管理者の管理

この章では、ローカル クラスタとリージョン クラスタでネットワーク管理者をセットアップする方法について説明します。この章には、多くの管理機能に関するローカルおよびリージョン クラスタのチュートリアルも含まれています。

管理者、グループ、ロール、テナント

ネットワーク管理者が Cisco Prime Network Registrarで実行できる機能のタイプは、割り当てられたロールに基づきます。ローカルおよびリージョン管理者は、これらのロールを定義して、ネットワーク管理機能の粒度を提供できます。Cisco Prime Network Registrar では、管理機能をセグメント化する基本ロールのセットが事前定義されています。これらの基本ロールから、特定のアドレス、ゾーン、およびその他のネットワーク オブジェクトの管理に限定された、さらに制約されたロールを定義できます。

管理者をロールに関連付けるためのメカニズムは、これらのロールを含むグループに管理者を配置することです。

管理者が表示できるデータと設定は、テナントによっても制限されます。管理者にテナント タグが割り当てられている場合、アクセスはテナントに割り当てられたか、読み取り専用のコア設定オブジェクトとしてテナントでの使用が可能にされた設定オブジェクトにさらに制限されます。

管理者とグループ、ロール、およびテナントとの関連

Cisco Prime Network Registrarには、管理者、グループ、ロール、およびテナントの4つの管理者オブジェクトがあります。

- 管理者（**Administrator**）- ログインしたアカウントは、1 つ以上の管理者グループとの関連付けによって、割り当てられたロールに基づいて特定の機能を実行できます。ローカルクラスタでは、これらの機能は、ローカルの中央構成管理（CCM）サーバーとデータベース、ホスト、ゾーン、アドレス空間、および DHCP を管理しています。リージョン クラスタでは、これらの機能は、リージョン CCM サーバーとデータベース、中央構成、およびリージョンのアドレス空間を管理しています。有効にするには、管理者を少なくとも 1 つのグループに割り当てる必要があります。

  管理者の追加については、管理者の管理 （18 ページ） を参照してください。

- グループ（**Group**）- ロールのグループ化。1 つ以上のグループを管理者に関連付ける必要があり、グループを使用可能にするには、グループに少なくとも 1 つのロールが割り当てられている必要があります。Cisco Prime Network Registrar の事前定義グループは、各ロールを一意のグループにマッピングします。

  グループの追加については、グループの管理 （21 ページ） を参照してください。

- ロール（**Role**）- 管理者が管理できるネットワーク オブジェクトと、管理者が実行できる機能を定義します。事前定義の一連のロールがインストール時に作成され、追加の制約付きロールを定義できます。一部のロールには、さらに機能的な制約を加えるサブロールが含まれています。

  ロールの追加については、ロールの管理 （23 ページ） を参照してください。

- テナント（**Tenant**）- 管理者のセットに関連付けられているテナント組織またはグループを識別します。テナントを作成すると、リージョンとローカルの両方のクラスタに保存されるデータは、テナント別にセグメント化されます。テナントが別のテナントのデータにアクセスすることはできません。

  テナントの追加については、テナントの管理 （12 ページ） を参照してください。

管理者タイプ

管理者には、スーパーユーザーと専門管理者の 2 つの基本タイプがあります。

- スーパーユーザー（**Superuser**）- Web UI、CLI、およびすべての機能への無制限のアクセス権を持つ管理者。この管理者タイプは少数のユーザーに制限する必要があります。管理者のスーパーユーザー権限は、他のすべてのロールをオーバーライドします。

ヒント インストール時、または Web UI に初めてログインするときに、スーパーユーザーとパスワードを作成する必要があります。

スーパーユーザーにテナントタグが割り当てられている場合、無制限のアクセスは、対応するテナントデータについてのみ付与されます。他のテナントのデータは表示できず、コア オブジェクトは読み取り専用アクセスに制限されます。

- 専門（**Specialized**）- 管理者が割り当てたロール（および該当する場合はサブロール）に基づいて、特定の DNS 転送またはリバース ゾーンを管理するなど、特別な機能を実行するために名前によって作成された管理者。専門管理者は、スーパーユーザーと同様に、パスワードを必要としますが、関連するロールを定義する少なくとも 1 つの管理者グループに割り当てられる必要もあります。CLI は **admin** コマンドを提供します。

  ローカル ゾーンまたはホスト管理者を作成する例については、管理者の作成 を参照してください。

  テナントタグが割り当てられている専門ユーザーは、関連するロールにも一致する、対応するテナントまたはコア データにのみアクセスできます。コア データは、さらに読み取り専用アクセスに制限されます。

ロール、サブロール、および制約

ライセンス タイプは、各ロールとサブロールの組み合わせに関連付けられます。ロールとサブロールは、そのライセンスがそのクラスタで使用可能な場合にのみ有効になります。

制約を適用することによって、管理者ロールを制限できます。たとえば、host-admin 基本ロールを使用して、192.168.50.0 サブネットに制約されている 192.168.50.0-host-admin という名前のホスト管理者を作成できます。管理者は、このロールを含むグループを割り当てた後、この制約を有効にしてログインします。ロールとサブロールの追加については、ロールの管理 （23 ページ） で説明しています。

ロールの制約を読み取り専用アクセスに制限することができます。管理者は、そのロールのデータを読み取ることはできますが、変更することはできません。ただし、制限されたデータが読み取り/書き込みロールにも関連付けられている場合、読み取り/書き込み権限は読み取り専用の制約に優先します。

ヒント ロール制約の追加の例は、制約付きのホスト管理者ロールの作成 にあります。

DNS とホスト管理者ロールの割り当ての間の相互作用により、制約のない dns-admin ロールをグループ内の任意の host-admin ロールと組み合わせることができます。たとえば、グループ内の dns-admin-readonly ロールと host-admin ロールを組み合わせる（およびグループに host-rw-dns-ro という名前を付ける）と、完全なホスト アクセス権と読み取り専用アクセス権がゾーンと RR に与えられます。ただし、制限付きの dns-admin ロールを host-admin ロールとともにグループに割り当て、次に管理者に割り当てると、制約付き dns-admin ロールが優先され、ログイン時の管理者権限によってホスト管理が排除されます。

特定のロールにはサブロールがあり、それによってロール機能をさらに制限できます。たとえば、ローカルの ccm-admin または regional-admin に owner-region サブロールが適用されると、

所有者とリージョンのみを管理できます。デフォルトでは、制約付きのロールを作成すると、可能なすべてのサブロールが適用されます。

事前定義されたロールについては、表 1 : ローカル クラスタ管理者の事前定義ロールと基本ロール （4 ページ）（ローカル）と 表 2 : リージョン クラスタ管理者の事前定義ロールと基本ロール （6 ページ）（リージョン）を参照してください。

表 *1:* ローカル クラスタ管理者の事前定義ロールと基本ロール

ローカル ロール	サブロールとアクティブな機能
addrblock-admin	コア機能：アドレス ブロック、サブネット、およびリバース DNS ゾーンを管理します（dns-admin も必要）。また、スコープ アクティビティを通知します。 • *ric-management*：DHCP フェールオーバー ペアとルータにサブネットをプッシュし、再利用します。 • *ipv6-management*：IPv6 プレフィックス、リンク、オプション、リース、および予約を管理します。 • *lease-history*：リース履歴データを照会、ポーリング、およびトリミングします。
ccm-admin	コア機能：アクセス コントロール リスト（ACL）と暗号キーを管理します。 • *authentication*：管理者を管理します。 • *authorization*：ロールとグループを管理します。 • *owner-region*：所有者とリージョンを管理します。 • *database*：データベースの変更エントリを表示し、CCM の変更セットをトリミングします。 • *security-management*：ACL と DNSSEC の設定を管理します。
cdns-admin	コア機能：メモリ内キャッシュを管理します（フラッシュ キャッシュとフラッシュ キャッシュ名）。 • *security-management*：ACL と DNSSEC の設定を管理します。 • *server-management*：DNSSEC 設定、フォワーダー、例外、DNS64、およびスケジュールされたタスクを管理し、サーバーを停止、開始、またはリロードします。

ローカル ロール	サブロールとアクティブな機能
cfg-admin	コア機能：クラスタを管理します。 • *ccm-management*：CCM サーバーの設定を管理します。 • *dhcp-management*：DHCP サーバーの設定を管理します。 • *dns-management*：DNS サーバーの設定を管理します。 • *cdns-management*：キャッシング DNS サーバーの設定を管理します。 • *ric-management*：ルータを管理します。 • *snmp-management*：SNMP サーバーの設定を管理します。 • *tftp-management*：TFTP サーバーの設定を管理します。
dhcp-admin	コア機能：DHCP スコープとテンプレート、ポリシー、クライアント、クライアントクラス、オプション、リース、および予約を管理します。 • *lease-history*：リース履歴データを照会、ポーリング、およびトリミングします。 • *ipv6-management*：IPv6プレフィックス、リンク、オプション、リース、および予約を管理します。 • *server-management*：DHCP サーバーの設定、フェールオーバー ペア、LDAP サーバー、拡張、および統計情報を管理します。
dns-admin	コア機能：DNS ゾーンとテンプレート、リソース レコード、セカンダリ サーバー、およびホストを管理します。 • *security-management*：DNS 更新ポリシー、ACL、および暗号キーを管理します。 • *server-management*：DNS サーバーの設定とゾーン分散を管理し、ゾーンと HA サーバーのペアを同期し、更新マップをプッシュします。 • *ipv6-management*：IPv6 ゾーンとホストを管理します。 • *enum-management*：DNS ENUM ドメインと番号を管理します。
host-admin	コア機能：DNS ホストを管理します。（管理者に制約付き dns-admin ロールも割り当てられた場合、これは host-admin の定義をオーバーライドするため、管理者には host-admin ロールが割り当てられないことに注意してください）。

表 *2:* リージョン クラスタ管理者の事前定義ロールと基本ロール

リージョンのロール	サブロールとアクティブな機能
central-cfg-admin	コア機能：クラスタを管理し、レプリカ データを表示します。 • *dhcp-management*：DHCP スコープテンプレート、ポリシー、クライアントクラス、フェールオーバー ペア、バーチャル プライベート ネットワーク（VPN）、およびオプションを管理します。サブネットを変更します。データを複製します。 • *ric-management*：ルータとルータ インターフェイスを管理し、レプリカ ルータのデータをプルします。 • *ccm-management*：CCM サーバーの設定を管理します。 • *snmp-management*：SNMP サーバーの設定を管理します。 • *ipv6-management*：IPv6 プレフィックス、リンク、オプション、リース、および予約を管理します。 • *cdns-management*：CDNS サーバーの設定を管理します。
central-dns-admin	コア機能：DNS ゾーンとテンプレート、ホスト、リソース レコード、およびセカンダリ サーバーを管理します。サブゾーンと逆引きゾーンを作成します。 • *security-management*：DNS 更新ポリシー、ACL、および暗号キーを管理します。 • *server-management*：DNS ゾーンと HA サーバー ペアを同期し、ゾーン分散を管理し、レプリカ ゾーン データをプルし、更新マップをプッシュします。 • *ipv6-management*：IPv6 ゾーンとホストを管理します。 • *enum-management*：DNS ENUM ドメインと番号を管理します。
central-host-admin	コア機能：DNS ホストを管理します。（管理者に制約付き central-dns-admin ロールも割り当てられた場合、これは central-host-admin の定義をオーバーライドするため、管理者には central-host-admin ロールが割り当てられないことに注意してください）。

