CHAPTER 15

ACE アプライアンスの管理

ここでは、ACE アプライアンス Device Manager を使用して ACE アプライアンスを管理する方法について説明します。

ACE アプライアンス Device Manager にログインする方法の詳細については、「ACE アプライアンス Device Manager へのログイン」（P.1-4）を参照してください。

（注） ACE CLI を使用して名前付きオブジェクト（実サーバ、仮想サーバ、パラメータ マップ、クラス マップ、ヘルス プローブなど）を設定するとき、Device Manager（DM）でサポートされるのは、1 ～ 64 文字の英数字文字列を使用したオブジェクト名であることに注意してください。オブジェクト名には、下線（_）、ハイフン（-）、ドット（.）、およびアスタリスク（*）の特殊文字を含めることができます。スペースは使用できません。

ACE CLI を使用して、DM でサポートされていない特殊文字を含んだ名前付きオブジェクトを設定した場合、DM を使用して ACE を設定できない場合があります。

Admin 機能の概要

[Admin] タブでは、ロールベース アクセス コントロールの管理、ACE アプライアンスの統計情報データの設定および表示を実行したり、ACE アプライアンス Device Manager のトラブルシューティング ツールを使用したりできます。

（注） 一部の Admin オプションは一部のユーザに対して表示されない場合があります。ログインに割り当てられたロールによって、使用可能なオプションが決まります。

表 15-1 で、[Admin] をクリックしたときに表示されるオプションについて説明します。

表 15-1　[Admin] メニュー オプション

メニュー	オプション	説明	参照先
Role-Based Access Control	Users	ユーザとそれらのコンテキストへのアクセスを管理します。	「ユーザの管理」（P.15-7）を参照してください。
	Active Users	アクティブなユーザのセッションを表示または終了します。	「現在のユーザ セッションの表示」（P.15-12）または「アクティブ ユーザ セッションの終了」（P.15-13）を参照してください。
	Roles	コマンドおよびリソースへのユーザのアクセスを管理します。	「ユーザ ロールの管理」（P.15-14）を参照してください。
	Domains	選択されたコンテキスト ユーザのグループと、選択されたコンテキスト オブジェクトのグループとのアソシエーションを管理します。	「ドメインの管理」（P.15-32）を参照してください。
Device Management		ACE アプライアンス Device Manager のステータスをチェックします。	「ACE アプライアンス統計情報のモニタリング」（P.15-36）を参照してください。
Tools		Cisco サポート ラインに問題を報告して診断パッケージを生成し、ACE アプライアンスから表示または追跡するファイルにアクセスして、すべての仮想コンテキスト設定を ACE アプライアンス からの CLI 設定で置き換えます。	「ACE アプライアンス Device Manager トラブルシューティング ツールの使用」（P.16-1）を参照してください。

関連トピック

- 「ACE アプライアンスの管理」（P.15-1）
- 「Cisco ACE アプライアンスへのアクセスの制御」（P.15-3）

Cisco ACE アプライアンスへのアクセスの制御

ACE アプライアンス Device Manager へのアクセスは、ACE アプライアンスにアクセスする場合と同じユーザ名およびパスワードを使用して制御されます。これにより、ローカル データベース、または外部 RADIUS、TACACS+、または LDAP サーバに対する認証が可能になります。ローカル データベースではなく AAA を使用した認証を選択した場合は、CLI を使用して AAA を設定する必要があります。AAA サーバを使用したリモート認証の設定方法の詳細については、『*Security Guide, Cisco ACE Application Control Engine*』を参照してください。

（注）

ACE は、ACE 上のローカル データベースを使用したローカル ユーザの認証、または 1 つ以上の AAA サーバを使用するリモート認証を通じたローカル ユーザの認証をサポートします。AAA リモート サーバは TACACS+、RADIUS、LDAP で分かれる独立したグループにまとめられます。認証によって、有効なユーザ名とパスワードの指定を要求することで、ACE へのユーザ アクセスを制御できます。認証を使用しないと、パスワードは検証されません。CLI から、ユーザ認証およびアカウンティング機能をサポートするように ACE アプライアンスを設定すると、Device Manager は、指定したリモート サーバによって実行されるタスクをサポートします。認証およびアカウンティングの詳細については、『*Security Guide, Cisco ACE Application Control Engine*』を参照してください。

