 正引きゾーンと逆引きゾーンの管理
  - アクセス コントロールの設定
  - SNMP トラップのイネーブル化
- ダイナミック ホストの DNS 更新
- 簡易ネットワーク管理プロトコル（SNMP）トラップの受信側
- トリビアル ファイル転送プロトコル（TFTP）サーバ

セットアップ機能とナビゲーション

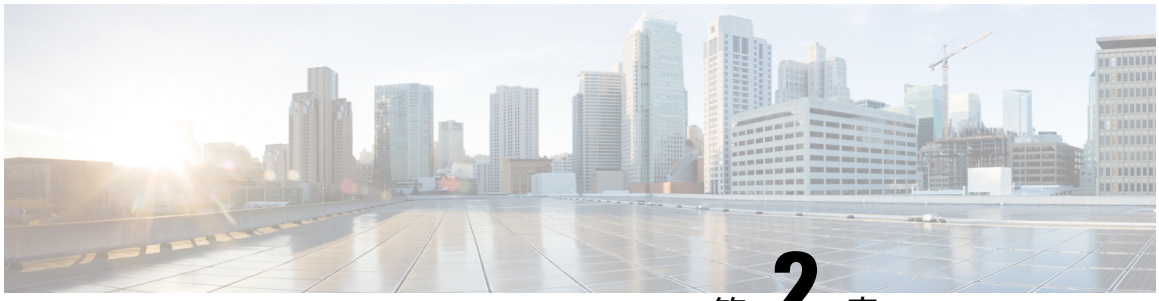
セットアップ ページ：

- 基本および拡張ユーザ モードから特別なセットアップ モードに移動します。基本および拡張ユーザ モードは、セットアップ インタビューを使用して環境を設定したあとで特別な設定を行うためのモードです。これらのモード（およびサーバ概念）の詳細については、『*Cisco Prime Network Registrar 10.1* アドミニストレーション ガイド』を参照してください。

- 機能をイネーブルにしたりディセーブルにしたりできる [このサーバを設定（Setup this Server）]ページが含まれ、このページがイネーブルになっているすべての機能のページの出発点となります。
- ページには、順に実行できるように [戻る（Back）]、[次へ（Next）]、および [終了（Finish）] ボタンがあります。ただし、[このサーバを設定（Set up this Server）] ページには [戻る（Back）] ボタンはありません。また、[セットアップインタビュータスク（Setup Interview Tasks）] ページには [戻る（Back）] ボタンと [次へ（Next）] ボタンはありません。[終了（Finish）] ボタンを使用すると、[セットアップ インタビュー タスク（Setup Interview Tasks）] ページに直接移動できます。

> ⚠ **注意** ブラウザの [戻る（Back）] ボタンと [進む（Forward）] ボタンを使用してセットアップ プロセスをナビゲートしないでください。ブラウザの [戻る（Back）] ボタンと [進む（Forward）] ボタンを使用すると、エラーが発生する可能性があります。

- 設定した基準に従って次のページを開く [次へ（Next）] ボタンが含まれます。たとえば、DNS サーバがイネーブルであるが、プライマリとして指定されていない場合、[高可用性（HA）DNSサーバ（High-Availability (HA) DNS server）]、[ゾーン分散（zone distribution）]、および [正引きゾーンと逆引きゾーンの設定（forward and backward zone configuration）] ページは省略されます。
- ローカルのセットアップ インタビューには [サービス（Services）]、[DHCP]、[CDNS]、[DNS]、[DNS 更新（DNS Update）]、[トラップ（Traps）]、および [終了（Finish）] タブがあるため、[このサーバを設定（Set up this Server）] ページでイネーブル ステータスであるかディセーブル ステータスであるかにかかわらずこれらの機能にアクセスできます。ただし、[このサーバを設定（Set up this Server）] ページで機能がディセーブルになっている場合、その機能はセットアップページでディセーブルと表示されます。特定のセットアップ ページでステータスを変更できます。変更すると、[このサーバを設定（Set up this Server）] ページのステータスがリセットされます。
- リージョン セットアップ インタビューには [サービス（Services）]、[DHCP]、[BYOD]、[セキュリティ（Security）]、および [終了（Finish）] タブがあるため、[このサーバを設定（Set up this Server）] ページでイネーブルになっている場合はこれらの機能にアクセスできます。
- トランザクションの場合とそうでない場合があります。クラスタやキーを作成する場合などは、値を入力するとすぐにデータベースへの書き込みが行われます。データベースへの書き込みが [次へ（Next）] または [終了（Finish）] をクリックしたときにのみ行われる場合もあります。
- [終了（Finish）] をクリックすると、データベースの書き込みを追跡し、レポート ページでそれらを要約します。
- 最初の選択デフォルト値を提供し、変更を次回のセットアップまで保持します（次回以降のセットアップでは、前に設定された値が新しいデフォルト値になります）。



