



# CHAPTER 5

## ロールベース アクセス コントロール の設定

この章では、Cisco 4700 シリーズ Application Control Engine (ACE) アプライアンスにロールベース アクセス コントロール (RBAC) を設定する方法について説明します。この章の構成は、次のとおりです。

- [概要](#)
- [Device Manager GUI を使用した RBAC の設定](#)
- [CLI を使用した RBAC の設定](#)

### 概要

この章を読むと、ACE アプライアンスが RBAC を使用してどのようにセキュリティ管理を提供しているか、およびネットワークのサブセットへのアクセス権限を持つサーバ保守ユーザを設定するにはどうすればいいかを基本的に理解できます。

巨大なネットワークの管理における最大の難問の 1 つは、セキュリティ管理の複雑さです。ACE アプライアンスを使用することにより、RBAC を通じて、各ユーザが使用できるコマンドおよびリソースを判断することができます。RBAC では、ユーザはドメインとロールに関連付けられています。

ドメインは実サーバや仮想サーバなどの物理ネットワーク リソースと仮想ネットワーク リソースの集まりです。

ユーザが入力できるコマンドや、特定のコンテキストでユーザが実行できるアクションなど、ユーザの権限はユーザ ロールによって決まります。ACE には、事前定義された多数のロールが用意されています。さらに、管理者はどのような場合でも、新規ロールを定義できます。

ACE には、次のロールが事前定義されています。これらを削除したり、修正したりすることはできません。

- **Admin** : 管理コンテキストで作成された場合、ユーザは、ACE 全体のすべてのコンテキスト、ドメイン、ロール、ユーザ、リソース、およびオブジェクトに完全にアクセスでき、それらを制御できます。ユーザ コンテキストで作成された場合、ユーザは、そのコンテキスト内のすべてのポリシー、ロール、ドメイン、サーバファーム、実サーバなどのオブジェクトに完全にアクセスでき、それらを制御できます。
- **Network Admin** : 次の機能に対し、完全にアクセスでき、それらを制御できます。
  - インターフェイス
  - ルーティング
  - 接続パラメータ
  - ネットワーク アドレス変換 (NAT)
  - VIP
  - コピー設定
  - **changeto** コマンド
  - **exec** コマンド
- **Network-Monitor** : **show** コマンドすべて、および **changeto** コマンド、**exec** コマンドにアクセスできます。これは、**username** コマンドを使用してユーザに明示的にロールを割り当てなかった場合のデフォルト ロールです。
- **Security-Admin** : コンテキストで次のセキュリティ関連機能に対し、完全にアクセスでき、それらを制御できます。
  - Access Control List (ACL; アクセス コントロール リスト)
  - アプリケーション インспекション
  - 接続パラメータ
  - インターフェイス
  - 認証およびアカウンティング (AAA)

- NAT
- コピー設定
- **changeto** コマンド
- **exec** コマンド
- **Server-Appln-Maintenance** : 次の機能に対し、完全にアクセスでき、それらを制御できます。
  - 実サーバ
  - サーバ ファーム
  - ロード バランシング
  - コピー設定
  - **changeto** コマンド
  - **exec** コマンド
- **Server-Maintenance** : 次の機能に対し、実サーバ メンテナンス、モニタリング、およびデバッグを実行できます。
  - 実サーバ : 修正権限
  - サーバ ファーム : デバッグ権限
  - VIP : デバッグ権限
  - プローブ : デバッグ権限
  - ロード バランシング : デバッグ権限
  - **changeto** コマンド : 作成権限
  - **exec** コマンド : 作成権限
- **SLB-Admin** : コンテキストで次の ACE 機能に対し、完全にアクセスでき、それらを制御できます。
  - 実サーバ
  - サーバ ファーム
  - VIP
  - プローブ
  - ロード バランシング (レイヤ 3/4 およびレイヤ 7)
  - NAT

- インターフェイス
- コピー設定
- **changeto** コマンド
- **exec** コマンド
- SSL-Admin : SSL 機能をすべて管理できます。
  - SSL : 作成権限
  - PKI : 作成権限
  - インターフェイス : 修正権限
  - コピー設定 : 作成権限
  - **changeto** コマンド : 作成権限
  - **exec** コマンド

次のようにして、RBAC を通じて、ユーザを作成し、権限を割り当てることができます。

---

**ステップ 1**   ドメインを作成し、このドメインのネットワーク リソースを選択します。

**ステップ 2**   ユーザを作成し、このユーザに次の項目を関連付けます。

- ロール (事前定義されたロール、またはカスタム ロール)
- ドメイン

---

この章では、ドメインとユーザの作成方法、およびこのユーザに事前定義されたロールと新規ドメインを関連付ける方法について説明します。事前定義されたロール、およびカスタム ロールの定義方法の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