リージョンのロール	サブロールとアクティブな機能
regional-admin	コア機能：ライセンスと暗号キーを管理します。 • *authentication*：管理者を管理します。 • *authorization*：ロールとグループを管理します。 • *owner-region*：所有者とリージョンを管理します。 • *database*：データベースの変更エントリを表示し、CCM の変更セットをトリミングします。 • *security-management*：ACL と DNSSEC の設定を管理します。
regional-addr-admin	コア機能：アドレス ブロック、サブネット、およびアドレス範囲を管理します。割り当てレポートを生成します。レプリカ アドレス空間データをプルします。 • *dhcp-management*：サブネットをプッシュし、再利用します。サブネットを DHCP フェールオーバー ペアに追加し、削除します。 • *lease-history*：リース履歴データを照会、ポーリング、およびトリミングします。 • *subnet-utilization*：サブネットとプレフィックス使用率データのクエリ、ポーリング、トリミング、およびコンパクト化を行います。 • *ipv6-management*：IPv6 プレフィックス、リンク、オプション、リース、および予約を管理します。

グループ

管理者グループは、管理者にロールを割り当てるために使用されるメカニズムです。したがって、グループは、使用可能な 1 つ以上の管理者ロールで構成される必要があります。Cisco Prime Network Registrar を初めてインストールすると、事前定義の各ロールに対応する事前定義のグループが作成されます。

同じ基本ロールを持つロールは結合されます。制約のない dhcp-admin ロールと制約付きの dns-admin ロールを持つグループは、dns-admin ロールに割り当てられた権限を変更しません。たとえば、いずれかのロールに制約なしの読み取り/書き込み権限が割り当てられている場合、他のロールには読み取り専用権限が割り当てられていても、そのグループには制約なしの読み取り/書き込み権限が割り当てられます。したがって、すべてのデータへの読み取り専用アクセスを許可しながら、ユーザーの読み取り/書き込み権限を制限するには、制約付きの読み取り/書き込みロールとともに、制約なしの読み取り専用ロールを含むグループを作成します。（グループ内の host-admin ロールと dns-admin ロールの組み合わせの実装については、ロール、サブロール、および制約 （3 ページ） を参照してください）。

外部認証サーバー

Cisco Prime Network Registrar には、CCM サーバーの認証および承認モジュールと統合された RADIUS クライアント コンポーネントと Active Directory（AD）クライアント コンポーネントが含まれています。外部認証を有効にするには、ローカルおよびリージョン クラスタで外部 RADIUS または AD サーバーのリストを設定し、すべての承認ユーザーがそれぞれのサーバーで適切に設定されていることを確認する必要があります。

外部認証が有効なとき、CCM サーバーは、RADIUS サーバーに対して RADIUS 要求を発行するか、設定済みリストから選択された AD サーバーに対して LDAP 要求を発行することによって、Web UI、SDK、または CLI を介したログインの試みを処理します。対応するサーバーがログイン要求を検証した場合、アクセスが許可され、CCM サーバーは RADIUS または AD サーバーが指定したグループ割り当てを持つ承認済みセッションを作成します。

（注） CCM サーバーのデータベースで定義されている管理者は、外部認証が有効になっている場合は無視されます。これらのユーザー名とパスワードを使用してログインしようとしても失敗します。外部認証を無効にするには、設定されているすべての外部サーバーを削除または無効にするか、*auth-type* 属性値を [ローカル（Local）] に変更する必要があります。

ヒント 外部認証サーバーにアクセスできない、または設定が間違っているためにすべてのログインが失敗する場合は、別の方法を使用してログインし問題を解決します。詳細については、管理者の管理 （18 ページ） を参照してください。

RADIUS 外部認証サーバーの設定

RADIUS サーバーを起動して実行し、ユーザーを作成したら、RADIUS ユーザーが Cisco Prime Network Registrar にログインするために必要な特定のグループとベンダー固有の属性（VSA）がいくつかあります。Cisco ベンダー id（9）を使用し、**cnr:groups=**group1, group2, group3 の形式を使用して、管理者ごとに Cisco Prime Network Registrar のグループ属性を作成します。

たとえば、管理者を組み込みグループ **dhcp-admin-group** および **dns-admin-group** に割り当てるには、次のように入力します。

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

スーパーユーザーのアクセス権限を割り当てるには、予約済みグループ名 **superusers** が使用されます。管理者にスーパーユーザー権限を与えるには、次のように入力します。

```
cnr:groups=superusers
```

スーパーユーザー権限は、他のすべてのグループよりも優先されます。

Cisco Prime Network Registrar に使用される VSA 名は、cisco-avpair です。次に、Cisco Prime Network Registrar 用の FreeRadius サーバーの設定例を示します。

ユーザーの場合：（これには、サーバーからのデフォルト情報が含まれます）

```
ciscoprime Cleartext-Password := "Cisco123" -> CPNR Username/Password
       Service-Type = Framed-User,
       cisco-avpair += "cnr:groups=superusers", -> CPNR group for CNR. This is the VSA.
       Framed-Protocol = PPP,
       Framed-IP-Address = 192.168.1.2, -> CPNR IP
       Framed-Filter-Id = "std.ppp",
       Framed-MTU = 1500,
```

クライアントの場合：

```
client CNR-HOST {
       ipaddr = 192.168.1.2 -> IP of CPNR server
       secret = P@$$W0rd! -> Password for CPNR Radius
```

RADIUS サーバーを保存してリロードすると（すべての設定が正しいことを前提として）、RADIUS で作成されたユーザーを使用して Cisco Prime Network Registrar にログインでき、認証が可能になります。

（注） Cisco Prime Network Registrar を使用して、外部ユーザー名とそのパスワードまたはグループを追加、削除、または変更することはできません。この設定を実行するには、RADIUS サーバーを使用する必要があります。

RADIUS 外部コンフィギュレーション サーバーの追加

外部コンフィギュレーション サーバーを追加するには、次の手順を実行します。

ローカルの詳細 Web UI とリージョンの詳細 Web UI

ステップ 1 [管理（Administration）] メニューから、[外部認証（External Authentication）] サブメニューの [Radius] を選択します。[Radius サーバーの一覧表示/追加（List/Add Radiuser Server）] ページが表示されます。

ステップ 2 [Radius] ペインで [Radiusの追加（Add Radius）] アイコンをクリックして、外部認証サーバーとして設定するサーバーの名前、IPv4 および/または IPv6 アドレスを入力し、[外部認証サーバーの追加（Add External Authentication Server）] ダイアログボックスで、このサーバーとの通信に使用する *key* 属性を設定し、[外部認証サーバーの追加（Add External Authentication Server）] をクリックします。CCM サーバーはキーを使用して、クライアントとサーバーによって共有される秘密鍵である *key-secret* 属性を設定します。

ステップ 3 外部認証サーバーを有効にするには、[Radiusサーバーの編集（Edit Radius Server）] ページで、*ext-auth* 属性の [有効（enabled）] チェックボックスをオンにして、[保存（Save）] をクリックします。

ステップ 4 [サーバーの管理（Manage Servers）] ページで *auth-type* 属性を RADIUS に変更し、[保存（Save）] をクリックしてから、Cisco Prime Network Registrar を再起動します。

（注） この時点で、ローカル認証が無効になっているために Cisco Prime Network Registrar にログインできない場合は、/var/nwreg2/{local | regional}/conf/priv 下にバックドアアカウントを作成し、ユーザー名とパスワードを使用して「local.superusers」という名前のファイルを作成する必要があります。

CLI コマンド

外部認証サーバーを作成するには、**auth-server** *name* **create** <*address* | *ip6address*> [*attribute*=*value* ...] を使用します（構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **auth-server** コマンドを参照してください）。

RADIUS 外部認証サーバーの削除

RADIUS 外部認証サーバーを削除するには、[Radius] ペインでサーバーを選択し、[Radiusの削除（Delete Radius）] アイコンをクリックして、削除を確定します。[閉じる（Close）] ボタンをクリックして、削除をキャンセルすることもできます。

AD 外部認証サーバーの設定

Cisco Prime Network Registrar 管理者が管理機能を実行するには、1 つ以上の管理者グループに割り当てられている必要があります。外部認証に AD サーバーを使用する場合、これらはユーザーごとにベンダー固有の属性として設定されます。Cisco ベンダー id（9）を使用し、Cisco Prime Network Registrar グループ属性を各管理者について、**cnr:groups=***group1*, *group2*, *group3* という形式で作成します。

たとえば、管理者を組み込みグループ **dhcp-admin-group** および **dns-admin-group** に割り当てるには、次のように入力します。

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

スーパーユーザーのアクセス権限を割り当てるには、予約済みのグループ名 **superusers** が使用されます。管理者にスーパーユーザー権限を与えるには、次のように入力します。

```
cnr:groups=superusers
```

スーパーユーザー権限は、他のすべてのグループよりも優先されます。

Cisco Prime Network Registrar にアクセスするにはグループを作成し、ユーザーをそのグループに追加する必要があります。ユーザー属性を選択して、**cnr:group1,group2,..** という形式でグループ情報を指定します。

Active Directory（AD）外部認証サーバーを設定するには、次のようにします。

ステップ 1 AD サーバーで、グループ スコープ**ドメイン ローカル**を使用して、*CPIPE*などの新しいグループを作成します。

ステップ 2 ユーザーを選択し、[**追加（Add**）] をクリックして、グループに追加します。

ステップ 3 [オブジェクト名の入力（Enter the Object Names）] ウィンドウで、[**CPNR**] を選択し、[**OK**] をクリックします。

ステップ 4 [AD サーバー オブジェクト（AD Server Object）] ウィンドウで、*ad-group-name* 属性として **CPNR** を選択し、*ad-user-attr-map* 属性として **info** を選択します。

（注） Cisco Prime Network Registrar を使用して、外部ユーザー名とそのパスワードまたはグループを追加、削除、または変更することはできません。この設定を実行するには、AD サーバーを使用する必要があります。

ケルベロスのレルムと KDC の設定

Cisco Prime Network Registrar が AD サーバーと通信するには、ケルベロスのレルムおよびKDC サーバーが必要です。変更は、次に示すように、**krb5.conf** *(/etc/krb5.conf)* ファイルで設定する必要があります。

```
default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
[libdefaults]
 ticket_lifetime = 1d
 default_realm = ECNR.COM
 default_tkt_enctypes = rc4-hmac
 default_tgs_enctypes = rc4-hmac
 dns_lookup_realm = false
 dns_lookup_kdc = false
 forwardable = true
[realms]
 ECNR.COM = {
 kdc = <kdc server host name>
admin_server = <kdc server host name>
 }
[domain_realm]
 .ecnr.com = ECNR.COM
 ecnr.com = ECNR.COM
```

AD 外部コンフィギュレーション サーバーの追加

外部コンフィギュレーション サーバーを追加するには、次の手順を実行します。

ローカルの詳細 Web UI とリージョンの詳細 Web UI

ステップ 1 [管理（Administration）] メニューから、[外部認証（External Authentication）] サブメニューの [Active Directory] を選択します。[Active Directory サーバーの一覧表示/追加（List/Add Active Directory Server）] ページが表示されます。

ステップ 2 [Active Directory] ペインで [**Active Directory サーバーの追加（Add Active Directory Server**）] アイコンをクリックし、外部認証サーバーとして設定するサーバーの名前、ホスト名、およびドメインを入力します。[Active Directory サーバーの追加（Add Active Directory Server）] ダイアログボックスで、このサーバーとの通信に使用されるベース ドメイン、LDAP ユーザー属性マップ、および AD グループ名を設定できます。[**Active Directory サーバーの追加（Add Active Directory Server**）] をクリックします。