第 2 章

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 （1 ページ）」を参照してください。

この章は、次の項で構成されています。

リージョン サービスの設定

リージョンの基本ユーザ 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。

- **Dynamic Host Configuration Protocol (DHCP)**：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 セットアップ用の一連のページを使用して DHCP 設定を行うか、ユーザ選択に基づいて DHCP 設定がバイパスされます。DHCP サービスの設定 （6 ページ）を参照してください。
- **Bring Your Own Device（BYOD：個人所有デバイス持ち込み）**：BYOD は、デバイスを認証および登録して IP ネットワーク リソースにアクセスするためのメカニズムを提供します。BYOD セットアップ用の一連のページを使用して BYOD 設定を行うか、ユーザ選択に基づいて BYOD 設定がバイパスされます。BYOD サービスの設定 （8 ページ）を参照してください。
- **セキュリティ（Security）**：セキュリティは、認証タイプを選択し、外部認証サーバを設定するためのオプションを提供します。セキュリティ （10ページ）を参照してください。

（注） [このサーバを設定（Setup this Server）] ページで選択した項目は保持されません。

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。

DHCP サービスの設定

このページでは、フェールオーバー、DHCPv4、DHCPv6 などのオプションのいずれかまたはすべてを選択して、DHCP サービスを設定できます。

DHCP フェールオーバー

フェールオーバーは、メインサーバが何らかの理由で使用できなくなった場合に、バックアップDHCPサーバがメインサーバを引き継ぐことを許可するように設計されたプロトコルです。このページでは、フェールオーバー関係にあるメイン サーバとバックアップ サーバの DHCP クラスタ名を設定できます。フェールオーバーペアを表示、変更、および削除することもできます。

新しく追加されたフェールオーバー ペアについては、「フェールオーバー ペアの同期」を実行する必要があります。同期の方向を選択できます。初期フェールオーバー設定の場合は、正確または完全な操作を使用します。

- [レポート（Report）] をクリックして、変更セットの詳細を表示します。
- [実行（Run）] <モード> をクリックして、変更を適用します。

DHCPv4

DHCP設定プロセスでは、IPv4アドレスの発行に必要な一連の設定ページを使用します。以下のページは、IPv4 アドレスの発行に必要な設定ページに関連しています。

DHCPv4：[スコープテンプレート（Scope Templates）] ページ

リージョンからローカル クラスタのスコープを作成するには、スコープ テンプレートを作成して後続のページで使用する必要があります。スコープは、DHCPサーバが管理するサブネット内にある1つ以上のダイナミック アドレスの範囲で構成されます。DHCPサーバがクライアントにリースを提供できるようにするには、1 つ以上のスコープを定義する必要があります。

スコープテンプレートで式を指定すると、スコープの作成時にスコープ名、IPアドレス範囲、および組み込みオプションを動的に作成できます。スコープテンプレートを使用すると、複数のスコープを設定する作業が簡単になります。

スコープ テンプレートを作成する手順は次のとおりです。

ステップ 1 [スコープ テンプレート（Scope Templates）] ペインで [スコープ テンプレートの追加（Add Scope templates）] アイコンをクリックします。

ステップ 2 [名前（Name）] フィールドにスコープ テンプレートの名前を入力し、[DHCP スコープテンプレートの追加（Add DHCP Scope template）] をクリックします。

ステップ 3 [保存（Save）] をクリックしてスコープテンプレートを保存し、[次へ（Next）] をクリックして次のページに移動します。

ステップ 4 [スコープ名の式（Scope Name Expression）] テキスト ボックスに「(concat "byod-" subnet)」と入力します。

ステップ 5 [範囲式（Range Expression）] テキスト ボックスに「(create-range first-addr last-addr)」と入力し、[保存（Save）] をクリックしてページを保存します。[次へ（Next）] をクリックします。

ステップ 6 [サブネットの追加（Add Subnet）] をクリックして、サブネットを作成します。

ステップ 7 [アドレス（Address）] フィールドにサブネット IP を入力し（例：10.76.206.0）、[サブネットの追加（Add subnet）] ボタンをクリックします。