また、リモート サーバ上でユーザに関連付けられたロールとドメインも Device Manager によってサポートされます。

ACE アプライアンス Device Manager は、AAA を設定しません。代わりに、機能へのアクセスに関してロールベース アクセス コントロールを使用します。ユーザがシステムにログインすると、ユーザが実行可能な特定のタスクと使用可能なシステムの領域は、*コンテキスト*、*ロール*、および *ドメイン*によって制御されます。ユーザのアクセスを制限する必要がある場合は、最初にロールとドメインのペアを割り当てる必要があります。

ユーザに割り当てられたロールによって、ユーザが実行可能なタスクと、階層内で表示可能な項目が定義されます。ロールは、事前に定義されるか、システム管理者によって設定されます。各ロール、ユーザ、およびドメインは、コンテキストに関連付けられます。管理コンテキストに関連付けられたロールとドメインだけが、その他のコンテキストを表示できます。詳細については、「ロールについて」（P.15-5）を参照してください。

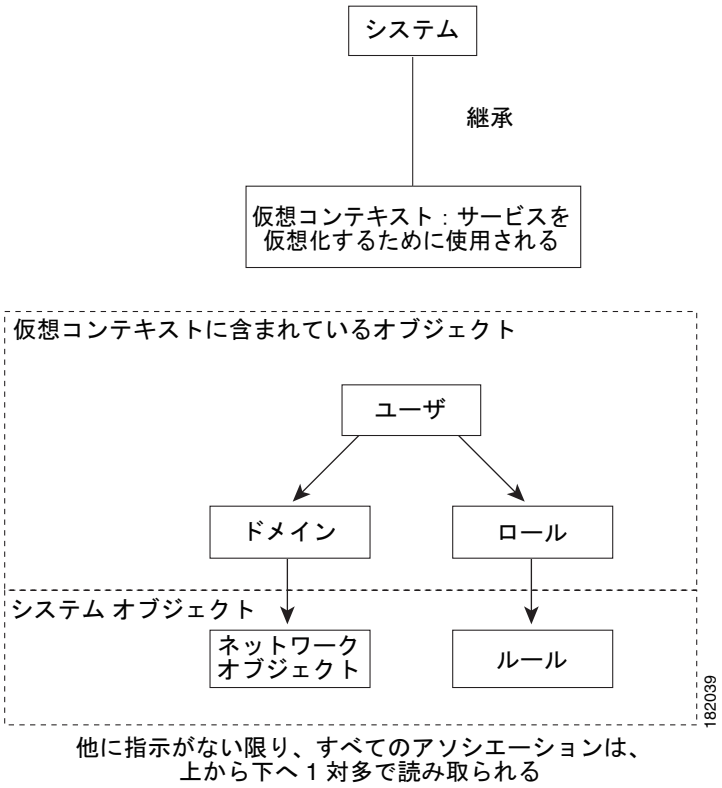
ドメインは、管理対象オブジェクトの集合です。ユーザにドメインへのアクセス権が付与されている場合、ドメインは、仮想コンテキストとして表示されるネットワーク上のオブジェクトのサブセットのフィルタとして動作します。ドメインによって制御されるシステム内のオブジェクトのタイプは、次のとおりです。

- 次に一覧表示されたすべてのオブジェクト
- Access list - Ethertype
- Access list - Extended
- Class-map
- Interface VLAN
- Interface BVI
- Parameter-map
- Policy-map
- Probe
- Real server
- Script

- Server Farm
- Sticky

したがって、ロールベース アクセス コントロールは、ユーザが、アクセス権の付与されているドメインに含まれるデバイスまたはサービスだけを表示でき、処理だけを実行できるように保証します。