ステップ 3 [サーバーの管理（Manage Servers）] ページで、*auth-type* 属性を Active Directory に変更し、[**保存（Save**）] をクリックしてから、Cisco Prime Network Registrar を再起動します。

CLI コマンド

外部認証サーバーを作成するには、**auth-server** *name* **create** <*address* | *ip6address*> [*attribute=value* ...] を使用します。

AD 外部認証サーバーの削除

AD 外部認証サーバーを削除するには、[Active Directory] ペインでサーバーを選択し、[**Active Directory サーバーの削除（Delete Active Directory Server**）] アイコンをクリックして、削除を確定します。[閉じる（Close）] ボタンをクリックして、削除をキャンセルすることもできます。

テナントの管理

Cisco Prime Network Registrar のマルチテナント アーキテクチャは、テナントがリージョンとローカルの両方のクラスタに保存されているデータをセグメント化できる機能を提供します。テナントが定義されると、データは各クラスタの組み込みデータベースでテナント別に分割されます。これは、各テナントにデータ セキュリティとプライバシーを提供すると同時に、クラウドまたはマネージド サービス プロバイダが一連のインフラストラクチャ サーバーに多くの小規模顧客の設定を統合したり、大規模顧客の設定をいくつかの専用サーバーに分散したりできる柔軟性を提供します。

特定のローカル クラスタを 1 つ以上のテナントに関連付けることができますが、ローカル クラスタ内では、特定のテナントに割り当てられたアドレス プールとドメイン名が重複しないようにする必要があります。

大規模顧客については、クラスタをテナントに明示的に割り当てることができます。この場合、ローカル クラスタ上のすべてのデータがテナントに関連付けられ、カスタマイズされたサーバー設定を含めることができます。または、インフラストラクチャ サーバーから多くのテナントにサービスを提供することもできます。このモデルでは、テナントは独自のアドレス空間とドメイン名を維持できますが、サービス プロバイダによって管理される共通のサーバー設定を共有します。パブリックまたはプライベート ネットワーク アドレスの使用は、テナントに重複しないアドレスが割り当てられるようにするために、サービス プロバイダによって管理される必要があります。

テナントを設定する際に知る必要があるキー ポイントは、次のとおりです。

- テナント管理者は、テナントのタグと識別子を定義するテナント オブジェクトによってデータにリンクされます。
- テナント オブジェクトは、すべてのクラスタ間で一貫性があり、一意である必要があります。
- タグまたは識別子を別のテナントに再利用しないでください。
- 1 つのクラスタに複数のテナントを設定できます。
- テナント管理者は、テナント オブジェクトを作成、変更、または削除することはできません。
- テナント管理者は、別のテナントのデータを表示または変更できません。

- テナントに割り当てられていないオブジェクトは、コアデータとして定義され、全てのテナントに対して読み取り専用モードで表示されます。

テナントの追加

テナントを追加するには、次の操作を行います。

ローカルおよびリージョン 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 [テナント（**Tenants**）] を選択します。[テナントの一覧表示/追加（List/Add Tenants）] ページが開きます。

ステップ 2 [テナント（Tenants）] ペインの [テナントの追加（Add Tenants）] アイコンをクリックして、テナント タグとテナント ID を入力し、[テナントの追加（**Add Tenant**）] をクリックします。名前と説明の属性は任意です。

（注） 同じテナント ID またはテナント タグを持つ複数のテナントを作成することはできません。

ステップ 3 [保存（Save）] をクリックします。

ページの上部にあるツールバーの [設定（Settings）] ドロップダウン リストには、[テナント（Tenant）] サブメニューの下にテナントが表示されます。

テナント固有の設定を行う必要があるときには、このドロップダウン リストを使用してテナントを選択できます。

CLI コマンド

テナントを追加するには、**tenant** *tag* **create** *tenant-id* [*attribute=value*] を使用します（構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **tenant** コマンドを参照してください）。

テナントの編集

テナントを追加するには、次の操作を行います。

ローカルおよびリージョン Web UI

ステップ 1 [テナントの一覧表示/追加（List/Add Tenants）] ページで、[テナント（Tenants）] ペインの目的のテナントの名前をクリックすると、選択したテナントの詳細を含む [テナントの編集（Edit Tenant）] ページが表示されます。

ステップ 2 [テナントの編集（Edit Tenant）] ページでテナントのテナント タグ、名前、または説明を変更し、[保存（**Save**）] をクリックします。テナント ID を変更することはできません。

テナントの削除

警告 **テナントを削除すると、テナントのすべてのデータも削除されます。**

テナントを削除するには、[テナント（Tenants）]ペインで目的のテナントの名前を選択し、[テナント（Tenants）] ペインで [**削除（Delete**）] アイコンをクリックして、削除を確定します。[閉じる（Close）] ボタンをクリックして、削除をキャンセルすることもできます。

（注） 特定のテナントに制限されたユーザーは、テナントを削除できません。

テナント データの管理

テナントに対して、次の 2 種類のデータを作成できます。

- テナントデータ。指定されたテナントに割り当てられ、他のテナントは表示できません。
- コア データは。すべてのテナントに対して読み取り専用モードで表示されます。

ローカルおよびリージョン Web UI

Web UI でテナント データ オブジェクトを作成するには、次の手順を実行します。

ステップ 1 目的のテナントのデータを設定するには、ページの上部にあるツールバーの [設定（Settings）] ドロップダウン リストをクリックして、[テナント（Tenant）] サブメニューで目的のテナントを選択します。

ステップ 2 オブジェクトを作成します。

テナントデータを作成するときには、ほとんどのオブジェクト名は、指定されたテナントに対して一意である必要があります。たとえば、テナント *abc* および *xyz* は両方とも、それぞれの設定に対してプライベートな独自のスコープ *test* を使用します。

（注） 管理者（Admin）、ゾーン（CCMZone、CCMReverseZone、および CCMSecondaryZone）、キー（Key）、およびクライアント（ClientEntry）は、すべてのテナントで一意である必要があります。

初期ログイン認証を実行し、ユーザーがテナントであるかどうかを確立するには、管理者名が一意である必要があります。ゾーンとキー クラスは、インターネット全体で一意であると予想される DNS ドメイン名を必要とするため、一意である必要があります。クライアント名は、着信した要求を照合するために DHCP サーバーが使用できる一意のクライアント識別子に対応している必要があります。

ローカルおよびリージョン Web UI

Web UI でコア データ オブジェクトを作成するには、次の手順を実行します。

ステップ 1 ページの上部にあるツールバーの [設定（Settings）] ドロップダウン リストから **[all]** を選択し、[テナント（Tenant）] サブメニューから目的のテナントを選択します。

ステップ 2 オブジェクトを作成し、オブジェクトのテナント割り当てを [なし（**none**）] に設定したままにします。デフォルトでは、[なし（**none**）] が [テナント（Tenant）] ドロップダウン リストで選択されます。そのままにしておくと、オブジェクトは特定のテナントに制限されません。

コアデータを使用して、テナントに提供するために選択したポリシーやクライアントクラスなどの共通の設定要素を提供できます。テナントは、設定内のこれらのオブジェクトを表示および参照できますが、変更または削除することはできません。コア データはすべてのテナントに対して表示されるため、オブジェクト名はすべてのテナントで一意である必要があります。

CLI コマンド

session set tenant=タグを使用して、選択したテナントを設定します。設定されている場合、テナント選択をクリアするには、**session unset tenant** を使用します（構文と属性の説明については、/docs ディレクトリにある CLIGuide .html ファイルの **session** コマンドを参照してください）。

（注） 作成後にオブジェクトのテナントまたはコアの指定を変更することはできません。テナントの割り当てを変更するには、オブジェクトを削除してから再作成する必要があります。

ヒント cnr_exim ツールを使用して、テナント データのセットを 1 つのテナントから別のテナントに移動することができます。

単一テナントへのローカル クラスタの割り当て

単一のテナントに割り当てられている場合、ローカル クラスタのコア データは読み取り専用アクセスに制限されません。これは、サーバーを停止して起動し、デフォルトを変更し、カスタム拡張機能をインストールする機能がテナントに与えられる可能性があることを意味します。クラスタが特定のテナントに割り当てられると、他のテナントはクラスタにログインできなくなります。

（注） ローカル クラスタとの同期に失敗した場合、クラスタはテナントに割り当てられません。接続の問題を解決し、再同期アイコンを使用してローカル クラスタ テナントを設定します。

リージョン Web UI

1 つのテナントにローカル クラスタを割り当てるには、次の手順を実行します。

ステップ 1 クラスタを新しいテナントに割り当てる場合は、[テナントの一覧表示/追加（List/Add Tenant）] ページでテナントを追加します（テナントの追加 （13 ページ） を参照）。

ステップ 2 [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**）] を選択します。[クラスタの一覧表示/追加（List/Add Clusters）] ページが表示されます。

ステップ 3 ページの上部にあるツールバーの [設定（Settings）] ドロップダウン リストから、**ステップ 1** で追加したテナントを選択し、[テナント（Tenant）] サブメニューで目的のテナントを選択します。

ステップ 4 [クラスタの管理（Manage Clusters）] ペインの [クラスタの管理を追加（**Add Manage Clusters**）] 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表示されます。

ステップ 5 [**クラスタの追加（Add Cluster**）] をクリックしてクラスタを追加します。クラスタの追加の詳細については、ローカル クラスタの作成 を参照してください。

（注） クラスタが特定のテナントに割り当てられると、変更または設定解除できません。

テナント データのプッシュとプル

リージョン Web UI では、リスト ページには、オブジェクトをローカル クラスタのリストに配布できるプッシュ オプションと、ローカル クラスタ オブジェクトをレプリカ データから中央の設定にマージできるプル オプションが含まれています。これらの操作はテナントとコアデータの両方で実行できますが、1 回の操作でプッシュまたはプルできるデータ セットは 1 つだけです。

ページの上部にあるツールバーの [設定（Settings）] ドロップダウン リストを使用して、[テナント（Tenant）] サブメニューで目的のテナントを選択し、プッシュまたはプルするデータのセットを指定します。

（注） テナントデータの一貫性のあるビューを維持するには、関連するすべてのクラスタに同じテナントのリストを設定する必要があります。テナントリストの管理に役立つ手順については、テナントのプッシュとプル （40 ページ） を参照してください。

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。

- **tenant** < *tag* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]
- **tenant** < *tag* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]
- **tenant** *tag* **reclaim** *cluster-list* [**-report-only** | **-report**]

外部認証を使用する場合のテナントの割り当て

外部RADIUS認証が設定されている場合、RADIUSサーバー設定に割り当てられているグループは、ユーザーのアクセス権限を確立します。テナントステータスを指定するには、テナントユーザーのグループのリストに、暗黙的なグループ名 ccm-tenant-*tag* または ccm-tenant-*id* を追加する必要があります。その他の割り当てられたグループは、同じテナントに割り当てられたコア グループまたはグループである必要があります。無効なグループは、ログイン時にユーザーのログイン情報を作成するときに無視されます。

たとえば、テナント*abc*のスーパーユーザーアクセスを割り当てるには、グループ属性を次のように指定します。

```
cnr:groups=superusers,ccm-tenant-abc
```

外部認証サーバー （8 ページ） を参照してください。

テナント データでの cnr_exim の使用

cnr_exim ツールを使用すると、テナントデータをエクスポートしたり、必要に応じてインポート時に別のテナントにデータを再割り当てしたりできます（cnr_exim データ インポートおよびエクスポート ツールの使用 を参照）。次の機能を使用できます。