ステップ 8 [プッシュ（Push）] アイコンをクリックして、サブネットをローカル クラスタにプッシュします。

ステップ 9 [クラスタ（Cluster）] または [フェールオーバー（Failover）] ドロップダウン リストから、サブネットをプッシュするローカル クラスタのホスト名を選択します。

ステップ 10 [スコープテンプレート（Scope Template）] ドロップダウン リストからスコープ テンプレートを選択します。

ステップ 11 [サブネットのプッシュ（Push Subnet）] ボタンをクリックし、[次へ（Next）] をクリックして **BYOD** の **セットアップ** ページに進みます。

DHCPv4：*[*サブネット（*Subnets*）*]* ページ

このページでは、サブネットを作成、変更、および削除して、ローカルクラスタまたはフェールオーバー ペアにプッシュすることができます。[プッシュ（Push）] アイコンをクリックして、サブネットをプッシュするローカル クラスタのホスト名またはフェールオーバー ペアの名前を選択します。

ステップ 1 [アドレス（Address）] フィールドにサブネット IP を入力し（例：10.76.206.0）、[サブネットの追加（Add subnet）] ボタンをクリックします。

ステップ 2 [プッシュ（Push）] アイコンをクリックして、サブネットをローカル クラスタにプッシュします。

ステップ 3 [クラスタ（Cluster）] または [フェールオーバー（Failover）] ドロップダウン リストから、サブネットをプッシュするローカル クラスタのホスト名を選択します。

ステップ 4 [スコープテンプレート（Scope Template）] ドロップダウン リストからスコープ テンプレートを選択します。

ステップ 5 [サブネットのプッシュ（Push Subnet）] ボタンをクリックし、[次へ（Next）] をクリックして **BYOD のセットアップ** ページに進みます。

DHCPv6

DHCPv6 設定プロセスでは、IPv6 アドレスの発行に必要な一連の設定ページを使用します。以下のページは、DHCP サーバで IPv6 リースを指定する際に必要となる設定に関連しています。

DHCPv6 プレフィックス テンプレート

DHCPv6プレフィックスを直接設定するか、プレフィックステンプレートを作成してプレフィックスを作成できます。

プレフィックスの作成時にプレフィックス テンプレートで式を指定すると、プレフィックス名、IP アドレス範囲、および組み込みオプションを動的に作成できます。

DHCPv6 プレフィックス

DHCPv6プレフィックスを作成、変更、削除し、選択したDHCPv6プレフィックスをローカルクラスタまたはフェールオーバーペアにプッシュすることができます。プレフィックスをプッシュする際、プレフィックス テンプレートは必須ではありません。

BYOD サービスの設定

未登録デバイスに指定する CDNS サーバ IP とリースの有効期間を指定し、[保存（Save）] をクリックする必要があります。この入力に基づいて、未登録デバイス（BYOD_Unregistered）のポリシー設定がリージョン サーバに自動的に作成されます。さらに、BYOD セットアップに必要なクライアント クラス（BYOD_Unregistered および BYOD_Registered）が、リージョン サーバに自動的に作成されます。後続のページで自動作成されたポリシーとクライアント クラスを編集できますが、BYODセットアップを手動で実行する場合を除き、自動作成されたポリシーとクライアント クラスを削除することはできません。

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。

CDNS サーバ

BYOD Web サーバにリダイレクトするスプーフィング DNS として機能する、関連のある CDNS サーバを選択します。BYOD 未登録のデバイスを接続するためのリース時間を設定します。

ポリシーとクライアント クラス

CDNS サーバとリース時間を設定すると、ポリシー（BYOD_Unregistered）およびクライアント クラス（BYOD_Registered と BYOD_Unregistered）が自動的に作成されます。

BYOD：未登録デバイスのスコープ/プレフィックスの作成

このページは、未登録デバイスに IPv4 および IPv6 アドレスのプールを作成する際に役立ちます。

[DHCPv4] タブ

ユーザには、スコープを分割するオプションと既存のスコープにタグを割り当てるオプションという 2 つのオプションがあります。このページには、各クラスタ/フェールオーバー ペアで BYOD が有効になっていないスコープがリストされます。[スコープの分割（Split Scope）] アイコンは、既存のスコープ < スコープ名 > を 2 つに分割します。1つは登録済みデバイス用、もう1つは未登録のデバイス用です。分割が正常に実行されると、ユーザは、サブネットが同