図 15-1　ロールベース アクセス コントロールの包含の概要



次に、ロールベース アクセス コントロールの包含の例を示します。

ドメイン		
東海岸のサーバ	中央のサーバ	西海岸のサーバ
ロール		
Web サーバ管理者		
ユーザ		
ユーザ A	ユーザ B	ユーザ C
（注） 各アソシエーションは、1 対多です。		

設定、モニタリング、管理などのその他のすべてのユーザ インターフェイスが、次のロールベース アクセス コントロール ポリシーに準じます。

- ロールは、ユーザが表示できる画面（または、それらの画面上の機能）を制限します。
- ドメインは、ロールによって許可された画面上に一覧表示されるオブジェクトを制限します。
- ユーザ（管理者以外）は、割り当てられているドメインのサブドメインだけを作成できます。ただし、親 / 子関係は、ドメイン間で保持されません。

- システム管理者ユーザ（Admin）は、すべてのオブジェクトを表示および修正できます。他のすべてのユーザは、図 15-1 に示すロールベース アクセス コントロールに準じます。

関連トピック

- 「ユーザのタイプ」（P.15-5）
- 「ロールについて」（P.15-5）
- 「操作権限について」（P.15-6）
- 「ドメインについて」（P.15-7）
- 「ユーザの管理」（P.15-7）

ユーザのタイプ

2 つのタイプのユーザが ACE アプライアンスを設定および監視します。

- デフォルト ユーザ : ACE アプライアンスがインストールされているデータセンターまたは IT 部門に関連付けられた個人。デフォルトの管理アカウント（ユーザ ID **admin**）は、システムに事前に設定されたシステム ユーザ アカウントです。admin ユーザ パスワードは、システムがインストールされたときに事前に設定されます。admin ユーザ パスワードは、ユーザ パスワードと同じ方法で変更できます（「ユーザの管理」（P.15-7）を参照）。

  事前定義されたシステム ロールは、ロール、ドメイン、および操作の権限の観点から見て指定されています。1 つのコンテキスト内では、各ロールは特定の操作およびドメインのセットと一緒に動作します。

- 割り当てられたユーザ : ACE アプライアンスへのアクセス権を付与する対象であるユーザ。ロールおよび所属するドメインを選択することで、ユーザに制限付きのアクセス権を割り当てることができます。ユーザは、他のコンテキストへの変更は許可されておらず、作成されたコンテキスト内で特定の操作およびドメインのセットで動作できます。

関連トピック

- 「ユーザの管理」（P.15-7）
- 「ユーザの管理上の注意事項」（P.15-8）
- 「ユーザのリストの表示」（P.15-8）
- 「ユーザ アカウントの作成」（P.15-9）

ロールについて

ユーザ ロールによって、ユーザが保持する権限、アクセス可能な機能、特定のコンテキストで実行可能な処理が決まります。

Cisco ACE アプライアンスには、事前定義されたロールのセットがあります（表 15-2（P.15-9）を参照）。また、システム管理者は追加のロールを定義できます。ロールは、ルールとして知られている、リソース タイプと操作の権限の観点から指定されます。ロールごとに、ルールは、ロールが作業可能なリソース タイプと、各リソース タイプに対してロールが実行可能な操作について権限を提供します。

各ユーザは 1 つのロールに割り当てられ（Network-Monitor がデフォルト）、そのロールに割り当てられたルールごとに指定されている操作権限を継承します。複数のユーザが、1 つのロールに割り当てられます。他の割り当てられたロールとは無関係に、ロールごとに異なるアクセス権限（ルールの形式で）を持つことができます。

メニューでユーザに対して表示されるオプションは、ユーザのロールに従ってフィルタされます。

（注）　ユーザのアクセスを制限するには、ロールとドメインの組み合わせを割り当てる必要があります。ロール / ドメイン ペアを割り当てないと、ユーザがどのロールを持っているかに関係なく、ユーザはどの特定のリソースにもアクセスできず、システムに対して権限がない場合と同じ状態になります。

すべてのユーザが、コンテキスト、ロール、およびドメインの組み合わせによって厳密に制限されます。たとえば、ユーザは、上位の権限またはアクセス権を持つ別のユーザや、ドメイン外部の別のユーザを作成することはできません。