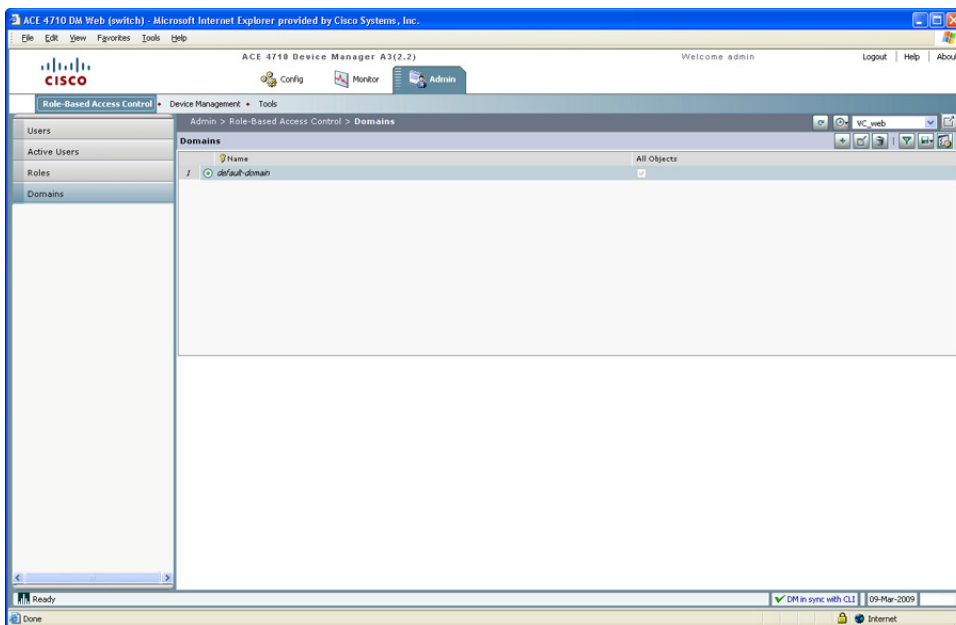
ドメインとユーザの作成には、ACE Device Manager GUI または Command-Line Interface (CLI; コマンドライン インターフェイス) を使用できます。

# Device Manager GUI を使用した RBAC の設定

この手順では、GUI を使用して、第 3 章「仮想コンテキストの作成」で作成したユーザ コンテキストを含むドメインを作成してから、これらのサーバを管理するためのサーバ保守ユーザ user1 を作成します。次のステップに従って、GUI を使用し、この RBAC セットアップを行います。

- ステップ 1 [VC\_web] を選択します。
- ステップ 2 [Admin] > [Role-Based Access Control] > [Domains] を選択します。[Domains] ペインが表示されます (図 5-1)。