じで IP アドレスの範囲が異なる 2 つのスコープが対応するローカル クラスタまたはフェールオーバー ペアに作成されていることを確認できます。新しいスコープ名はBYOD_Unregistered_ < スコープ名 > となり、BYOD_Unregistered タグを選択します。既存のスコープでは、範囲のみが変更されます。

スコープ範囲が未登録の IP アドレスは、ユーザが指定するパーセンテージに基づいて決定されます。たとえば、10.0.0.0/24 サブネットの最大ホスト数は 254 であるため、254 の 10% で 25 ホストとなります。ただし、ホストの数を 2 の累乗で分割してサブネットを検出するため、ホストは 16 個になります。サブネット 10.0.0.0/28 は、Access Control List（ACL：アクセス コントロール リスト）でネットワーク アクセスを制限するために使用されます。上位/先頭が「n」のアドレスが使用され、ルータのサブネット ID と最初の IP アドレスが残されます。このサブネットでは、最大 14 の BYOD デバイスを使用できます。

[タグ（Tag）] アイコンを割り当てると、BYOD デバイスに専用サブネットを割り当てる際に役立ちます。必要な DHCP/CDNS サーバの設定全体が、セットアップ インタビューによって自動的に実行されます。BYOD のリージョン サーバで自動作成されたポリシーとクライアント クラスは、分割または割り当てオプションを初めて実行するときに、ローカル クラスタまたはフェールオーバーペアに自動的にプッシュされます。「デフォルト」のクライアントは、ローカルクライアントデータベースにも作成されます。未登録のデバイスは、すべてこの「デフォルト」のクライアント設定にマッピングされます。

CDNS では、ドメインのリダイレクト機能を使用して未登録のデバイスから BYOD の Web サーバに HTTP リクエストをリダイレクトします。単一の CDNS サーバは、スプーフィング DNS および実際の DNS サーバとして使用できます。「BYODRule」という名前のドメインのリダイレクト ルールと、CDNS サーバ内の「BYOD」という名前の ACL は、最初に分割/割り当て操作が実行されたときに、セットアップインタビューによって自動作成されます。ACL の「一致リスト」は、分割/割り当て操作が実行されるたびにサブネットで更新されます。

（注） 自動作成された BYOD ポリシー/クライアント クラスを削除しても、スコープ/プレフィックスのタグの分割または割り当ては行われません。

[DHCPv6] タブ

DHCPv4 と同様に、ユーザには、プレフィックスを分割するか、タグを既存のプレフィックスに割り当てるかの 2 つのオプションがあります。このページには、各クラスタ/フェールオーバー ペアで BYOD が有効になっていないプレフィックスがリストされます。[プレフィックスの分割（Split Prefix）] アイコンは、既存のプレフィックス < プレフィックス名 > のアドレス範囲（50-50%）を 2 つのプレフィックスに分割します。1 つは登録済みデバイス用、もう 1 つは未登録デバイス用です。分割が正常に実行されると、ユーザは、プレフィックスアドレスが同じで IP アドレスの範囲が異なる 2 つのプレフィックスが対応するローカル クラスタまたはフェールオーバー ペアに作成されていることを確認できます。新しいプレフィックス名は BYOD_Unregistered_ < プレフィックス名 > となり、BYOD_Unregistered タグを選択します。既存のプレフィックスでは、範囲のみが変更されます。[タグの割り当て（Assign a Tag）] アイコンは、BYOD デバイスに専用プレフィックスを割り当てる際に役立ちます。

未登録のスコープを作成するには、次の手順を実行します。

ステップ 1 [スコープの作成（Scope Creation）] ページの [クラスタ（Cluster）] ペインで、クラスタ/フェールオーバーペアを選択します。

ステップ 2 スコープ ツリーからスコープを選択し、パーセンテージ値を入力します。プレフィックスの場合、分割は 50-50 の割合になります。

ステップ 3 [スコープの分割（Split Scope）] アイコンをクリックして BYOD 未登録のスコープの範囲を分割するか、[タグの割り当て（Assign Tag）] アイコンをクリックして、BYOD 未登録のスコープの完全な範囲を割り当てます。

BYOD の HTTPS 設定

BYOD ではキーストア ファイルは必須ではありません。キーストア ファイルがアップロードされていなくても、[デバイス登録（Device Registration）] ページを HTTP でロードできます。キーストア ファイルがアップロードされると、[デバイス登録（Device Registration）] ページをロードする前に HTTP リクエストが HTTPS に自動的にリダイレクトされます。

