中央構成の管理

この章では、Cisco Prime Network Registrar リージョン クラスタで中央構成を管理する方法について説明します。

中央構成タスク

リージョン クラスタでの中央構成管理には、次のものが含まれます。

- サーバー クラスタのセットアップ、データの複製、およびDHCP使用率とリース履歴データのポーリング。
- ルータのセットアップ（ルータおよびルータ インターフェイスの管理 を参照）。

- DHCP スコープテンプレート、ポリシー、クライアントクラス、オプション、ネットワーク、バーチャル プライベート ネットワーク（VPN）などのネットワーク オブジェクトの管理。
- DHCP フェールオーバー サーバー ペアの管理。

これらの機能は、central-cfg-admin ロールが割り当てられている管理者のみが使用できます。（central-cfg-admin の機能の完全なリストについては、表 2 を使用してください）。中央構成管理には、管理者のセットアップやリージョン サーバーのステータスの確認は含まれません。これらの機能は、従来のライセンスの使用 （19 ページ） および サーバーの管理 で説明されているように、リージョン管理者によって実行されます。

Cisco Prime Network Registrar サービスのデフォルト ポート

次の表に、Cisco Prime Network Registrar サービスに使用されるデフォルトのポートを示します。

表 *1 : Cisco Prime Network Registrar* サービスのデフォルト ポート

ポート番号	プロトコル	サービス
53	TCP/UDP	DNS
53	TCP/UDP	DNS のキャッシング
67	UDP	DHCP クライアントからサーバーへ
68	UDP	DHCP サーバーからクライアントへ
69	UDP	TFTP（オプション）クライアントからサーバーへ
162	TCP	SNMP トラップ サーバーからサーバーへ
389	TCP	DHCP サーバーから LDAP サーバーへ
546	UDP	DHCPv6 サーバーからクライアントへ
547	UDP	DHCPv6 クライアントからサーバーへ
647	TCP	DHCP フェールオーバー サーバーからサーバーへ
653	TCP	高可用性（HA）DNS サーバーからサーバーへ
853	TCP	DNS over TLS

ポート番号	プロトコル	サービス
1234	TCP	ローカル クラスタ CCM サーバーからサーバーへ
1244	TCP	リージョン クラスタ CCM サーバーからサーバーへ
4444	TCP	SNMP クライアントからサーバーへ
8080	HTTP	ローカル クラスタ クライアントからサーバー Web UI へ
8090	HTTP	リージョン クラスタ クライアントからサーバー Web UI へ
8443	HTTPS	ローカル クラスタ セキュア クライアントからサーバー Web UI へ
8453	HTTPS	リージョン クラスタ セキュア クライアントからサーバー Web UI へ

ファイアウォールの考慮事項

DNS（キャッシングまたは権限）サーバーがステートフル ファイアウォールの背後に展開されている場合（物理ハードウェアまたは conntrack などのソフトウェア）、次のことを行うことをお勧めします。

- 可能な場合は、少なくとも UDP DNS トラフィックについて、ステートフル サポートを無効にします。
- ステートフル サポートを無効にできない場合は、許可状態テーブル エントリの数を大幅に増加させる必要があります。

通常、DNS クエリは多くの異なるクライアントから着信し、同じクライアントからの要求が異なる送信元ポートを使用する場合があります。毎秒数千のクエリがあると、これらのさまざまなソースの数が大きくなり、ファイアウォールがステートフル トラッキングを使用している場合は、この状態を維持し、一定期間にわたって実行する必要があります。したがって、クエリ トラフィック レートと状態時間間隔を指定して、ファイアウォールが十分な状態を維持できるようにする必要があります。

ファイアウォールを使用している場合は、使用しているサービスに応じて、一部のポート（Cisco Prime Network Registrar サービスのデフォルト ポート （2 ページ）を参照）に対してファイアウォールを開く必要があります。

DNS パフォーマンスとファイアウォール接続追跡

（注） Red Hat および CentOS Linux の多くのディストリビューションでは、デフォルトで、ファイアウォールと接続追跡がインストールされ、有効になります。

Cisco Prime Network Registrar のキャッシングおよび権威 DNS サーバーは、毎秒処理クエリ数（QPS）が非常に大きくなるように設計されており、多くの場合、それを実現するように展開されます。通常、クエリの大部分は、解決時間の短い UDP ベースであり、さまざまな送信元ポートを持つ多数のクライアントから送信されます。DNS トラフィックのファイアウォール接続追跡が使用されている場合、ファイアウォールはこれらの要求を追跡用の新しい接続として扱います。UDP はコネクションレス型プロトコルであるため、ファイアウォールは接続のモニターリングを停止するために接続タイムアウトに依存する必要があります。ファイアウォール接続モニターリングタイムアウトは、通常、DNS 解決時間に比べて非常に長いため、ファイアウォールは、完了した要求をモニターするために引き続きリソースを使用します。これにより、ファイアウォールが設定制限にすぐに達し、最大 90% の要求がドロップされて DNS サーバーに到達しないため、DNS パフォーマンスが大幅に低下します。

シスコでは、DNS サーバーのオペレーティングシステム上でファイアウォールを使用しないことを強くお勧めします。ファイアウォールは、DNS サーバーの OS の外部にある個別のアプライアンスで実行してください。ファイアウォールを無効にできない場合は、DNS トラフィックの接続追跡を無効にする必要があります。DNS 接続追跡が無効になっていても、ファイアウォールが同じ場所に配置されていると、システムと DNS のパフォーマンスが 25 ー 30 % 低下する可能性があることに注意してください。

（注） シスコは、DNS トラフィックのファイアウォール接続追跡を使用した展開をサポートしていません。

ファイアウォールの無効化

次に、ファイアウォールの停止と無効化の例を示します。CentOS 7 または Red Hat 7 および 8 は **firewalld** を使用します。これらのコマンドはルートとして実行する必要があることに注意してください。

firewalld

```
# systemctl stop firewalld
# systemctl disable firewalld
```

DNS トラフィックの接続追跡の無効化

DNS のファイアウォール接続追跡を無効にする例を次に示します。CentOS 7 または Red Hat 7 および 8 は **firewalld** または **firewall-cmd** を使用します。これらのコマンドはルートとして実行する必要があり、IPv4 と IPv6 には個別の設定があることに注意してください。

firewall-cmd（IPv4）

```
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p udp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p udp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p udp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p udp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p udp --dport 53 -j
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p udp --sport 53 -j
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p udp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p udp --sport 53
-j ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p tcp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw OUTPUT 0 -p tcp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p tcp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 raw PREROUTING 0 -p tcp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p tcp --dport 53 -j
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p tcp --sport 53 -j
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp --sport 53
-j ACCEPT
```

firewall-cmd（IPv6）

```
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p udp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p udp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p udp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p udp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p udp --dport 53 -j
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p udp --sport 53 -j
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p udp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p udp --sport 53
-j ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p tcp --dport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw OUTPUT 0 -p tcp --sport 53 -j
CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p tcp --dport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 raw PREROUTING 0 -p tcp --sport 53
-j CT --notrack
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p tcp --dport 53 -j
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p tcp --sport 53 -j
```

```
 ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p tcp --dport 53
-j ACCEPT
# firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -p tcp --sport 53
-j ACCEPT
```

Umbrella を使用するためのキャッシュ DNS の設定

Cisco Umbrella は、フィッシングやマルウェアなどのインターネット上の脅威に対する防御の最前線となります。Umbrella を解決に使用するようにキャッシング DNS を設定することにより、シスコの Umbrella のクラウドサービスで、要求されたドメイン/ホストに関する最新の応答を提供することが可能になります。詳細については、『*Cisco Prime Network Registrar 11.1* 権威およびキャッシング *DNS* ユーザ ガイド』の「Umbrella を使用するためのキャッシュ DNS の設定」の項を参照してください。

（注） Umbrella サービスを最大限に活用するには、Cisco Umbrella とビジネス関係を持つ必要があります。

ライセンシング

Cisco Prime Network Registrar には、CCM、権威 DNS、キャッシング DNS、および DHCP サービス、またはこれらのサービスの組み合わせに対して個別のライセンスが必要です。Cisco Prime Network Registrar 11.1 のライセンスファイルには、ライセンスの永続部分およびサブスクリプション部分に対応する 2 組のライセンスが含まれています。将来のアップグレードにはサブスクリプション ライセンスを購入する必要があります。初期サブスクリプションは常に 3 年間で、更新によって 1 年間延長されます。ライセンシングに関する詳細は、『*Cisco Prime Network Registrar 11.1* インストール ガイド』の「ライセンス ファイル」の項を参照してください。

ログイン後に、リージョンサーバーに追加のサービスベースのライセンスを追加できます。ファイルからロードされた個々のライセンスは削除しないでください。アップグレード後には古いバージョンの DNS および DHCP ライセンスを削除できます。サーバーがアップグレードされていない場合は、古いバージョンの CDNS ライセンスを保持する必要があります。

Cisco Prime Network Registrar 11.1 は、スマートライセンシングと従来のライセンシングの両方をサポートしています。ただし、ハイブリッドモデルはサポートされていません。つまり、一度に使用できるのは、どちらか 1 つのライセンスタイプです。Cisco Prime Network Registrar の以前のバージョン（10.x 以前）では、FLEXlmライセンスのみがサポートされていました。このライセンスでは、あるバージョンの永久ライセンスを購入し、Cisco Prime Network Registrar サーバーが新しいメジャーバージョンにアップグレードされるまで使用します。その時点で、新しいライセンスを購入する必要があり、このサイクルが繰り返されます。この方法の欠点の 1 つは、Cisco Prime Network Registrar サーバーがアップグレードまたは購入されるたびに、ライセンスファイルが電子メールで配信されることです。このファイルは、リージョンサーバーにロードしてアプリケーションを有効にします。

スマートライセンシングは従来型の別のライセンシングシステムではありません。これは、ライセンスが個々のシスコ製品にインストールされないソフトウェア資産管理システムに似ているものと見なすことができます。従来のソフトウェアモデルよりも大幅に柔軟性が高く、ライセンスのアクティブ化と管理が簡単になります。シスコライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

次のトピックでは、 Cisco Prime Network Registrar でのシスコのスマートライセンシングと従来のライセンシングの使用方法について説明します。

- シスコ スマート ライセンスの使用 （7 ページ）
- 従来のライセンスの使用 （19 ページ）

シスコ スマート ライセンスの使用

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコ ライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

スマートライセンシングの場合、購入したすべてのライセンスは顧客固有のスマートアカウントの Cisco Smart Software Manager（CSSM）または CSSM On-Prem（サテライト）という一元化されたシステム内に保持されます。Cisco Prime Network Registrar サーバー（リージョン）は、定期的にライセンス使用情報を CSSM またはサテライトに送信します。スマートアカウントにログインすると、ライセンス使用率情報を取得できます。

Cisco Prime Network Registrar では、スマートライセンシングがデフォルトで有効になっています。何らかの理由で無効にしていた場合は有効にしてから Web UI または CLI を使用して Cisco Prime Network Registrar を CSSM（またはサテライト）に登録します。この登録が成功するまで、評価モード（最大 90 日）になります。評価モードの間は、評価期間が終了するまでは選択した機能のライセンスが付与されています。90 日間の評価期間後、製品が CSSM（またはサテライト）に登録されていない場合か、または予約もインストールされていない場合は、すべての機能がコンプライアンス違反（OOC）としてマークされます。スマートライセンスは有効なままとなり、引き続き Cisco Prime Network Registrar を CSSM（またはサテライト）に登録するか、または予約をインストールすることができます。登録が成功すると、すべての Cisco

Prime Network Registrar ライセンスタイプが CSSM（またはサテライト）で使用可能になります。

以降のトピックでは、Cisco Smart Licensing を使用して Cisco Prime Network Registrar のライセンスをセットアップし、管理する方法について説明します。

Cisco Prime Network Registrar でのスマートライセンシングのセットアップ

Cisco Smart Licensing をセットアップしてライセンスの管理に使用できるようにするには、次の手順を実行します。

ステップ 1 Cisco Prime Network Registrar では、スマートライセンシングがデフォルトで有効になっています。何らかの理由で無効にしている場合は、有効にしてください。スマート ライセンスの有効化 （8 ページ）を参照してください。

ステップ 2 Cisco Systems でスマート アカウントを作成します。これを実行するには、Smart Account Request に移動し、Web サイトの指示に従います。

ステップ 3 Cisco Prime Network Registrar と CSSM（またはサテライト）間の通信をセットアップします。Cisco Prime Network Registrar と CSSM 間のトランスポートモードの設定 （9 ページ）を参照してください。

ステップ 4 Web UI または CLI を使用して CSSM（またはサテライト）に Cisco Prime Network Registrar を登録します。CSSM（またはサテライト）への Cisco Prime Network Registrar の登録 （10 ページ）を参照してください。

ステップ 5 スマートライセンスの使用状況をモニターします。スマートライセンスの使用状況の表示 （11 ページ）を参照してください。

スマート ライセンスの有効化

Cisco Prime Network Registrar では、新規インストールと以前のバージョンからのアップグレードの両方で、スマートライセンシングがデフォルトで有効になっています。何らかの理由でスマートライセンシングを無効にした場合は、次の手順を実行して有効にします。

リージョン詳細 *Web UI*

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 2 [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページの [スマート ソフトウェア ライセンシングを使用する（Use Smart Software Licensing）] ボタンをクリックします。

次のタスク

Cisco Prime Network Registrar と CSSM 間のトランスポートモードの設定 （9 ページ）の説明に従って、Cisco Prime Network Registrar と CSSM（またはサテライト）間の転送モードを設定します。

CLI コマンド

smart コマンドを使用してスマート ライセンシング コンフィギュレーションモードを有効にし、**license smart enable** コマンドを使用してスマートライセンシングを有効にします。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart enable
```

Cisco Prime Network Registrar と CSSM 間のトランスポートモードの設定

Cisco Prime Network Registrar リージョンサーバーは、転送設定に基づいて Call Home またはスマートトランスポートを使用して CSSM と通信します。Call Home がデフォルトの転送設定です。Cisco Prime Network Registrar のスマートエージェントと CSSM の間で通信が確立されます。

（注） 通信にスマートトランスポートを使用する場合は、CSSM サーバーの URL を明示的にデフォルトまたはカスタム URL に設定する必要があります。これを行うには、**license smart url [default | *url*]** コマンドを使用します。

（注） スマートトランスポートは、libcurl（OpenSSL で構築）に依存します。システムに存在する libcurl が OpenSSL で構築されていない場合、CSSM との通信は成功しません。この状況では、Call Home をトランスポート設定として使用するか、またはシステムに libcurl（OpenSSL で構築）をインストールする必要があります。

Cisco Prime Network Registrar と CSSM 間でトランスポートモードを設定するには、次の手順を実行します。

リージョン詳細 *Web UI*

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 2 [トランスポート設定（Transport Settings）] の横にある [表示/編集（View/Edit）] リンクをクリックして、[トランスポート設定（Transport Settings）] ページを開きます。通信モード（[Call Home設定（Call Home Settings）] または [スマートトランスポート設定（Smart Transport Settings）] の下）を選択します。

- [直接モード（Direct mode）]：Cisco Prime Network Registrar はインターネットを介して使用率情報を直接送信します。追加のコンポーネントは必要ありません。
- [トランスポートゲートウェイ（Transport Gateway）]：Cisco Prime Network Registrar はローカルにインストールされたサテライトに使用率情報を送信します。サテライトとの同期を維持するために、シスコと情報を定期的に交換します。この同期は、接続された環境では自動的に行われ、切断された環境では手動で行われます。

- [HTTP/HTTPS プロキシ（HTTP/HTTPS Proxy）]：Cisco Prime Network Registrar はプロキシサーバーを使用してインターネット経由で使用率情報を送信します。すべての市販のプロキシが動作します。

ステップ 3 [保存（Save）] をクリックして、転送設定を保存します。

次のタスク

Cisco Prime Network Registrar を CSSM（またはサテライト）にまだ登録していない場合、Cisco Prime Network Registrar は評価モードで実行します（90 日の制限があります）。CSSM（またはサテライト）への Cisco Prime Network Registrar の登録 （10 ページ）の説明に従い、製品を登録します。

CLI コマンド

smart コマンドを使用して スマート ライセンス コンフィギュレーション モードを有効にしてから、**license smart transport [callhome | smart]** コマンドを使用してスマートライセンシングのトランスポートタイプを設定します。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart transport [callhome | smart]
```

次に、

- **callhome** トランスポート設定を使用する場合は、次のコマンドを使用して URL を指定します。

  ```
  nrcmd-R [smartlic]> call-home destination address http url
  ```

- **smart** トランスポート設定を使用する場合は、次のコマンドを使用して URL を指定します。

  ```
  nrcmd-R [smartlic]> license smart url [default|url]
  ```

CSSM（またはサテライト）への Cisco Prime Network Registrar の登録

Cisco Prime Network Registrar を CSSM（またはサテライト）に登録するには、CSSM（またはサテライト）からトークンを取得し、Cisco Prime Network Registrar の Web UI または CLI に入力する必要があります。この作業が必要になるのは 1 回限りです。

始める前に

Cisco Systems のスマートアカウントが必要です。スマートアカウントがない場合は、「Smart Account Request」に移動し、Web サイトの指示に従います。また、[トランスポート設定（Transport Settings）]（Cisco Prime Network Registrar の [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページ）で指定された URL に接続できることを確認します。

ステップ 1 CSSM または Smart Software Manager サテライトでスマートアカウントにログインします。

ステップ 2 この製品インスタンスで使用するライセンスが含まれている仮想アカウントに移動します。

ステップ 3 製品インスタンスの登録トークン（これによりスマートアカウントを識別）を生成し、そのトークンをコピーするか、または保存します。

リージョン詳細 Web UI

ステップ 4 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 5 [登録（Register）] ボタンをクリックして、[スマート ソフトウェア ライセンシング製品登録（Smart Software Licensing Product Registration）] ページを開きます。

ステップ 6 CSSM または Smart Software Manager サテライトから生成した製品インスタンス登録トークンを貼り付けます。

ステップ 7 [登録（Register）] をクリックします。

CLI コマンド

smart コマンドを使用してスマート ライセンス コンフィギュレーション モードを有効にし、次に **license smart register idtoken** *token* を使用して CSSM（またはサテライト）に Cisco Prime Network Registar を登録します。ここで、 *token* は CSSM（またはサテライト）から作成した製品インスタンス登録トークンです。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart register idtoken token
```

スマートライセンスの使用状況の表示

スマートライセンシングが有効になっている場合、Cisco Prime Network Registrar は、ライセンスのリース数（DHCP の場合）、RR の数（権威 DNS の場合）、およびキャッシング DNS サーバーの数に関する情報を表示しません。実際のライセンス数については、CSSM（またはサテライト）を参照する必要があります。ただし、Cisco Prime Network Registrar の Web UI または CLI を使用して、現在使用中のライセンス数を表示できます。

リージョン詳細Web UI

現在のライセンスの使用状況を Web UI に表示するには、[管理（Administration）] メニューから [ユーザーアクセス（User Access）] サブメニューの [スマートライセンシング（Smart Licenses）] を選択します。スマートライセンスの使用状況の詳細は、ページ下部の [スマートライセンスの使用状況（Smart License Usage）] セクションで確認できます。

CLI コマンド

smart コマンドを使用してスマート ライセンス コンフィギュレーション モードを有効にしてから、**show license summary** コマンドを使用して、システムで現在使用されているライセンスの承認状態とそれらのライセンスを表示します。

```
nrcmd-R> smart

nrcmd-R [smartlic]> show license summary
```

ライセンスの承認と ID 証明書の更新

ライセンス承認の更新

登録後、スマートエージェントは、CSSM（またはサテライト）に送信された権限付与要求に対する正常な応答を受信すると、承認済みまたはコンプライアンス違反の状態になります。承認期間はスマート ライセンシング システムによって 30 日ごとに自動的に更新されます。ライセンスが「承認済み」または「コンプライアンス違反」の状態にある限り、認証期間が更新されます。

次の更新サイクルまで 30 日間待機しないように手動で承認を更新するには、次の手順を実行します。

リージョン詳細*Web UI*

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 2 [アクション（Actions）] ボタンをクリックし、[今すぐ承認を更新する（Renew Authorization Now）] をクリックします。

承認期間が終了すると（90日後）、承認期限切れ状態が開始されます。

CLI コマンド

smart コマンドを使用してスマート ライセンス コンフィギュレーションモードを有効にし、**license smart renew auth** コマンドを使用して手動で承認を更新します。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart renew auth
```

ID 証明書の更新

ID 証明書の有効期限は 1 年です。6 ヵ月経過すると、エージェントは証明書の更新を試みます。エージェントがCSSMと通信できない場合は、有効期限（1年）までID証明書の更新を試みます。1年が経過すると、エージェントは未識別状態に戻り、評価期間の有効化を試みます。CSSM は製品インスタンスをデータベースから削除します。

ID 証明書を手動で更新するには、次の手順を実行します。

リージョン詳細*Web UI*

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 2 [アクション（Actions）] ボタンをクリックし、[今すぐ登録を更新する（Renew Registration Now）] をクリックします。

CLI コマンド

smart コマンドを使用してスマート ライセンス コンフィギュレーションモードを有効にし、**license smart renew ID** コマンドを使用して手動で ID 証明書を更新します。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart renew ID
```

CSSM（またはサテライト）への Cisco Prime Network Register の再登録

Cisco Prime Network Register と CSSM（またはサテライト）間の通信障害が原因で登録が失敗した場合は、製品の登録を再試行できます。Cisco Prime Network Register を CSSM（またはサテライト）に再登録するには、次の手順を実行します。

始める前に

CSSM（またはサテライト）から製品インスタンスの登録トークンを取得していることを確認します。詳細については、CSSM（またはサテライト）への Cisco Prime Network Registrar の登録 （10 ページ）を参照してください。

リージョン詳細Web UI

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 2 [アクション（Actions）] ボタンをクリックし、[再登録（ReRegister）] をクリックします。

CLI コマンド

smart コマンドを使用してスマート ライセンス コンフィギュレーション モードを有効にし、次に **license smart register idtoken** *token* [**force**] コマンドを使用して Cisco Prime Network Register を CSSM（またはサテライト）に再登録します。ここで、*token* は CSSM（またはサテライト）から生成された製品インスタンス登録トークンです。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart register idtoken token force
```

Cisco Prime Network Register の登録解除

Cisco Prime Network Register リージョンサーバーの登録をキャンセルするには、次の手順を実行します。

リージョン詳細Web UI

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 2 [アクション（Actions）] ボタンをクリックし、[登録解除（DeRegister）] をクリックします。

登録解除後、製品は評価モードに移行し、製品インスタンスが CSSM から削除されます。

CLI コマンド

smart コマンドを使用してスマート ライセンス コンフィギュレーション モードを有効にし、**license smart deregister** コマンドを使用して Cisco Prime Network Register リージョンサーバーの登録をキャンセルします。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart deregister
```

スマート ソフトウェア ライセンスの無効化

Cisco Prime Network Registrar では、スマートライセンシングがデフォルトで有効になっています。何らかの理由でスマートライセンシングを無効にするには（たとえば、従来のライセンシングを使用する場合）、次の手順を実行します。

リージョン詳細Web UI

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [スマートライセンス（Smart Licenses）] を選択して [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページを開きます。

ステップ 2 [アクション（Actions）] ボタンをクリックし、[スマート ソフトウェア ライセンシングの無効化（Disable Smart Software Licensing）] をクリックします。

CLI コマンド

smart コマンドを使用してスマート ライセンシング コンフィギュレーションモードを有効にし、**no license smart enable** コマンドを使用してスマートライセンシングを無効にします。

```
nrcmd-R> smart

nrcmd-R [smartlic]> no license smart enable
```

スマートライセンスの予約の使用

Cisco Prime Network Registrar は、リージョンサーバーに対してライセンスのプールを予約できるスマートライセンスの予約モードをサポートしています。CSSMで予約要求コードを指定することで、スマートソフトウェアライセンスを予約できます。この方法では、使用状況情報を

CSSMに通知せずに、製品インスタンスにソフトウェアライセンスを展開できます。これは、安全性の高いネットワークで役立ちます。

スマートライセンスの予約には、次の 2 つのタイプがあります。

- **永久ライセンスの予約（PLR）**：PLR は、外部環境との通信が不可能な安全性が非常に高い環境向けに設計された一連の機能です。永続ライセンスでは、License Authority への定期的なアクセスは必要ありません。PAK ライセンスの場合と同様に、ライセンスを購入して Cisco Prime Network Registrar のライセンスキーをインストールします。
- **特定ライセンスの予約（SLR）**：SLR は、ノードロックライセンシングに似た強制的なライセンシングモデルです。PLR と SLR の主な違いは、SLR では必要なライセンスのみを選択できるのに対し、PLR では製品のすべての機能をアクティブ化する単一のライセンスである点です。スマートアカウントを持つユーザーは、SLR 機能をサポートする製品インスタンスがあれば、SLR 機能を使用できます。

PLR/SLR の有効化

Cisco Prime Network Registrar では、スマートライセンスの予約は CLI を介してのみ設定することができます。

Cisco Prime Network Registrar で PLR/SLR を有効にするには、次の手順を実行します。

ステップ 1 次のコマンドを使用して、Cisco Prime Network Registrar リージョンサーバーでスマートライセンスの予約を有効にします。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart reservation
```