ユーザによって現在参照されているロールは、削除できません。事前定義されたロールは、変更または削除できません。

関連トピック

- 「ユーザ ロールの管理上の注意事項」（P.15-15）
- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）
- 「ユーザ ロールの表示」（P.15-29）
- 「ユーザ ロールの作成」（P.15-29）
- 「ユーザ ロールの修正」（P.15-31）
- 「ユーザ ロールの削除」（P.15-31）

操作権限について

操作権限は、指定されたコンテキストでユーザが何を実行できるかを定義します。2 つのアクセス レベルがあります。第 1 レベルは、許可または拒否アクセス権です。第 2 レベルは、ユーザによる実行を許可または拒否する操作権限です。たとえば、ACE アプライアンスの各機能には割り当てられた権限があります。ユーザの権限が不十分な場合は、その機能は使用できません。最低の権限レベルから最高の権限レベルまでで、次の操作権限を許可または拒否することができます。

- 監視：ユーザに統計情報の表示とパラメータ収集の指定を許可します。
- 修正：ユーザに、設定などの、システム オブジェクトに関連付けられた永続的な情報の変更を許可します。
- デバッグ：ユーザに既存の問題に関する情報の収集を許可します。
- 作成：ユーザに、システム オブジェクトの制御、たとえば、システム オブジェクトの作成、有効化、起動などを許可します。また、削除権限も持ちます。

権限は階層型です。ユーザが修正権限を持つ場合は、監視権限も持っています。ユーザが作成権限またはデバッグ権限を持つ場合は、修正権限も持っています。Admin だけが、リソース クラス管理アクセス権を持っています。

（注）　作成機能には、自動的に修正機能が含まれますが、逆は当てはまりません（修正権限を持つユーザは、自動的に項目を作成できるようにはなりません）。

関連トピック

- 「ユーザ ロールの管理上の注意事項」（P.15-15）
- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）
- 「ユーザ ロールの管理」（P.15-14）

ドメインについて

Cisco ACE アプライアンス には、すべてのオブジェクトを含む、事前定義されたデフォルトのドメインがあります。事前定義されたドメインは修正または削除できません。システム管理者は追加のドメインを定義できます。ドメインは、ユーザにアクセス権を付与する管理対象オブジェクトの集合です。カスタマイズしたドメインを設定することで、ネットワーク上のオブジェクトのサブセットをフィルタできます。その後、ユーザに、このドメインへのアクセス権を付与します。

たとえば、ユーザは、アクセス権を持つドメインに含まれるものだけを表示できます（行のフィルタリングによって実現されます）。デフォルトのドメインに 50 のオブジェクトが含まれ、カスタマイズしたドメイン dom1 が Rserver rs1、Rserver rs2、Serverfarm sf1、Serverfarm sf2、および Accesslist extended acl1 のドメイン オブジェクトから構成される場合、ドメイン dom1 に関連付けられたユーザは、コンテキスト全体の中で、これらの 5 つのオブジェクトだけを表示できます。

任意のテーブルでユーザに対して表示される行は、そのユーザがアクセス権を持つドメインに従ってフィルタされます。

（注） ユーザのアクセスを制限するには、ロールとドメインの組み合わせを割り当てる必要があります。ロール/ドメイン ペアを割り当てないと、ユーザがどのロールを持っているかに関係なく、ユーザはどの特定のリソースにもアクセスできず、システムに対して権限がない場合と同じ状態になります。

関連トピック

- 「ドメインの管理」（P.15-32）
- 「ドメインの管理上の注意事項」（P.15-33）

ユーザの管理

システムへのログインを許可するユーザを指定するには、ロールベース アクセス コントロール機能を使用します。ここでは、ユーザ アカウントを管理する方法について説明します。

- 「ユーザの管理上の注意事項」（P.15-8）
- 「ユーザのリストの表示」（P.15-8）
- 「ユーザ アカウントの作成」（P.15-9）
- 「ユーザ アカウントの修正」（P.15-11）
- 「ユーザ アカウントの削除」（P.15-11）
- 「現在のユーザ セッションの表示」（P.15-12）