- 各テナントの標準オブジェクト セットの作成
- テナント データの新しいテナントへの移動

（注） 特定のテナントに制限されたユーザーは、そのテナントのデータのみをエクスポートまたはインポートできます。

テナント オブジェクトの標準セットの作成

テナントオブジェクトの標準セットを使用して、スコープ、ゾーンテンプレート、ポリシー、クライアントクラスなどの共通オブジェクトを提供できます。これらの設定をカスタマイズするオプションをテナントに提供するには、コア データ オブジェクトの代わりにこれらを使用できます。

テナント オブジェクトの標準セットを作成するには、次の手順を実行します。

ステップ 1 プレースホルダとして使用するテンプレートテナントユーザーを作成し（tag=*template* および id=*9999*）、各テナントで再利用するオブジェクトのセットを作成します。

ステップ 2 cnr_exim ツールを使用して、テンプレート設定をエクスポートします。

```
cnr_exim  -f template -x -e template.bin
```

ステップ 3 cnr_exim ツールを使用して、テナント *abc* のテンプレート設定をインポートします。

```
cnr_exim -f  template -g abc -i template.bin
```

（注） テンプレート テナント ユーザーがクラスタに存在しなくても、データをインポートできるため、他のクラスタで template.bin エクスポート ファイルを再利用できます。エクスポート ファイルを作成したら、必要に応じて、元のクラスタのプレースホルダ テナントを削除して、関連付けられているすべてのテンプレート データを削除することもできます。

テナント データの移動

テナントの ID は、テナントを削除してから再作成することによってのみ変更できます。これが必要な場合にテナントのデータを保持するには、次の手順を実行します（テナントのテナント タグが *xyz* であることを前提とします）。

ステップ 1 cnr_exim ツールを使用して、テナント *xyz* の設定をエクスポートします。

```
cnr_exim -f xyz -x -e xyz.bin
```

ステップ 2 テナント *xyz* を削除します。

ステップ 3 修正されたテナント id を使用してテナントを再作成します。

ステップ 4 cnr_exim ツールを使用して、設定を再インポートします。

```
cnr_exim -f xyz -g  xyz -i xyz.bin
```

管理者の管理

初めてログインすると、Cisco Prime Network Registrarには 1 人の管理者（スーパーユーザー アカウント）が割り当てられます。このスーパーユーザーは、Web UI のすべての機能を実行でき、通常は他の主要な管理者を追加します。ただし、ccm-admin および regional-admin 管理者は、管理者の追加、編集、および削除を行うこともできます。管理者を作成するには、以下が必要です。

- 名前を追加します。
- パスワードを追加します。
- 管理者がスーパーユーザー権限を持っている必要があるかどうかを指定します（通常は非常に限定的な方法で割り当てられます）。
- スーパーユーザーを作成しない場合は、管理者が属するグループを指定します。これらのグループには適切なロール（および場合によってはサブロール）の割り当てが必要であり、それによって適切な制約が設定されます。

Cisco Prime Network Registrar にログインできるすべてのロール（スーパーユーザー、ccm-admin、または regional-admin 権限を持つユーザー）を誤って削除した場合は、/var/nwreg2/{local | regional}/conf/priv/local.superusers ファイルで管理者名とパスワードのペアを作成することによって回復できます。このファイルを作成し、*admin password* という形式の行を含める必要があります。次のログインセッションには、この管理者名とパスワードを使用します。local.superusers ファイル内のすべてのユーザーに「local$」というプレフィックスを付ける必要があります。

これにより、すべてのユーザーの先頭に local$ が付くので、local.superusers ファイルがいつ使用されたのかを特定するために役立ちます。local$ で始まるユーザーは、local.superusers ファイルのエントリに対して検証されます。これらのユーザーは、ローカル CCM ユーザーデータベースのユーザーに対してチェックされることも、外部認証を使用することもありません。

（注）
- 管理者名は大文字と小文字が区別されないため、local$ および internal$ プレフィックスも大文字と小文字が区別されません。
- **nrcmd -N** *admin* で local$ または internal$ ユーザーを使用する場合は、$ をエスケープする必要があります（そのため、local\$ または internal\$ を使用）。代わりに、nrcmd でユーザーのプロンプトを表示させることができます（この場合、エスケープは不要）。

重要 local.superusers ファイルを使用すると、セキュリティが低下します。したがって、このファイルは、一時的にすべてのログインアクセスを失う場合など、緊急時にのみ使用してください。ログイン後、通常の方法でスーパーユーザー アカウントを作成してから、local.superusers ファイルまたはその内容を削除します。管理上の変更を追跡するには、個人ごとに新しい管理者アカウントを作成する必要があります。

このファイルをそのままにしておく場合は、一般的な読み取りアクセスから保護されていることを確認してください（読み取りアクセスは ccmsrv でのみ必要）。

外部認証が有効になっていて、外部認証サーバーにアクセスできないか、または設定が間違っているためにログインに失敗した場合、CCM サーバーのデータベースで定義されている管理者を使用してログインできます。この場合、ユーザー名に「internal$」（ログイン中）プレフィックスを付けて、内部 CCM サーバーのデータベースが管理者の認証と承認に使用されるように指定する必要があります。

管理者の追加

管理者を追加するには、次の手順を実行します。

ローカルおよびリージョン 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 [テナント（**Administrators**）] を選択します。[管理者の一覧表示/追加（List/Add Administrators）] ページが開きます（例については、管理者の作成 を参照してください）。

ステップ 2 [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て、[管理者を追加（Add admin）] ダイアログボックスで、[名前（Name）] フィールドに名前を入力し、[パスワード（Password）] フィールドにパスワードを入力し、[パスワードの確認（Confirm Password）] フィールドにパスワードを再入力して、[管理者を追加（Add admin）] をクリックします。

ステップ 3 [使用可能なグループ（Groups Available）] リストから 1 つ以上の既存のグループを選択し（または管理者がスーパーユーザーである必要があるかどうか）、[保存（**Save**）] をクリックします。

管理者の編集

管理者を編集するには、[管理者（Administrators）] ペインで管理者を選択し、[管理者の編集（Edit Administrator）] ページで名前、パスワード、スーパーユーザーのステータス、またはグループ メンバーシップを変更し、[**保存（Save**）] をクリックします。アクティブなグループは、[選択済み（Selected）] リストに表示されます。

セッション制限が設定されている場合、[セッション数無制限（Unlimited Sessions?）] チェックボックスをオンにすることで、無制限の数の同時トークンおよびユーザーセッションが管理者に許可されることを示すことができます。詳細については、セッション管理 （42 ページ）を参照してください。

（注） 現在ログインしている管理者のユーザーロールに変更があるたびに、Web UI がログアウトします。

管理者の削除

管理者を削除するには、[管理者（Administrators）] ペインで管理者を選択し、[管理者の削除（Delete Administrators）] 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。

管理者の一時停止/再開

管理者のログインアクセスを一時停止するには、[管理者（Administrators）] ペインでその管理者を選択し、右側のペインで [管理者の編集（Edit Administrator）] ページの上部にある [一時停止（Suspend）] ボタンをクリックします。

（注） 管理者のログインが有効になっている場合は、[一時停止（Suspend）] アクションのみが使用可能になります。一時停止されている場合は、[再開（Reinstate）] アクションのみが使用可能になります。

CLI コマンド

管理者を作成するには、**admin** *name* **create** [*attribute=value*] を使用します。

管理者を削除するには、**admin** *name* **delete** を使用します。

管理者のログインアクセスを一時停止するには、**admin** *name* **suspend** を使用します。

管理者のログインアクセスを復帰させるには、**admin** *name* **reinstate** を使用します。

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。push の場合、**-omitrelated** が指定されていない限り、関連付けられたロールとグループも（置換モードを使用して）プッシュされます。

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

パスワードの管理

パスワードは、Web UI および CLI への管理者アクセスのためのキーです。Web UI では、[ログイン（Login）]ページでパスワードを入力します。CLI では、最初に **nrcmd** プログラムを呼び出すときにパスワードを入力します。ローカルまたはリージョンCCM管理者またはスーパーユーザーは、管理者パスワードを変更できます。

入力時にパスワードを公開しないようにすることができます。Web UI では、ログインするか、パスワードを追加しても、ページにはアスタリスクしか表示されません。CLI では、管理者を作成し、パスワードを省略し、**admin** 名前 **enterPassword**を使用してパスワードを公開しないようにすることができます。この場合、プロンプトにはパスワードはアスタリスクとして表示されます。この操作は、パスワードをプレーン テキストとして公開する通常の**admin** *name* **set password** コマンドの代わりに行うことができます。

管理者は、クラスタで自分のパスワードを変更できます。パスワードの変更をリージョンサーバーからすべてのローカルクラスタに反映させる場合は、リージョンクラスタにログインします。最初に、セッションのadmin-edit-mode が synchronous に設定されていることを確認してから、パスワードを更新します。

（注） パスワードの長さは 255 文字以下でなければなりません。

グループの管理

スーパーユーザー、ccm-admin、または regional-admin は、管理者グループを作成、編集、および削除できます。管理者グループの作成には、次の作業が含まれます。

- 名前を追加します。
- オプションの説明を追加します。
- 関連ロールを選択します。

グループの追加

グループを追加するには、次の手順を実行します。

ローカル詳細およびリージョン 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 [グループ（**Groups**）] を選択します。[管理者グループの一覧表示/追加（List/Add Administrator Groups）] ページが開きます（例については、ホスト管理者に割り当てるグループの作成 を参照してください）。

ステップ 2 [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て、[CCM 管理者グループの追加（Add CCMAdminGroup）] ダイアログボックスに名前とオプションの説明を入力し、[CCM 管理者グループの追加（Add CCMAdminGroup）] をクリックします。

ステップ 3 [使用可能なロール（Roles Available）] リストから 1 つ以上の既存のロールを選択し、[保存（Save）] をクリックします。

グループの編集

グループを編集するには、[グループ（Groups）] ペインで編集するグループの名前をクリックして、[管理者グループの編集（Edit Administrator Group）] ページを開きます。このページでは、名前、説明、またはロール メンバーシップを変更できます。[選択済み（Selected）] リストでアクティブなロールを表示できます。

グループの削除

グループを削除するには、[グループ（Groups）] ペインでグループを選択し、[**グループの削除（Delete Groups**）] アイコンをクリックして、削除を確定します。[閉じる（Close）] ボタンをクリックして、削除をキャンセルすることもできます。

CLI コマンド

グループを作成するには、**group** *name* **create** [*attribute=value*] を使用します。

グループを削除するには、**group** *name* **delete** を使用します。

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。push 操作では、これを防止するために **-omitrelated** が指定されていない限り、関連するロール（置換モードを使用）および関連する所有者とリージョン（保証モードを使用）もプッシュされます。

- **group** < *name* | **all** > **pull** < **ensure** | **replace** > *cluster-name* [**-report-only** | **-report**]
- **group** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-report-only** | **-report**]

- **group** *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

ロールの管理

スーパーユーザー、ccm-admin、またはregional-admin管理者は、管理者ロールを作成、編集、および削除できます。管理者ロールの作成には、次の作業が含まれます。

- 名前を追加します。
- 基本ロールを選択します。
- ロールを制約なしにするか、または読み取り専用にするかを指定する場合があります。
- 場合によっては制約を追加します。
- グループを割り当てる可能性があります。

ロールの追加

ロールを追加するには、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 [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**）] を選択します。[管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページが開きます。

ステップ 2 [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、名前を入力し、テナントと基本ロールを選択して、[ロールの追加（Add Roles）] ダイアログボックスに名前と基本ロールを入力し、[ロールの追加（Add Role）] をクリックします。