ステップ 2 次のコマンドを使用して要求コードを生成します。この要求コードをコピーするか、ファイルとして保存します。

```
nrcmd-R [smartlic]> license smart reservation request [local | all]
```

（注） Cisco Prime Network Registrar でコードを生成するには、**local** オプションを使用することをお勧めします。

ステップ 3 CSSM に予約要求コードを入力します。

a) CSSM でスマートアカウントにログインします。
b) [ライセンス予約（License Reservation）] ボタンをクリックして、[スマートライセンスの予約（Smart License Reservation）] ページを開きます。
c) [予約要求コード（Reservation Request Code）] テキスト領域に要求コードを貼り付けるか、または [参照（Browse）] オプションを使用してファイルとして追加します。
d) [Next] をクリックします。

ステップ 4 予約するライセンスのタイプ（[PNR-PLR] または [特定のライセンスの予約（Reserve a specific license）]）を選択します。特定のライセンスを選択する場合は、リストから必要な数のライセンスを選択します。[Next] をクリックします。

ステップ 5 前の手順で入力した情報をプレビューして確認し、[認証コードの生成（Generate Authorization Code）] をクリックします。この認証コードをクリップボードにコピーするか、またはファイルとしてダウンロードし、Cisco Prime Network Registrar サーバーに保存します。

ステップ 6 次のいずれかのコマンドを使用して、Cisco Prime Network Registrar に認証コードをインストールします。

- 前の手順で認証コードをコピーした場合は、次のコマンドを使用します。認証コードは二重引用符で囲んでください。

  ```
  nrcmd-R [smartlic]> license smart reservation install auth-code
  ```

- 前の手順で認証コードをファイルとしてダウンロードした場合は、次のコマンドを使用します。

  ```
  nrcmd-R [smartlic]> license smart reservation install file file-path
  ```

（注） 認証コードは長い文字列である可能性があるため、SLR のインストール時にはファイルをインストールするオプションの使用を推奨します。それ以外の場合は、承認コードを二重引用符で囲みます。

予約済みライセンスの更新

CSSM で予約数を更新できます。予約済みライセンスを更新するには、次の手順を実行します。

ステップ 1 CSSM でスマートアカウントにログインします。

ステップ 2 [製品インスタンス（Product Instance）] タブで必要な製品インスタンスに移動し、[アクション（Actions）] > [予約済みライセンスの更新（Update Reserved Licenses）] をクリックします。[ライセンス予約の更新（Update License Reservation）] ページが開きます。

ステップ 3 [特定のライセンスの予約（Reserve a specific license）] オプションボタンを選択し、必要に応じて予約数を更新します。[次へ（Next）] をクリックします。

ステップ 4 [承認コードを生成（Generate Authorization Code）] をクリックします。この認証コードをクリップボードにコピーするか、またはファイルとしてダウンロードし、Cisco Prime Network Registrar サーバーに保存します。

ステップ 5 次のいずれかのコマンドを使用して、Cisco Prime Network Registrar に認証コードをインストールします。このコマンドは、確認コードを生成します。

- 前の手順で認証コードをコピーした場合は、次のコマンドを使用します。認証コードは二重引用符で囲んでください。

  ```
  nrcmd-R [smartlic]> license smart reservation install auth-code
  ```

- 前の手順で認証コードをファイルとしてダウンロードした場合は、次のコマンドを使用します。

  ```
  nrcmd-R [smartlic]> license smart reservation install file file-path
  ```

（注） 認証コードは長い文字列である可能性があるため、SLR のインストール時にはファイルをインストールするオプションの使用を推奨します。それ以外の場合は、承認コードを二重引用符で囲みます。

ステップ 6 CSSM に確認コードを入力します。

a) CSSM の [ライセンス予約の更新（Update License Reservation）] ページに移動し、[確認コードの入力（Enter Confirmation Code）] をクリックします。

b) [予約確認コード（Reservation Confirmation Code）] テキスト領域に確認コードを貼り付けるか、または [参照（Browse）] オプションを使用してファイルとして追加します。

c) [OK] をクリックします。

製品インスタンスの削除

ライセンス予約から製品インスタンスを削除するには、次の手順を実行します。

ステップ 1 次のコマンドを使用してリターンコードを生成します。この要求コードをコピーします。

```
nrcmd-R> smart

nrcmd-R [smartlic]> license smart reservation return [local | all]
```

（注） Cisco Prime Network Registrar でコードを生成するには、**local** オプションを使用することをお勧めします。

ステップ 2 CSSM でスマートアカウントにログインします。

ステップ 3 [製品インスタンス（Product Instance）] タブで必要な製品インスタンスに移動し、[アクション（Actions）] > [削除（Remove）] をクリックします。[製品インスタンスの削除（Remove Product Instance）] ページが開きます。

ステップ 4 [予約リターンコード（Reservation Return Code）] テキスト領域にリターンコードを貼り付けます。

ステップ 5 [製品インスタンスの削除（Remove Product Instance）] をクリックします。

ステップ 6 次のコマンドを使用して、スマートライセンスの予約を無効にします。

```
nrcmd-R> smart

nrcmd-R [smartlic]> no license smart reservation
```

スマート製品の登録とライセンス認証ステータス

製品登録ステータス

ライセンス登録ステータスは、製品が Cisco.com のシスコ スマート ソフトウェア ライセンシングに正常に登録されているかどうかを表します。

ライセンス登録ステータス	説明
未設定/オンボーディング（Unconfigured/Onboarding）	スマートライセンスは初期化されていますが、まだ有効になっていません。スマートライセンシングが無効になっている場合は、Cisco Prime Network Registrar サーバーはこの状態に移行します。
未登録/未確認（Unregistered/Unidentified）	Cisco Prime Network Registrar でスマートライセンシングは有効になっていますが、Cisco Prime Network Registrar は CSSM（またはサテライト）にまだ登録されていません。この状態では、ライセンスが付与された機能を90日間の評価期間中は自由に使用できます。
登録済み（Registered）	Cisco Prime Network Registrar が CSSM（またはサテライト）に登録されています。Cisco Prime Network Registrar は ID 証明書を受信しています。この ID 証明書は、将来シスコのライセンシング担当者との通信に使用されます。証明書は 1 年間有効で、6 ヵ月後に自動的に更新されて継続的な運用が保証されます。
この登録通知の有効期限が切れました（Registration Expired）	Cisco Prime Network Registrar は有効期限までに登録を正常に更新できず、CSSM（またはサテライト）から削除されています。登録の有効期限が切れた後は、新しい登録 ID トークンを使用した CSSM（またはサテライト）への登録が必要です。

ライセンス認証ステータス

ライセンス認証ステータスは、購入したライセンスに対するライセンスの使用状況、および Cisco Smart Licensing に準拠しているかどうかを表しています。購入したライセンス数を超えると、その製品ステータスは**コンプライアンス違反**となります。

ライセンス認証ステータス	説明
評価モード	Cisco Prime Network Registrar は評価モードで実行されています（90 日で期限切れになります）。
承認済み（準拠）（Authorized (In Compliance)）	Cisco Prime Network Registrar に有効なスマート アカウントがあり、登録されています。製品が要求するすべてのライセンスの使用が承認されています。
コンプライアンス違反	Cisco Prime Network Registrar は購入したライセンスの数を超過しています。（特に、製品インスタンスの仮想アカウントに、1 つ以上のライセンス タイプが不足しています）。
評価期限切れ	評価期間が終了し、Cisco Prime Network Registrar はライセンスのない状態になっています。

ライセンス認証ステータス	説明
認証が期限切れ（Authorization Expired）	Cisco Prime Network Registrar は認証の有効期限前にライセンス認証を正常に更新できませんでした。CSSM（またはサテライト）は90日間通信がないため、このサーバーのすべての使用中のライセンスをプールに返します。

従来のライセンスの使用

従来のライセンシングを使用するには、最初にスマートライセンシングを無効にする必要があります（スマート ソフトウェア ライセンスの無効化（14 ページ）を参照）。次に、ライセンスデータを初めて入力する場合は、Web UI へのログインを参照してください。

リージョンクラスタまたはローカルクラスタにログインするときに、システムの全体的なライセンシングステータスが確認されます。有効なシステムライセンスがない場合、ログインは拒否されます。違反があった場合は、違反と詳細が通知されます。この通知は、ユーザー セッションごとに1回だけ実行されます。また、違反を示すメッセージが各ページに表示されるようにすることもできます。

リージョン Web UI

[製品ライセンスの一覧表示/追加（List/Add Product Licenses）]ページを開くには、**Administration > User Access** から **Licenses** を選択します。**Choose File** をクリックしてライセンス ファイルを探し、ファイルをクリックして、**Open** をクリックします。ファイル内のライセンスIDが有効な場合、ライセンス キーがライセンスのリストに表示され、「ライセンス ファイル”*filename*"が正常に追加されました（Successfully added license file “filename".）」というメッセージが表示されます。ID が有効でない場合は、[ライセンス（License）] フィールドにファイルの内容が表示され、「オブジェクトは無効です（Object is invalid）」というメッセージが表示されます。

ページの上部にある [ライセンス使用状況（License Utilization）] セクションには、ライセンスのタイプ、ライセンスに許可されるノード数、および実際に使用されているノード数が表示されます。プラス記号（+）をクリックして、セクションを展開します。ライセンスされた各サービスのライセンス使用状況が、このセクションに個別に表示されます。

[使用権（Right To Use）] と [使用中（In Use）] の数が、ライセンスされた各サービスについて表示されます。使用権の値は、そのサービスに追加されたすべてのライセンスのカウントの集約です。[使用合計（total in use）] の値は、すべてのローカル クラスタから取得された最新の使用率の数値を集約したものです。このセクションには、使用権または使用中カウントがプラスのサービスのみが表示されます。[使用中（In Use）] の数が [使用権（Right To Use）] の数を超えると、「License exceed count」というエラーメッセージが表示されます。

以前のバージョンの Cisco Prime Network Registrar のライセンスと使用数は、別のセクションの「ip-node」に表示されます。

Expert モード 属性を使用すると、すべてのローカル クラスタからライセンス使用率が収集される頻度を指定できます。この設定を変更したときには、サーバーを再起動して、変更を有効にする必要があります。この属性は、[CCM サーバーの編集（Edit CCM Server）] ページで設定できます。デフォルトは 4 時間です。

従来のライセンスの追加

シスコは、製品に付属しているソフトウェア ライセンス請求証明書に従って、Web で Cisco Prime Network Registrar 製品承認キー（PAK）を登録した後、1 つ以上のライセンス ファイルを電子メールでユーザーに送信します。シスコは、FLEXlm システムを通じて従来のライセンスを管理しています。

（注） ライセンスファイルのロードに失敗した場合は、ファイルが適切に書式化されたテキストファイルであり、余分な文字が含まれていないことを確認してください。電子メールからファイルを抽出して、システム間で移動すると、このような問題が発生することがあります。

ファイルがある場合は、次のようにします。

リージョン Web UI

ステップ 1 見つけやすいディレクトリ（またはデスクトップ）にライセンス ファイルを置きます。

ステップ 2 [製品ライセンスの一覧表示/追加（List/Add Product Licenses）] ページで、**Choose File** ボタンをクリックして、各ファイルを参照します。

（注） [製品ライセンスの一覧表示/追加（List/Add Product Licenses）] オプションは、リージョンでのみ使用できます。

ステップ 3 [ファイルの選択（Choose file）] ウィンドウで、最初のライセンス ファイルの場所を検索し、**Open** をクリックします。

ステップ 4 ライセンス キーが受け入れ可能な場合、[スーパーユーザー管理者の追加（Add Superuser Administrator）] ページがすぐに表示されます。

ステップ 5 さらにライセンスを追加するには、**Administration** メニューから、**Licenses User Access** サブメニューの を選択して、[製品ライセンスの一覧表示/追加（List/Add Product Licenses）] ページを開きます。**Choose File** をクリックして、追加のライセンス ファイルを見つけ、**Open** をクリックします。ファイル内のキーが受け入れ可能な場合は、キー、タイプ、カウント、および有効期限が表示され、評価キーであるかどうかも表示されます。キーが受け入れられない場合、ページには、ライセンステキストとエラー メッセージが表示されます。ライセンス タイプのリストについては、従来のライセンスの使用 （19 ページ） を参照してください。

ライセンスのテーブルの上に [ライセンス使用率（License Utilization）] エリアがあります。展開すると、ライセンスのタイプが、使用可能なノードの総数と実際に使用されているノード数とともに表示されます。

Cisco Prime Network Registrar が分散システムとしてインストールされている場合、ライセンス管理はリージョン クラスタから実行されます。ローカル クラスタにライセンスを追加するためのオプションはありません。

CLI コマンド

license ファイルを使用して、**create** ファイルに格納されているライセンスを登録します。参照されるファイルには、コマンドを実行する場所の絶対パスが含まれています。次に例を示します。

```
nrcmd-R> license "C:\licenses\product.licenses" create
```

license list を使用して、作成されたすべてのライセンス（キーによって識別されます）のプロパティを一覧表示し、**license listnames** を使用して、キーだけを一覧表示します。特定のライセンス キーのプロパティを表示するには、**license** キー **show** を使用します。

ライセンス履歴

[ライセンス履歴（License History）] ページでは、指定された時間内に使用されたライセンスを表示できます。ライセンス履歴をチャート形式で表示できます。ここでは、一定期間にわたるさまざまなサービスのライセンス使用状況履歴を 1 つのビューで確認できます。また、データは時系列の逆順で表示されるため、最新のデータが上部に表示されます。設定された使用とサービスに基づいて、チャートの Y 軸は異なる場合があります。

ライセンス履歴を表示するには、次の手順を実行します。

リージョン Web UI

ステップ 1 **Administration** メニューから [**ユーザー アクセス（User Access**）] サブメニューの **License History** を選択して、[ライセンス使用状況履歴の表示（View License Utilization History）] ページを開きます。

ステップ 2 [**ライセンス履歴フィルタの設定（Set License History Ffilter**）] 属性でフィルタ設定を指定します。指定された数の時間バケットに収まるようにフィルタ オプションに一致するデータセットをダウンサンプリングするには、[**結果のダウンサンプリング（Down-sample results**）] チェックボックスをオンにします。

ステップ 3 [**フィルタの適用（Apply Filter**）] をクリックして、指定した時間枠のライセンス履歴を表示します。

- 詳細は、[**ライセンス履歴チャート（License History Charts**）] タブにチャート形式で表示されます。チャートの下にある [**チャート タイプ（Chart Type**）] アイコンをクリックして、チャート タイプを変更できます。使用可能なチャートのタイプは、縦棒グラフ、折れ線グラフ、面グラフ、および散布図です。チャートの下にある [**テーブル ビュー（Table View**）] アイコンをクリックすると、チャート データが表形式で表示されます。
- [**ライセンス テーブル（License Table**）] タブをクリックすると、ライセンス履歴の詳細が表形式で表示されます。

CLI コマンド

すべてまたは選択したサービスの経時的なライセンス使用履歴を表示するには、**license showUtilHistory** [**-start** *start-time*] [**-end** *end-time*] [**-service cdns** | **dns** | **dhcp** |...| **all**] コマンドを使用します。

ライセンス使用率

リージョン CCM サーバーは、ローカル クラスタからライセンス使用率情報を定期的に収集し、収集した使用率と登録済みライセンスに基づいて、ライセンスが準拠しているかどうかについてローカル クラスタを更新します。

リージョン サーバーは、ローカル クラスタから次のメトリックを収集して、ライセンス数を求めます。

- **DHCP サービス**：アクティブなリース数は、DHCPv4 と DHCPv6 のリースカウントを合計して求められます。

  Cisco Prime Network Registrar 11.0 以降では、DHCPv4 カウントは、次の式で求めます。DHCP サーバーの**サーバー**カテゴリ *active-leases* + *reserved-leases* – *reserved-active-leases* 統計。DHCPv6 カウントは、次の式で求めます。DHCP サーバーの **dhcpv6** カテゴリ *active-leases* + *reserved-leases* – *reserved-active-leases* 統計。

- **認証 DNS サービス** - このカウントは、DNS サーバーの **サーバー** カテゴリの *total-rrs* 統計からのものです。

- **キャッシュ DNS サービス** - CDNS がクラスタでライセンスされている場合、カウントは 1 です。

（注）

- フェールオーバー ペアと HA DNS ペアの場合、1 つのクラスタのみに接続されます。通常、到達可能な場合は main です。リージョンに有効なフェールオーバー ペアと HA DNS 情報がない場合、DHCP または DNS のライセンス使用率の計算が誤っている可能性があります。
- クラスタのレプリカデータが最新であることを確認し（ローカル クラスタとの同期 （27 ページ）を参照）、アドレス空間やゾーンデータをプルします。

CLI コマンド

license showUtilization [**-rescan**] コマンドを使用して、RTU（使用権）に対する使用済み IP ノードの数を表示します。**-rescan** オプションがリージョンで指定されている場合、ローカルクラスタのライセンシングスキャンが開始され、ライセンスの使用率が更新されます。

NAT の背後にあるローカル クラスタの登録

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。最初にリージョン クラスタをインストールし、リージョン クラスタ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 クラスタは、インストール プロセス時にリージョン クラスタに登録することによって、リージョンに登録できます。ただし、ローカル クラスタが NAT インスタンスの背後にある場合、初期要求がリージョン クラスタに到達しないため、登録が失敗する可能性があります。

Cisco Prime Network Registrar では、ローカルクラスタから登録を開始することによって、NAT インスタンスの背後にあるローカルクラスタを登録できます。NAT インスタンスによってスパンされているローカルクラスタを登録するには、Cisco Prime Network Registrar 以降がリージョンとローカルの両方のクラスタにインストールされていることを確認する必要があります。また、ローカル クラスタのライセンス使用状況を確認することもできます。

（注） リージョン クラスタが NAT インスタンスの背後にあるときにローカル クラスタを登録するには、リージョン サーバーからローカル クラスタを登録し、サービスを選択して、データを再同期することによって、リージョン サーバーからローカル クラスタを登録する必要があります。

NAT インスタンスの背後にあるローカル クラスタを登録するには、次の手順を実行します。

ローカル Web UI

ステップ 1 **Administration** メニューから、**User Access** サブメニューの **Licenses** を選択して [List Licenses] ページを開きます。

[ライセンスの一覧表示（List Licenses）] ページで、リージョン クラスタの詳細を追加します。

a) リージョン クラスタの IP アドレス（IPv4 または IPv6）を入力します。
b) リージョン クラスタの SCP ポートを入力します（1244 がプリセット値です）。
c) 登録するローカル クラスタの IP アドレス（IPv4 または IPv6）を選択します。
d) ローカル クラスタに登録するコンポーネント サービスを選択します。

ステップ 2 [**登録（Register）**] をクリックします。

（注） リージョンCCMサーバーは、カウントされたすべてのサービス（DHCP、DNS、およびCDNS）について、Cisco Prime Network Registrar システム内のすべてのローカル クラスタのライセンス使用状況履歴を維持します。

ローカル クラスタのライセンス使用状況を表示するには、[**ポーリング ステータスのチェック（Check Poll Status**）] をクリックします。

新しい UUID の生成

新しい UUID を生成して登録するには、次の手順を実行します。

ローカル Web UI

ステップ 1 [管理（Administration）] メニューから、[ユーザーアクセス（User Access）] サブメニューの [ライセンス（Licenses）] を選択して [ラインセンスの一覧表示（List Licenses）] ページを開きます。

ステップ 2 リージョンクラスタの詳細を追加します。

ステップ 3 [新しいホスト識別子の生成（Generate new host identifier）] チェックボックスをオンにします。
ステップ 4 [登録（Register）] をクリックします。

CLI コマンド

ローカル クラスタを登録または再登録するには、次のコマンドを使用します。

```
nrcmd> license register [cdns|dns|dhcp[,...]] [<regional-ip>|<regional-ipv6>]
[<regional-port>] [-new-uuid]
nrcmd> license register cdns|dns|dhcp[,...] <regional-ip> <regional-ipv6> [<regional-port>]
 [-new-uuid]
```

サーバー クラスタの設定

サーバー クラスタは、ローカル クラスタの場所にある CCM、DNS、CDNS、 DHCP、および TFTP サーバーのグループです。たとえば、組織には、DNS サーバーと DHCP サーバーの Boston および Chicago クラスタが存在する場合があります。中央管理者は、これらのクラスタでのアドレスの割り当て方法に影響を与えるか、または DHCP 使用率またはリース履歴データをポーリングすることができます。中央管理者は、必要な権限が存在する場合、サーバーの変更の表示または再起動のために、これらのローカル クラスタに接続することもできます。

[クラスタ サーバーのツリーの表示（View Tree of Cluster Servers）] ページで、作成したクラスタを表示します。これを表示するには、**Clusters** をクリックします。ページにクラスタが入力されると、いくつかの豊富な情報が表示され、いくつかの有用な機能が提供されます。ローカル クラスタに同等の管理者アカウントが存在する場合、[ローカルに移動（Go Local）] アイコンを使用して、ローカル クラスタ Web UI へのシングルサインオンが可能になります。

[クラスタのツリーの表示（View Tree of Clusters）] ページは、[リモート クラスタのリスト/追加（List/Add Remote Clusters）] ページで手動でクラスタを追加することによって、またはサーバー クラスタも作成するルータの追加および同期によって自動的に値が入力されている場合があります。クラスタ名は、クリックしてクラスタ情報を編集できるリンクです。再同期、レプリケーション、およびポーリング機能については、この章で詳しく説明します。

DHCP サーバーには、クラスタの DHCP サーバーの横に [関連サーバー（Related Servers）] アイコンが表示される場合があります。このアイコンをクリックすると、[DHCP サーバーの関連サーバーのリスト（List Related Servers for DHCP Server）] ページが表示されます。これらのサーバーは、DNS、TFTP、 または DHCP フェールオーバー サーバーです。

ローカル クラスタの追加

リージョン クラスタへのローカル クラスタの追加は、central-cfg-admin ロールの中核機能です。

クラスタを追加するために必要な最小限の値は、マシン名、IP アドレス（IPv4 または IPv6）、管理者のユーザー名、およびパスワードです。クラスタ名は一意である必要があり、その IP アドレスは CNRDB データベースが配置されているホストと一致している必要があります。ローカル クラスタ管理者から SCP および HTTP ポート、ユーザー名、およびパスワードを取

得します。Cisco Prime Network Registrar の SCP ポートのインストールのプリセット値は 1234 であり、HTTP ポートは 8080 です。

また、*use-ssl* 属性をオプションまたは必須に設定することで、ローカル サーバーへのアウトバウンド接続をセキュアにするかどうかを設定することもできます。デフォルトでは [オプション（optional）] に設定されており、有効にするには、Cisco Prime Network Registrar Communications Security オプションがインストールされている必要があります。

リージョン Web UI

[操作（Operate）] メニューから、[サーバー（Servers）] サブメニューの [サーバーの管理（Manage Servers）] を選択します。[サーバーの管理（Manage Servers）] ページが開きます。このページでローカル クラスタを確認します。[リモートクラスタの一覧表示/追加（List/Add Remote Clusters）] ページでサーバー クラスタを追加することもできます。[リモートクラスタの一覧表示/追加（List/Add Remote Clusters）] ページには、次の機能があります。

- ローカル管理用のローカル クラスタ Web UI に接続します。
- ローカル クラスタと再同期して、そこで更新を調整します。
- データをリージョン クラスタのレプリカ データベースにプルします。
- レプリカをパージして、クラスタを削除/再追加することなく、不良なレプリカ データをクリアします。レプリカのパージを実行するときには、手動でレプリケーションを実行して、レプリカ データを再度取得する必要があります。

（注） このオプションは、エキスパート モードでのみ表示されます。

- ローカル クラスタに DHCP 使用率データを照会します。この機能は、少なくともサブネット使用率のサブロールを持つregional-addr-admin ロールが割り当てられているユーザーに対してのみ表示されます。
- ローカル クラスタにリース履歴データを照会します。この機能は、少なくともリース履歴サブロールを持つ regional-addr-admin ロールが割り当てられているユーザーに対してのみ表示されます。