サーバのリロード

BYOD の CDNS サーバと DHCP サーバに加えられた変更は、対応するサーバを選択し、[サーバのリロード（Reload Servers）] ページの [サーバのリロード（Reload servers）] ボタンをクリックすることで反映されます。

セキュリティ

ドロップダウン リストで認証タイプを選択します（ローカル/Radius/Active Directory）。

認証タイプがローカルの場合、ローカル CCM データベースを使用して、ユーザ名/パスワード クレデンシャルを使用した認証や、Cisco Prime Network Registrar WebUI/CLI/SDK を使用したログインが行われます。

BYOD では、Active Directory サーバの設定が必須です。[デバイス登録（Device Registration）] ページでは、GSSAPI メカニズムを使用して、指定したクレデンシャルの Active Directory に対する検証が実行されます（デフォルト）。

認証タイプが Radius/Active Directory の場合は、次の手順を実行します。

ステップ 1 Radius/Active Directory で、[次へ（Next）] をクリックして対応するサーバを設定します。

ステップ 2 Radius では、[Radiusの追加（Add Radius）] アイコンをクリックします。名前とアドレスを入力し、[外部認証サーバの追加（Add External Authentication Server）] ボタンをクリックします。

ステップ 3 Active Directory では、[Active Directoryサーバの追加（Add Active Directory Server）] アイコンをクリックします。名前、アドレス、およびドメインを入力し、[外部認証サーバの追加（Add External Authentication Server）] ボタンをクリックします。

セットアップ インタビュー サマリー レポート

[セットアップ インタビュー サマリー レポート（Setup Interview Summary Report）] ページには、セットアップページで実行したアクションが要約され、BYOD のスコープ/プレフィックス使用状況レポートが表示されます。

ローカル サービスの設定

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 のインストール時、または 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 （12 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 （12 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 （18 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 （20 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で固有の 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 （24 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」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 （14 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 （14 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 （17 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 クラスを割り当てる場合は、*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 （15 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 クラスを割り当てる 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 （15 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 （16 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、『』 の「*Configuring Clients*」の項 *Cisco Prime Network Registrar 10.1 DHCP* ユーザ ガイド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、『』の「*Configuring Clients*」の項 *Cisco Prime Network Registrar 10.1 DHCP* ユーザ ガイド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、『』の「*Editing Clients and Their Embedded Policies*」の項 *Cisco Prime Network Registrar 10.1 DHCP* ユーザ ガイド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 （14 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 （25 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 （20 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 （19 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 （20 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 （21 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、マスター通信、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 （23 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。

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マスター名（hostmaster.example.com. など）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(『』の「*Configuring Primary Forward Zones*」 *Cisco Prime Network Registrar 10.1* 権威およびキャッシング *DNS* ユーザ ガイドの項を参照）。[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マスター名（hostmaster.example.com. など）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 (『』の 「*Adding Reverse Zones as Zones*」 *Cisco Prime Network Registrar 10.1* 権威およびキャッシング *DNS* ユーザ ガイドの項を参照）。[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）。
- マスター サーバが応答しているか（masters-responding）応答していないか（masters-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（Set up 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。

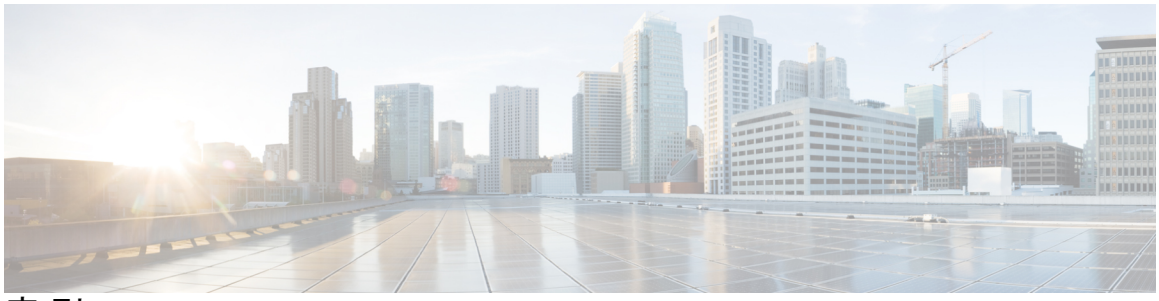
セットアップ インタビュー タスク

[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。



索 引

は

ほ

め

れ