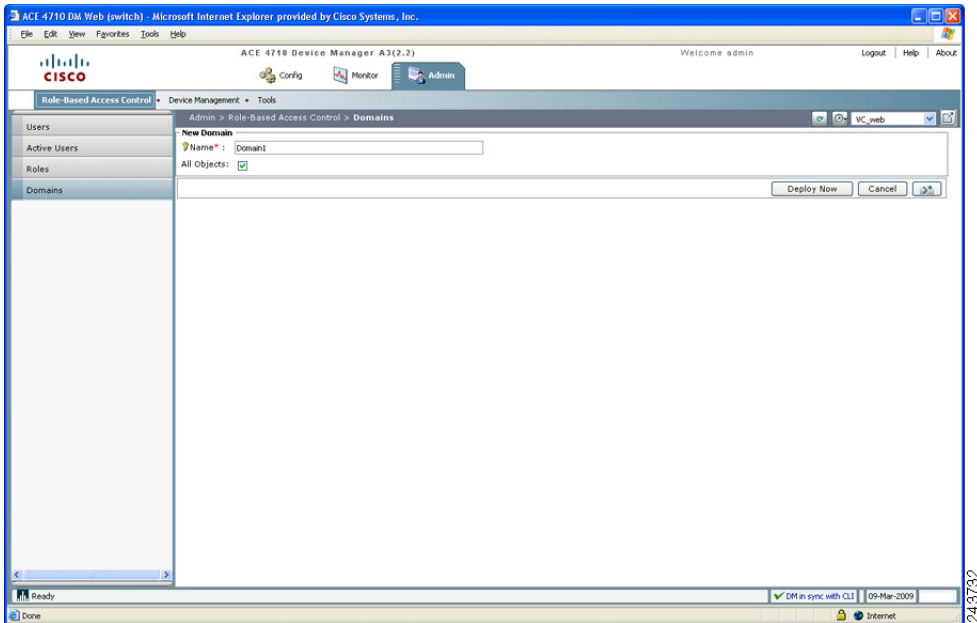
図 5-1 [Domains] ペイン



## ■ Device Manager GUI を使用した RBAC の設定

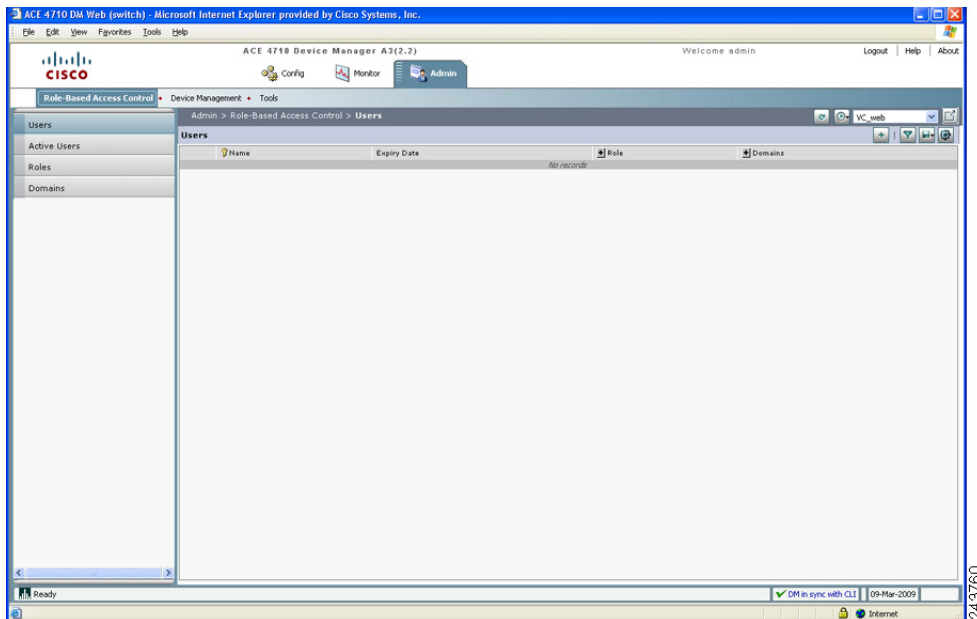
- ステップ 3** [Add] をクリックして新しいドメインを追加します。新しい [Domain] ウィンドウが表示されます (図 5-2)。

図 5-2 [Domains] ウィンドウ



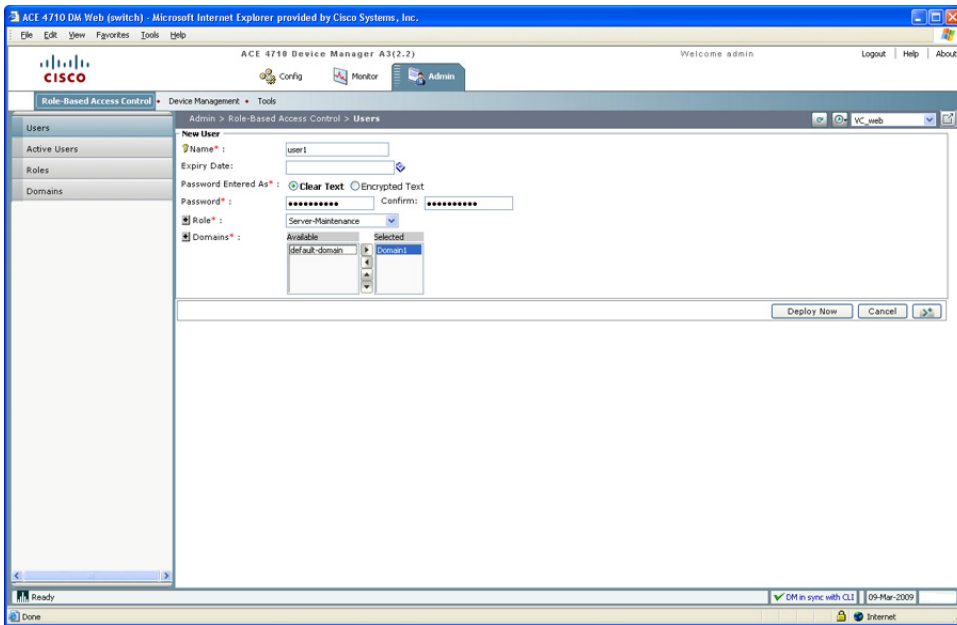
- ステップ 4** [Name] に「Domain1」と入力します。
- ステップ 5** [All Objects] チェックボックスをオンにします。
- ステップ 6** [Deploy Now] をクリックします。コンテキスト VC\_web にすべてのオブジェクトを含むドメインが作成されます。
- ステップ 7** ユーザを作成するために、[Role-Based Access Control] > [Users] を選択します。[Users] ペインが表示されます (図 5-3)。