クラスタを追加するには、[クラスタの管理（**Manage** Clusters）] ペインの [クラスタの追加（**Add Cluster**）] アイコンをクリックします。[クラスタの追加（Add Cluster）] ダイアログボックスが開きます。ローカル クラスタの追加例については、ローカル クラスタの作成（83 ページ）を参照してください。**Add Cluster** をクリックして、[リモートクラスタの一覧表示/追加（List/Add Remote Clusters）] ページに戻ります。

ローカル Web UI

ローカル Web UI でクラスタを管理することもできます。詳細については、ローカル Web UI でのクラスタの構成 を参照してください。

CLI コマンド

クラスタを追加するには、**cluster** *name* **create** <*address* | *ipv6-address*> [*attribute=value ...*] を使用して、クラスタに名前を付けて、アドレスを指定し、重要な属性を設定します。次に例を示します。

```
nrcmd> cluster example-cluster create 192.168.100.101 admin=admin password=changeme
```

ローカルクラスタで完全に同期するには、管理者がスーパーユーザーである必要があることに注意してください。

ローカル クラスタの編集

リージョン クラスタでのローカル クラスタの編集は、central-cfg-admin ロールのコア機能です。

リージョン Web UI

ローカル クラスタを編集するには、[クラスタの管理（Manage Clusters）] ペインで名前をクリックして、[リモート クラスタの編集（Edit Remote Cluster）] ページを開きます。このページは、基本的には [リモート クラスタのリスト/追加（List/Add Remote Clusters）] ページと同じですが、追加の属性設定解除機能があります。ローカルで実行するサービス（dhcp、dns、cdns、または none）を選択するには、**Local Services** エリアにあるチェックボックスをオンまたはオフにします。変更を行ってから、**Save** をクリックします。

ローカル Web UI

ローカル Web UI でクラスタを編集することもできます。詳細については、ローカル Web UI でのクラスタの構成 を参照してください。

CLI コマンド

ローカル クラスタを編集するには、 **cluster** *name* **set** *attribute=value* [*attribute=value ...*] を使用して、属性を設定またはリセットします。次に例を示します。

```
nrcmd> cluster Example-cluster set poll-replica-interval=8h
```

ローカル クラスタへの接続

Web UI で、ローカル クラスタに同等の管理者アカウントがある場合は、[リモート クラスタのリスト/追加（List/Add Remote Clusters）] ページの [**接続（Connect）**] アイコンをクリックして、ローカル クラスタの [サーバーの管理（Manage Servers）] ページにシングルサインオンできます。リージョン クラスタの Web UI に戻るには、ローカル クラスタ ページの右上隅にある [**戻る（Return）**] アイコンをクリックします。ローカル クラスタで同等のアカウントを持っていない場合、[接続（Connect）] アイコンをクリックすると、ローカル クラスタのログイン ページが開きます。

ローカル クラスタとの同期

同期は、統一された方法で連携できるように、リージョンとローカルのクラスタを設定します。同期するタイミング：

1. ローカル サーバーのリストが、リージョン クラスタにコピーされます。
2. シングルサインオンのために、リージョンとローカルのクラスタ間で共有秘密が確立されます。

同期は、リージョン クラスタにローカル クラスタを作成するときに 1 回実行されます。ただし、変更はローカルクラスタで定期的に実行されることもあり、その場合は同期を再実行する必要があります。たとえば、ローカル接続を行うために使用されるユーザー名とパスワードを変更する場合があります。再同期は自動的に行われません。[リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページの [**再同期（Resync**）] アイコンをクリックする必要があります。結果として、成功の場合は肯定確認、失敗の場合はエラー メッセージが表示されます。

ローカルクラスタをアップグレードするときには、クラスタも再同期する必要があります。同期を有効にするには、ローカルクラスタに指定されたユーザーアカウントがスーパーユーザーである必要があります。同期エラー メッセージが表示された場合は、ローカル クラスタをチェックして、正常に動作していることを確認します。

（注） リージョン クラスタでクラスタを再同期すると、レプリカ データの自動再初期化が行われます。その結果、大規模なサーバー構成の場合、再同期に数分かかることがあります。ただし、レプリカ データを更新するための個別のアクションが不要であるという利点があります。

ローカル クラスタ データの複製

レプリケーションは、ローカル サーバーからリージョン クラスタのレプリカ データベースに設定データをコピーします。レプリケーションは、DHCP オブジェクト データをリージョン サーバー データベースにプルする前に実行する必要があります。レプリケーション時：

1. ローカル データベースの現在のデータがリージョン クラスタにコピーされます。これは通常、一度だけ行われます。
2. 最後のレプリケーション後にプライマリデータベースに加えられた変更がすべてコピーされます。

レプリケーションは所定の時間間隔で行われます。[リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページの [**複製（Replicate**）] アイコンをクリックして、即時レプリケーションを強制することもできます。

[サーバー クラスタの追加（Add Server Cluster）] ページで自動レプリケーション間隔を設定するか、または [サーバー クラスタの編集（Edit Server Cluster）] ページで、*poll-repolica-interval* 属性を使用して調整できます。この間隔は 4 時間に事前設定されています。また、

poll-replica-offset 属性を使用して、レプリカ データをポーリングする固定の時間帯を設定することもできます。デフォルト値は 0 時間（オフセットなし）です。*Poll-replica-rrs* 属性は、他のデータ レプリケーションを無効にせずにRRデータの複製を制御します。この属性は、[サーバーの管理（Manage Servers）] ページと [クラスタの管理（Manage Cluster s）] ページに表示され、値は none、all、および protected です。*poll-replica-rr* が none に設定されている場合、このクラスタの RR データは複製されません。設定を解除すると、CCM サーバーの設定が適用されます。

注意 レプリカ データベースが何らかの方法で破損している場合、リージョン CCM サーバーは起動しません。この問題が発生した場合は、リージョンサービスを停止し、/var/nwreg2/regional/data/replica ディレクトリにあるレプリカ データベース ファイル（および /logs サブディレクトリのログ ファイル）を削除（または移動）してから、リージョンサーバーを再起動します。これを行うと、データ損失なしでレプリカ データベースが再作成されます。

レプリカ データの表示

Web UI では、[操作（**Operate**）] メニューの [サーバー（**Servers**）] サブメニューから [レプリカデータの表示（**View Replica Data**）] を選択することによって、リージョン クラスタのレプリカ データベースにキャッシュされているレプリカ データを表示できます。[レプリカ クラス リストの表示（View Replica Class List）] ページが開きます。

リージョン Web UI

次のものを選択します。

1. [クラスタの選択（Select Cluster）] リストのクラスタ。
2. [クラスの選択（Select Class）] リストのオブジェクト クラス。
3. 選択したクラスタとクラスのデータを複製します。[**クラスタのデータの複製（Replicate Data For Cluster**）] ボタンをクリックします。
4. レプリカ データを表示します。[レプリカ クラス リストの表示（**View Replica Class List**）] をクリックします。選択したオブジェクトのクラスタと特定のクラスの [クラスタのレプリカ データの一覧表示（List Replica Data for Cluster）] ページが開きます。このページでは、次の操作を実行できます。

   - オブジェクトの名前をクリックすると、リージョン クラスタのビューページが開きます。[レプリカの一覧表示（List Replica）] ページに戻るには、**Return to** *object* **List** をクリックします。

（注） [レプリカ アドレス ブロックの一覧表示（List Replica Address Blocks）] および [レプリカ サブネットの一覧表示（List Replica Subnets）] ページでは、この機能は提供されません。ローカル クラスタのアドレス ブロックまたはサブネットを表示するには、[**ローカルに移動（Go local**）] アイコンを使用します。

- [**接続（Connect**）] アイコンをクリックして、ローカル クラスタにあるオブジェクトのリスト ページに移動します。[レプリカ *object* の一覧表示] ページに戻るには、[**戻る（Return**）] アイコンをクリックします。

[クラスタのレプリカ データの一覧表示（List Replica Data for Cluster）] ページの [戻る（**Return**）] をクリックして、[レプリカ クラス リストの表示（View Replica Class List）] ページに戻ります。

レプリカ データのパージ

リージョン Web UI（エキスパート モードのみ）では、[リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページの [**レプリカのパージ（Purge Replica**）] アイコンをクリックすることによって、クラスタを削除/再追加することなく、不良なレプリカ データをクリアできます。レプリカのパージを実行するたびに、手動で複製を実行して、レプリカ データを再度取得する必要があります。

クラスタのデータの非アクティブ化、再アクティブ化、およびリカバリ

ハードディスク エラーが発生して、構成データが失われたと思われる場合は、クラスタの非アクティブ化が必要になることがあります。クラスタを非アクティブ化し、問題を解決し、レプリカ データベースからクラスタ データを回復してから、クラスタを再アクティブ化することができます。これにより、クラスタを削除してから、プロセスで失われたすべてのデータでクラスタを再作成する必要がなくなります。データのリカバリが完了したら、クラスタを再起動する必要があります。

クラスタのデータを非アクティブ化、再アクティブ化、および回復するには、central-config-admin ロールが必要です。

回復されない（手動で復元する必要がある）データには、次のものが含まれます。

- **cnr.conf** ファイルの内容（cnr.conf ファイルの変更 を参照）
- Web UI 構成ファイル
- 保護されていない DNS リソース レコード
- 管理者アカウント

（注） ローカル シークレット db が失われた場合、古い参照は復元されても無効です。パスワードを回復するには、管理者の中央管理を使用してから、それらをローカル クラスタにプッシュする必要があります。ローカル クラスタ パートナー オブジェクトの場合、[リージョンから同期 （sync from regional）] を実行すると、有効なオブジェクトが作成されますが、古いクラスタ オブジェクトを削除しておかなければならない場合があります。

- リース履歴
- 拡張スクリプト

（注） データを別の IP アドレスに復元するには、DHCP フェールオーバー サーバー ペアや高可用性（HA）DNS サーバー ペア アドレスなど、手動での再設定が必要です。

場合によっては、復元操作で「要求されたキー/データペアが見つかりません（Requested key/data pair not found）」というエラーが返されるか、またはローカルクラスタ上の一部のオブジェクトに重複エントリが作成されます。この問題は、復元操作を実行する前に、ローカルクラスタに破損または不正なインデックスを持つオブジェクトがある場合に発生します。これを解決するには、次のいずれかのアクションを実行します。最初のオプションを推奨しますが、常に機能するとは限りません。このような状況でのみ、2 番目のアクションを実行します。

- ローカルクラスタで Cisco Prime Network Registrar を停止し、ローカルクラスタのデータベースに対して rebuild_indexes を実行します。次に、Cisco Prime Network Registrar ローカルクラスタを起動し、復元操作を再試行します。
- ローカルクラスタで Cisco Prime Network Registrar を停止し、データディレクトリの既存の内容をバックアップの場所に移動します。Cisco Prime Network Registrar ローカルクラスタをもう一度起動し、新規データベースを作成します（すべてのデータベースを作成するには 2 つの停止/起動シーケンスが必要です）。ローカルクラスタをリージョンクラスタに登録し、リージョンクラスタから復元操作を実行します。

リージョン Web UI

クラスタの [**非アクティブ化（Deactivate**）] ボタンをクリックして、クラスタを非アクティブします。これにより、ボタンはすぐに [再アクティブ化（Reactivate)] に変わり、クラスタのステータスが表示されます。クラスタを非アクティブ化すると、データの削除、同期、複製、およびDHCP使用率とリース履歴のポーリングが無効化されます。これらの操作は、クラスタが非アクティブになっている間は使用できません。

クラスタを非アクティブにすると、クラスタの [データの回復（Recover Data）] 列に [回復（Recover）] アイコンが表示されます。レプリカ データを回復するには、このアイコンをクリックします。これにより、個別の進行中ステータス ウィンドウが開き、リカバリの進行中は

Web UI ページでの操作ができなくなります。リカバリが成功するとすぐに、無効になっていた機能が再び有効になり、使用可能になります。

クラスタを再アクティブ化するには、[**再アクティブ化（Reactivate**）] ボタンをクリックします。ボタンが [非アクティブ化（Deactivate）] に戻り、ステータスがアクティブとして表示されます。

CLI コマンド

次のクラスタ コマンドは、リージョン クラスタに接続されている場合にのみ使用できます。

表 *2:* クラスタ コマンド

操作	コマンド
アクティブ化	**cluster** *name* **activate**
非アクティブ化	**cluster** *name* **deactivate**
再同期	**cluster** *name* **resynchronize**
同期	**cluster** *name* **sync**
レプリカ データの更新	**cluster** *name* **updateReplicaData**
レプリカ データの削除	**cluster** *name* **removeReplicaData**
データの回復	**cluster** *name* **recoverData**
リース履歴のポーリング	**cluster** *name* **pollLeaseHistory**
リース履歴状態の取得	**cluster** *name* **getLeaseHistoryState**
サブネット使用率のポーリング	**cluster** *name* **pollSubnetUtilization**
レプリカ データの表示	**cluster** *name* **viewReplicaData** < *class-name* | *cli-command* > [**-listbrief** | **-listcsv**]

クラスタ レポートの表示

リージョン Web UI の [クラスタ レポート（Cluster Report）] ページには、選択したクラスタの関連情報がグラフィカル/チャートベースで表示されます。これにより、クラスタ固有のデータをリージョン クラスタから簡単にモニターおよび視覚化できます。このレポート ページには、クラスタ接続のステータス（接続済み、未接続など）が表示されます。また、クラスタでライセンス付与されているサービスのステータス（DHCP がアップ、DNS がダウンなど）、

サーバーの概要、システム メトリック、DNS/CDNS のトップ名、およびリソースの概要も表示されます。

クラスタ レポートを表示するには、次の手順を実行します。

リージョン Web UI

ステップ 1 [操作（**Operate**）] メニューから [**サーバー（Servers**）] サブメニューの [**クラスタの管理（Manage Clusters**）] を選択して、[リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページを開きます。

ステップ 2 左のペインのクラスタの名前をクリックします。

ステップ 3 [リモート クラスタの編集（Edit Remote Cluster）] ページの [**クラスタ レポート（Cluster Report**）] タブをクリックします。選択したクラスタに関連する情報が表示されます。クラスタの現在のシステムおよびリソース メトリックは、チャート/表の形式で表示されます。チャートの下にある [**表示（Show**）] アイコン（Show）を使用すると、データがチャートまたは表形式で表示されます。また、[**チャート タイプ（Chart Type**）] アイコン（）を使用すると、チャートのタイプを変更できます。使用可能なチャートのタイプは、縦棒グラフ、折れ線グラフ、面グラフ、および散布図です。

中央構成管理サーバー

ローカル クラスタとリージョン クラスタの CCM サーバーは、Cisco Prime Network Registrar の動作とユーザー インターフェイスのインフラストラクチャを提供します。CCM サーバーは、Cisco PrimeNetwork Registrarデータベース（CCM DB）の読み取り、書き込み、および変更を行います。CCM サーバーの主な目的は、ユーザーからプロトコル サーバー、およびサーバーからユーザーにデータを保存して伝搬することです。

変更セットは、データ ストアに対する変更の基本単位です。これは、複製サーバーに差分変更を送信し、データ ストアに対する変更の監査ログを提供します。変更セットは、単一のネットワーク オブジェクトに対する 1 つ以上の変更のグループである変更エントリのリストで構成されます。Web UI には、各データ ストアの変更セットのビューが表示されます。

CCM サーバーの管理

ログと起動ログを表示できます。サーバー属性を編集できます。

ログと起動ログを表示するには、ローカル クラスタ Web UI の **Operate** メニューから、[**サーバー（Servers**）] サブメニューの [**サーバーの管理（Manage Servers**）] を選択して、[サーバーの管理（Manage Servers）] ページを開きます。次の表で説明するように、CCM サーバーの *log-settings* 属性を使用して、必要なログカテゴリを有効または無効にします。ログカテゴリは、情報メッセージにのみ適用されます。エラーおよび警告レベルのログメッセージは、常にログファイルに書き込まれます。

表 *3 : CCM* ログ 設定

ログ設定 (数値同等)	説明
all（0）	サーバーに、すべてのカテゴリのメッセージをログに記録させます。この設定はデフォルトでイネーブルになっています。
authentication（2）	サーバーに、ユーザーまたはトークンセッション認証中のメッセージをログに記録させます。
database（1）	サーバーに、シャドウバックアップなどのデータベース操作に関するメッセージをログに記録させます。
dnssec（9）	サーバーに、DNSSEC処理関連のメッセージをログに記録させます。DNSSECキーがCCMサーバーによって作成、削除、有効化、無効化、またはロールオーバーされると、メッセージがログに記録されます。また、サーバーに、ゾーンでDNSSECが無効になったときやゾーンに署名または再署名するタスクがスケジュールされたときにメッセージをログに記録させます。
lease-history（10）	サーバーに、リース履歴ポーリングが開始されたときや終了したときにメッセージをログを記録させます。
licensing（5）	サーバーに、ローカルクラスタ登録に関するメッセージや、リージョンおよびローカルクラスタのライセンス使用状況が収集またはレポートされたときにメッセージをログに記録させます。
replica（7）	サーバーに、レプリカポーリングが開始されたときやローカルクラスタが正常に復元されたときにメッセージをログに記録させます。
scheduled-tasks（4）	サーバーに、CCM サーバーがタスクをスケジュールしたときやスケジュールされたタスクが完了したときにメッセージをログに記録させます。
scp-details（3）	サーバーに、SCP メッセージ応答や CCM と他のサーバーの間の内部 SCP 通信をログに記録させます。CLI や Web UI からの通信などの外部 SCP 要求は、常にログに記録されます。
server-events（6）	サーバーに、プロトコルサーバーから CCM サーバーに送信されたすべてのサーバーイベント（SNMP トラップに関するイベントなど）をログに記録させます。
utilization（8）	サーバーに、使用率ポーリングが開始されたときや終了したときにメッセージをログに記録させます。

CCM サーバーのプロパティの編集

[CCM サーバーの編集（Edit CCM Server）] ページを使用して、CCM サーバーのプロパティを編集できます。

ローカルおよびリージョン Web UI

ステップ 1 CCM サーバーのプロパティにアクセスするには、**Operate** メニューから [**管理（Manage） Servers**] を選択して、[サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 左側の [サーバーの管理（Manage Servers）] ペインの **CCM** をクリックします。[ローカルCCMサーバーの編集（Edit Local CCM Server）] ページが表示されます。このページには、すべての CCM サーバー属性が表示されます。

ステップ 3 必要に応じて設定を変更します。

ステップ 4 **Save** をクリックして、CCM サーバー属性の変更を保存します。

トリビアル ファイル転送

Trivial File Transfer Protocol（TFTP）は、コネクションレス型トランスポート層プロトコルであるユーザー データグラム プロトコル（UDP）を使用して、ネットワーク経由でファイルを転送する方法です。Cisco Prime Network Registrar は TFTP サーバーを保持しているため、システムは Data Over Cable Service Interface Specification（DOCSIS）規格に準拠したケーブル モデムにデバイス プロビジョニング ファイルを提供できます。TFTP サーバーは、ファイルをモデムに送信する際に、DOCSIS ファイルをローカル メモリにバッファします。TFTP 転送の後、サーバーはローカル メモリからファイルをフラッシュします。TFTP は、非 DOCSIS コンフィギュレーション ファイルもサポートしています。

Cisco Prime Network Registrar TFTP サーバーの機能の一部を次に示します。

- RFC 1123、1350、1782、および 1783 に準拠
- 高性能なマルチスレッド アーキテクチャを含む
- IPv6 をサポートします。
- パフォーマンス強化のためにデータをキャッシュ
- Web UI で、および CLI の場合は **tftp** コマンドを使用して設定および制御可能。
- 柔軟なパスとファイルアクセス制御を含む
- TFTP 接続とファイル転送の監査ロギングを含む
- Cisco Prime Network Registrar の /var/nwreg2/{local | regional}/data/tftp にデフォルトのルート ディレクトリがある。

TFTP サーバーの表示と編集

ローカル クラスタで、TFTP サーバーを編集して属性を変更できます。ccm-admin ロールの server-management サブロールが割り当てられている必要があります。

ローカル Web UI

ステップ 1 **Operate** メニューから、**Servers** サブメニューの **Manage Servers** を選択して、[サーバーの管理（Manage Servers）] ページを開きます（サーバーの管理 を参照）。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [TFTP] をクリックして、[ローカルTFTPサーバーの編集（Edit Local TFTP Server）] ページを開きます。

任意の属性の名前をクリックすると、その属性の説明ウィンドウを開くことができます。

ステップ 3 属性値を設定解除するには、[Unset?] 列のチェックボックスをオンにします。

ステップ 4 変更内容を保存するには **Save** をクリックし、変更をキャンセルには **Revert** をクリックします。

CLI コマンド

属性値を表示するには、**tftp show** を使用します。属性を設定または有効にするには、**tftp set** *attribute=value* [*attribute=value ...*] または **tftp enable** *attribute* を使用します。また、**tftp serverLogs show** および **tftp serverLogs nlogs**=*number* **logsize**=*size* を使用することもできます。

TFTP サーバー ネットワーク インターフェイスの管理

TFTP サーバーのネットワーク インターフェイスを管理できます。

ローカル詳細 Web UI

TFTP サーバーに関連付けられているネットワーク インターフェイスを管理するには、[サーバーの管理（Manage Servers）] ページで、選択したローカル TFTP サーバーの **Network Interfaces** タブをクリックします。デフォルトで設定されているネットワーク インターフェイスを表示し、追加のネットワークインターフェイス作成して編集することができます。作成して編集するには、ccm-admin ロールの server-management サブロールが割り当てられている必要があります。

[ネットワーク インターフェイス（Network Interfaces）] ページの列は、次のとおりです。

- **Name**- LAN アダプタ、ループバック、ファスト イーサネット インターフェイスなど、ネットワーク インターフェイスの名前。名前が [Configured Interfaces] 列にある場合、そのインターフェイスを編集および削除できます。名前をクリックすると、[TFTP サーバー ネットワーク インターフェイスの編集（Edit TFTP Server Network Interface）] ページが開き、インターフェイスの名前とアドレスを編集できます。変更を加えてから、このページの **Save** をクリックします。
- **IP Address**- ネットワーク インターフェイスの IP アドレス。
- **IPv6 Address**- ネットワーク インターフェイスの IPv6 アドレス（該当する場合）。
- **Flags**- インターフェイスがゼロブロードキャスト、仮想、v4、v6、非マルチキャスト、または受信専用のいずれであるかを示すフラグ。

- **Configure** - 新しいネットワーク インターフェイスを設定するには、インターフェイス名の横にある [**設定（Configure**）] アイコンをクリックします。これにより、選択したインターフェイスに基づきますが、より一般的な IP アドレスを持つ別のインターフェイスが作成され、この TFTP サーバーの設定済みインターフェイスに追加されます。
- **List of available interfaces for this TFTP server** - ユーザー設定のネットワーク インターフェイス。それぞれの名前と関連付けられたアドレスが表示されます。インターフェイス名をクリックして編集するか、[**削除（Delete**）] アイコンをクリックして削除します。

サーバーの管理に戻るには、**Revert** をクリックします。

CLI コマンド

tftp-interface コマンドを使用します。

簡易ネットワーク管理

Cisco Prime Network Registrar Simple Network Management Protocol（SNMP）通知サポートを使用すると、DHCP および DNS カウンタを照会し、エラー条件と DNS および DHCP サーバーに関する問題の警告を受け、障害または差し迫った障害の条件を示す可能性のあるしきい値条件をモニターすることができます。

Cisco Prime Network Registrar は、SNMPv2c および SNMPv3 標準に従って SNMP トラップ プロトコル データ ユニット（PDU）を実装します。各トラップ PDU には、次のものが含まれます。

- 汎用通知コード（企業固有の場合）。
- 発生したイベントまたはしきい値の超過を示すコードを含む特定通知フィールド。
- 特定のイベントに関する追加情報を含む変数バインディング フィールド。
- SNMPv3 トラップを送信する場合、受信者の設定要件に応じて、オプションのログイン情報が含まれる場合があります。

詳細については、管理情報ベース（MIB）を参照してください。SNMP サーバーは、MIB 属性の読み取りのみをサポートしています。属性への書き込みはサポートされていません。

次の MIB ファイルが必要です。

- **Traps**- CISCO-NETWORK-REGISTRAR-MIB.my および CISCO-EPM-NOTIFICATION-MIB.my
- **DNS server** - CISCO-DNS-SERVER-MIB.my