（注） ACE は、ACE 上のローカル データベースを使用したローカル ユーザの認証、または 1 つ以上の AAA サーバを使用するリモート認証を通じたローカル ユーザの認証をサポートします。AAA リモート サーバは TACACS+、RADIUS、LDAP で分かれる独立したグループにまとめられます。認証によって、有効なユーザ名とパスワードの指定を要求することで、ACE へのユーザ アクセスを制御できます。認証を使用しないと、パスワードは検証されません。CLI から、ユーザ認証およびアカウンティング機能をサポートするように ACE アプライアンスを設定すると、Device Manager は、指定したリモート サーバによって実行されるタスクをサポートします。認証およびアカウンティングの詳細については、『*Security Guide, Cisco ACE Application Control Engine*』を参照してください。

また、リモート サーバ上でユーザに関連付けられたロールとドメインも Device Manager によってサポートされます。

ユーザの管理上の注意事項

- 管理コンテキストで作成されたユーザの場合、デフォルトのアクセス スコープは ACE 全体になります。
- 新規ユーザにロールを割り当てない場合、デフォルトのユーザ ロールは Network-Monitor です。その他のコンテキストで作成したユーザは、コンテキスト全体がアクセスのデフォルト スコープとなります。
- ユーザは、ドメインとユーザ ロールに関連付けられるまでログインできません。
- 既存のユーザに関連付けられているロールとドメインは削除できません。

ユーザのリストの表示

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Users] を選択します。次のフィールドを持つ [Users] テーブルが表示されます。

- Name
- Expiry Date
- Role
- Domains

ステップ 2　この画面のオプションを使用して、新規ユーザを作成したり、アクセス権を持つ既存のユーザを修正または削除したりすることができます（表 15-2 を参照）。

関連トピック

- 「ユーザ アカウントの作成」（P.15-9）
- 「ユーザ アカウントの削除」（P.15-11）
- 「ユーザの管理」（P.15-7）
- 「ユーザの管理上の注意事項」（P.15-8）

ユーザ アカウントの作成

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Users] を選択します。[Users] テーブルにユーザのリストが表示されます。

ステップ 2　[Add] をクリックします。

ステップ 3　次の必須フィールドを埋めます（特に注記がないかぎり）。

表 15-2　ユーザ属性

フィールド	説明
Name	システム内でユーザを識別するための名前を指定します（最大 24 文字）。文字、数字、および下線だけを使用できます。フィールドは、大文字と小文字を区別します。
Expiry Date[1]	ユーザ名がシステム内で使用可能な日付
Password Entered As	パスワードをクリア テキストとして入力するか、または暗号化するかを指定します。
Password	このユーザ アカウントのパスワードを指定できます。パスワードは、8 文字以上にする必要があります。
Confirm	パスワードが正しく入力されたことを確認します。

表 15-2　ユーザ属性 （続き）

フィールド	説明
Role	ユーザがこのシステム内で何を実行できるかを定義します。次のオプションから選択するか、専用のロールを作成します。 • Admin • Network-Admin • Network-Monitor • Security-Admin • Server-Appln-Maintenance • Server-Maintenance • SLB-Admin • SSL-Admin （注）　SSL-Admin ロールは ACE NPE ソフトウェア バージョンでは使用できません（「ACE No Payload Encryption ソフトウェア バージョン関する情報」（P.1-2）を参照）。 （注）　ユーザのアクセスを制限するには、ロールとドメインの組み合わせを割り当てる必要があります。 事前に定義されたロールの詳細については、表 15-4（P.15-16）を参照してください。
Domains	ネットワーク内のデバイスとそれらのコンポーネント（物理および論理）を編成する手段