図 5-3 [Users] ペイン



**ステップ 8** [Add] をクリックします。[Users] ウィンドウが表示されます (図 5-4)。

図 5-4 [Users] ウィンドウ

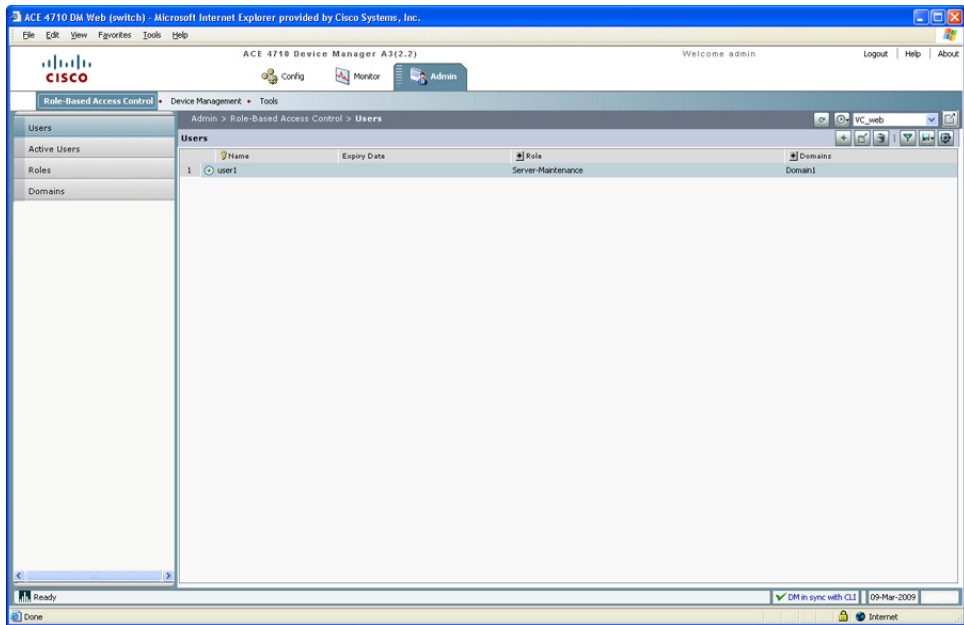


243761

- ステップ 9** 次のユーザ アトリビュートを入力します。残りのアトリビュートは空白、またはデフォルト値のままにしておきます。
- [Name] : user1
  - [Password] : MYPASSWORD
  - [Confirm] : MYPASSWORD
  - [Role] : Server-Maintenance
- ステップ 10** [Domain1] を選択し、右矢印ボタンをクリックします。Domain1 が [Available] リストから [Selected] リストに移動されます。
- ステップ 11** [default-domain] を選択し、左矢印ボタンをクリックします。default-domain が [Selected] リストから削除されます。
- ステップ 12** [Deploy Now] をクリックして、新しいユーザ user1 にロール Server-Maintenance とドメイン Domain1 を関連付けます。この新しいユーザが [Users] ペインに追加されます (図 5-5)。



図 5-5 user1 が追加された [Users] ペイン



243759

## CLI を使用した RBAC の設定

次のステップに従って、CLI を使用し、RBAC を設定します。

- ステップ 1** CLI プロンプトをチェックし、目的のコンテキストで操作が行われていることを確認します。必要に応じて、正しいコンテキストに変更します。

```
host1/Admin# changeto VC_web  
host1/VC_web#
```

- ステップ 2** 設定モードに入ります。

```
host1/VC_web# Config  
host1/VC_web(config)#
```

## ■ CLI を使用した RBAC の設定

**ステップ 3** このコンテキストに対応したドメインを作成します。

```
host1/VC_web(config)# domain Domain1
host1/VC_web(config-domain)#
```

**ステップ 4** VC\_web コンテキストのオブジェクトをすべて、このドメインに割り当てます。

```
host1/VC_web(config-domain)# add-object all
host1/VC_web(config-domain)# exit
host1/VC_web(config)#
```

**ステップ 5** 新しいユーザ `user1` を設定し、このユーザに、定義済みロール `TECHNICIAN` とドメイン `Domain1` を割り当てます。

```
host1/VC_web(config)# username user1 password 5 MYPASSWORD role
TECHNICIAN domain Domain1
```



**(注)** パスワードに対するパラメータ `5` は、MD5 ハッシュ強化暗号化パスワードに対するパラメータです。クリア テキスト パスワードの場合は `0` を使用します。

```
host1/VC_web(config)# exit
```

**ステップ 6** ユーザおよびドメインの設定を表示します。

```
host1/VC_web# show running-config role
host1/VC_web# show running-config domain
```

---

この章では、ネットワークのサブセットで限定された機能を実行するためのユーザを作成しました。次に、サーバ ロード バランシングのための仮想サーバを作成します。