（注） キャッシング DNS サーバーは、動作するときに DNS MIB のサブセットのみを必要とします。キャッシング DNS サーバーは、*server-start* および *server-stop* 通知イベントのみをサポートします。

- **DHCPv4 server** - CISCO-IETF-DHCP-SERVER-MIB.my
- **DHCPv4 server capability** - CISCO-IETF-DHCP-SERVER-CAPABILITY.my
- **DHCPv4 server extensions** - CISCO-IETF-DHCP-SERVER-EXT-MIB.my
- **DHCPv4 server extensions capability** - CISCO-IETF-DHCP-SERVER-EXT-CAPABILITY.my
- **DHCPv6 server** - CISCO-NETREG-DHCPV6-MIB.my（試験的）

（注） このMIB、CISCO-NETREG-DHCPV6-MIBは、新しいDHCPv6関連の統計および新しいDHCPv6トラップのクエリをサポートするために定義されています。

これらの MIB ファイルは、Cisco Prime Network Registrar インストールパスの /misc ディレクトリにあります。

次のURLには、試験的なCISCO-NETREG-DHCPV6-MIB.myファイルを除くすべてのファイルが含まれています。

ftp://ftp.cisco.com/pub/mibs/supportlists/cnr/cnr-supportlist.html

次の依存関係ファイルも必要です。

- **Dependency for DHCPv4 and DHCPv6**- CISCO-SMI.my
- **Additional dependencies for DHCPv6**- INET-ADDRESS-MIB.my

これらの依存関係ファイルは、次の URL にあるすべての MIB ファイルとともに使用できます。

ftp://ftp.cisco.com/pub/mibs/v2/

MIB 属性のオブジェクト識別子（OID）を取得するには、次の URL にある同等の名前の .OID ファイルに移動します。

ftp://ftp.cisco.com/pub/mibs/oid/

SNMP サーバーのセットアップ

SNMPサーバーへのクエリを実行するには、サーバーのプロパティをセットアップする必要があります。

ローカルおよびリージョン Web UI

ステップ 1 [操作（Operate）] メニューから **Servers** サブメニューの **Manage Servers** を選択して、[サーバーの管理（Manage Servers）] ページを開きます（サーバーの管理 を参照）。

ステップ 2 [サーバーの管理（Manage Servers）] ペインの [SNMP] をクリックして、[ローカルSNMPサーバーの編集（Edit Local SNMP Server）] ページを開きます。

ステップ 3 *Community string* 属性は、サーバーにアクセスするためのパスワードです。（コミュニティ文字列は、読み取り専用のコミュニティ文字列です）。プリセット値は **public** です。

ステップ 4 [ログ設定（Log Settings）]、[その他のオプションと設定（Miscellaneous Options and Settings）]、および [詳細オプションと設定（Advanced Options and Settings）] を指定できます。

- **trap-source-addr**- 発信トラップに使用するオプションの送信者アドレス。
- **trap-source-ip6address**- 発信トラップに使用するオプションの送信元 IPv6 アドレス。
- **server-active**- SNMP サーバーがクエリーに対してアクティブであるかどうかを決定します。デフォルト値は true です。false に設定すると、サーバーは実行されますが、クエリにはアクセスできず、トラップは送信されません。
- **cache-ttl**- SNMP キャッシュがクエリーに応答する時間を決めます。デフォルトは 60 秒です。

ステップ 5 SNMP サーバー インターフェイスを管理するには、詳細モードで、**Network Interfaces** タブをクリックします。デフォルトで設定されているネットワーク インターフェイスを表示し、追加のネットワーク インターフェイス作成して編集することができます。作成して編集するには、ccm-admin ロールの server-management サブロールが割り当てられている必要があります。インターフェイスのプロパティは、TFTP サーバーのプロパティと同様です（TFTP サーバー ネットワーク インターフェイスの管理 （35 ページ） を参照）。

ステップ 6 サーバーのトラップ受信者を追加するには、次のようにします。

a) **Trap Recipients** タブをクリックします。
b) トラップ受信者の名前を入力します。
c) トラップ受信者の IPv4 アドレスまたは IPv6 アドレスを入力します。
d) **Add Trap Recipient** をクリックします。
e) 追加のトラップ受信者ごとに繰り返します。

ステップ 7 トラップ受信者を編集するには、次のようにします。

SNMPv2c：

a) [トラップ受信者（Trap Recipients）] タブでトラップ受信者の名前をクリックして、[トラップ受信者の編集（Edit Trap Recipient）] ページを開きます。
b) **[設定（Settings）]** セクションで次の属性を設定します。

- *ip-addr*：このトラップ受信者の IP アドレスを指定します。
- *port-number*：このトラップ受信者のオプションの IP ポート番号です。
- *community*：このトラップ受信者の SNMP コミュニティストリングです。
- *agent-addr*：この受信者に送信されるトラップでソースエージェントのアドレスとして使用する IP アドレスです。
- *tenant-id*：このオブジェクトのテナント所有者を識別します。
- *ip6address*：このトラップ受信者の IPv6 アドレスを指定します。
- *v6-port-number*：このトラップ受信者のオプションの IPv6 ポート番号です。

SNMPv3：

a) [ローカルSNMPサーバーの編集（Edit Local SNMP Server）] ページで、*local-proxy-only* の **[有効（enabled）]** オプションを選択します。この属性は、サーバーがローカルおよびプロキシを使用した送信元からのクエリのみを受け入れるか、または任意の送信元からのクエリを受け入れるかを定義します。SNMPv3 を使用する場合は、これを有効にすることをお勧めします。この設定を有効にすると、SNMP インターフェイス設定がすべて上書きされます。

b) [トラップ受信者（Trap Recipients）] タブでトラップ受信者の名前をクリックして、[トラップ受信者の編集（Edit Trap Recipient）] ページを開きます。

c) [SNMPv2c] セクションにリストされている属性に加えて、**[SNMPv3設定（SNMPv3 Settings）]** セクションで次の属性を設定できます。ほとんどの場合、コミュニティストリング属性はオプションです（受信者の設定によって変わります）。

- *snmp-user*：このトラップ受信者の SNMP ユーザー名です。
- *snmp-trap-msg*：このクライアントが TRAP または INFORM メッセージを必要とするかどうかを定義します。
- *snmp-security*：使用するセキュリティレベルを指定します。
  - no-auth：認証なし、プライバシーなし。
  - auth-nopriv：アカウント認証に SHA を使用します。認証パスワードが必要です。
  - auth-priv：アカウント認証に SHA を使用し、通信プライバシーに AES を使用します。認証パスワードとプライバシーパスワードの両方が必要です。
- *snmp-auth-password*：アカウント認証のパスワードを指定します。
- *snmp-priv-password*：通信プライバシーのパスワードを指定します。
- *snmp-v3-protocol*：この受信者に UDP または TCP 経由でメッセージを送信する必要があるかを指定します。
- *snmp-engine-id*：必要に応じて、受信者のエンジン ID を指定します。

ステップ 8 SNMP サーバーの設定を完了するには、**Save** をクリックします。

CLI コマンド

SNMP サーバーにアクセスできるように CLI でコミュニティ文字列を設定するには、**snmp set community=***name* を使用します。トラップ送信元 IPv4 アドレスを設定するには、**snmp set trap-source-addr=***value* を使用します。トラップ送信元 IPv6 アドレスを設定するには、**snmp set trap-source-ip6address=***value* を使用します。SNMP サーバーを非アクティブにするには **snmp disable server-active** を使用し、キャッシュの存続可能時間を設定するには **snmp set cache-ttl=***time* を使用します。

トラップ受信者を設定するには、**trap-recipient** *name* **set** *attribute=value* [*attribute=value ...*] を使用します。次に例を示します。

```
nrcmd> trap-recipient example-recipient set ip-addr=192.168.0.34
nrcmd> trap-recipient example-recipient set ip6address=2001:4f8:ffff:0:8125:ef1b:bdcb:4b4e
```

トラップ受信者の *agent-address*、*community*、および *port-number* の値を追加することもできます。

その他の SNMP 関連のコマンドとしては、起動時にサーバーを実行しないようにする **snmp disable server-active** と、インターフェイスを設定する **snmp-interface** コマンドがあります。**addr-trap** コマンドについては、TFTP サーバー ネットワーク インターフェイスの管理 （35 ページ） で説明しています。

通知の仕組み

Cisco Prime Network Registrar SNMP 通知サポートにより、標準の SNMP 管理ステーションは DHCP サーバーと DNS サーバーから通知メッセージを受信できます。これらのメッセージには、SNMP トラップをトリガーしたイベントの詳細が含まれています。

Cisco Prime Network Registrar は、アプリケーション コードが検出して信号を送信した事前定義イベントに応じて通知を生成します。各イベントは、特定のパラメータのセットまたは現在の値のセットとともに伝送することもできます。たとえば、*free-address-low-threshold* イベントは、10% 未使用の値のスコープ内で発生する可能性があります。そのようなイベントでは、他のスコープと値も可能であり、各タイプのイベントには異なるパラメータが関連付けられています。

次の表では、通知を生成するイベントについて説明します。

表 *4 : SNMP* 通知イベント

イベント	通知
別の DHCP サーバーとのアドレス競合が検出された（*address-conflict*）	アドレスが別の DHCP サーバーと競合しています。
DNS キューが満杯（*dns-queue-size*）	DHCP サーバーの DNS キューがいっぱいになり、DHCP サーバーが要求の処理を停止します。（これは、通常、まれな内部条件です）。
重複する IP アドレスが検出された（*duplicate-address* と *duplicate-address6*）	重複する IPv4 または IPv6 アドレスが発生しています。
重複する IPv6 プレフィックスが検出された（*duplicate-prefix6*）	重複する IPv6 プレフィックスが発生しています。
フェールオーバー設定の不一致（*failover-config-error*）	DHCP フェールオーバー設定がパートナー間で一致しません。

イベント	通知
未使用アドレスしきい値（*free-address-low* と *free-address-high*、または *free-address6-low* と *free-address6-high*）	IPv4 または IPv6 の空きアドレスの数が上限しきい値を超えたときには high トラップ。または、以前に high トラップをトリガーした後に、空きアドレスの数が下限しきい値を下回ったときには low トラップ。
高可用性（HA）DNS 設定の不一致（*ha-dns-config-error*）	HA DNS 設定がパートナー間で一致しません。
HA DNS パートナーが応答していない（*ha-dns-partner-down*）	HA DNS パートナーが DNS サーバーへの応答を停止しています。
HA DNS パートナーが応答（*ha-dns-partner-up*）	HA DNS パートナーが、無応答の後、応答しています。
DNS プライマリサーバーが応答しない（*primary-not-responding*）	プライマリ DNS サーバーが DNS サーバーへの応答を停止しています。
DNS プライマリサーバーが応答している（*primary-responding*）	プライマリ DNS サーバーが応答しなくなった後に、応答しています。
他のサーバーが応答していない（*other-server-down*）	DHCP フェールオーバー パートナー、または DNS または LDAP サーバーが、DHCP サーバーへの応答を停止しています。
他のサーバーが応答（*other-server-up*）	DHCP フェールオーバー パートナー、または DNS または LDAP サーバーが、無応答の後、応答しています。
DNS セカンダリ ゾーン期限切れ（*secondary-zone-expired*）	DNS セカンダリ サーバーは、ゾーン転送中にクエリに応答するときに、ゾーンデータの権限を要求できなくなります。
サーバーの起動（*server-start*）	DHCP または DNS サーバーが起動または再初期化されました。
サーバー停止（*server-stop*）	DHCP または DNS サーバーが停止しています。

リソース モニターリング SNMP 通知

SNMP トラップがリソース制限アラームに対して有効になっている場合、Cisco Prime Network Registrar は、モニター対象のリソースがクリティカル レベルまたは警告レベルを超えたときに SNMP トラップを生成します。SNMP トラップは、次のリソース制限について生成されます。

- リソースの値が警告またはクリティカル限界を超えたとき（これらは、値がいずれかのしきい値を超えている限り、定期的に送信されます）。

- リソースの値が警告限界より下のレベルに戻ったとき。

SNMP サーバーは、CISCO-EPM-NOTIFICATION MIB を使用してトラップを生成します。マッピングは、次のとおりです。

表 *5: CISCO-EPM-NOTIFICATION-MIB* トラップ属性のマッピング

トラップ属性名	オブジェクト ID	タイプ	リソースイベントの値
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdminString (SIZE(1..16))	"1.2"
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	タイムスタンプ	リソースイベント状態の最終変更時刻
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	タイムスタンプ	現在の時刻
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdminString (SIZE(1..20))	イベントの一意 ID - 16 進数のみ
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32 (1..250)	1（確認応答されなかった場合）
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdminString (SIZE(1..255))	"1,Not acknowledged"
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	整数	未使用
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32 (1..250)	100（Raw アラームの場合）
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	SnmpAdminString (SIZE(1..255))	"100,Raw alarm"
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	InetAddressType	クラスタ サーバー アドレス タイプ - IPv4（1）または IPv6（2）
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	InetAddress	クラスタ アドレス（ローカル クラスタのオブジェクトに基づく）
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	SnmpAdminString (SIZE(1..255))	アプリケーション
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	InetAddressType	未使用
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	InetAddress	未使用

トラップ属性名	オブジェクト ID	タイプ	リソース イベントの値
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	OctetString (SIZE(1..1024))	"," と書式化された説明
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer32	クリアの場合は 0、警告の場合は 2、クリティカルの場合は 5
cenAlarmSeverityDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	SnmpAdminString (SIZE(1..255))	文字列アラームの重大度、"0,Clear"、"2,Warning"、または "5,Critical" のいずれか
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Integer32 (0..100)	未使用
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	OctetString (SIZE(1..1024))	未使用
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	SnmpAdminString (SIZE(1..255))	モニター対象リソースの名前
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	SnmpAdminString (SIZE(1..255))	サーバー名（dhcp、dns、cdns、...）
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	SnmpAdminString (SIZE(1..255))	"Network Registrar"
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	整数	3（イベント）
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Guage (0..100)	未使用
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	SnmpAdminString (SIZE(1..255))	未使用
cenCustomerIdentification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	SnmpAdminString (SIZE(1..255))	未使用
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	SnmpAdminString (SIZE(1..255))	未使用
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	SnmpAdminString (SIZE(1..255))	cenAlarmInstanceID

リソース制限アラームの詳細については、リソース制限アラームのモニターリング （62 ページ） を参照してください。

SNMP 通知イベントの処理

Cisco Prime Network Registrar が通知を生成すると、通知の 1 つのコピーを各受信者に SNMP トラップ PDU として送信します。すべてのイベント（およびスコープまたはプレフィックス）は、受信者とその他の通知設定データのリストを共有し、通知を初期化すると、サーバーはそれらを読み取ります。

SNMP 属性は、次の 3 つの方法で設定できます。

- DHCP サーバーの場合、スコープまたはプレフィックス（またはそれらのテンプレート）のトラップを特に設定していない場合、デフォルトの未使用アドレス トラップ設定を有効にするトラップを含みます。
- *free-address-config* 属性を設定することによって、スコープまたはプレフィックス（またはそのテンプレート）レベルで。
- DNS サーバーの場合、*traps-enabled* 設定が含まれます。

SNMP 通知を使用するには、トラップ通知を送信する場所を示すトラップ受信者を指定する必要があります。デフォルトでは、すべての通知が有効になっていますが、明示的に受信者を定義する必要があります。そうでない場合、通知は送信されません。使用する IP アドレスは、多くの場合、**localhost** です。

DHCP サーバーは特別なトラップ設定を提供します。これにより、特に DHCPv4 および DHCPv6 の空きアドレスに関する通知を送信できるようになります。トラップ設定名、モード、低しきい値および高しきい値のパーセンテージを設定できます。モードによって、スコープが空きアドレス レベルを集約する方法が決まります。

DHCP v4 通知

DHCP v4 のモードとしきい値は、次のとおりです（非アクティブ化されたスコープまたはプレフィックスの処理 （45 ページ） も参照）。

- **scope mode**—各スコープが独自の空きアドレス レベルを個別に追跡します（デフォルト）。
- **network mode** - このトラップ設定で設定されたすべてのスコープが（スコープまたはスコープ テンプレートの *free-address-config* 属性を通じて）、同じ *primary-subnet* を共有する場合、空きアドレス レベルを集約します。
- **selection-tags mode** - スコープがプライマリ サブネットを共有し、一致する選択タグ値のリストを持つ場合、空きアドレス レベルを集約します。
- **low-threshold**- DHCP サーバーが低しきい値トラップを生成し、高しきい値を再度有効にする空きアドレスのパーセンテージ。スコープの空きアドレス レベルは、次の計算です。

```
100 * available-nonreserved-leases
total-configured-leases
```

- **high-threshold**- DHCP サーバーが高しきい値トラップを生成し、低しきい値を再度有効にする空きアドレスのパーセンテージ。

DHCP v6 通知

DHCP v6 のモードとしきい値は、次のとおりです（非アクティブ化されたスコープまたはプレフィックスの処理 （45 ページ） も参照）。

- **prefix mode** - 各プレフィックスが独自の空きアドレス レベルを個別に追跡します。
- **link mode** - すべてのプレフィックスが同じリンクを共有している場合、リンクに設定されているすべてのプレフィックスが独自の空きアドレス レベルを集約します。
- **v6-selection-tags mode** - プレフィックスがリンクを共有し、一致する選択タグ値のリストを持つ場合、プレフィックスは空きアドレス レベルを集約します。
- **low-threshold**- DHCP サーバーが低しきい値トラップを生成し、高しきい値を再度有効にする空きアドレスのパーセンテージ。プレフィックスの空きアドレス レベルは、次の計算になります。

```
100 * max-leases - dynamic-leases
max-leases
```

- **high-threshold**- DHCP サーバーが高しきい値トラップを生成し、低しきい値を再度有効にする空きアドレスのパーセンテージ。

非アクティブ化されたスコープまたはプレフィックスの処理

非アクティブ化されたスコープまたはプレフィックスは、そのカウンタを他のスコープまたはプレフィックスと集約しません。たとえば、プレフィックスを **link** または **v6-selection-tags** トラップモードで設定し、その後、プレフィックスを非アクティブにすると、そのカウンタは集約の合計カウントから消えます。非アクティブ化されたプレフィックスのリースに対する変更は、集約合計には適用されません。

したがって、非アクティブ化されたスコープまたはプレフィックスのクライアントを検出するには、イベント モードを **scope** または **prefix** に設定する必要があり、いずれかの集約モード（**network**、**selection-tags**、**link**、または **v6-selection-tags**）には設定しないでください。

たとえば、非アクティブ化されたプレフィックスに対してトラップを設定する使用事例は、ネットワーク番号の再設定です。この場合、新しいプレフィックス（集約として、すべてのクライアントに十分な領域があることを確認します）と古いプレフィックスの両方をモニターして、リースが解放されるようにする必要がある場合があります。また、古いプレフィックスの上限しきい値を 90% または 95% に設定して、ほとんどのアドレスが解放されたときにトラップが発生するようにすることもできます。

ローカル Web UI

DHCP サーバーの SNMP 属性にアクセスするには、**Operate** メニューから **Manage Servers** を選択し、左側のペインの **DHCP** をクリックします。[DHCP サーバーの編集（Edit DHCP Server）] ページの [SNMP 設定]（基本モード）または [SNMP 設定]（詳細モード）で、SNMP 属性を確認できます。

4 つの *lease-enabled* 値（free-address6-low、free-address6-high、duplicate-address6、duplicate-prefix6）は DHCPv6 のみに関係します。トラップをイネーブルにするとともに、デ

フォルトの free-address トラップ設定を名前で指定でき、明示的に設定されていないすべてのスコープとプレフィックスまたはリンクに影響します。

トラップ設定を追加するには、次の手順を実行します。

ステップ 1 詳細モードで、**Deploy** メニューから [**DHCP**] サブメニューの **Traps** を選択して、DHCP トラップ設定にアクセスします。[トラップ設定の一覧表示/追加（List/Add Trap Configurations）] ページが表示されます。

ステップ 2 左側のペインの [**トラップの追加（Add Trap**）] アイコンをクリックして、[AddrTrapConfig の追加（Add AddrTrapConfig）] ページを開きます。

ステップ 3 名前、モード、およびしきい値のパーセンテージを入力して、**Add AddrTrapConfig** をクリックします。

トラップ設定の編集

トラップ設定を編集するには、次の手順を実行します。

ステップ 1 [トラップ（Traps）] ペインで目的のトラップ名をクリックして、[トラップ設定の編集（Edit Trap Configuration）] ページを開きます。

ステップ 2 名前、モード、またはしきい値の割合を変更します。

ステップ 3 [*enabled*] 属性の **on** オプションをクリックして、トラップ設定を有効にします。

ステップ 4 **Save** をクリックして、変更を有効にします。

トラップ設定の削除

トラップ構成を削除するには、[トラップ（Traps）]ペインでトラップを選択し、[**削除（Delete**）] アイコンをクリックして、削除を確定またはキャンセルします。

リージョン Web UI

リージョン Web UI では、ローカル Web UI と同様にトラップ構成を追加および編集できます。また、[トラップ構成のリスト/追加（List/Add Trap Configurations]）ページで、レプリカ トラップ構成をプルしたり、トラップ構成をローカル クラスタにプッシュしたりすることもできます。

サーバーのアップ/ダウン トラップ

すべてのダウン トラップには、対応するアップ トラップが続く必要があります。ただし、このルールは、次のシナリオでは厳密には適用されません。

1. フェールオーバー パートナーまたは LDAP サーバーまたは DNS サーバーまたは HA DNS パートナーが長時間ダウンしている場合は、ダウン トラップが定期的に発行されます。アップ トラップは、そのサーバーまたはパートナーがサービスに戻るときにのみ生成されます。

2. DHCP または DNS サーバーがリロードまたは再起動されると、パートナーまたは関連するサーバーの以前の状態は保持されず、重複するダウンまたはアップ トラップが発生する可能性があります。

（注） 他のフェールオーバー パートナーまたは LDAP サーバーまたは DNS サーバーまたは HA DNS パートナーのアップまたはダウン トラップは、そのパートナーまたはサーバーと通信するためにのみ発生します。そのため、他のパートナーまたはサーバーがダウンしたり、サービスに戻ったりしたときには、発生しない可能性があります。

CLI コマンド

ローカル クラスタで DHCP サーバーのトラップ値を設定するには、**dhcp set traps-enabled=***value* を使用します。また、*default-free-address-config* 属性をトラップ設定に設定することもできます。次に例を示します。

```
nrcmd> dhcp set traps-enabled=server-start,server-stop,free-address-low,free-address-high

nrcmd> dhcp set default-free-address-config=v4-trap-config
```

（注） *default-free-address-config*（または IPv6 の場合は *v6-default-free-address-config*）を定義しなかった場合、Cisco Prime Network Registrar は、**default-aggregation-addr-trap-config** という名前の内部の非リストトラップ設定を作成します。このため、作成したトラップ設定にその名前を使用しないようにしてください。

DHCPv4 および DHCPv6 のトラップ設定を定義するには、設定の **addr-trap** 名前　**create** の後に属性=値のペアを続けて使用します。次に例を示します。

```
nrcmd> addr-trap v4-trap-conf create mode=scope low-threshold=25% high-threshold=30%

nrcmd> addr-trap v6-trap-conf create mode=prefix low-threshold=20% high-threshold=25%
```

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。

- **addr-trap** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]
- **addr-trap** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]
- **追加トラップ**名**再利用**クラスタリスト[**-レポートのみ**|**-レポート**]

SNMP クエリの処理

SNMP クライアント アプリケーションを使用して、次の MIB を照会できます。

- CISCO-DNS-SERVER-MIB.my

- CISCO-IETF-DHCP-SERVER-MIB.my
- CISCO-IETF-DHCP-SERVER-EXT-MIB.my
- CISCO-NETREG-DHCPV6-MIB.my（試験的）

SNMP サーバーは、これらの MIB のいずれかで定義されている属性のクエリを受信すると、その属性値を含む応答 PDU を返します。たとえば、（インターネット経由で使用可能な）NET-SNMP クライアント アプリケーションを使用して、次のいずれかのコマンドを使用して、特定のアドレスの DHCPDISCOVER パケットの数を取得できます。

```
C:\net-snmp5.2.2\bin>snmpget -m ALL -v 2c -c public
192.168.241.39.iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.
ciscoIetfDhcpSrvMIB.ciscoIetfDhcpv4SrvMIBObjects.cDhcpv4Counters.cDhcpv4CountDiscovers

CISCO-IETF-DHCP-SERVER-MIB::cDhcpv4CountDiscovers.0 = Counter32: 0
C:\net-snmp5.2.2\bin>snmpget -m ALL -v 2c -c public
192.168.241.39 1.3.6.1.4.1.9.10.102.1.3.1

CISCO-IETF-DHCP-SERVER-MIB::cDhcpv4CountDiscovers.0 = Counter32: 0
```