ステップ 3 [管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページで、ロールの制約、サブロールの制限、またはグループ選択を指定し、[保存（**Save**）] をクリックします。

ロールの編集

ロールを編集するには、[ロール（Roles）] ペインでロールを選択し、[管理者ロールの編集（Edit Administrator Role）] ページで、名前または制約、サブロールの制限、またはグループ選択を変更します。アクティブなサブロールまたはグループは、[選択済み（Selected）] リストに表示されます。[保存（**Save**）] をクリックします。

ロールの削除

ロールを削除するには、[ロール（Roles）] ペインでロールを選択し、[ロールの削除（Delete Role）] アイコンをクリックして、削除を確定します。

（注） デフォルト ロールは削除できません。

CLI コマンド

管理者ロールを追加および編集するには、**role** *name* **create** *base-role* [*attribute=value*] を使用します（構文と属性の説明については、/docs ディレクトリにある CLIGuide.html ファイルの **role** コマンドを参照してください）。基本ロールには、デフォルト グループが関連付けられています。他のグループを追加するには、*groups* 属性（カンマ区切りの文字列値）を設定します。

リージョン クラスタに接続されているときには、次の pull、push、および reclaim コマンドを使用できます。push および reclaim コマンドでは、クラスタのリストまたは「all」を指定できます。push 操作では、関連グループ（置換モードを使用）および関連する所有者とリージョン（保証モードを使用）もプッシュされます。pull 操作では、関連する所有者とリージョンが（保証モードを使用して）プルされます。どちらの操作についても、これを防止するために **-omitrelated** を指定して、ロールのみをプッシュまたはプルします。

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

きめ細かい管理

きめ細かい管理により、権限のないユーザーがゾーン、アドレスブロック、サブネット、およびルータインターフェイスを誤って変更するのを防止できます。また、許可されたユーザーのみが、特定のスコープ、プレフィックス、およびリンクを表示または変更することも保証します。きめ細かい管理では、管理者は特定のスコープ、プレフィックス、およびリンクのセットに制限されます。制限付き管理者は、許可されたスコープ、プレフィックス、およびリンク オブジェクトのみを表示または変更できます。CCM サーバーは、所有者およびリージョン制約を使用して、IPv4 アドレス空間オブジェクト、および DNS ゾーン関連オブジェクト（CCMZone、CCMReverseZone、CCMSecondaryZone、CCMRRSet、および CCMHost）を承認およびフィルタリングします。ゾーンは、所有者とリージョンによって制約されます。CCMSubnetの所有者またはリージョン属性は、スコープへのアクセスを制御します。また、プレフィックスおよびリンク オブジェクトの所有者またはリージョン属性は、プレフィックスとリンクへのアクセスを制御します。

ローカル詳細およびリージョン詳細 Web UI

ステップ 1 [**管理（Administration**）] メニューから [**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 2 [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、カスタム ロールの名前、たとえば、my-dhcp を入力し、テナント を選択し、[ロール（Role）] ドロップダウン リストから [**dhcp-admin**] を選択して、[**ロールの追加（Add role**）] をクリックします。

ステップ 3 [DHCP 管理者ロールの追加（Add DHCP Administrator Role）] ページで、必要に応じて [**True**] または [**False**] オプション ボタンをクリックします。

ステップ 4 [使用可能（Available）] フィールドで必要なサブロールを選択して、[選択済み（Selected）] フィールドに移動します。

ステップ 5 [**制約の追加（Add Constraint**）] をクリックします。

a) [ロール制約の追加（Add Role Constraint）] ページで、必要に応じてフィールドを変更します。

b) [**制約の追加（Add Constraint**）] をクリックします。制約のインデックス番号は 1 である必要があります。

ステップ 6 [**保存（Save**）] をクリックします。

カスタムロールの名前が、[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。

関連項目

スコープレベルの制約 （25 ページ）

プレフィックスレベルの制約 （27 ページ）

リンクレベルの制約 （28 ページ）

スコープレベルの制約

dhcp-admin ユーザーは、次の条件のいずれかが満たされた場合にスコープを表示または変更できます。

- スコープのサブネットの所有者が、dhcp-admin 所有者に一致します。
- スコープのサブネットのリージョンが、リージョン ロールの制約と一致します。
- 親アドレス ブロックの所有者またはリージョンが、dhcp-admin 所有者またはリージョン ロールの制約と一致します。所有者またはリージョンが定義されている最も直接的な親アドレス ブロックが優先されることに注意してください。

次の条件も有効です。

- 一致する所有者またはリージョンの制約が読み取り専用としてマークされている場合は、スコープの表示だけができます。
- スコープにプライマリ ネットワークが定義されている場合、プライマリ サブネットとその親アドレスブロックの所有者またはリージョンの制約は、セカンダリ サブネットをオーバーライドします。
- 親サブネットまたはアドレスブロックに所有者またはリージョンの制約が定義されていない場合は、スコープにアクセスできます。
- 制約なしの dhcp-admin ユーザーの場合は、すべてのスコープにアクセスできます。

（注） これらの階層的な承認チェックは、スコープ、サブネット、および親アドレスブロックに適用されます。addrblock-admin 所有者/リージョン制約に関する同一の階層型承認チェックが、アドレス ブロックとサブネットに適用されます。dhcp-admin および addrblock-admin 権限がある場合は、いずれかのロールでアクセスが許可されていれば、アドレスブロックとサブネットにアクセスできます。

スコープレベル制約の例：

```
Parent CCMAddrBlock 10.0.0.0/8 has owner 'blue' set.
    Scope 'A' has subnet 10.0.0.0/24 has parent CCMSubnet with owner 'red'.
    Scope 'B' has subnet 10.0.1.0/24 has parent CCMSubnet with no owner set.
    Scope 'C' has subnet 10.10.0.0/24 has parent CCMSubnet with owner 'green' and
primary-subnet 10.0.0.0/24.
    Scope 'D' has subnet 100.10.0.0/24 has parent CCMSubnet with owner unset, and no
parent block.

    Scope 'A' owner is 'red'.
    Scope 'B' owner is 'blue'.
    Scope 'C' owner is 'red'.
    Scope 'D' owner is unset. Only unconstrained users can access this scope.
```

ローカル詳細 Web UI

スコープを追加するには、次の手順を実行します。

ステップ 1 [**設計（Design）**] メニューから、[**DHCPv4**] サブメニューの [**スコープ（Scopes）**] を選択して、[DHCP スコープの一覧表示/追加（List/Add DHCP Scopes）] ページを開きます。

ステップ 2 [スコープ（Scopes）] ペインの [**スコープの追加（Add Scopes**）] アイコンをクリックして、[DHCP スコープの追加（Add DHCP Scope）] ダイアログボックスで名前、サブネット、プライマリ サブネットを入力し、ポリシーを選択し、selection-tag-list を入力し、スコープ テンプレートを選択します。

ステップ 3 [**DHCP スコープの追加（Add DHCP Scope**）] をクリックします。[DHCP スコープの一覧表示/追加（List/Add DHCP Scopes）] ページが表示されます。

ステップ 4 必要に応じて、フィールドまたは属性の値を入力します。

ステップ 5 属性値を設定解除するには、[設定解除（Unset?）] 列のチェックボックスをオンにし、ページの下部にある [フィールドの設定解除（Unset Fields）] をクリックします。

ステップ 6 [**保存（Save**）] をクリックして、スコープを追加するか、[**元に戻す（Revert**）] をクリックして変更をキャンセルします。

ヒント 新しいスコープ値を追加するか、既存の値を編集する場合は、[**保存（Save**）] をクリックしてスコープ オブジェクトを保存します。

プレフィックスレベルの制約

次のいずれかを持っている場合は、プレフィックスを表示または変更できます。

- dhcp-admin の ipv6-management サブロール、またはローカル クラスタの addrblock-admin ロール。
- central-cfg-admin、またはリージョン クラスタの regional-addr-admin ロール。

次の条件のいずれかが当てはまる場合は、プレフィックスを表示または変更できます。

- 親リンクの所有者またはリージョンが、ユーザーに対して定義されている所有者またはリージョンのロール制約と一致します。
- このプレフィックスの所有者またはリージョンが、ユーザーに対して定義されている所有者またはリージョンのロール制約と一致します。
- 親プレフィックスの所有者またはリージョンが、ユーザーに対して定義されている所有者またはリージョンのロール制約に一致します。

次の条件のいずれかが当てはまる場合は、プレフィックスを表示または変更できます。

- ユーザーについて一致する所有者またはリージョンの制約が読み取り専用としてマークされている場合は、プレフィックスの表示のみができます。
- プレフィックスが親リンクを参照している場合、リンクの所有者またはリージョン制約は、リンクの所有者またはリージョンの制約が設定されている場合に適用されます。
- 親リンクまたはプレフィックスが所有者またはリージョンの制約を定義していない場合は、所有者またはリージョンのロール制約がユーザーに対して定義されていない場合にのみ、このプレフィックスにアクセスできます。
- 制約なしのユーザーの場合は、すべてにアクセスできます。

プレフィックスレベルの制約の例：

```
Link 'BLUE' has owner 'blue' set.
    Parent Prefix 'GREEN' has owner 'green' set.
    Prefix 'A' has owner 'red' set, no parent prefix, and no parent link.
    Prefix 'B' has owner 'yellow' set, parent Prefix 'GREEN' and parent link 'BLUE'.
    Prefix 'C' has no owner set, parent prefix 'GREEN', and no parent link.
    Prefix 'C' has no owner set, no parent prefix, and no parent link.

    Prefix 'A' owner is 'red'.
    Prefix 'B' owner is 'blue'.
```

```
Prefix 'C' owner is 'green'.
Prefix 'D' owner is unset. Only unconstrained users can access this prefix.
```

ローカル詳細およびリージョン詳細 Web UI

ユニファイド v6 アドレス空間を表示するには、次の手順を実行します。

ステップ 1 [設計（Design）] メニューから、[DHCPv6] サブメニューの [アドレス ツリー（Address Tree）] を選択して、[DHCPv6 アドレス ツリー（DHCP v6 Address Tree）] ページを開きます。

ステップ 2 プレフィックスを表示するには、名前、アドレス、および範囲を追加してから、DHCP タイプと可能なテンプレートを選択します（『*Cisco Prime Network Registrar 11.1 DHCP* ユーザ ガイド』の「IPv6 アドレス空間の表示」の項を参照してください）。

ステップ 3 所有者ドロップダウン リストから所有者を選択します。

ステップ 4 リージョン ドロップダウン リストからリージョンを選択します。

ステップ 5 [**プレフィックスの追加（Add Prefix**）] をクリックします。新しく追加されたプレフィックスが [DHCP v6 アドレス ツリー（DHCP v6 Address Tree）] ページに表示されます。

ローカル詳細およびリージョン詳細 Web UI

DHCP プレフィックスを一覧表示または追加するには、次の手順を実行します。

ステップ 1 [設計（Design）] メニューから、[DHCPv6] サブメニューの [プレフィックス（Prefixes）] を選択して、[DHCPv6 プレフィックスの一覧表示/追加（List/Add DHCP v6 Prefixes）] ページを開きます。

ステップ 2 [プレフィックス（Prefixes）] ペインの [プレフィックスの追加（Add Prefixes）] アイコンをクリックして、プレフィックスの名前、アドレス、および範囲を入力し、DHCP タイプと可能なテンプレートを選択します。