1. 不要。

ステップ 4　この設定を展開するには、[Deploy Now] をクリックします。[Users] テーブルが再度表示されます。

ステップ 5　別のユーザを追加するには、[Add Another] をクリックします。

関連トピック

- 「ユーザ アカウントの修正」（P.15-11）
- 「ユーザ アカウントの削除」（P.15-11）
- 「ユーザのリストの表示」（P.15-8）
- 「ユーザの管理」（P.15-7）
- 「ユーザの管理上の注意事項」（P.15-8）

ユーザ アカウントの修正

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Users] を選択します。[Users] テーブルが表示されます。

ステップ 2　修正するユーザ アカウントを選択します。

ステップ 3　[Edit] をクリックします。

ステップ 4　[User details] 画面が表示されます。変更を加え（表 15-2 を参照）、[Deploy Now] をクリックします。

その後、[Users] テーブルが表示されます。

関連トピック

- 「ユーザ アカウントの作成」（P.15-9）
- 「ユーザ アカウントの削除」（P.15-11）
- 「ユーザのリストの表示」（P.15-8）
- 「ユーザの管理」（P.15-7）
- 「ユーザの管理上の注意事項」（P.15-8）

ユーザ アカウントの削除

次の手順で、ユーザを削除できます。また、[Active Users] ウィンドウからユーザを削除することもできます。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Users] を選択します。ユーザ、ロール、ドメイン、およびその他のユーザ情報を示す [Users] テーブルが表示されます。

ステップ 2　削除するユーザ アカウントを選択します。

ステップ 3　[Delete] をクリックします。

削除の確認を求めるウィンドウが表示されます。

ステップ 4　ユーザ アカウントを削除するには、[OK] をクリックします。または、ユーザを削除せずに手順を終了するには、[Cancel] をクリックします。[OK] をクリックすると、ウィンドウは [Users] テーブルとともにリフレッシュされ、削除したユーザ アカウントの表示は消えます。

関連トピック

- 「ユーザ アカウントの作成」（P.15-9）
- 「ユーザ アカウントの修正」（P.15-11）
- 「ユーザのリストの表示」（P.15-8）
- 「ユーザの管理」（P.15-7）
- 「ユーザの管理上の注意事項」（P.15-8）

現在のユーザ セッションの表示

現在、システムにログインしているユーザのリストを表示し、必要に応じてそれらのセッションを終了できます。

使用可能なドメイン内のユーザだけを表示できます。

（注） ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Active Users] を選択します。

[Active User Sessions] 画面に、ログインしている各アクティブ ユーザに関する次の情報が表示されます。

表 15-3　[Active User Session] 画面の情報

カラム	説明
Name	ACE appliance Device Manager へのログインに使用される名前
Type of Login	ログインに使用する方式。たとえば、WEB または CLI
Login From IP	ホストの IP アドレス
Time Of Login	ユーザがログインした時間

ステップ 2　アクティブな Web セッションを終了するには、[Terminate] をクリックします（詳細については、「アクティブ ユーザ セッションの終了」（P.15-13）を参照してください）。CLI ユーザ セッションは終了できません。

関連トピック

- 「アクティブ ユーザの削除」（P.15-13）
- 「アクティブ ユーザ セッションの終了」（P.15-13）
- 「ユーザのリストの表示」（P.15-8）
- 「ユーザの管理」（P.15-7）
- 「ユーザの管理上の注意事項」（P.15-8）

アクティブ ユーザの削除

次の手順で、ユーザを削除できます。[Admin] > [Role-Based Access Control] > [Users] メニューを使用して、ユーザを削除することもできます。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Active Users] を選択します。

ステップ 2　削除するユーザ アカウントを含むテーブルの行を選択します。

ステップ 3　[Delete] をクリックします。

選択したユーザが、ACE アプライアンス Device Manager から削除されます。

関連トピック

- 「現在のユーザ セッションの表示」（P.15-12）
- 「アクティブ ユーザ セッションの終了」（P.15-13）
- 「ユーザの管理」（P.15-7）

アクティブ ユーザ セッションの終了

ユーザ セッションを終了すると、そのユーザは、ユーザ セッションを開始したインターフェイスからログアウトされます。ユーザが設定に変更を加えている場合は、設定のロックが解除され、確定されていない設定の変更は廃棄されます。