どちらのコマンドも同じ結果を返します。最初のコマンドは完全なMIB属性名を照会し、2番目は OID に相当するものを照会します（エラーが発生する可能性が低いです）。前述したように、OID に相当する MIB 属性は、次の URL にある関連ファイルにあります。

ftp://ftp.cisco.com/pub/mibs/oid/

たとえば、CISCO-IETF-DHCP-SERVER-MIB.oid ファイルには、前のクエリの例に対応する次の OID 定義が含まれています。

```
"cDhcpv4CountDiscovers" "1.3.6.1.4.1.9.10.102.1.3.1"
```

SNMP クエリのエラー状態には、次のようなものがあります。

- 要求 PDU で送信されたコミュニティ文字列が、設定した内容と一致しません。
- 要求PDUのバージョンが、サポートされているバージョン（SNMPv2）と同じではありません。
- クエリ対象のオブジェクトのインスタンスがサーバー内にない場合、対応する [変数バインディング タイプ （variable binding type）] フィールドが SNMP_NOSUCHINSTANCE に設定されます。GetNext を使用すると、次の属性がない場合、対応する [変数バインディング タイプ（variable binding type）] フィールドが SNMP_ENDOFMIBVIEW に設定されます。
- OID に一致するものがない場合、対応する [変数バインディング タイプ（variable binding type）] フィールドが SNMP_NOSUCHOBJECT に設定されます。GetNext を使用すると、SNMP_ENDOFMIBVIEW に設定されます。
- 属性のクエリによって返された不正な値がある場合、応答 PDU のエラー ステータスは SNMP_ERR_BAD_VALUE に設定されます。

Cisco Prime Network Registrar SNMP とシステム SNMP の統合

Cisco Prime Network Registrar 11.1 以降では、Cisco Prime Network Registrar SNMP サーバーは、プロキシメカニズムを介してシステムの SNMP サーバーに自動的に統合されます。システムの SNMP サーバーで SNMPv3 を使用する場合は、適切なシステムツールを使用してログイン情報を管理する必要があります。

ポーリング プロセス

リージョン クラスタが DHCP 使用率またはリース履歴をローカル クラスタにポーリングするときには、まず、現在時刻までに使用可能なすべてのデータを要求します。この時刻は履歴データベースに記録され、後続のポーリングでは、この時刻より新しいデータのみを要求します。すべての時刻は、各ローカル クラスタの時刻に対して相対的に保存され、その時刻は、そのクラスタのタイムゾーンに合わせて調整されます。

各サーバーの時刻が同期されていない場合、奇妙なクエリ結果が表示されることがあります。たとえば、リージョン クラスタの時刻がローカル クラスタの時刻より遅れていた場合、収集された履歴は、リージョンクラスタでの時間範囲クエリに対して未来のものになる可能性があります。その場合、クエリの結果は空のリストになります。複数のクラスタからマージされたデータも、ローカルクラスタ間の時差により、順序が正しくない場合があります。このタイプの不整合があると、トレンドの解釈が困難になります。これらの問題を回避するには、すべてのクラスタでネットワーク タイム サービスを使用することを強く推奨します。

使用率とリース履歴データのポーリング

ローカルがリージョンまたはデフォルトのポーリング(1時間ごと)または手動ポーリングで登録されている場合、DHCP 使用率データが収集されます。使用可能なすべてのスコープとプレフィックスの情報がリージョン サーバーによって収集されます。リージョン データベースを更新するためのデフォルトのポーリング間隔は 1 時間です。サーバーにポーリングするには、[リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページの [**リース履歴（Lease History**）] アイコンをクリックします。この手動ポーリングでは、サーバーがフェールオーバー関係にある場合、データはサーバーがメインであるサブネットについてのみ取得されます。

アドレス空間の権限を持っている場合（regional-addr-admin ロールを割り当てられ、少なくとも、subnet-utilization および lease-history サブロールが割り当てられている場合）、DHCP 使用率またはリース履歴データを照会することができます。そのためには、**Operate** メニューから [使用率（Utilization）] または [リース履歴（Lease History）] オプションを選択します（*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド の「使用率履歴レポートの生成」の項、または *Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド の「*IP* リース履歴の実行」の項を参照）。

ポーリング間隔の調整

DHCP 使用率およびリース履歴の自動ポーリング間隔は、その他の属性とともに調整できます。これらの属性は、次の優先順位を使用して、リージョンクラスタの3つの場所で設定されます。

1. **Cluster**これらの値はサーバー全体の設定を上書きしますが、これらの値が設定解除されている場合はサーバー値が使用されます。クラスタの値は、クラスタを追加または編集するときに設定されます。CLI で、**cluster** コマンドを使用して、次の表に示す属性を設定します。

2. **Regional CCM server**（プリセットのポーリング間隔は 1 時間です）- これは **Servers** をクリックした後、ローカル CCM サーバー リンクをクリックしてアクセスできる [CCM サーバーの編集（Edit CCM Server] ページで設定されます。CLI で、**ccm** コマンドを使用して、次の表に示す属性を設定します。

（注） リース履歴収集がローカルクラスタ DHCP サーバーで明示的に有効になっていない場合（リース履歴収集の有効化 （51 ページ） を参照）、ポーリングがデフォルトでオンになっている場合でも、データは収集されません。DHCP サーバーでの DHCP 使用率の収集は、リージョンクラスタでのポーリングとは異なり、ポーリングによって自動的に収集がトリガーされることはありません。新しいポーリングで新しいデータをピックアップする前に、DHCP使用率の収集が行われる必要があります。この収集は 15 分ごとに事前設定されているため、ポーリング間隔はこの間隔よりも大きい値に設定する必要があります（自動ポーリング間隔は1時間ごとに事前設定されています）。

表 *6 : DHCP* 使用率およびリース履歴のポーリングのリージョン属性

属性タイプ	DHCP 使用率	リース履歴
ポーリング間隔 - データをポーリングする頻度	*addrutil-poll-interval* 0（ポーリングなし）～ 1 年、CCM サーバーの場合は 1 時間に事前設定	*lease-hist-poll-interval* 0（ポーリングなし）～ 1 年、CCM サーバーの場合は 4 時間に事前設定
再試行間隔 - ポーリングが失敗した後の再試行回数	*addrutil-poll-retry* 0 ～ 4 回再試行	*lease-hist-poll-retry* 0 ～ 4 回再試行
オフセット - ポーリングを保証する時間帯	*addrutil-poll-offset* 0 ～ 24h（0h = 深夜）	*lease-hist-poll-offset* 0 ～ 24h（0h = 深夜）

ポーリングオフセット属性は、ポーリング間隔に関連して、ポーリングが 1 日の特定の時間帯（24 時間制で設定）に行われることを保証します。たとえば、間隔を 4h に、オフセットを 6h（午前 6 時）に設定した場合、ポーリングは毎日午前 2 時、午前 6 時、午前 10 時、午後 2 時、午後 6 時、午後 10 時に行われます。

リース履歴収集の有効化

ステップ 1 クライアントが要求したリースを得られるように、スコープとアドレス範囲を使用してローカル クラスタ DHCP サーバーを設定します。

ステップ 2 リース履歴データの収集を明示的に有効にします。設定する DHCP サーバー属性は、次のとおりです。

- *ip-history* - リース履歴データベースを有効または無効にします。v4-only（DHCPv4）、v6-only（DHCPv6）、または both。
- *ip-history-max-age* - 履歴レコードの有効期間を制限します（4 週間に事前設定）。

  CLI で、**dhcp set ip-history=<value> (v4-only, v6-only, both, or disable)** コマンドを使用して属性を設定します。

ステップ 3 ステージング DHCP 編集モードで、ローカル クラスタ DHCP サーバーをリロードします。

ステップ 4 リージョン クラスタで、この DHCP サーバーを含むクラスタを作成します。

ステップ 5 リージョン Web UI で、[リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページの [リース履歴設定（Lease History Settings）] セクションに移動します。

ステップ 6 表 6 : DHCP 使用率およびリース履歴のポーリングのリージョン属性 （50 ページ） で属性を設定します。

ステップ 7 **Save** をクリックします。

ステップ 8 [リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページで、クラスタ名の横にある [**レプリカ（Replica）**] アイコンをクリックします。

ステップ 9 リース履歴データの初期セットの取得に関連するクラスタの [**リース履歴（Lease History）**] アイコンをクリックします。このデータはポーリング間隔ごとに自動的に更新されます。

DHCP スコープ テンプレートの管理

スコープテンプレートは、特定の共通属性を複数のスコープに適用します。これらの共通属性には、式に基づくスコープ名、ポリシー、アドレス範囲、式に基づく組み込みポリシー オプションが含まれます。ローカル クラスタから追加またはプルしたスコープ テンプレートは、[DHCP スコープ テンプレートの一覧表示/追加（List/Add DHCP Scope Templates）] ページに表示されます（**Design > DHCPv4** メニューから **Scope Templates** を選択します）。

スコープ テンプレートの作成と編集、およびスコープへの適用の詳細については、『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「スコープテンプレートの作成と適用」の項を参照してください。リージョン クラスタ Web UI には、スコープ テンプレートをローカル クラスタにプッシュし、ローカル クラスタからプルする機能が追加されています。

ローカル クラスタへのスコープ テンプレートのプッシュ

作成したスコープテンプレートをリージョンクラスタから任意のローカルクラスタにプッシュできます。Web UI で、[DHCP スコープ テンプレートの一覧表示/追加（List/Add DHCP Scope Templates）] ページに移動し、次のいずれかを実行します。

- 特定のテンプレートをクラスタにプッシュする場合は、左側の [スコープ テンプレート（Scope Templates）] ペインからスコープ テンプレートを選択して、**Push**（ページの上部にある）をクリックします。[DHCP スコープ テンプレートのプッシュ（Push DHCP Scope Template）] ページが開きます。
- 使用可能なすべてのスコープ テンプレートをプッシュする場合は、[スコープ テンプレート（Scope Templates）] ペインの上部にある [**すべてプッシュ（Push All**）] アイコンをクリックします。[ローカル クラスタへのデータのプッシュ（Push Data to Local Clusters）] ページが開きます。

リージョン Web UI

[DHCP スコープ テンプレートのプッシュ（Push DHCP Scope Template）] ページと [ローカル クラスタへのデータのプッシュ（Push Data to Local Clusters）] ページでは、プッシュするデータ、ローカルクラスタと同期する方法、およびプッシュ先のクラスタを識別します。データ同期モードは次のとおりです。

- 保証（**Ensure**）(プリセット値): 既存のデータに影響を与えずに、ローカル クラスターに新しいデータが含まれるようになります。
- **Replace**- ローカルクラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**-「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカルクラスターに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能（Available）]フィールドで宛先クラスタを選択し、[選択済み（Available）]フィールドに移動します。

ヒント　同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であるため、変更しない限り、このページにアクセスするたびに有効になります。

これらの選択を行った後**Push Data to Clusters**、 をクリックします。[スコープ テンプレート データのプッシュ レポートの表示（View Push Scope Template Data Report）] ページが開きます。

CLI コマンド

リージョン クラスタに接続されているときには、**scope-template** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからのスコープ テンプレートのプル

明示的に作成するのではなく、ローカル クラスタのレプリカ データからスコープ テンプレートをプルすることもできます。（クラスタ名の横にある [**複製（Replicate**）] アイコンをクリックして、ポリシーのレプリカ データを更新しておいてください）。リージョン Web UI でスコープ テンプレートをプルするには、[スコープ テンプレート（Scope Templates）] ペインの上部にある [**データのプル（Pull Data**）] アイコンをクリックします。

リージョン Web UI

[プルするレプリカ DHCP スコープ テンプレート データの選択（Select Replica DHCP Scope Template Data to Pull）] ページには、ローカル クラスタのスコープ テンプレートのリージョン サーバーのレプリカ データのツリー ビューが表示されます。ツリーには2つのレベルがあり、1つはローカル クラスタ、もう1つは各クラスタのスコープ テンプレートです。クラスタから個々のスコープ テンプレートをプルすることも、すべてのスコープ テンプレートをプルすることもできます。個々のスコープ テンプレートをプルするには、クラスタのツリーを展開して、名前の横にある **Pull Scope Template** をクリックします。クラスタからすべてのスコープ テンプレートをプルするには、**Pull All Scope Templates** をクリックします。

スコープ テンプレートをプルするには、同期モードも選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョン クラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値) - 地域クラスターに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**-「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスターに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

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

DHCP ポリシーの管理

すべての DHCP サーバーには、1 つ以上のポリシーが定義されている必要があります。ポリシーは、リース期間、ゲートウェイ ルータ、およびその他の設定パラメータを、DHCP オプションと呼ばれるものとして定義します。ポリシーは1回だけ定義し、複数のスコープに適用する必要があるため、複数のスコープがある場合は特に役立ちます。

DHCP ポリシーの作成と編集、およびスコープへの適用の詳細については、『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「DHCP ポリシーの設定」の項を参照してください。リージョン クラスタ Web UI には、ローカル クラスタにポリシーをプッシュし、ローカル クラスタからプルする機能が追加されています。また、ポリシーを再利用する機能も提供されます。

ローカル クラスタへのポリシーのプッシュ

また、作成したポリシーをリージョン クラスタから任意のローカル クラスタにプッシュすることもできます。リージョン Web UI で、[DHCP ポリシーの一覧表示/追加（List/Add DHCP Policies）] ページに移動し、次のいずれかを実行します。

- 特定のポリシーをクラスタにプッシュする場合は、左側の [ポリシー（Policies）] ペインからポリシーを選択して、**Push**（ページの上部にある）をクリックします。
- すべてのポリシーをプッシュする場合は、[ポリシー（Policies）] ペインの上部にある [**すべてプッシュ（Push all）**] アイコンをクリックします。

リージョン Web UI

[ローカル クラスタへの DHCP ポリシー データのプッシュ（Push DHCP Policy Data to Local Clusters）]ページでは、プッシュするデータ、ローカル クラスタと同期する方法、およびプッシュ先のクラスタを識別します。データ同期モードは次のとおりです。

- 保証（**Ensure**）(プリセット値): 既存のデータに影響を与えずに、ローカル クラスターに新しいデータが含まれるようになります。
- **Replace**- ローカル クラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**-「すべてプッシュ」操作のみに使用できます。データを上書きし、ローカル クラスターに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能（Available）]フィールドで宛先クラスタを選択し、[選択済み（Available）]フィールドに移動します。次に **Push Data to Clusters** をクリックして、[ポリシー データのプッシュ レポートの表示（View Push Policy Data Report）] ページを開きます。

ヒント　同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であり、変更しない限り、このページにアクセスするたびに有効になります。

CLI コマンド

リージョン クラスタに接続されているときには、**policy** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからのポリシーのプル

明示的に作成する代わりに、ローカル クラスタのレプリカデータからポリシーをプルすることもできます。（リージョン Web UI では、クラスタ名の横にある [**複製（Replicate**）] アイコンをクリックして、ポリシーのレプリカデータを更新しておいてください）。ポリシーをプルす

るには、[ポリシー（Policies）] ペインの上部にある [**データのプル（Pull Data**）] アイコンをクリックします。

リージョン Web UI

[プルするレプリカ DHCP ポリシー データの選択（Select Replica DHCP Policy Data to Pull）] ページには、ローカル クラスタのポリシーのリージョン サーバーのレプリカ データのツリービューが表示されます。ツリーには 2 つのレベルがあり、1 つはローカル クラスタ、もう 1 つは各クラスタのポリシーです。個々のポリシーをクラスタからプルすることも、すべてのポリシーをプルすることもできます。個々のポリシーをプルするには、クラスタのツリーを展開して、名前の横にある [ポリシーのプル（**Pull Policy**）] をクリックします。クラスタからすべてのポリシーをプルするには、[すべてのポリシーをプル（**Pull All Policies**）] をクリックします。

すべてのポリシーをプルするには、同期モードも選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョン クラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値) - 地域クラスターに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスターに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

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

DHCP クライアントクラスの管理

クライアントクラスは、共通のネットワークに接続したユーザーに差別化されたサービスを提供します。管理基準に基づいてユーザー・コミュニティをグループ化し、各ユーザーが適切なサービス・クラスを受け取れるようにすることができます。Cisco Prime Network レジストラー クライアントクラス機能を使用して、設定パラメータを制御できますが、最も一般的な用途は次のとおりです。

- **Address leases** - 一連のクライアントがアドレスを保持する期間。
- **IP address ranges**：クライアントアドレスを割り当てるリースプールの元。
- **DNS server addresses**：クライアントが DNS クエリを送信する場所。
- **DNS hostnames**：クライアントを割り当てる名前。
- **Denial of service**：許可されていないクライアントにリースを提供するかどうか。

クライアントクラスの作成および編集の詳細については、『*Cisco Prime Network Registrar 11.1 DHCP*ユーザ ガイド』の「クライアントクラスとクライアントの管理」の章を参照してくださ

い。リージョン クラスタ Web UI には、クライアントクラスをローカル クラスタにプッシュし、ローカルクラスタからプルする機能が追加されています。また、クライアントクラスを再利用する機能も提供されます。

ローカル クラスタへのクライアントクラスのプッシュ

また、ユーザーが作成したクライアントクラスをリージョン クラスタから任意のローカル クラスタにプッシュすることもできます。リージョン Web UI で、[DHCP クライアント クラスの一覧表示/追加（List/Add DHCP Client Classes）] ページに移動し、次のいずれかを実行します。

- Web UI で特定のクライアントクラスをクラスタにプッシュする場合は、左側の [クライアント クラス（Client Classes）] ペインからクライアントクラスを選択し、**Push**（ページの上部にある）をクリックします。[DHCP クライアント クラスのプッシュ（Push DHCP Client Class）] ページが開きます。
- すべてのクライアントクラスをプッシュする場合は、[クライアント クラス （Client Classes）] ペインの上部にある [**すべてプッシュ（Push All**）] アイコンをクリックします。[ローカル クラスタへのデータのプッシュ（Push Data to Local Clusters）] ページが開きます。

リージョン Web UI

[DGCP クライアント クラスのプッシュ（Push DHCP Client Class）] ページと [ローカル クラスタへのデータのプッシュ（Push Data to Local Clusters）] ページには、プッシュするデータ、ローカルクラスタとの同期方法、およびプッシュ先のクラスタが示されます。データ同期モードは次のとおりです。

- 保証（**Ensure**）(プリセット値): 既存のデータに影響を与えずに、ローカル クラスターに新しいデータが含まれるようになります。
- **Replace**- ローカルクラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**-「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカルクラスターに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能（Available）]フィールドで宛先クラスタを選択し、[選択済み（Available）]フィールドに移動します。次に **Push Data to Clusters** をクリックして、[クライアントクラスデータ プッシュ レポートの表示（View Push Client-Class Data Report）] ページを開きます。

ヒント　同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であり、変更しない限り、このページにアクセスするたびに有効になります。

CLI コマンド

リージョン クラスタに接続されているときには、**client-class** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからのクライアントクラスのプル

明示的に作成する代わりに、ローカル クラスタのレプリカ データからクライアントクラスをプルすることもできます。（Web UI では、クラスタ名の横にある [**複製（Replicate**）] アイコンをクリックして、クライアントクラスのレプリカデータを更新しておいてください）。クライアントクラスをプルするには、[クライアント クラス（Client Classes）] ペインの上部にある [**データのプル（Pull Data**）] アイコンをクリックします。

リージョン Web UI

[プルするレプリカ DHCP クライアントクラス データの選択（Select Replica DHCP Client-Class Data to Pull）] ページには、ローカル クラスタのクライアントクラスのリージョン サーバーのレプリカ データのツリー ビューが表示されます。ツリーには 2 つのレベルがあり、1 つはローカル クラスタ、もう 1 つは各クラスタ内のクライアントクラスです。クラスタから個々のクライアントクラスをプルすることも、すべてのクライアントクラスをプルすることもできます。個々のクライアントクラスをプルするには、クラスタのツリーを展開して、名前の横にある **Pull Client-Class** をクリックします。クラスタからすべてのクライアントクラスをプルするには、**Pull All Client-Classes** をクリックします。

クライアントクラスをプルするには、同期モードも選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョン クラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値) - 地域クラスターに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**-「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスターに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

リージョン クラスタに接続したら、**client-class** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] コマンドを使用できます。

仮想プライベート ネットワークの管理

バーチャル プライベート ネットワーク（VPN）は、キーによって識別される特殊なアドレス空間です。VPN では、アドレスが個別のキーによって区別されるため、ネットワーク内でのアドレスの重複が許されます。ほとんどの IP アドレスは、VPN 外のグローバル アドレス空間に

存在します。管理者が central-cfg-admin ロールの dhcp-management サブロールを割り当てられている場合にのみ、リージョン VPN を作成できます。

VPNの作成と編集、およびさまざまなネットワーク オブジェクトへの適用の詳細については、『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「DHCP を使用したバーチャル プライベート ネットワークの設定」の項を参照してください。リージョン Web UI には、VPN をローカル クラスタにプッシュし、ローカル クラスタからプルする機能が追加されています。また、VPN を再利用する機能も提供されます。

ローカル クラスタへの VPN のプッシュ

作成した VPN をリージョン クラスタから任意のローカル クラスタにプッシュできます。リージョン Web UI で、[VPN の一覧表示/追加（List/Add VPNs）] ページに移動し、次のいずれかを実行します。

- Web UI で特定の VPN をクラスタにプッシュする場合は、左側の [VPN] ペインから VPN を選択して、**Push**（ページの上部にある）をクリックします。[VPN のプッシュ（Push VPN）] ページが開きます。
- すべての VPN をプッシュする場合は、[VPN] ペインの上部にある [**すべてプッシュ（Push All**）] アイコンをクリックします。[ローカル クラスタへのデータのプッシュ（Push Data to Local Clusters）] ページが開きます。

リージョン Web UI

[VPN のプッシュ（Push VPN）] ページと [ローカル クラスタへのデータのプッシュ（Push Data to Local Clusters）] ページでは、プッシュするデータ、ローカル クラスタと同期する方法、およびプッシュ先のクラスタを識別します。データ同期モードは次のとおりです。

- 保証（**Ensure**）(プリセット値): 既存のデータに影響を与えずに、ローカル クラスターに新しいデータが含まれるようになります。
- **Replace**- ローカル クラスタに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**-「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカル クラスターに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能（Available）]フィールドで宛先クラスタを選択し、[選択済み（Available）]フィールドに移動します。次に **Push Data to Clusters** をクリックして、[VPN データのプッシュ レポートの表示（View Push VPN Data Report）] ページを開きます。

ヒント　同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であり、変更しない限り、このページにアクセスするたびに有効になります。

CLI コマンド

リージョン クラスタに接続されているときには、**vpn** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] コマンドを使用できます。クラスタのリストまたは「all」を指定できます。

レプリカ データからの VPN のプル

VPN を明示的に作成するのではなく、ローカル クラスタからプルすることができます。（リージョン Web UI では、クラスタ名の横にある [**レプリカ（Replica）**] アイコンをクリックして、VPN レプリカ データを更新しておいてください）。レプリカ データをプルするには、左側の [VPN] ペインの上部にある [**データのプル（Pull Data）**] アイコンをクリックして、[プルするレプリカ VPN データの選択（Select Replica VPN Data to Pull）] ページを開きます。

このページには、ローカル クラスタの VPN のリージョン サーバーのレプリカ データのツリー ビューが表示されます。このツリーには 2 つのレベルがあり、1 つはローカル クラスタ、もう 1 つは各クラスタ内の VPN です。個々の VPN をプルすることも、すべてをプルすることもできます。個々の VPN をプルするには、クラスタのツリーを展開して、名前の横にある **Pull VPN** をクリックします。すべての VPN をプルするには、**Pull All VPNs** をクリックします。

VPN をプルするには、同期モードを選択する必要があります。

- **Ensure**-既存のデータに影響を与えずに、リージョン クラスタに新しいデータが含まれることを確認します。
- **Replace**(プリセット値) - 地域クラスターに固有の他のオブジェクトに影響を与えずにデータを置き換えます。
- **Exact**- 「すべてプル」操作でのみ使用可能です。データを上書きし、地域クラスターに固有の他のオブジェクトを削除するため、このオプションは慎重に使用してください。