ステップ 3 所有者ドロップダウン リストから所有者を選択します。

ステップ 4 リージョン ドロップダウン リストからリージョンを選択します。

ステップ 5 [IPv6 プレフィックスの追加（Add IPv6 Prefix）] をクリックします。新しく追加されたプレフィックスが [DHCP v6 プレフィックスの一覧表示/追加（List/Add DHCP v6 Prefixes）] ページに表示され、左側の [プレフィックス（Prefixes）] ペインにも表示されます。

リンクレベルの制約

次の場合、リンクを表示または変更できます。

- ユーザーは、ローカル クラスタの dhcp-admin または addrblock-admin ロールの ipv6-management サブロールとして、またはリージョン クラスタの central-cfg-admin または regional-addr-admin ロールとして承認されています。

- リンクの所有者またはリージョンは、ユーザーに定義されている所有者またはリージョン ロールの制約に一致します。
- リンクに所有者またはリージョンが定義されていず、ユーザーに対して所有者またはリージョン ロールの制約が定義されていない場合に限ります。

制約なしのユーザーの場合は、すべてのリンクにアクセスできます。

次に、リンク レベルの制約の例を示します。

```
Link 'BLUE' has owner 'blue' set.
    Link 'ORANGE' has owner unset.

    Link 'BLUE' owner is 'blue'.
    Link 'ORANGE' owner is unset. Only unconstrained users can access this link.
```

ローカルおよびリージョン Web UI

リンクを追加するには、次の手順を実行します。

ステップ 1 [**設計（Design**）] メニューから、[**DHCPv6**] サブメニューの [**リンク（Links**）] を選択して、[DHCPv6 リンクの一覧表示/追加（List/Add DHCP v6 Links）] ページを開きます。

ステップ 2 [リンク（Links）] ペインの [**リンクの追加（Add Links**）] アイコンをクリックし、名前を入力してから、リンク タイプを選択し、グループを入力します。

ステップ 3 [**リンクの追加（Add Link**）] をクリックします。新しく追加された DHCPv6 リンクが、[DHCPv6 リンクの一覧表示/追加（List/Add DHCP v6 Links）] ページに表示されます。

管理者の一元管理

リージョンまたはローカル CCM 管理者として、次のことができます。

- ローカルおよびリージョン クラスタ管理者、グループ、およびロールを作成および変更します。
- 管理者、グループ、およびロールをローカル クラスタにプッシュします。
- ローカル クラスタの管理者、グループ、およびロールを中央クラスタにプルします。

これらの各機能には、少なくとも 1 つのリージョン CCM 管理者サブロールが定義されている必要があります。次の表に、これらの操作に必要なサブロールを示します。

表 *3*：集中管理者管理に必要なサブロール

集中管理者管理アクション	必要なリージョン サブロール
管理者の作成、変更、プッシュ、プル、または削除	認証

集中管理者管理アクション	必要なリージョン サブロール
グループまたはロールの作成、変更、プッシュ、プル、または削除	承認
関連付けられた所有者またはリージョンによるグループまたはロールの作成、変更、プッシュ、プル、または削除	承認所有者リージョン
外部認証サーバーの作成、変更、プッシュ、プル、または削除	認証
テナントの作成、変更、プッシュ、プル、または削除	認証

管理者のプッシュとプル

リージョン クラスタ Web UI の [管理者の一覧表示/追加（List/Add Administrators）] ページで、ローカル クラスタに管理者をプッシュしたり、管理者をプルしたりすることができます。

リージョンクラスタで、ローカルとリージョンの両方のロールを持つ管理者を作成できます。ただし、ローカルクラスタはリージョンのロールを認識しないため、関連付けられているローカル ロールのみをプッシュまたはプルできます。

ローカル クラスタへの管理者のプッシュ

ローカルクラスタに管理者をプッシュするには、1つ以上のクラスタとプッシュ モードを選択する必要があります。

リージョン Web UI

ステップ 1 [管理（Administration）] メニューから [管理者（Administrators）] を選択します。

ステップ 2 [管理者の一覧表示/追加（List/Add Administrators）] ページで、[管理者（Administrators）] ペインの **[すべてプッシュ（Push All）]** アイコンをクリックして、ページにリストされているすべての管理者をプッシュします。[ローカルクラスタへのデータのプッシュ（Push Data to Local Clusters）] ダイアログボックスが開きます。

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クリックして、プッシュ モードを選択します。すべての管理者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。単一の管理者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 クラスタの既存の管理者データを置換する場合にのみ、[置換（Replace）] を選択します。ローカル クラスタで管理者データベースの正確なコピーを作成し、それによって、リージョン クラスタで定義されていないすべての管理者を削除する場合にのみ、[完全（Exact）] を選択します。

ステップ 4 デスティネーション クラスタの [使用可能（Available）] フィールドで 1 つ以上のローカル クラスタを選択し、それらを [選択済み（Selected）] フィールドに移動します。

ステップ 5 **Push Data to Clusters** をクリックします。

ステップ 6 [プッシュ データ レポートの表示（View Push Data Report）] ダイアログボックスで、プッシュの詳細を確認して、[OK] をクリックして、[管理者の一覧表示/追加（List/Add Administrators）] ページに戻ります。

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、**admin** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-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。push の場合、**-omitrelated** が指定されていない限り、関連付けられたロールとグループも（置換モードを使用して）プッシュされます。

ローカル クラスタへの管理者の自動プッシュ

新しいユーザー名とパスワードの変更は、リージョン クラスタからローカル クラスタに自動的にプッシュできます。これを行うには、リージョン クラスタで同期編集モードを有効にする必要があります。編集モードは、現在の Web UI セッションに対して設定されます。または、CCM サーバー設定に設定されているすべてのユーザーのデフォルトとして設定されます。

同期モードが設定されている場合は、ユーザー名とパスワードに対する後続のすべての変更がローカル クラスタと同期されます。リージョン サーバーでパスワードを変更でき、この変更はローカル クラスタに自動的に反映されます。

管理者ユーザーの場合は、リージョン クラスタのユーザー ログイン情報に対して複数の変更を加えることができます。これらの変更はすべて、自動的にローカル クラスタにプッシュされます。

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

ステップ 3 同期ラジオ ボタンを使用して、admin、dhcp、および dns のリージョン編集モードの値を選択します。

ステップ 4 **webui-mode** ドロップダウンリストから webui モード値を選択します。

ステップ 5 idle-timeout 値を入力します。

ステップ 6 属性値を設定解除するには、**[設定解除（Unset?）]** 列のチェックボックスをオンにしてから、ページの下部にある **[フィールドの設定解除（Unset Fields）]** をクリックします。属性値を設定解除または変更するには、**[保存（Save）]** をクリックするか、**[キャンセル（Cancel）]** をクリックして変更をキャンセルします。

（注） アスタリスクでマークされている属性の値を入力します。これらは、CCM サーバーの動作に必要なためです。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。

リージョンモードでの CLI への接続

CLI にはリージョンモードで接続する必要があります。リージョン モードには、-R フラグが必要です。同期編集モードを設定するには、次のようにします。

```
nrcmd-R> session set admin-edit-mode=synchronous
```

レプリカ データベースからの管理者のプル

ローカル クラスタからの管理者のプルは、主に、他のローカル クラスタにプッシュできる管理者の初期リストを作成する場合にのみ役立ちます。ローカル管理者は、リージョン クラスタ自体では有効ではありません。これらの管理者にはリージョン ロールが割り当てられていないためです。

管理者をプルするとき、実際にはリージョン クラスタのレプリカ データベースからプルします。ローカル クラスタの作成では、最初にデータが複製され、定期的なポーリングによって複製が自動的に更新されます。ただし、レプリカ データがローカル クラスタと完全に最新であることを確実にするには、データをプルする前に強制的に更新できます。

リージョン 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 **[グループ（Administrators）]** を選択します。

ステップ 2 [管理者の一覧表示/追加（List/Add Administrators）] ページで、[管理者（Administrators）] ペインの [データのプル（**Pull Data**）] をクリックします。[プルするレプリカ管理者データの選択（Select Replica Admin Data to Pull）] ダイアログボックスが開きます。

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 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。ほとんどの場合、デフォルトの [置換（Replace）] モードのままにしておきますが、リージョン クラスタですでに定義されている既存の管理者プロパティを保持するには [保証（Ensure）] を選択します。または、ローカル クラスタの管理者データベースの正確なコピーを作成するには、[完全（Exact）] を選択します（非推奨）。

ステップ 5 クラスタの横にある [コア管理者のプル（**Pull Core Administrators**）] をクリックするか、クラスタ名を展開して [管理者のプル（**Pull Administrator**）] をクリックして、クラスタ内の個々の管理者をプルします。

ステップ 6 [プルするレプリカ管理者データの選択（Select Replica Admin Data to Pull）] ダイアログボックスで、変更設定データを表示し、**[OK]** をクリックします。[管理者の一覧表示/追加（List/Add Administrators）] ページに戻ると、プルした管理者がリストに追加されています。

（注） リージョン クラスタがなく、1 つのローカル クラスタから別のクラスタに管理者、ロール、またはグループをコピーする場合は、それらをエクスポートしてから、cnr_exim ツールを使用して、ターゲット クラスタに再インポートすることができます（cnr_exim データ インポートおよびエクスポート ツールの使用 を参照）。ただし、このツールは管理者パスワードを保持しないため、ターゲット クラスタで手動でリセットする必要があります。パスワードのセキュリティを維持するために、この方法が実装されています。エクスポート コマンドは、次のとおりです。

```
cnr_exim -c admin -x -e outputfile.txt
```

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、**admin** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] コマンドを使用できます。

外部認証サーバーのプッシュとプル

リージョン Web UI の [RADIUS サーバーの一覧表示/追加（List/Add RADIUS Server）] ページまたは [Active Directory サーバーの一覧表示/追加（List/Add Active Directory Server）] ページで、すべての外部認証サーバーをローカル クラスタにプッシュしたり、ローカル クラスタから外部認証サーバーデータをプルしたりできます。

RADIUS 外部認証サーバーのプッシュ

外部認証サーバーをローカル クラスタにプッシュするには、次の手順を実行します。

リージョンの詳細 Web UI

ステップ 1 [管理（Administration）] メニューから、[外部認証（External Authentication）] サブメニューの [Radius] を選択して、リージョン Web UI で [RADIUS サーバーの一覧表示/追加（List/Add RADIUS Server）] ページを表示します。

ステップ 2 [Radius] ペインの [すべてプッシュ（Push All）] アイコンをクリックして、ページにリストされているすべての外部認証サーバーをプッシュするか、[プッシュ（Push）] をクリックして、個々の外部認証サーバーをプッシュします。[ローカルクラスタへのデータのプッシュ（Push Data to Local Clusters）] ダイアログボックスが開きます。

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。

- すべての外部認証サーバー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。
- 単一の外部認証サーバー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。

  上記のいずれの場合も、[保証（Ensure）] がデフォルトのモードです。

ローカル クラスタの既存の外部認証サーバー データを置換する場合のみ、[置換（Replace）] を選択します。ローカル クラスタに外部認証サーバー データの正確なコピーを作成し、それによって、リージョン クラスタで定義されていないすべての外部認証サーバーを削除する場合にのみ、[完全（Exact）] を選択します。

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。

RADIUS 外部認証サーバーのプル

外部認証サーバーのデータをローカル クラスタからプルするには、次の手順を実行します。

リージョンの詳細 Web UI

ステップ 1 [管理（Administration）] メニューから、[外部認証（External Authentication）] サブメニューの [Radius] を選択して、リージョン Web UI で [Radius サーバーの一覧表示/追加（List/Add Radius Server）] ページを表示します。

ステップ 2 [Radius サーバーの一覧表示/追加（List/Add Radius Server）] ページで、[Radius] ペインの [データのプル（Pull Data）] をクリックします。[プルするレプリカ外部認証サーバー データの選択（Select Replica External Authentication Server Data to Pull）] ダイアログボックスが開きます。

ステップ 3 クラスタの [レプリカ データの更新（Update Replica Data）] 列の [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 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。

ローカル クラスタの既存の認証サーバー プロパティを保持するには、[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。

（注） [完全 （Exact）] を選択して、ローカル クラスタで外部認証サーバーデータの正確なコピーを作成することは推奨されません。

ステップ 5 クラスタの横にある [**すべての外部認証サーバーのプル（Pull All External Authentication Servers**）] をクリックします。

ステップ 6 [レプリカ認証サーバーのプルの報告（Report Pull Replica Authentication servers）] ページで、プルの詳細を確認し、[**実行（Run**）] をクリックします。

[レプリカ認証サーバーのプルの実行（Run Pull Replica Authentication servers）] ページで、変更設定データを確認し、[**OK**] をクリックします。[認証サーバーの一覧表示/追加（List/Add Authentication Server）] ページに戻ると、プルされた外部認証サーバーがリストに追加されています。

AD 外部認証サーバーのプッシュ

外部認証サーバーをローカル クラスタにプッシュするには、次の手順を実行します。

リージョンの詳細 Web UI

ステップ 1 [管理（Administration）] メニューから、[外部認証（External Authentication）] サブメニューの [Active Directory] を選択して、リージョン Web UI で [Active Directoryサーバーの一覧表示/追加（List/Add Active Directory Server）] ページを表示します。

ステップ 2 [Active Directory] ペインで [すべてプッシュ（Push All）] をクリックして、外部認証サーバーをプッシュします。[ローカルクラスタへのデータのプッシュ（Push Data to Local Clusters）] ダイアログボックスが開きます。

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。

- すべての外部認証サーバー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。
- 単一の外部認証サーバー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。

  上記のいずれの場合も、[保証（Ensure）] がデフォルトのモードです。

ローカル クラスタの既存の外部認証サーバー データを置換する場合のみ、[置換（Replace）] を選択します。ローカル クラスタに外部認証サーバー データの正確なコピーを作成し、それによって、リージョン クラスタで定義されていないすべての外部認証サーバーを削除する場合にのみ、[完全（Exact）] を選択します。

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。

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、**auth-ad-server** < *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。

AD 外部認証サーバーのプル

ローカル クラスタから AD 外部認証サーバーのデータをプルするには、次の手順を実行します。

リージョンの詳細 Web UI

ステップ 1 [管理（**Administration**）] メニューから、[外部認証（**External Authentication**）] サブメニューの[**Active Directory**] を選択して、リージョン Web UI で [Active Directory サーバーの一覧表示/追加（List/Add Active Directory Server）] ページを表示します。

ステップ 2 [Active Directory サーバーの一覧表示/追加（List/Add Active Directory Server）] ページで、[Active Directory] ペインの [データのプル（**Pull Data**）] をクリックします。[プルするレプリカ外部認証サーバー データの選択（Select Replica External Authentication Server Data to Pull）] ダイアログボックスが開きます。

ステップ 3 クラスタの [レプリカ データの更新（Update Replica Data）] 列の [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 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。

ローカル クラスタの既存の認証サーバー プロパティを保持するには、[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。

（注） [完全 （Exact）] を選択して、ローカル クラスタで外部認証サーバーデータの正確なコピーを作成することは推奨されません。

ステップ 5 クラスタの横にある [すべての外部認証サーバーのプル（**Pull All External Authentication Servers**）] をクリックします。

ステップ 6 [レプリカ認証サーバーのプルの報告（Report Pull Replica Authentication servers）] ページで、プルの詳細を確認し、[実行（**Run**）] をクリックします。

[レプリカ認証サーバーのプルの実行（Run Pull Replica Authentication servers）] ページで、変更設定データを確認し、[**OK**] をクリックします。[認証サーバーの一覧表示/追加（List/Add Authentication Server）] ページに戻ると、プルされた外部認証サーバーがリストに追加されています。

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、**auth-ad-server** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] コマンドを使用できます。

グループのプッシュとプル

グループのプッシュとプルは、管理者をローカル クラスタの一貫したロールのセットに関連付ける上で不可欠です。リージョン クラスタ Web UI の [管理者グループの一覧表示/追加（List/Add Administrator Groups）] ページで、グループをローカル クラスタにプッシュしたり、グループをプルしたりできます。

ローカル クラスタへのグループのプッシュ

ローカル クラスタにグループをプッシュするには、1 つ以上のクラスタとプッシュ モードを選択する必要があります。

リージョン 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 **[グループ（Groups）]** を選択します。

ステップ 2 [管理者グループの一覧表示/追加（List/Add Administrator Groups）] ページで、[グループ（Groups）] ペインの [すべてプッシュ（**Push All**）] アイコンをクリックして、ページにリストされているすべてのグループをプッシュします。または [プッシュ（**Push**）] をクリックして、個々のグループをプッシュします。[ローカル クラスタへのデータのプッシュ（Push Data to Local Clusters）] ダイアログボックスが開きます。

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。すべてのグループ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 つのグループ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 クラスタの既存のグループ データを置換する場合にのみ、[置換（Replace）] を選択します。ローカル クラスタにグループ データの正確なコピーを作成し、それによって、リージョン クラスタで定義されていないすべてのグループを削除する場合にのみ、[完全（Exact）] を選択します。

ステップ 4 デフォルトでは、関連付けられているロールと所有者がグループとともにプッシュされます。ロールは置換モードでプッシュされ、所有者は保証モードでプッシュされます。関連付けられているロールまたは所有者のプッシュを無効にするには、それぞれのチェックボックスをオフにします。

ステップ 5 デスティネーション クラスタの [使用可能（Available）] フィールドで 1 つ以上のローカル クラスタを選択し、それらを [選択済み（Selected）] フィールドに移動します。

ステップ 6 **Push Data to Clusters** をクリックします。

ステップ 7 [プッシュ グループ データ レポートの表示（View Push Group Data Report）] ダイアログボックスで、プッシュの詳細を確認して、[OK] をクリックし、[管理者グループの一覧表示/追加（List/Add Administrator Groups）] ページに戻ります。

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、**group** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-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。この操作では、関連するロール（置換モードを使用）と関連する所有者とリージョン（保証モードを使用）もプッシュされます。これを防止し、グループだけをプッシュする場合は、**-omitrelated** を指定します。

レプリカ データベースからのグループのプル

ローカル クラスタからの管理者グループのプルは、主に、他のローカル クラスタにプッシュできるグループの初期リストを作成する場合にのみ役立ちます。ローカル グループは、リージョン クラスタ自体では有効ではありません。これらのグループには、リージョン ロールが割り当てられていないためです。

グループをプルするときには、実際にはリージョン クラスタのレプリカ データベースからプルします。ローカル クラスタの作成では、最初にデータが複製され、定期的なポーリングによって複製が自動的に更新されます。ただし、レプリカ データがローカル クラスタと完全に最新であることを確実にするには、データをプルする前に強制的に更新できます。

リージョン 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 [グループ（**Groups**）] を選択します。

ステップ 2 [管理者グループの一覧表示/追加（List/Add Administrator Groups）] ページで、[グループ（Groups）] ペインの [データのプル（**Pull Data**）] アイコンをクリックします。[プルするレプリカ CCMAdminGroup データの選択（Select Replica CCMAdminGroup Data to Pull）] ダイアログボックスが開きます。

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 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。ほとんどの場合、デフォルトの [置換（Replace）] モードのままにしておきますが、ローカル クラスタの既存のグループ プロパティを保持するには [保証（Ensure）] を選択します。または、ローカル クラスタのグループ データの正確なコピーを作成するには、[完全（Exact）] を選択します（非推奨）。

ステップ 5 クラスタの横にある **Pull Core Groups** をクリックするか、クラスタ名を展開して、**Pull Group** をクリックして、クラスタ内の個々のグループをプルします。

ステップ 6 [レプリカ グループのプルの報告（Report Pull Replica Groups）] ページで、プルの詳細を確認し、[実行（Run）] をクリックします。

ステップ 7 [レプリカ グループのプルの実行（Run Pull Replica Groups）] ページで、変更設定データを確認し、[OK] をクリックします。[管理者グループの一覧表示/追加（List/Add Administrator Groups）] ページに戻ると、プルしたグループがリストに追加されています。

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、**group** < *name* | **all** > **pull** < **ensure** | **replace** > *cluster-name* [**-report-only** | **-report**] コマンドを使用できます。

ロールのプッシュとプル

リージョン クラスタ Web UI の [管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページで、ロールをローカルクラスタにプッシュしたり、ロールをプルしたりすることができます。また、サブロールの権限に応じて、関連付けられたグループと所有者をプッシュしたり、関連付けられた所有者をプルしたりすることもできます（表 3 : 集中管理者管理に必要なサブロール （29 ページ） を参照）。

ローカル クラスタへのロールのプッシュ

管理者ロールをローカル クラスタにプッシュするには、1 つ以上のクラスタとプッシュ モードを選択する必要があります。

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 [ロール（**Roles**）] を選択します。

ステップ 2 [管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページで、[ロール（Roles）] ペインの **Push All** アイコンをクリックして、ページにリストされているすべてのロールをプッシュするか、または **Push** をクリックして、個々のロールをプッシュします。[ローカルクラスタへのデータのプッシュ（Push Data to Local Clusters）] ダイアログボックスが開きます。

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。すべてのロール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 つのグループ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 クラスタの既存のロールデータを置き換える場合にのみ、[置換（Replace）] を選択します。ローカル クラスタにロールデータの正確なコピーを作成し、それによって、リージョン クラスタで定義されていないすべてのロールを削除する場合にのみ、[完全（Exact）] を選択します。

ステップ 4 デフォルトでは、関連付けられたグループと所有者がロールとともにプッシュされます。グループは置換モードで、所有者は保証モードでプッシュされます。関連付けられているロールまたは所有者のプッシュを無効にするには、それぞれのチェックボックスをオフにします。

- 関連付けられたグループのプッシュを無効にし、グループがローカル クラスタに存在しない場合、ロールの名前に基づくグループがローカル クラスタで作成されます。
- 関連付けられた所有者のプッシュを無効にし、所有者がローカル クラスタに存在しない場合、そのロールは意図した制約を使用して設定されません。グループをローカル クラスタに個別にプッシュするか、または owner-region サブロールが割り当てられているリージョン管理者が、ロールをプッシュする前にグループをプッシュしたことを確認する必要があります。

ステップ 5 デスティネーション クラスタの [使用可能（Available）] フィールドで 1 つ以上のローカル クラスタを選択し、それらを [選択済み（Selected）] フィールドに移動します。

ステップ 6 **Push Data to Clusters** をクリックします。

ステップ 7 [ロール データのプッシュ レポートの表示（View Push Role Data Report）] ページで、プッシュの詳細を確認してから、**OK** をクリックして、[管理者ロールの一覧表示/追加] ページに戻ります。

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、**role** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-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。この操作では、関連するグループ（置換モードを使用）および関連する所有者とリージョン（保証モードを使用）もプッシュされます。これを防止し、ロールだけをプッシュするには、**-omitrelated** を指定します。

レプリカ データベースからのロールのプル

ローカル クラスタからの管理者ロールのプルは、主に、他のローカル クラスタにプッシュできるロールの初期リストを作成する場合にのみ役立ちます。ローカル ロールは、リージョン クラスタ自体では有用ではありません。