CLI コマンド

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

DHCP フェールオーバー ペアの管理

DHCP フェールオーバーでは、バックアップ DHCP サーバーは、メイン サーバーが何らかの理由でネットワークから切断された場合、メイン サーバーを引き継ぐことができます。フェールオーバーを使用して、冗長ペアとして動作するように 2 つのサーバーを設定できます。1 つのサーバーがダウンした場合、もう 1 つのサーバーがシームレスに引き継ぐため、新しい DHCP クライアントはアドレスを取得でき、既存のクライアントはアドレスを更新することができます。新しいリースを要求するクライアントは、どちらのサーバーがリース要求に応答するかを知る必要はありません。これらのクライアントは、メイン サーバーがダウンしている場合でもリースを取得できます。

リージョン Web UI では、[DHCP フェールオーバー ペアの一覧表示/追加（List/Add DHCP Failover Pairs）] ページで、作成されたフェールオーバー ペアを表示できます。このページにアクセスするには、**DHCP** をクリックしてから、**Failover** をクリックします。この機能は、centra-cfg-admin ロールの dhcp-management サブロールが割り当てられている管理者のみが使用できます。

フェールオーバー ペアの作成と編集の詳細については、『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「フェールオーバー サーバー ペアのセットアップ」の項を参照してください。リージョン クラスタ Web UI には、ローカル クラスタからアドレスをプルしてフェールオーバー ペアを作成する機能が追加されています。

フェールオーバー ペアのアドレス空間をプルするには、regional-addr-admin 権限が必要です。

リージョン Web UI

ステップ 1 [DHCPフェールオーバーペアの一覧表示/追加（List/Add DHCP Failover Pairs）] ページまたは [ユニファイドアドレス空間の表示（View Unified Address Space）] ページで、[フェールオーバーペア（Failover Pairs）] ペインの [プルv4データ（Pull v4 Data）] または [プルv6データ（Pull v6 Data）] アイコンをクリックします。

ステップ 2 [プルレプリカアドレス空間の選択（Select Pull Replica Address Space）] ページで、データ同期モード（**Update**、**Complete**、または **Exact**）を選択します。これらのモードを選択した結果については、ページの表を参照してください。

ステップ 3 [フェールオーバー ペアの同期（Synchronize Failover Pair）] タブの **Report** ボタンをクリックし、[**戻る**（**Return**）] をクリックします。

ステップ 4 [プル レプリカ アドレス空間の報告（Report Pull Replica Address Space）] ページの **Run** をクリックします。

ステップ 5 [プル レプリカ アドレス空間の実行（Run Pull Replica Address Space）] ページの **OK** をクリックします。

CLI コマンド

リージョン クラスタに接続されている場合は、次のコマンドを使用して、アドレス空間（および予約）をプルできます。

- **ccm pullAddressSpace** < **update** | **complete** | **exact** > [**-omitreservations**] [**-report-only** | **-report**]
- **ccm pullIPv6AddressSpace** < **update** | **complete** | **exact** > [**-report-only** | **-report**]

リース予約の管理

リージョン クラスタから作成したリース予約をローカル クラスタのいずれかにプッシュできます。リージョン クラスタ Web UI で、[DHCPv4 予約の一覧表示/追加（List/Add DHCPv4 Reservations）] ページまたは [DHCPv6 予約の一覧表示/追加（List/Add DHCPv6 Reservations）] ページに移動し、左側の予約ペインの [**すべてプッシュ**（**Push All**）] アイコンをクリックしま

す。個々の予約をプッシュすることはできないことに注意してください。プッシュ先のクラスタがDHCPフェールオーバー設定の一部である場合、予約をプッシュすると、パートナーサーバーにもプッシュされます。

DHCPv4 予約

DHCPv4 予約を作成するには、親サブネット オブジェクトがリージョン サーバーに存在している必要があります。リージョンで保留中の予約の編集がある場合は、それらをサブネットのローカル クラスタまたはフェールオーバー ペアにプッシュできます。サブネットがプッシュされていない場合は、親スコープがローカル クラスタまたはペアに追加されます。

サブネットがローカルクラスタまたはペアにプッシュされると、予約がそのクラスタまたはペアにプッシュされます。スコープとサブネットを別のローカル クラスタまたはフェールオーバー ペアに移動するには、最初にサブネットを回収する必要があります。

DHCPv6 予約

DHCPv6予約を作成するには、親プレフィックスがリージョンサーバーに存在している必要があります。保留中の予約またはプレフィックスの変更がある場合は、ローカルクラスタに更新をプッシュできます。

プレフィックスがローカル クラスタにプッシュされると、そのローカル クラスタのみを更新できます。プレフィックスを別のローカルクラスタに移動するには、最初に再利用する必要があります。

リージョン Web UI

表示されるページで、プッシュするデータ、ローカル クラスタと同期する方法、およびプッシュ先のクラスタを識別できます。データ同期モードは、次のとおりです。

- 保証（**Ensure**）- 既存のデータに影響を与えずに、ローカル クラスタに新しいデータがあることを確認します。
- **Replace**（プリセット値）- ローカル クラスタに固有の他のオブジェクトに影響を与えずに、データを置き換えます。
- **Exact**-「すべてプッシュ」操作でのみ使用できます。データを上書きし、ローカルクラスターに固有の他のオブジェクトを削除するため、この方法は注意して使用してください。

[使用可能（Available）]フィールドで宛先クラスタを選択し、[選択済み（Available）]フィールドに移動します。

ヒント 同期モードとクラスタ選択の設定は、現在のログインセッションの間は永続的であるため、変更しない限り、このページにアクセスするたびに有効になります。

これらの選択を行った後**Push Data to Clusters**、 をクリックします。[プッシュ予約データ レポートの表示（View Push Reservations Data Report）] ページが開きます。このページの **OK** をクリックします。

また、[DHCP v6 予約のリスト/追加（List/Add DHCP v6 Reservations）] ページでレプリカ アドレス空間をプルし、そのときに予約を省略するかどうかを選択することもできます。このオプションは、マージする予約に保留中の変更がないことが確認された場合にのみ、処理時間を短縮するために使用してください。プルの予約を省略するには、**[予約を省略？（Omit Reservations?）]** チェックボックスをオンにして、**Pull Data** をクリックします。

『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「DHCPv6 アドレス」の項を参照してください。

リソース制限アラームのモニターリング

リソース制限アラームを使用すると、Cisco Prime Network Registrar システム リソースをモニターして、1 つ以上の製品リソースが潜在的に危険なレベルに入り、注意が必要なときに通知を受けることができます。リソース制限アラームは、リソース制限情報を整理して統合して伝達するように設計されています。

（注） リソース制限に関連するログ メッセージは、ccm_monitor_log ファイルに記録されます。ログ ファイルの詳細については、ログ ファイル を参照してください。

モニター対象の各リソースの重要レベルと警告レベルの両方について、事前定義されたしきい値レベルをリセットできます。

Cisco Prime Network Registrar は、Web UI および CLI で、モニター対象リソースの現在のステータス、現在の値、およびピーク値を報告します。ピーク値は、設定されたリソース制限アラームの警告または危機的な限界と比較され、リソース制限アラームのステータスが [OK]、[Warning]、または [Critical] と表示されます。Cisco Prime Network Registrar では、結果の条件が発生しなくなり、ピーク値がリセットされるまで、Web UI と CLI にアラームが表示されます。

リソース制限アラームは、設定したポーリング間隔に基づいて定期的に更新されます。ポーリング間隔の設定の詳細については、リソース制限アラームのポーリング間隔の設定 （65 ページ） を参照してください。

SNMP トラップがリソース制限アラームに対して有効になっている場合、Cisco Prime Network Registrar は、モニター対象のリソースがクリティカル レベルまたは警告レベルを超えたときに SNMP トラップを生成します。SNMP トラップは、現在の値が設定された警告または危機的レベルを超えたときに生成されます。

Cisco Prime Network Registrar 11.1 以降、リソース監視は *queued-binding-updates* を監視し、値が設定された *queued-binding-updates-warning-level* および *queued-binding-updates-critical-level*を超える場合、標準のリソース監視の通知をトリガーします。（デフォルトはリソース監視の *lease-count* 値の 10% と 25% です。最小値は 1,000 バインディング更新です）。

Cisco Prime Network Registrar 11.1 以降では、権威およびキャッシュ DNS サーバーの DNS セキュリティイベント数の警告および重要レベルを設定することもできます。

リソース制限アラームは、リージョンとローカルクラスタの両方で設定できます。リソース制限アラーム データは、個々のローカル クラスタ レベルで統合されます。リージョン クラスタ レベルで使用可能なリソース制限アラームは、リージョン クラスタにのみ関係します。次の表に、リージョンまたはローカルクラスタで使用可能なリソース制限アラームのタイプを示します。

表 *7:* リソース制限アラーム

	リージョン クラスタ	ローカル クラスタ
データの空き領域/データ パーティション	✓	✓
シャドウ バックアップ時間	✓	✓
メモリのデフォルト（詳細モードで利用可能）	✓	✓
CCM メモリ	✓	✓
CNR サーバー エージェント メモリ	✓	✓
DHCP メモリ	x	✓
CDNS メモリ	x	✓
DNS メモリ	x	✓
SNMP メモリ	✓	✓
Tomcat メモリ	✓	✓
TFTP メモリ	x	✓
リース数	x	✓
ゾーン数	x	✓
リソース レコード数	x	✓
トラップの設定	✓	✓
証明書の有効期限（詳細モードで利用可能）	✓	✓
DNS セキュリティイベント（詳細モードで利用可能）	✓	✓

キューに入れられたバインディングの更新	x	✓

リソース制限アラームしきい値の設定

[**CCM サーバーの編集（Edit CCM Server**）] ページを使用して、リソース制限アラームの警告および重大制限を設定できます。

ローカルおよびリージョン Web UI

ステップ 1 CCM サーバーのプロパティにアクセスするには、[**操作（Operate**）] メニューの [**サーバーの管理（Manage Servers**）] を選択して、[サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 左側の [サーバーの管理（Manage Servers）] ペインの [CCM] をクリックします。[ローカルCCMサーバーの編集（Edit Local CCM Server）] ページが表示されます。このページには、すべての CCM サーバー属性が表示されます。

ステップ 3 [**リソース制限の設定（Configure Resource Limits**）] タブをクリックします。

ステップ 4 必要に応じて設定を変更します。

（注） リソース制限アラームの SNMP トラップを有効にするには、[トラップ設定（Trap Configuration）] グループの [トラップの有効化（Enable Traps）] オプションを選択します。

ステップ 5 [**保存（Save**）] をクリックして、CCM サーバー属性の変更を保存します。

CLI コマンド

ローカルまたはリージョン クラスタでリソース制限アラームを設定するには、**resource set** *attribute* = *value* [*attribute* = *value* ...] を使用します。現在の設定をレビューするには、**resource show** を使用し、リソースに関するレポートを生成するには、**resource report** [**all** | **full** | **levels**] コマンドを使用します。

定義された警告および重大レベルを表示するには、**resource report levels** コマンドを使用します。

次のシナリオでは、109 ステータス メッセージが報告されます（少なくとも 1 つのリソースが重大または警告状態になっている場合）。

- **resource report** コマンドを実行します。
- CLI を使用してクラスタに接続します。
- CLI を終了します。

リソース制限アラームのポーリング間隔の設定

Cisco Prime Network Registrar がサーバーからアラームデータをポーリングして、Web UI データを更新する頻度を設定できます。*stats-history-sample-interval* は、CCM サーバー システムのポーリング レートを制御します。

ステップ 1 アラーム ポーリング間隔を編集するには、[設定（Settings）] ドロップダウン リスト（メイン ページの上部）で [**ユーザー環境設定（User Preferences**）] に移動して、ユーザー環境設定を編集する必要があります。

ステップ 2 ユーザー環境設定を行った後、[**ユーザー環境設定の変更（Modify User Preferences**）] をクリックします。

リソース制限アラームの表示

リソース制限アラームは [アラーム（Alarms）] ページに表示されます。アラームの概要を表示するには、Cisco Prime Network Registrar Web UI で、Web UI の上部にある [**アラーム（Alarms**）] アイコンをクリックします。[アラーム（Alarms）] ページが開き、各リソース制限アラームのリソース、タイプ、ステータス、リソース使用率、および現在の値が表示されます。各リソース制限のピーク値に基づいて、リソース制限のステータスは、Web UI および CLI に [OK]、[Warning]、または [Critical] と表示されます。アラームは、設定したポーリング間隔に基づいて定期的に更新されます。ポーリング間隔の設定の詳細については、リソース制限アラームのポーリング間隔の設定 （65 ページ） を参照してください。

（注） リソースが警告または重大な状態にある場合、リソース制限アラームは [設定の概要（Configuration Summary）] ページにも表示されます。

リソース制限アラームのピーク値のリセット

Cisco Prime Network Registrar は、各リソース制限のピーク値を維持します。ピーク値は、現在の値がピーク値を超えた場合にのみ更新されます。ピーク値は、設定されたリソース制限アラームの警告または危機的な限界と比較され、リソース制限アラームのステータスが [OK]、[Warning]、または [Critical] と表示されます。

ピーク値が設定された警告または重大な制限を超えると、ピーク値が明示的にリセットされるまで、リソース制限アラームのステータスがそれぞれ [警告 （Warning）] または [クリティカル （Critical）]（Web UI および CLI で）として表示されます。ピーク値をリセットするには、次の手順を実行します。

ステップ 1 Web UI の上部にある [アラーム（Alarms）] アイコンをクリックして、[アラーム（Alarms）] ページを開きます。

ステップ 2 ピーク値をリセットするアラームを選択します。

ステップ 3 [アラームのリセット（**Reset Alarm**）] ボタンをクリックして、ピーク値をクリアします。

CLI コマンド

ローカルまたはリージョンクラスタでピーク値をリセットするには、**resource reset** [*name* [,*name* [,...]]] を使用します。

（注） リソース名が指定されていない場合、すべてがリセットされます。

リソース制限アラーム データのエクスポート

リソース制限アラーム データを CSV ファイルにエクスポートできます。リソース制限アラームをエクスポートするには、次の手順を実行します。

ステップ 1 Web UI の上部にある [アラーム（Alarms）] アイコンをクリックして、[アラーム（Alarms）] ページを開きます。

ステップ 2 [**CSV にエクスポート（Export to CSV**）] をクリックします。

ステップ 3 [ファイルのダウンロード（File Download）] ポップアップ ウィンドウが表示されます。[**保存（Save**）] をクリックします。

ステップ 4 [名前を付けて保存（Save As）]ポップアップ ウィンドウで、ファイルの保存場所を選択して、[**保存（Save**）] をクリックします。

証明書の管理（Certificate Management）

Cisco Prime Network Registrar は、製品のさまざまな部分（Web UI、キャッシング DNS、および権威 DNS）で SSL/TLS 証明書を使用します。Cisco Prime Network Registrar では、証明書ファイルを入力し、Cisco Prime Network Registrar コンポーネントに基づいて適切な場所に保存できます。また、証明書の有効期限を追跡し、証明書の有効期限が近づいたときに警告することもできます。

Cisco Prime Network Registrar で SSL/TLS キーまたは証明書を作成することはできません。openssl や keytool などのツールを使用して個別に作成する必要があります。次に例を示します。

openssl を使用して自己署名証明書（cert.pem）を作成するには、次のコマンドを使用します。

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

keytool を使用して認証局（CA）要求を行うには、『*Cisco Prime Network Registrar 11.1* インストール ガイド』の「独自の Web UI アクセス用証明書のインストール」の項を参照してください。

証明書を取得したら、Web UI、CLI、または REST API を介して Cisco Prime Network Registrar に追加できます。証明書の内容は、追加されるオブジェクトの *certificate-contents* 属性に追加さ

れます。CCM は証明書ファイルの内容を検証し、*certificate-contents* に基づいて証明書オブジェクト属性を自動的に入力します。証明書オブジェクトを作成し、CCM データベースに追加します。

証明書がシステムにロードされると、CPNR はその証明書の期限切れの監視を開始します。

Web UI 証明書の場合、CCM は証明書ファイルの内容もファイル（<cnr.datadir>/conf/cert/cnrcert_*certificate-name*.pem）も保存します。権威 DNS 証明書の場合、サーバーは *certificate-contents* を読み取り、それらを直接使用します。キャッシュ DNS の TLS および HTTPS 証明書の場合、キャッシング DNS サーバーは *certificate-contents* の内容に基づいて証明書ファイルを生成し、<cnr.datadir>/cdns/tls/*certificate-name* に保存します。この証明書ファイルは、リロードするたびに上書きされます。

ローカルクラスタで、権威 DNS 証明書やキャッシング DNS 証明書が複数ある場合、権威 DNS サーバーとキャッシング DNS サーバーは、オブジェクトのリストから適切なコンポーネントの最初の証明書のみを選択します。

（注） Web UI 証明書の場合、証明書オブジェクトを削除すると、関連する Web UI 証明書ファイル（<cnr.datadir>/conf/cert/cnrcert_*certificate-name*.pem）が削除されます。DNS 証明書をキャッシュする場合は、証明書ファイル（<cnr.datadir>/cdns/tls/*certificate-name*）を手動で削除する必要があります。

表 *8 : SSL/TLS* 証明書の属性

属性	説明
名前	管理対象の証明書の名前。
説明	管理対象の証明書の説明。
タイプ	証明書を使用する Cisco Network Registrar コンポーネントを指定します。
バージョン	証明書の SSL バージョンを指定します。このフィールドは、証明書の内容から自動的に入力されます。
シリアル番号（Serial Number） （*serial-number*）	証明書のシリアル番号を指定します。このフィールドは、証明書の内容から自動的に入力されます。
発効日 （*validity-not-before*）	証明書の有効期間の開始を示す日時を指定します。このフィールドは、証明書の内容から自動的に入力されます。
有効期限 （*validity-not-after*）	証明書の有効期間の終了を示す日時を指定します。このフィールドは、証明書の内容から自動的に入力されます。

属性	説明
発行元（Issuer）	証明書を発行したエンティティに関する情報を指定します。このフィールドは、証明書の内容から自動的に入力されます。
Subject	証明書を受信するエンティティに関する情報を指定します。このフィールドは、証明書の内容から自動的に入力されます。
Public Key Algorithm（*public-key-algorithm*）	公開キーのアルゴリズムとサイズを指定します。このフィールドは、証明書の内容から自動的に入力されます。
署名アルゴリズム（*signature-algorithm*）	署名のアルゴリズムとサイズを指定します。このフィールドは、証明書の内容から自動的に入力されます。

DNS TLS と管理対象証明書

TLS を有効にする場合は、権威 DNS サーバーとキャッシング DNS サーバーでさまざまな TLS 設定を行う必要があります。証明書の属性は *tls-service-pem* です。ただし、管理対象証明書を使用する場合、サーバーは証明書オブジェクトを使用し、*tls-service-pem* 属性は無視されます。サービスの設定手順は次のとおりです。

1. サーバーは TLS が有効かどうかを確認し、*tls-service-key* 属性を読み取ります。
2. サーバーは、そのコンポーネントタイプの管理対象証明書を検索します（つまり、type=cdns の証明書はキャッシング DNS サーバー用です）。
3. サーバーが管理対象証明書を検出すると、最初の証明書を選択し、残りの証明書は無視します（存在する場合）。TLS 設定ログメッセージには、管理対象証明書が使用されていることを示す tls-service-pem=*certificate-name* (managed) がリストされます。
4. サーバーは *tls-service-pem* 属性を無視し、代わりに証明書オブジェクトを使用します。管理対象証明書が使用されていない場合、サーバーは *tls-service-pem* 属性を読み取り、TLS 設定ログメッセージには tls-service-pem=*filename* と表示されます。

権威 DNS サーバーとキャッシング DNS サーバーの TLS 設定の詳細については、『*Cisco Prime Network Registrar 11.1* 権威およびキャッシング *DNS* ユーザ ガイド』の「キャッシング DNS サーバーの管理」の章と「権威 DNS サーバーの管理」の章の「TLS の設定の指定」の項を参照してください。

SSL/TLS 証明書の追加

Cisco Prime Network Registrar に SSL/TLS 証明書を追加するには、次の手順を実行します。

始める前に

openssl や keytool などのツールを使用して、SSL/TLS キーまたは証明書（cert.pem）を作成します。

ローカル詳細およびリージョン詳細 Web UI

ステップ 1 [設計（Design）] メニューから、[セキュリティ（Security）] サブメニューの [SSL/TLS証明書（SSL/TLS Certificates）] を選択して [SSL/TLS証明書の一覧表示/追加（List/Add SSL/TLS Certificates）] ページを開きます。

ステップ 2 [SSL/TLS証明書（SSL/TLS Certificates）] ペインの [SSL/TLS証明書の追加（Add SSL / TLS Certificates）] アイコンをクリックします。[SSL/TLS証明書の追加（Add SSL / TLS Certificates）] ページが開きます。

ステップ 3 管理する証明書の名前を入力し、証明書を使用する Cisco Network Registrar コンポーネントのタイプを選択します。

ステップ 4 [ファイルの選択（Choose File）] ボタンをクリックして、証明書ファイルを参照します。**cert.pem** ファイル（公開キー）を選択し、[開く（Open）] をクリックして追加します。

ステップ 5 [SSL/TLS証明書の追加（Add SSL/TLS Certificates）] をクリックします。

CLI コマンド

SSL/TLS 証明書を追加するには、**certificate** *name* **create** *type* **file**=*file* [*attribute*=*value*...] を使用します。

SSL/TLS 証明書を削除するには、**certificate** *name* **delete** を使用します。

証明書の属性値を変更するには、**certificate** *name* **set** *attribute*=*value* を使用します。

（注） 証明書オブジェクトの属性の多くは証明書の内容に基づいており、変更できません。現在、変更できるのは *description* 属性の値のみです。

SSL/TLS 証明書のプルとプッシュ

リージョンクラスタの Web UI の [SSL/TLS証明書の一覧表示/追加（List/Add SSL/TLS Certificates）] ページのローカルクラスタに対して SSL/TLS 証明書をプッシュしたり、プルしたりできます。

ローカルクラスタへの SSL/TLS 証明書のプッシュ

ローカルクラスタに SSL/TLS 証明書をプッシュするには、次の手順を実行します。

リージョン詳細Web UI

ステップ 1 [設計（Design）] メニューから、[セキュリティ（Security）] サブメニューの [SSL/TLS証明書（SSL/TLS Certificates）] を選択してリージョン Web UI に [SSL/TLS証明書の一覧表示/追加（List/Add SSL/TLS Certificates）] ページを表示します。

ステップ 2 [SSL/TLS証明書（SSL/TLS Certificates）] ペインの [すべてプッシュ（Push All）] アイコンをクリックしてページに一覧表示されているすべてのSSL/TLS証明書をプッシュするか、または[SSL/TLS証明書（SSL/TLS Certificates）] ペインで SSL/TLS 証明書を選択し、[プッシュ（Push）] アイコンをクリックして [SSL/TLS証明書のプッシュ（Push SSL/TLS Certificates）] ページを開きます。

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

- すべての SSL/TLS 証明書をプッシュする場合は、[保証（Ensure）]、[置換（Replace）]、または [完全（Exact）] を選択できます。
- 1 つの SSL/TLS 証明書をプッシュする場合は、[保証（Ensure）] または [置換（Replace）] を選択できます。

いずれの場合も、[保証（Ensure）] がデフォルトのモードです。

ローカルクラスタでSSL/TLS 証明書を置換する場合にのみ、[置換（Replace）] を選択します。ローカルクラスタで SSL/TLS 証明書データの正確なコピーを作成する場合にのみ [完全（Exact）] を選択します。これにより、リージョンクラスタで定義されていないすべての SSL/TLS 証明書が削除されます。

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

ステップ 5 [SSL/TLS証明書データのプッシュレポートの表示（View Push SSL/TLS Certificate Data Report）] ページでプッシュの詳細を表示し、**OK** をクリックして [SSL/TLS証明書の一覧表示/追加（List/Add SSL/TLS Certificates）] ページに戻ります。

レプリカデータベースからの SSL/TLS 証明書のプル

レプリカデータベースから SSL/TLS 証明書をプルするには、次の手順を実行します。

リージョン詳細Web UI

ステップ 1 [設計（Design）] メニューから、[セキュリティ（Security）] サブメニューの [SSL/TLS証明書（SSL/TLS Certificates）] を選択して [SSL/TLS証明書の一覧表示/追加（List/Add SSL/TLS Certificates）] ページを開きます。

ステップ 2 [SSL/TLS証明書（SSL/TLS Certificates）] ペインで [データのプル（Pull Data）] アイコンをクリックします。これにより、[プルするレプリカSSL/TLS証明書データの選択（Select Replica SSL/TLS Certificates Data to Pull）] ページが開きます。