ロールをプルするときには、実際にはリージョン クラスタのレプリカ データベースからプルします。ローカル クラスタの作成では、最初にデータが複製され、定期的なポーリングによって複製が自動的に更新されます。ただし、レプリカ データがローカル クラスタと完全に最新であることを確実にするには、データをプルする前に強制的に更新できます。

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 [ロール（Roles）] を選択します。

ステップ 2 [管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページで、[ロール（Roles）] ペインの [データのプル（**Pull Data**）] アイコンをクリックします。[プルするレプリカ管理者ロールデータの選択（Select Replica Administrator Role Data to Pull）] ダイアログボックスが開きます。

ステップ 3 クラスタの [レプリカ データの更新（Update Replica Data）] 列の [**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 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。ほとんどの場合、デフォルトの [置換（Replace）] モードのままにしておきますが、ローカル クラスタの既存のロール プロパティを保持するには [保証（Ensure）] を選択します。または、ローカル クラスタのロール データの正確なコピーを作成するには、[完全（Exact）] を選択します（非推奨）。

ステップ 5 owner-region サブロール権限を持っている場合は、関連するすべての所有者をロールとともにプルするかどうかを決定できます。これは常に保証モードになります。この選択はデフォルトで有効になっています。

ステップ 6 クラスタの横にある **Pull Core Roles** をクリックするか、クラスタ名を展開して、**Pull Role** をクリックして、クラスタ内の個々のロールをプルします。

ステップ 7 [レプリカ ロールのプルの報告（Report Pull Replica Roles）] ページで、**Run** をクリックします。

ステップ 8 [レプリカ ロールのプルの実行（Run Pull Replica Roles）] ページで、変更設定データを確認し、**OK** をクリックします。[管理者ロールの一覧表示/追加（List/Add Administrator Roles）] ページに戻ると、プルしたロールがリストに追加されています。

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、**role** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] コマンドを使用できます。この操作によって、関連する所有者とリージョンが（保証モードを使用して）プルされます。これを防止し、ロールだけをプルするには、**-omitrelated** を指定します。

テナントのプッシュとプル

リージョン Web UI の [テナントの一覧表示/追加（List/Add Tenants）] ページで、すべてのテナントをローカル クラスタにプッシュしたり、ローカル クラスタからテナント データをプルしたりすることができます。

ローカル クラスタへのテナントのプッシュ

テナントをローカル クラスタにプッシュするには、次の手順を実行します。

リージョン Web UI

スコープを追加するには、次の手順を実行します。

ステップ 1 **Administration** メニューから、**Tenants User Access** サブメニューの を選択して、リージョン Web UI で [テナントの一覧表示/追加（List/Add Tenants）] ページを表示します。

ステップ 2 [テナント（Tenants）] ペインの **Push All** アイコンをクリックして、ページにリストされているすべてのテナントをプッシュするか、**Push** をクリックして、個々のテナントをプッシュします。[ローカル クラスタへのテナント データのプッシュ（Push Tenant Data to Local Clusters）] ページが開きます。

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。

- すべてのテナント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 つのテナント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 クラスタのテナント データを置換する場合のみ、[置換（Replace）] を選択します。ローカル クラスタのテナント データの正確なコピーを作成して、それによって、リージョン クラスタで定義されていないすべてのテナントを削除する場合にのみ、[完全（Exact）] を選択します。

ステップ 4 **Push Data to Clusters** 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ときには、**tenant** < *tag* | **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 データベースからのテナントのプル

レプリカ データベースからテナントをプルするには、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、 **Tenants User Access** サブメニューの を選択して、[テナントの一覧表示/追加（List/Add Tenants）] ページを開きます。

ステップ 2 [テナントの一覧表示/追加（List/Add Tenants）] ページで、[テナント（Tenants）] ペインの **Pull Data** アイコンをクリックします。[プルするレプリカ テナント データの選択（Select Replica Tenant Data to Pull）] ダイアログボックスが開きます。

ステップ 3 クラスタの [レプリカ データの更新（Update Replica Data）] 列の [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 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。

ローカル クラスタの既存のテナント 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。

（注） [完全（Exact）] を選択して、ローカル クラスタのテナント データの正確なコピーを作成することは推奨されません。

ステップ 5 **Pull Replica** をクリックします。

ステップ 6 [プルするレプリカ テナント データの選択（Select Replica Tenant Data to Pull）] ページで、[**すべてのテナントをプル（Pull all Tenants**）] をクリックして、プルの詳細を表示し、**Run** をクリックします。

[レプリカ テナントのプルの実行（Run Pull Replica Tenants）] ページで、変更設定データを表示し、**OK** をクリックします。[テナントの一覧表示/追加（List/Add Tenants）] ページに戻ると、プルしたテナントがリストに追加されています。

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、**tenant** < tag | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] コマンドを使用できます。

セッション管理

Cisco Prime Network Registrar は、ユーザーセッションをモニターし、セッション管理に関するシステム設定を管理し、各ユーザーのログイン情報をレポートする管理者機能を提供します。各ユーザーのログインおよびログアウトの詳細を提供するために、セッションイベントが追加されます。

ユーザー セッション

アプリケーションページの右上隅にある歯車アイコン（  ）をクリックすると、アカウントがいつ、どこで使用されたのかを確認できます。最初のログインでは、ユーザー名とホストだけが表示されます。2 回目のログインでは、最後に成功したログインが日時とともに表示されます。ログインに失敗すると、次に成功したログインでは、ログイン試行の失敗回数が表示されます。

スーパーユーザー管理者は、1 人のユーザーの同時セッション数を制限して、アカウントの共有や過度の使用を防ぐことができます。また、ログイン試行の失敗回数を制限して、自動ログイン攻撃から保護することもできます。再試行制限に達すると、ユーザーアカウントは一時停止されます。

セッション制御属性を設定するには、次の手順を実行します。

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、[サーバー（Servers）] サブメニューの [サーバー管理（Manage Servers）] を選択して [サーバー管理（Manage Server）] 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 次のフィールドに必要な値を入力します。

- **admin-failed-login-limit**：管理者アカウントが一時停止されるまでに許可されるユーザーまたはトークンログイン試行の失敗の最大回数を指定します。0 に設定すると、制限は適用されません。この値を 1 または 2 にすることは推奨されません。
- **admin-user-session-limit**：単一管理者の同時ユーザーセッションの最大数を指定します。0 に設定すると、制限は適用されません。
- **admin-token-session-limit**：単一管理者の同時トークンセッションの最大数を指定します。シングルサインオン接続が、最も一般的なトークンセッションです。Web UI は、リソースモニターリングおよびダッシュボード表示のためにトークンセッションを開くこともあります。0 に設定すると、制限は適用されません。この値を 1 または 2 にすることは、予期しない Web UI 障害が発生する可能性があるため、推奨されません。
- **admin-suspended-timeout**：一時停止の管理者アカウントが管理上再開されていない場合に、一時停止のままにする時間を指定します。0 に設定すると、アカウントを再開するには管理アクションが必要になります。アカウントが自動的に再開される場合は最大 30 分の追加の遅延が発生する可能性があります。

ステップ 4 [保存（Save）] をクリックして設定を保存します。

ステップ 5 サーバーを再起動し、変更を確認します。

CLI コマンド

ユーザーアカウントを一時停止するには、**admin** *name* **suspend** を使用します。

ユーザーアカウントを再開するには、**admin** *name* **reinstate** を使用します。

アクティブユーザーセッション

アクティブユーザーセッションは、[CCM ユーザー接続（CCM User Connections）] ページに一覧表示されます。このレポートページは、スーパーユーザーだけが使用できます。

CCM ユーザー接続レポートを表示するには、次の手順を実行します。

ローカルおよびリージョン Web UI

[操作（Operate）] メニューの [レポート（Reports）] サブメニューで [CCM ユーザー接続（CCM User Connections）] を選択し、[CCM ユーザー接続（CCM User Connections）] ページを開きます。すべてのアクティブユーザーセッションが、管理者名、接続に関連付けられている認証のタイプ（管理者認証タイプ）、接続開始時間、要求の総数、およびクライアントの送信元の詳細とともに表示されます。

[送信元クライアント（Client Source）] 列には、接続に関する追加情報が表示されます（利用可能な場合）。これらの情報には、次のようなものがあります。

- 着信 HTTP/HTTPS 接続の送信元アドレスとポート（web UI および REST セッションの場合）。

- 受信した CLI、ツール、または SDK セッションの送信元アドレス、ポート、およびユーザー情報。使用可能な場合は、開始側のユーザーの SSH 接続用アドレスとポートも指定できます（これは、ユーザーの SSH_CONNECTION 環境変数に基づいています）。
- ほかにも次のような役に立つインジケータがあります。
  - ローカル クラスタとリージョン クラスタ間の CCM 接続に対する「Regional-to-local management」または「Local-to-regional management」。
  - ローカル クラスタ間のフェールオーバー、HA 同期、またはその他の CCM 間接続に対する「Local-to-local management」。
  - サーバーを識別するサーバー関連の接続（および場合によっては追加の詳細情報）については、< および > で囲まれたその他の ID。

（注） この情報はクライアントによって CCM に提供されるため、スプーフィングの対象となる可能性がありますが、情報として扱う必要があるため権限はありません。

（注） [CCM ユーザー接続（CCM User Connections）] では、2 つの認証タイプ（管理者認証タイプ：1) ユーザーと 2) トークン）をサポートしています。

- Cisco Prime Network Registrar は、アプリケーションレベルの 2 ～ 3 個のスレッドを実行して、ダッシュボードとリソースモニターを操作します。これらは、トークンタイプの接続として表示されます。したがって、ログアウトしてもこれらの接続は存続し、バックグラウンドで実行され続けるため、トークンタイプの接続の要求数が増加します。すべての接続（主にトークンタイプ）をクリアする場合は、Cisco Prime Network Registrar を再起動する必要があります。
- Cisco Prime Network Registrar からログアウトせずにブラウザを閉じると、ユーザータイプの接続は 2 時間（デフォルトのセッションタイムアウト）維持されます。

CLI コマンド

アクティブユーザーセッションを表示するには、**ccm listConnections** を使用します。

セッションイベントのログ

スーパーユーザー管理者は、セッションイベントのログエントリを表示するか Web UI の上部にある [アラーム（Alarms）] アイコンをクリックしてセッションイベントを表示することにより、セッションアクティビティをモニターできます。

セッションイベントのログを表示するには、次の手順を実行します。

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、[サーバー（Servers）] サブメニューの [サーバー管理（Manage Servers）] を選択して [サーバー管理（Manage Server）] 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 [モニターのログ（Monitor Logs）] タブをクリックしてセッションイベントのログを表示します。

CCM は、ユーザーが CCM に認証されるときに、クライアントが提供する追加の送信元情報（詳細については、アクティブユーザーセッション （43 ページ）を参照）をログに記録します。また、接続が閉じられるときに情報が提供される場合は、その情報をログに記録します。この情報は、ユーザーログイン（ユーザー設定）情報に関連する変更ログエントリにも示されます。

（注） この情報は、Cisco Prime Network Registrar 10.1 CLI および SDK 以降でのみ提供されます（Cisco Prime Network Registrar 10.0 以前のクライアントでは、この追加情報がレポートされないため、CCM はそれをログに記録しない）。

（注） Cisco Prime Network Registrar 11.1 以降では、Web UI および REST API を介してログインした管理者の場合、SCP 操作ごとに実際のクライアントの詳細（IP およびポート）がログに記録されます。

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