ステップ 3 クラスタの [レプリカデータの更新（Update Replica Data）] 列で [レプリカ（Replica）] アイコンをクリックします。（自動複製間隔については、ローカル クラスタ データの複製 （27 ページ）を参照してください）。

ステップ 4 [モード（Mode）] ラジオ ボタンのいずれかを使用して、複製モードを選択します。

ステップ 5 ローカルクラスタの既存の SSL/TLS 証明書データを保持するには、[保証（Ensure）] を選択しますが、それ以外の場合は、デフォルトの [置換（Replace）] モードのままにします。

ステップ 6 [すべてのSSL/TLS証明書のプル（Pull all SSL/TLS Certificates）] ボタンをクリックしてプルの詳細を表示し、[実行（Run）] をクリックします。

CLI コマンド

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。

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

Cisco Prime Network Registrar による SSL/TLS 証明書の使用

CPNR はさまざまなサービスに SSL/TLS 証明書を使用しますが、そのほとんどは証明書管理によって管理されます。

Web UI

Cisco Prime Network Registrar は、Cisco Prime Network Registrar Web UI の製品インストールの一部として自己署名証明書を生成しますが、ユーザーは独自の証明書を使用することもできます。『*Cisco Prime Network Registrar 11.1* 権威およびキャッシング *DNS* ユーザ ガイド』の「独自の Web UI アクセス用証明書のインストール」を参照してください。証明書は、証明書管理に追加してモニタリングおよびアラームに使用できます。証明書が期限切れまたは無効な場合、ユーザーは Web UI にアクセスできなくなりますが、これは CLI およびシステムコマンドを使用して修復できます。

Web UI 証明書は、Cisco Prime Network Registrar のすべてのサポート対象バージョンで使用されます。

構成管理サーバー

Cisco Prime Network Registrar は、Web UI/CLI から Cisco Prime Network Registrar 構成管理サーバー（ccm）への通信に使用する CPNR 構成管理サーバーの製品インストールの一部として自己署名証明書を生成しますが、ユーザーは独自の証明書を使用することもできます。『*Cisco Prime Network Registrar 11.1* 権威およびキャッシング *DNS* ユーザ ガイド』の「独自の Web UI アクセス用証明書のインストール」を参照してください。

初期証明書は、インストールプロセスの一部として生成されます。その後、ユーザーはこれらの証明書を手動で更新できます。

証明書は、証明書管理に追加してモニタリングおよびアラームに使用できます。証明書が期限切れになった場合や証明書が無効な場合、ユーザーは Web UI にアクセスできなくなりますが、これはシステムコマンドを使用して修復できます。

Cisco Prime Network Registrar 設定管理証明書は、サポート対象のすべてのバージョンの Cisco Prime Network Registrar で使用されます。

権威 DNS サーバー

権威 DNS サーバーは、DNS over TLS/HTTPS（DoT/DoH）のサポートを提供するときに SSL/TLS 証明書を使用します。有効にすると、ユーザーは証明書管理に追加する SSL/TLS 証明書を指定するか、証明書を手動で入力できます。『Cisco Prime Network Registrar 11.1 Authoritative and Caching DNS User Guide』の「Specifying TLS Settings」セクションを参照してください。

権威 DNS TLS 証明書は、Cisco Prime Network Registrar 11.0 で導入され、そのリリースより前では使用されていませんでした。

キャッシュ DNS サーバー

キャッシング DNS サーバーは、TLS/HTTPS（DoT/DoH）を介したキャッシング/再帰 DNS サービスを提供するために有効になっている場合、SSL/TLS 証明書を使用します。有効にすると、ユーザーは証明書管理に追加する SSL/TLS 証明書を指定するか、証明書を手動で入力できます。『Cisco Prime Network Registrar Authoritative and Caching DNS User Gudie』の「Specifying TLS Settings」セクションを参照してください。

キャッシング DNS サーバーは、オペレーティングシステムの一部として提供される証明書を含む証明書バンドルを使用することもできます。

キャッシング DNS TLS 証明書は、Cisco Prime Network Registrar 11.0 で導入され、そのリリースより前では使用されていませんでした。

証明書有効期限の通知

CCM は、証明書の有効性に基づいてリソース管理オブジェクトを作成します。リソース設定に基づいて証明書の有効期限をモニターし、アラートを発行します。

certificate-expiration-warning-level 属性は、証明書の有効期限の警告レベルを指定します。現在の時間がこの値を超えると、警告通知がトリガーされます。デフォルトは 25% です。*certificate-expiration-critical-level* 属性は、証明書の有効期限の重大度レベルを指定します。現在の時間がこの値を超えると、重大度通知がトリガーされます。デフォルト値は 10% です。

証明書の有効期限に関するこれらのしきい値を設定するには、次の手順を実行します。

ローカル詳細およびリージョン詳細 Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 左側の [サーバーの管理（Manage Servers）] ペインの [CCM] をクリックします。[ローカルCCMサーバーの編集（Edit Local CCM Server）] ページが表示されます。

ステップ 3 [リソース制限の設定（**Configure Resource Limits**）] タブをクリックします。

ステップ 4 **[証明書の有効期限（Certificate Expiration）]** セクションで *certificate-expiration-warning-level* と *certificate-expiration-critical-level* 属性を見つけます。要件に応じて、これらの属性の値を設定します。

ステップ 5 [保存（Save）] をクリックして設定を保存します。

CLI コマンド

resource set certificate-expiration-warning-level=*value* を使用して、証明書の有効期限の警告レベルを設定します。

resource set certificate-expiration-critical-level=*value* を使用して、証明書の有効期限の重大度レベルを設定します。

ローカル クラスタ管理チュートリアル

このチュートリアルでは、Example Company のローカル クラスタの基本的なシナリオについて説明します。クラスタの管理者は、ユーザー、ゾーン データ、DHCP データ、アドレス空間データ、およびサーバーについて一般に責任を負います。タスクは、2 つのゾーン（example.com と boston.example.com）、ゾーン内のホスト、およびサブネットをセットアップすることです。また、ローカル クラスタは、リージョン クラスタ管理チュートリアル （81 ページ） に述べられているように、サンノゼのリージョンクラスタが中央構成を実行し、別のクラスタのローカルクラスタ管理者とアドレス空間を複製できるように、特別な管理者アカウントも作成する必要があります。

関連項目

管理者の責任とタスク （73 ページ）

管理者の作成 （74 ページ）

アドレス インフラストラクチャの作成 （75 ページ）

ゾーン インフラストラクチャの作成 （76 ページ）

制約付きのホスト管理者ロールの作成 （78 ページ）

ホスト管理者に割り当てるグループの作成 （80 ページ）

ホスト アドレス範囲のテスト （80 ページ）

管理者の責任とタスク

ローカル クラスタ管理者には、次の責任とタスクがあります。

- **example-cluster-admin**- スーパーユーザーによって作成されます。
  - Boston クラスタでは、他のローカル管理者を作成します（example-zone-admin と example-host-admin）。

- ローカル クラスタの基本的なネットワーク インフラストラクチャを作成します。
- example-host-role を boston.example.com ゾーン内のアドレス範囲に制限します。
- example-zone-admin が example-host-admin に割り当てる example-host-group（example-host-role で定義）を作成します。

- **example-zone-admin**：
  - example.com ゾーンと boston.example.com ゾーンを作成し、後者のゾーンを保守します。
  - example-host-group を example-host-admin に割り当てます。
- **example-host-admin**- ローカル ホスト リストと IP アドレスの割り当てを保守します。

管理者の作成

この例では、ボストンのスーパーユーザーが、管理者の責任とタスク （73 ページ） に説明されているように、ローカル クラスタ、ゾーン、およびホスト管理者を作成します。

ローカル基本 Web UI

ステップ 1 ボストンのローカル クラスタで、スーパーユーザー（通常は **admin**）としてログインします。

ステップ 2 基本モードで、[管理（**Administration**）] メニューから [管理者（**Administrators**）] を選択します。

ステップ 3 ローカル クラスタ管理者（スーパーユーザーアクセス権を持つ）を追加します。[管理者の一覧表示/追加（List/Add Administrators）] ページで。

a) [管理者（Administrators）] ペインの [管理者の追加（Add Administrators）] アイコンをクリックし、[名前（Name）] フィールドに **example-cluster-admin** と入力します。
b) [パスワード（Password）] フィールドと [パスワードの再入力（Confirm password）] フィールドに **exampleadmin** と入力し、[管理者の追加（Add Admin）] をクリックします。
c) [スーパーユーザー（Superuser）] チェックボックスをオンにします。
d) [グループ（Groups）] リストからグループを選択しないでください。
e) [保存（**Save**）] をクリックします。

ステップ 4 同じページでローカル ゾーン管理者を追加します。

a) [管理者（Administrators）] ペインの [管理者の追加（Add Administrators）] アイコンをクリックし、[名前（Name）] フィールドに **example-zone-admin** と入力し、[パスワード（Password）] フィールドと [パスワードの再入力（Confirm Password）] フィールドに **examplezone** と入力して、[管理者の追加（Add Admin）] をクリックします。
b) [管理者の編集（Edit Administrator）] ページの [グループ（Groups）] セクションにある [追加（Add）] をクリックして、[グループ（Groups）] ウィンドウを開きます。**ccm-admin-group**、**dns-admin-group**、および **host-admin-group** を選択して、[**選択（Select**）] をクリックします。選択されたグループが、[管理者の編集（Edit Administrator）] ページの [グループ（Groups）] セクションに表示されます。

dns-admin-group は、DNS ゾーンおよびサーバーを管理する dns-admin ロールですでに事前定義されています。ccm-admin-group では、example-zone-admin は後で制約付きロールで example-host-admin をセットアップできます。host-admin-group は、主に、ゾーン内のホスト作成をテストします。

c) [保存（**Save**）] をクリックします。

ステップ 5 同じページでローカル ホスト管理者を追加します。

a) [管理者（Administrators）] ペインの [管理者の追加（Add Administrators）] アイコンをクリックし、[名前（Name）] フィールドに **example-host-admin** と入力し、[パスワード（Password）] フィールドに **examplehost** と入力して、[管理者の追加（Add Admin）] をクリックします。

b) この時点ではグループを選択しないでください。（example-zone-admin は、後で、example-host-admin を制約付きロールを持つグループに割り当てます）。

c) [保存（**Save**）] をクリックします。

（注） 管理者に制約を適用する方法の詳細については、制約付きのホスト管理者ロールの作成（78 ページ） を参照してください。

アドレス インフラストラクチャの作成

クラスタでゾーンとホストを管理するための前提条件は、基盤となるネットワークインフラストラクチャを作成することです。ネットワーク設定は、多くの場合、すでに存在し、インポートされています。ただし、このチュートリアルでは、白紙の状態から始めることを前提としています。

ローカルの example-cluster-admin は次に、静的 IP アドレスが割り当てられる boston.example.com ゾーン内のホストに対して許可されるアドレス範囲を作成します。これらのアドレスは、100 ~ 200 の範囲のホストを持つ 192.168.50.0/24 サブネット内にあります。

ローカル詳細 Web UI

ステップ 1 ローカル クラスタで、スーパーユーザーとしてログアウトし、**example-cluster-admin** ユーザーとしてパスワード **exampleadmin** を使用してログインします。管理者はスーパーユーザーであるため、すべての機能を使用できます。

ステップ 2 **Advanced** をクリックして、詳細モードに入ります。

ステップ 3 [**設計（Design**）] メニューから、[**DHCPv4**] サブメニューの [**サブネット（Subnets**）] を選択して、[サブネットの一覧表示/追加（List/Add Subnets）] ページを開きます。

ステップ 4 [サブネットの一覧表示/追加（List/Add Subnets）] ページで、boston.example.com サブネット アドレスを入力します。

a) [サブネット（Subnets）] ペインの [**サブネットの追加（Add Subnets**）] アイコンをクリックし、[アドレス（Address）] フィールドに **192.168.50** と入力します。

b) [マスク（mask）] ドロップダウン リストで **24** を選択します。このサブネットは、通常のクラス C ネットワークになります。

c) [所有者（Owner）]、[リージョン（Region）]、および [アドレス タイプ（Address Type）] フィールドはそのままにしておきます。必要な場合は説明を追加します。
d) **Add Subnet** をクリックします。

ステップ 5 192.168.50.0/24 アドレスをクリックして、[サブネットの編集（Edit Subnet）] ページを開きます。

ステップ 6 [IP 範囲（IP Ranges）] フィールドに、静的アドレスの範囲を入力します。
a) [開始（Start）] フィールドに **100** と入力します。次のフィールドにタブ移動します。
b) [終了（End）] フィールドに **200** と入力します。
c) **Add IP Range** をクリックします。アドレスの範囲がフィールドの下に表示されます。

ステップ 7 **Save** をクリックします。

ステップ 8 **Address Space** をクリックすると、[ユニファイド アドレス空間の表示（View Unified Address Space）] ページが開きます。192.168.50.0/24 サブネットがリストに表示されます。[**更新（Refresh**）] アイコンをクリックします。

ゾーン インフラストラクチャの作成

このシナリオでは、example-cluster-admin は、example.com ゾーンとそのサブゾーンを含めて、Example Company のゾーンをローカルに作成する必要があります。example-cluster-admin は、いくつかの初期ホスト レコードも boston.example.com ゾーンに追加します。

転送ゾーンの作成

まず、example.com と boston.example.com の転送ゾーンを作成します。

ローカル基本 Web UI

ステップ 1 ローカル クラスタで、**example-zone-admin** ユーザーとしてパスワード **examplezone** でログインします。

ステップ 2 **Design** メニューから、**Auth DNS** サブメニューの**Forward Zones** を選択します。[ゾーンの一覧表示/追加（List/Add Zones）] ページが開きます。

ステップ 3 example.com ゾーンを作成します（フィールド間移動にはタブを使用します）。
a) [転送ゾーン（Forward Zones）] ペインの [**転送ゾーンの追加（Add Forward Zone**）] アイコンをクリックし、[名前（Name）] フィールドに **example.com** と入力します。
b) [ネームサーバー FQDN（Nameserver FQDN）] フィールドに、**ns1** と入力します。
c) [連絡先の電子メール（Contact E-Mmail）] フィールドに、**hostadmin** と入力します。
d) [シリアル番号（Serial Number）] フィールドに、シリアル番号を入力します。
e) **Add Zone** をクリックします。

ステップ 4 前の手順と同じ値を使用して、同じ方法で **boston.example.com** ゾーンを作成します。
a) 既存のゾーンにプレフィックスが追加されたゾーンを作成すると、[親ゾーンにサブゾーンを作成（Create Subzone in Parent Zone）] ページが開きます。これは、ゾーンが潜在的なサブゾーンである可能性があるためです。このゾーンを example.com のサブゾーンとして作成するには、[親ゾーンにサブゾーンを作成（Create Subzone in Parent Zone）] ページ の **Create as Subzone** をクリックします。

b) ネームサーバーはゾーンごとに異なるため、複数のゾーンを関連付けるには、グルー アドレス（A）レコードを作成する必要があります。[A レコード（A record）] フィールドに 192.168.50.1 と入力して、**Specify Glue Records** をクリックします。次に、**Report**、**Run**、および **Return** をクリックします。

c) [ゾーンの一覧表示/追加（List/Add Zones）] ページに example.com と boston.example.com が表示されます。

ステップ 5 **Advanced** をクリックしてから **Show Forward Zone Tree** をクリックして、ゾーンの階層を表示します。リスト モードに戻るには、**Show Forward Zone List** をクリックします。

逆引きゾーンの作成

次に、example.com と boston.example.com の逆引きゾーンを作成します。これにより、追加された各ホストの逆引きアドレス ポインタ（PTR）レコードを追加できます。Example.com の逆引きゾーンは、192.168.50.0 サブネットに基づきます。boston.example.com の逆引きゾーンは、192.168.60.0 サブネットに基づきます。

ローカル基本 Web UI

ステップ 1 ローカル クラスタで、前のセクションと同じように、example-zone-admin ユーザーとしてログインします。

ステップ 2 [**設計（Design**）] メニューから、**Reverse Zones** サブメニューの **Auth DNS** を選択します。

ステップ 3 [逆引きゾーンの一覧表示/追加（List/Add Reverse Zones）] ページで、[逆引きゾーン（Reverse Zones）] ペインの [**逆引きゾーンの追加（Add Reverse Zone**）] アイコンをクリックし、[名前（Name）] フィールドに **50.168.192.in-addr.arpa** と入力します。（ループバック アドレス 127.in-addr.arpa の逆引きゾーンは既に存在ます）。

ステップ 4 転送ゾーンの値を使用し、必要なフィールドに入力して、逆引きゾーンを作成します。

a) **Nameserver - ns1.example.com.** を入力します（必ず末尾のドットを含めてください）。

b) **Contact E-Mail - hostadmin.example.com.** を入力します（必ず末尾のドットを含めてください）。

c) [**シリアル番号（Serial number**）] - シリアル番号を入力します。

ステップ 5 **Add Reverse Zone** クリックして、ゾーンを追加し、[逆引きゾーンの一覧表示/追加（List/Add Reverse Zones）] ページに戻ります。

ステップ 6 boston.example.com ゾーンについて同じことをしますが、ゾーン名として **60.168.192.in-addr.arpa** を使用し、**ステップ 4** と同じネームサーバーと連絡先電子メール値を使用します。（テーブルから値をカットアンドペーストすることができます）。

最初のホストの作成

ボストン クラスタでホストを作成できることを確認するために、example-zone-admin は example.com ゾーンで 2 つのホストの作成を試みます。

ローカル詳細 Web UI

ステップ 1 example-zone-admin ユーザーとして、**Advanced** をクリックして詳細モードに入ります。

ステップ 2 [設計（**Design**）] メニューから、**Hosts** サブメニューの **Auth DNS** を選択します。[ゾーンのホストの一覧表示/追加（List/Add Hosts for Zones）] ページが開きます。ウィンドウの左側にある [ゾーンの選択（Select Zones）] ボックスに、boston.example.com と example.com が表示されます。

ステップ 3 ゾーンのリストの example.com をクリックします。

ステップ 4 アドレス 192.168.50.101 を持つ最初の静的ホストを追加します。

a) [名前（Name）] フィールドに **userhost101** と入力します。

b) [IPアドレス（IP Address(es)）] フィールドに完全なアドレス **192.168.50.101** を入力します。[IPv6アドレス（IPv6 Address(es)）] フィールドと [エイリアス（Alias(es)）] フィールドは空白のままにします。

c) [PTRレコードの作成（Create PTR Records?）] チェックボックスがオンになっていることを確認します。

d) **Add Host** をクリックします。

ステップ 5 同じ方法で、2 番目のホスト **userhost102** をアドレス **192.168.50.102** で追加します。2 つのホストが、[ゾーンのホストの一覧表示/追加（List/Add Hosts for Zone）] ページにネームサーバー ホストとともに表示されます。

制約付きのホスト管理者ロールの作成

チュートリアルのこの部分では、ボストンの example-cluster-admin は boston.example.com ゾーンにアドレス制約付きの example-host-role を作成します。

ローカル詳細 Web UI

ステップ 1 example-zone-admin ユーザとしてログアウトし、**example-cluster-admin** ユーザー（パスワード **exampleadmin**）としてログインします。

ステップ 2 [詳細（**Advanced**）] をクリックして、詳細モードに入ります。

ステップ 3 [管理（**Administration**）] メニューから、[ユーザー アクセス（User Access）] サブメニューの [ロール（**Roles**）] を選択して、[管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページを開きます。

ステップ 4 example-host-role を追加します。

a) [ロール（Roles）] ペインの [ロールの追加（Add Role）] アイコンをクリックして、[ロールの追加（Add Roles）] ダイアログボックスを開きます。

b) [名前（Name）] フィールドに **example-host-role** と入力します。

c) [ロールの追加（Add Role）] をクリックします。example-host-role が、[管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページのロールのリストに表示されます。

ステップ 5 ロールの制約を追加します。

a) [制約の追加（**Add Constraint**）] をクリックします。

b) [ロールの制約の追加（Add Role Constraint）] ページで、[ホスト制限（Host Restrictions）] まで下にスクロールします。
c) *all-forward-zones* 属性について、**false** ラジオ ボタンをクリックします。
d) *zones* 属性として、**boston.example.com** と入力します。
e) *ipranges* 属性として、範囲 **192.168.50.101–192.168.50.200** を入力します。
f) *zone-regexpr*および *host-regexpr* 属性フィールドには、正規表現を入力して、それぞれゾーンとホストを正規表現構文で照合します。（よく使用される正規表現の値については、次の表を参照してください）。

表 *9*：一般的な正規表現の値

値	一致
.（ドット）	任意の文字（ワイルドカード）。ドット文字そのもの（ドメイン名など）に一致させるには、バックスラッシュ（\）を使用してエスケープする必要があります（**\.com** は .com に一致します）。
\char	続くリテラル文字（*char*）、または *char* には特別な意味があります。特にドット（**.**）やもう 1 つのバックスラッシュなどのメタ文字をエスケープするために使用されます。特別な意味としては、10 進数に一致させる **\d**、非数字に一致させる **\D**、英数字に一致させる **\w**、および空白に一致させる **\s** などがあります。
*char***?**	先行する 1 個または 0 個の *char* は、その文字が任意であることを意味します。たとえば、**example\.?com** は example.com または examplecom に一致します。
*char******	先行する 0 個以上の *char*。たとえば、**ca*t** は ct、cat、および caaat に一致します。この反復メタキャラクタは、文字セットで反復処理を行います（**[**文字セット**]**を参照）。
*char***+**	先行する 1 個以上の *char*。たとえば、**ca+t** は cat と caaat に一致します（ct には一致しません）。
[*charset***]**	ブラケットで囲まれた任意の文字（文字セット）。**[a–z]**（任意の小文字と一致する）など、文字範囲を含めることができます。***** 繰り返しメタ文字が適用されている場合、検索エンジンは、一致に影響を与えるために必要な回数だけセットを繰り返します。たとえば、**a[bcd]*b** は、abcbd を見つけます（2 回目のセットを繰り返すことによって）。メタ文字の多く（ドットなど）は非アクティブであり、文字セット内ではリテラルと見なされることに注意してください。
[^*charset***]**	*charset* 以外の任意の文字。たとえば、**[^a-zA-Z0-9]** は非英数字に一致します（**\W** を使用することと同じ）。文字セットの外側のキャレットは異なる意味を持つことに注意してください。
^	行頭。
$	行末。

g) **Add Constraint** をクリックします。制約のインデックス番号は 1 になります。

ステップ 6 **Save** をクリックします。

ホスト管理者に割り当てるグループの作成

ボストンの example-cluster-admin は、example-host-role を含む example-host-group を作成して、example-zone-admin がこのグループを example-host-admin に割り当てることができるようにします。

ローカル詳細 Web UI

ステップ 1 example-cluster-admin として、詳細もノードのままで、[**管理（Administration**）] メニューから **Groups** サブメニューを選択して、[管理者グループの一覧表示/追加（List/Add Administrator Groups）] ページを開きます。

ステップ 2 example-host-group を作成して、それに example-host-role を割り当てます。

a) [グループ（Groups）]ペインの[**グループの追加（Add Groups**）]アイコンをクリックし、[名前（Name）] フィールドに **example-host-group** と入力します。
b) [ベース ロール（Base Role）] ドロップダウン リストから、**example-host-role** を選択します。
c) **Add Group** をクリックします。
d) **Group for the example-host-role** のような説明を追加して、[**保存（Save**）] をクリックします。

ステップ 3 example-cluster-admin としてログアウトしてから、**example-zone-admin** ユーザー（パスワード **examplezone**）としてログインします。

ステップ 4 example-zone-admin として、example-host-group を example-host-admin に割り当てます。

a) 基本モードで、**Administration**メニューから **Administrators** を選択します。
b) [管理者の一覧表示/追加（List/Add Administrators）] ページで、example-host-admin をクリックして管理者を編集します。
c) [管理者の編集（Edit Administrator）] ページで、[使用可能（Available）] リストの **example-host-group** を選択し、<< をクリックして、[選択済み（Selected）] リストに移動します。
d) **Save** をクリックします。example-host-admin は [List/Add Administrators] ページの [Groups] 列に example-host-group が表示されているのを確認できます。

ホスト アドレス範囲のテスト

example-host-admin は次に、範囲外のアドレスをテストし、受け入れ可能なアドレスを追加します。

ローカル詳細 Web UI

ステップ 1 ローカル クラスタで、example-zone-admin としてログアウトしてから、**example-host-admin** として（パスワード **examplehost** を使用して）ログインします。

ステップ 2 **Advanced** をクリックして、詳細モードに入ります。

ステップ 3 **Design** メニューから、**Auth DNS** サブメニューの **Hosts** を選択します。

ステップ 4 [ゾーンのホストの一覧表示/追加] ページで、範囲外のアドレスを入力してみてください（[有効な IP 範囲（Valid IP Ranges）] フィールドの有効なアドレスの範囲に注意してください）。

a) [名前（Name）] フィールドに **userhost3** と入力します。

b) [IP アドレス（IP Address(es)）**192.168.50.3**] フィールドに、故意に範囲外のアドレスを入力します。

c) **Add Host** をクリックします。エラー メッセージが表示されます。

ステップ 5 有効な IP アドレスを入力します。

a) **userhost103** を入力します。

b) [IP アドレス（IP Address(es)] フィールドに **192.168.50.103** を入力します。

c) **Add Host** をクリックします。ホストがアドレスとともにリストに表示されます。

リージョン クラスタ管理チュートリアル

このチュートリアルは、ローカル クラスタ管理チュートリアル（73 ページ） で説明されているシナリオの拡張です。リージョン クラスタのチュートリアルでは、サンノゼに 2 名の管理者（リージョン クラスタ管理者と中央設定管理者）がいます。彼らの目的は、これらのクラスタのサーバーを使用して、DNS ゾーン配布、ルータ設定、および DHCP フェールオーバー設定を作成するために、ボストンおよびシカゴのローカル クラスタとアクティビティを調整することです。構成は、次のとおりです。

- サンノゼの 1 つのリージョン クラスタ マシン。
- 2 つのローカル クラスタ マシン（ボストンに 1 つ、シカゴに 1 つ）。
- シカゴに 1 つの Cisco uBR7200 ルータ。

管理者の責任とタスク

リージョン管理者には、次の責任とタスクがあります。

- **example-regional-admin**- サンノゼのリージョン クラスタで、example-cfg-admin を作成するスーパーユーザーによって作成されます。
- **example-cfg-admin**：
  - ボストンおよびシカゴのクラスタを定義し、それらとの接続を確認します。
  - ルータおよびルータ インターフェイスを追加します。

- ローカル クラスタからゾーン データをプルして、ゾーン配布を作成します。
- サブネットとポリシーを作成し、アドレス空間をプルして、ボストンとシカゴのDHCP フェールオーバー ペアを設定します。

リージョン クラスタ管理者の作成

リージョンのスーパーユーザーは、まず、クラスタとユーザーの管理を実行するために、グループとともに定義された example-regional-administrator を作成します。

リージョン Web UI

ステップ 1 スーパーユーザーとしてリージョンクラスタにログインします。

ステップ 2 [管理（**Administration**）] メニューから [ユーザーアクセス（User Access）] サブメニューの [管理者（**Administrators**）] を選択して、このページのローカル クラスタ バージョンの [管理者の一覧表示/追加（Add Administrators）] ページを開きます。これは基本的に同じです。

ステップ 3 [管理者（Administrators）] ペインの [管理者の追加（Add Administrators）] アイコンをクリックし、[名前（Name）] フィールドに **example-regional-admin** と入力し、[パスワード（Password）] フィールドと [パスワードの再入力（Confirm Password）] フィールドに **examplereg** と入力して、[管理者の追加（Add Admin）] をクリックします。

ステップ 4 [管理者の編集（Edit Administrator）] ページの [グループ（Groups）] セクションにある [追加（Add）] をクリックして、[グループ（Groups）] ウィンドウを開きます。**central-cfg-admin-group**（クラスタ管理のため）および **regional-admin-group**（ユーザー管理のため）を選択し、[選択（Select）] をクリックします。選択されたグループが、[管理者の編集（Edit Administrator）] ページの [グループ（Groups）] セクションに表示されます。

ステップ 5 **Save** をクリックします。

中央構成管理者の作成

このチュートリアルの一部として、example-regional-admin は次に、ログインして、example-cfg-admin を作成します。これは、リージョンの設定およびアドレス管理能力を持つ必要があります。

リージョン Web UI

ステップ 1 スーパーユーザーとしてログアウトし、**example-regional-admin** としてパスワード **examplereg** でログインします。管理者には、ホストとアドレス空間のすべての管理権限があることに注意してください。

ステップ 2 [管理（**Administration**）] メニューから、[ユーザー アクセス（User Access）] サブメニューの [管理者（**Administrators**）] を選択して、[管理者の一覧表示/追加（List/Add Administrators）] ページを開きます。

ステップ 3 [管理者（Administrators）] ペインの [**管理者の追加（Add Administrators**）] アイコンをクリックし、[名前（Name）] フィールドに **example-cfg-admin** と入力し、[パスワード（Password）] フィールドと [パスワードの再入力（Confirm Password）] フィールドに **cfgadmin** と入力して、[**管理者の追加（Add Admin**）] をクリックします。

ステップ 4 [管理者の編集（Edit Administrator）] ページの [グループ（Groups）] セクションにある [追加（Add）] をクリックして、[グループ（Groups）] ウィンドウを開きます。**central-cfg-admin-group** および **regional-addr-admin-group** を選択して、[選択（Select）] をクリックします。選択されたグループが、[管理者の編集（Edit Administrator）] ページの [グループ（Groups）] セクションに表示されます。

ステップ 5 **Save** をクリックします。example-cfg-admin に割り当てられた 2 つのグループが表示されます。

管理者の制約を追加することもできます。[制約の追加（**Add Constraint**）] をクリックし、[ロールのロール制約の追加（Add Role Constraint for Role）] ページで、読み取り専用、所有者、またはリージョン制約を選択し、 [制約の追加（**Add Constraint**）] をクリックします。

ローカル クラスタの作成

example-cfg-admin は次に、ボストンとシカゴの 2 つのローカル クラスタを作成します。

リージョン Web UI

ステップ 1 example-regional-admin としてログアウトし、**example-cfg-admin** としてパスワード **cfgadmin** でログインします。

ステップ 2 **Operate** メニューから、**Manage Clusters** サブメニューの **Servers** を選択して、[リモート クラスの一覧表示/追加（List/Add Remote Clusters）] ページを開きます。

ステップ 3 [**Add Manage Clusters**クラスタの管理（Manage Clusters）] ペインの アイコンをクリックします。

ステップ 4 [クラスタの追加（Add Cluster）] ダイアログボックスで、管理者から提供されたデータに基づいてボストン クラスタを作成します。

a) [名前（Name）] フィールドに **Boston-cluster** と入力します。
b) [IPv4 アドレス（IPv4 Address）] フィールドにボストン サーバーの IPv4 アドレスを入力します。
c) [IPv6 アドレス（IPv6 Address）] フィールドにボストン サーバーの IPv6 アドレスを入力します。
d) [管理者名（Admin Name）] フィールドに **example-cluster-admin** と入力し、[管理者パスワード（Admin Password）] フィールドに **exampleadmin** と入力します。
e) [SCP ポート（SCP Port）] フィールドに、インストール時に設定された、クラスタにアクセスする SCP ポートを入力します（**1234** はプリセット値です）。
f) **Add Cluster** をクリックします。

ステップ 5 同じ方法でシカゴ クラスタを作成しますが、[名前（name）] フィールドに **Chicago-cluster** を使用し、残りの値はシカゴ管理者から提供されたデータに基づいて入力し、**Add Cluster** をクリックします。2 つのクラスタが [リモート クラスタの一覧表示/追加（List/Add Remote Clusters）] ページに表示されます。

ステップ 6 ボストン クラスタに接続します。Boston-cluster の横にある [**ローカルに移動（Go Local**）] アイコンをクリックします。ローカル クラスタの [サーバーの管理（Manage Servers）] ページが開いた場合、クラスタ

への管理者の接続が確定されます。リージョン クラスタ Web UI に戻るには、[**リージョンに移動（Go Regional**）] アイコンをクリックします。

ステップ 7 シカゴのクラスタに接続して、同じ方法で接続を確認します。

ステップ 8 ボストンのクラスタ同期から 2 つの転送ゾーンのデータを複製できることを確認します。

a) **Operate** メニューから、 **Servers** サブメニューの **View Replica Data** を選択します。
b) [レプリカ クラス リストの表示（View Replica Class List）] ページで、[クラスタの選択（Select Cluster）] リストの Boston-cluster をクリックします。
c) [クラスの選択（Select Class）] リストの **Forward Zones** をクリックします。
d) [**データの複製（Replicate Data**）] をクリックします。
e) **View Replica Class List** をクリックします。[クラスタのレプリカ転送ゾーンの一覧表示（List Replica Forward Zones for Cluster）] ページに、boston.example.com ゾーンと example.com ゾーンが表示されます。

ルータの追加とインターフェイスの変更

次の example-cfg-admin は、リージョン クラスタを引き継ぎ、ルータを追加し、インターフェイスの 1 つを変更して DHCP リレー エージェントを設定します。サブネットを手動で追加します。

リージョン詳細 Web UI

ステップ 1 example-cfg-admin として、[**展開（ Deploy**）] メニューから、**Router Configuration** サブメニューの **Router List** を選択します。

ステップ 2 [ルータの一覧表示/追加（List/Add Routers）] ページで、[ルータ リスト（Router List）] ペインの [**ルータの追加（Add router**）] アイコンをクリックします。

ステップ 3 [ルータの追加（Add Router）] ダイアログボックスで、管理者からのデータに基づいてルータを追加します。

a) [名前（name）] フィールドにルータの識別名を指定します。この例では、**router-1** と入力します。
b) [説明（description）] フィールドにルータの説明を入力します。
c) アドレス フィールドに、ルータの管理インターフェイス アドレスを入力します。
d) ip6address フィールドに、ルータの IPv6 管理インターフェイスのアドレスを入力します。
e) 所有者とリージョンを選択します。
f) **Add Router** をクリックします。これで、ルータが [ルータの一覧表示/追加（List/Add Routers）] ページに表示されます。

ステップ 4 ルータが作成されたことを確認します。**Router Tree** をクリックすると、[ルータのツリーの表示（View Tree of Routers)] ページに、router-1 のルータ インターフェイスの階層が表示されます。

ステップ 5 ルータの DHCP リレー エージェントを設定します。

a) ルータの新しいインターフェイスを作成します。

b) [ルータのツリーの表示（View Tree of Routers）] ページのインターフェイス名をクリックして、[ルータ インターフェイスの編集（Edit Router Interface）] ページを開きます。（または、[ルータの一覧表示/追加（List/Add Routers）] ページから、ルータに関連付けられている [**インターフェイス（Interfaces**）] アイコンをクリックし、[ルータのルータ インターフェイスの一覧表示（List Router Interfaces for Router）] ページのインターフェイス名をクリックします）。

c) [ルータ インターフェイスの編集（Edit Router Interface）] ページで、[ip-helper] フィールドに DHCP サーバーの IP アドレスを入力します。

d) ページ下部の **Save** をクリックします。

ステップ 6 ルータ管理者とともに、DHCP リレー エージェントが正常に追加されたことを確認します。

構成管理者へのゾーン管理の追加

Chicago クラスタにはゾーンがセットアップされていないため、example-cfg-admin はリージョン クラスタでゾーンを作成して、ゾーン分散の一部にすることができます。ただし、example-regional-admin は、まず、example-cfg-admin を変更して、ゾーンを作成できるようにする必要があります。

リージョン Web UI

ステップ 1 example-cfg-admin としてログアウトし、**example-regional-admin** としてログインします。

ステップ 2 **[管理（Administration）]** メニューから、[ユーザー アクセス（User Access）] サブメニューの [グループ（Administrators）] を選択します。

ステップ 3 [管理者の一覧表示/追加（List/Add Administrators）] ページで、[管理者（Administrators）] ペインから example-cfg-admin をクリックします。

ステップ 4 [管理者の編集（Edit Administrator）] ページで、[使用可能なグループ（Groups Available）] リストの central-dns-admin-group をクリックし、（<< を使用して）[選択済み（Selected）] リストに移動します。[選択済み（Selected）] リストに central-cfg-admin-group、regional-addr-admin-group、および central-dns-admin-group が表示されます。

ステップ 5 **Save** をクリックします。変更が [管理者の一覧表示/追加（List/Add Administrators）] ページに反映されます。

ローカル クラスタのゾーンの作成

example-cfg-admin は次に、ボストンおよびシカゴ ゾーンとのゾーン分散のための chicago.example.com ゾーンを作成します。

リージョン Web UI

ステップ 1 example-regional-admin としてログアウトし、**example-cfg-admin** としてログインします。

ステップ 2 [設計（Design）] メニューから、[**Auth DNS**] サブメニューの **Forward Zones** を選択します。

ステップ 3 [転送ゾーン（Forward Zones）] ペインの **Add Forward Zone** アイコンをクリックします。

ステップ 4 [ゾーンの追加（Add Zone）] ダイアログボックスで、次のように入力します。

a) **Name - chicago.example.com**。
b) **Nameserver FQDN - ns1**。
c) **Contact E-mail - hostadmin**。
d) **Nameservers - ns1**（**Add Nameserver** をクリック）。
e) **Add DNS Zone** をクリックします。

ステップ 5 **Reverse Zones** サブメニューをクリックします。

ステップ 6 [逆引きゾーンの一覧表示/追加（List/Add Reverse Zones）] ページで、適切な属性が設定された Chicago ゾーンの **60.168.192.in-addr.arpa** 逆引きゾーンを作成します。

ゾーン データのプルとゾーン分散の作成

example-cfg-admin は次に、ボストンとシカゴからゾーン データをプルして、ゾーン分散を作成します。

リージョン Web UI

ステップ 1 example-cfg-admin として、**Design** メニューから **Auth DNS** サブメニューの **Views** を選択して、[ゾーン ビューの一覧表示/追加（List/Add Zone Views）] ページを表示します。

ステップ 2 [ゾーン ビューの一覧表示/追加（List/Add Zone Views）] ページで、レプリカ データベースからゾーンをプルします。

a) [Views] ペインの **Pull Data** アイコンをクリックします。
b) [プルするレプリカ DNS ビュー データの選択（Select Replica DNS View Data to Pull）] ダイアログボックスで、データ同期モードをデフォルトの [Update] のままにして、**Report** をクリックして、[プル レプリカ ゾーン データの報告（Report Pull Replica Zone Data）] ページを開きます。
c) プルするデータの変更セットに注目してから、**Run** をクリックします。
d) [プルレプリカゾーンデータの実行（Run Pull Replica Zone Data）] ページで、 **OK** をクリックします。

ステップ 3 [ゾーンビューの一覧表示/追加（List/Add Zone Views）] ページで、ボストンクラスタゾーン分散に、[名前（Name）]列でインデックス番号（**1**）が割り当てられていることに注意してください。番号をクリックします。

ステップ 4 [ゾーン ビューの編集（Edit Zone Views）] ページの [プライマリ サーバー（Primary Server）] フィールドで、Boston-cluster をクリックします。Boston クラスタの IP アドレスはプライマリサーバーリスト（つまり、セカンダリサーバーのプライマリサーバーリスト）の最初のプライマリサーバーとなります。

ステップ 5 Chicago-cluster の DNS サーバーを Boston-cluster のセカンダリ サーバーにするには、次のようにします。

a) [セカンダリ サーバー（Secondary Servers）] エリアの **Add Server** をクリックします。

b) [ゾーン分散セカンダリ サーバーの追加（Add Zone Distribution Secondary Server）] ページで、[セカンダリ サーバー（Secondary Server）] ドロップダウン リストから **Chicago-cluster** を選択します。

c) **Add Secondary Server** をクリックします。

ステップ 6 [ゾーン分散の編集（Edit Zone Distribution）] ページの [転送ゾーン（Forward Zones）] エリアで、**chicago.example.com** を [選択済み（Selected）] リストに移動します。

ステップ 7 [逆引きゾーン（Reverse Zones）] エリアで、**60.168.192.in-addr.arpa** を [選択済み（Selected）] リストに移動します。

ステップ 8 **Modify Zone Distribution** をクリックします。

サブネットの作成とアドレス空間のプル

example-cfg-admin は次に、リージョン クラスタにサブネットを作成します。このサブネットは、ローカル クラスタからプルされた他の 2 つのサブネットと結合されて、DHCP フェールオーバー サーバー構成を作成します。

リージョン詳細 Web UI

ステップ 1 example-cfg-admin として、**Design** メニューから**DHCPv4** サブメニューの **Subnets** を選択して、[サブネットの一覧表示/追加（List/Add Subnets）] ページを開きます。ルータを追加することによって作成されたサブネットが表示されます（ルータの追加とインターフェイスの変更 （84 ページ） に）。

ステップ 2 [サブネット（Subnets）] ペインの [**サブネットの追加（Add Subnets）**] アイコンをクリックして、追加のサブネット 192.168.70.0/24 を作成します。

a) [アドレス/マスク（Address/Mask）] フィールドにサブネット ネットワーク アドレスとして **192.168.70**（省略形）を入力します。

b) ネットワーク マスクとして **24**（255.255.255.0）を選択したままにします。

c) **Add Subnet** をクリックします。

ステップ 3 **Address Space** をクリックして、作成したサブネットを確認します。

ステップ 4 [ユニファイド アドレス空間の表示（View Unified Address Space）] ページで、**Pull Replica Address Space** をクリックします。

ステップ 5 [プル レプリカ アドレス空間の選択（Select Pull Replica Address Space）] ページで、すべての項目をデフォルトのままにして、**Report** をクリックします。

ステップ 6 [プル レプリカ アドレス空間の報告（Report Pull Replica Address Space）] ページに、クラスタからの 2 つのサブネットの変更セットが表示されます。**Run** をクリックします。

ステップ 7 **OK** をクリックします。プルされた 2 つのサブネットが、[サブネットの一覧表示/追加（List/Add Subnets）] ページに表示されます。

DHCP ポリシーのプッシュ

example-cfg-admin は次に、DHCP ポリシーを作成し、ローカル クラスタにプッシュします。

リージョン Web UI

ステップ 1 example-cfg-admin として、**Design** メニューから **DHCP Settings** サブメニューの **Policies** を選択します。

ステップ 2 [DHCP ポリシーの一覧表示/追加（List/Add DHCP Policies）] ページで、[ポリシー（Policies）] ペインの **Add Policies** アイコンをクリックします。

ステップ 3 [DHCP ポリシーの追加（Add DHCP Policy）] ダイアログボックスで、すべてのローカル クラスタの中央ポリシーを作成します。

a) [名前（Name）] フィールドに **central-policy-1** と入力します。[オファーのタイムアウト（Offer Timeout）] 値と [猶予期間（Grace Period）] の値はそのままにしておきます。
b) [**DHCP ポリシーの追加（Add DHCP Policy**）] をクリックします。
c) [DHCP ポリシーの編集（Edit DHCP Policy）] ページの [DHCPv4 オプション（DHCPv4 Options）] セクションで、[名前（Name）] ドロップダウン リストから **dhcp-lease-time [51] (unsigned time)** を選択し、[値（Value）] フィールドに、リース期間として **2w**（2 週間）と入力します。
d) **Add Option** をクリックします。
e) [**保存（Save**）] をクリックします。

ステップ 4 ローカル クラスタにポリシーをプッシュします。

a) ポリシー central-policy-1 を選択して、**Push** ボタンをクリックします。
b) [DHCP ポリシー データをローカル クラスタにプッシュ（Push DHCP Policy Data to Local Clusters）] ページで、[データ同期モード（Data Synchronization Mode）] を **Ensure** のままにします。これにより、ポリシーがローカル クラスタで複製されますが、その名前のポリシーがすでに存在する場合は、その属性は置き換えられません。
c) ページの [デスティネーション クラスタ（Destination Clusters）] セクションの **Select All** をクリックします。
d) **<<** をクリックして、両方のクラスタを [選択済み（Selected）] フィールドに移動します。
e) **Push Data to Clusters** をクリックします。
f) プッシュ操作の結果を表示するには、[DHCP ポリシー データのプッシュ レポートの表示（View Push DHCP Policy Data Report）] ページを表示します。

スコープ テンプレートの作成

example-cfg-admin は、次に、フェールオーバー サーバー ペアの作成を処理する DHCP スコープ テンプレートを作成します。

リージョン Web UI

ステップ 1 example-cfg-admin ユーザーとして、[**設計（Design**）] メニューから **DHCPv4** サブメニューの **Scope Templates** を選択します。

ステップ 2 [DHCPスコープテンプレートの一覧表示/追加（List/Add DHCP Scope Templates）] ページで、[スコープテンプレート（Scope Templates）] ペインの **Add Scope Templates** アイコンをクリックします。[名前（Name）] フィールドに **scope-template-1** と入力して、[**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 テンプレートが [DHCP スコープ テンプレートの一覧表示/追加（List/Add DHCP Scope Templates）] ページに表示されます。スコープ テンプレートの基本プロパティを設定します。フィールドに次の値を入力するか選択します。

a) **Scope Name Expression** - 派生スコープの名前を自動生成するには、example-scope 文字列と、スコープに対して定義されたサブネットを連結します。これを行うには、フィールドに **(concat "example-scope-" subnet)** と入力します（カッコも含めて）。

b) **Policy** - ドロップダウン リストの **central-policy-1** を選択します。

c) **Range Expression - (create-range 2 100)** と入力することによって、サブネットの残り（2 番目のアドレスから最後のアドレスまで）に基づいてアドレス範囲を作成します。

d) **Embedded Policy Option Expression - (create-option "routers" (create-ipaddr subnet 1))** と入力することによって、組み込みポリシーでスコープのルータを定義し、サブネット内の最初のアドレスを割り当てます。

ステップ 4 **Save** をクリックします。

フェールオーバー ペアの作成と同期

example-cfg-admin は次に、フェールオーバー サーバー ペア関係を作成し、フェールオーバー ペアを同期します。ボストンの DHCP サーバーがメインになり、シカゴのサーバーがバックアップになります。

リージョン Web UI

ステップ 1 example-cfg-admin ユーザーとして、[**展開（Deploy**）] メニューから、**DHCP** サブメニューの **Failover Pairs** を選択します。

ステップ 2 [DHCPフェールオーバーペアの一覧表示/追加（List/Add DHCP Failover Pairs）] ページで、[フェールオーバーペア（Failover Pairs）] ペインの **Add Failover Pair** アイコンをクリックします。

ステップ 3 [DHCP フェールオーバー ペアの追加（Add DHCP Failover Pair）] ダイアログボックスで、次の値を入力または選択します。

a) **Failover Pair Name - central-fo-pair** を入力します。

b) **Main Server - Boston-cluster** をクリックします。

c) **Backup Server - Chicago-cluster** をクリックします。

d) **Scope Template - scopetemplate-1** をクリックします。
e) **Add Failover Pair** をクリックします。

ステップ 4 フェールオーバー ペアをローカル クラスタと同期します。

a) [DHCPフェールオーバーペアの一覧表示/追加（List/Add DHCP Failover Pairs）] ページで、[同期（Synchronize）] 列の [レポート（Report）] アイコンをクリックします。
b) [フェールオーバー ペアの同期の報告（Report Synchronize Failover Pair）] ページで、ネットワーク データのソースとして **Local Server** を受け入れます。
c) 同期の方向として **Main to Backup** を受け入れます。
d) 操作 **Update** を受け入れます。
e) ページ下部の **Report** をクリックします。
f) [フェールオーバー ペア同期レポートの表示（View Failover Pair Sync Report）] ページで、**Run Update** をクリックします。
g) **Return** をクリックします。

ステップ 5 フェールオーバー設定を確認し、ボストン クラスタでサーバーをリロードします。

a) [DHCP フェールオーバー ペアの一覧表示/追加（List/Add DHCP Failover Pairs）] ページで、Boston-cluster の横にある [**ローカルへ移動（Go Local**）] アイコンをクリックします。
b) [DHCP サーバーの管理（Manage DHCP Server）] ページの [**リロード（Reload**）] アイコンをクリックします。
c) ページの上部にある [**リージョンへ移動（Go Regional**）] アイコンをクリックして、リージョン クラスタに戻ります。

ステップ 6 フェールオーバー設定を確認し、同じ方法でシカゴ クラスタにサーバーをリロードします。

CLI コマンド

フェールオーバー ペアを作成するには、**failover-pair** *name* **create** *main-cluster*/*address backup-cluster*/*address* [*attribute=value ...*] を使用します。次に例を示します。

```
nrcmd> failover-pair example-fo-pair create Example-cluster Boston-cluster
```

フェールオーバー ペア設定を同期するには、**failover-pair** *name* **sync** {**update** | **complete** | **exact**} [{**main-to-backup** | **backup-to-main**}] [**-report-only** | **-report**] を使用します。次に例を示します。

```
nrcmd> failover-pair example-fo-pair sync exact main-to-backup -report
```

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。