操作の進行中にユーザ セッションを終了すると、現在の操作は停止されませんが、以降の操作は拒否されます。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Active Users] を選択します。

ステップ 2　終了するユーザ セッションを含むテーブルの行を選択します。

ステップ 3　[Terminate] をクリックします。

選択したユーザは、強制的にシステムからログアウトされます。

関連トピック

- 「現在のユーザ セッションの表示」（P.15-12）
- 「アクティブ ユーザの削除」（P.15-13）
- 「ユーザの管理」（P.15-7）
- 「Cisco ACE アプライアンスへのアクセスの制御」（P.15-3）

ユーザ パスワードの変更

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Users] を選択します。ユーザのテーブルが表示されます。

ステップ 2　修正するユーザ アカウントを選択します。

ステップ 3　[Edit] をクリックします。

ステップ 4　属性テーブルでパスワード属性を変更します（表 15-2 を参照）。

ステップ 5　[Deploy Now] をクリックして、この設定を展開し、[Users] テーブルに戻ります。

関連トピック

- 「ユーザの管理」（P.15-7）
- 「Admin パスワードの変更」（P.15-14）

Admin パスワードの変更

各 ACE アプライアンス では、デバイスに admin ユーザ アカウントが組み込まれています。ルート ユーザ ID は **admin** で、パスワードはシステムのインストール時に設定されます。Admin パスワードの変更方法の詳細については、「アカウント パスワードの変更」（P.1-6）を参照してください。

ユーザ ロールの管理

ユーザ定義のロールを追加、修正、および削除するには、ロール機能を使用します。事前定義されたロールは、背景付きの灰色の斜体テキストで表示され、削除または修正できません。

ユーザのロールによって、ユーザがアクセス可能なタスクが決まります。各ロールは、このロールにどの機能へのアクセスが含まれるかを定義するアクセス権またはルールに関連付けられます。

ここでは、ユーザ ロールを管理する方法について説明します。

- 「ユーザ ロールの管理上の注意事項」（P.15-15）
- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）
- 「仮想サーバに関連する RBAC ユーザ ロール要件」（P.15-27）
- 「ユーザ ロールの表示」（P.15-29）

ユーザ ロールの管理上の注意事項

ロールを管理する際は、次の注意事項を留意してください。

- 管理者は、すべてのロールを表示および修正できます。
- その他のユーザは、そのユーザに割り当てられたロールだけを表示できます。
- デフォルトのロールは変更できません。
- ロールのアクセス権は、管理コンテキストで作成されたか、管理コンテキスト以外のコンテキストまたはユーザ コンテキストで作成されたかによって異なります。ユーザにコンテキスト間の切り替えを許可する場合は、そのユーザが事前定義されたロールを持っていることを確認してください。ユーザをホーム コンテキストだけに制限する場合は、そのユーザにカスタマイズしたユーザ ロールを割り当てます。
- デフォルトのロールだけが使用できる特定のロール機能があります。たとえば、管理コンテキストの Admin ロールは **changeto** および **system** アクセス権を持ち、ライセンス管理、リソース クラス管理、HA セットアップなどのタスクを実行できます。ユーザが作成したロールは、これらの機能を使用できません。

事前定義されたロールについて

表 15-4 に、事前定義されたロールとそれらの権限を定義しています。この表には、管理コンテキストとユーザ コンテキスト（管理コンテキスト以外のコンテキスト）でのルールの違いについても記載されています。ロールベース アクセス コントロールの詳細については、『*Virtualization Guide, Cisco ACE Application Control Engine*』を参照してください。事前定義されたロールを ACE アプライアンス Device Manager タスクおよび機能にマッピングする方法の詳細については、表 15-5 を参照してください。

changeto コマンド（ユーザが他のコンテキストに切り替えることができる）を使用するには、管理コンテキストの事前定義されたロールのうち 1 つを保持している必要があります。admin 以外のコンテキストまたはユーザ コンテキストは、**changeto** コマンドへのアクセス権を持っていません。それらは、ホーム コンテキストだけにアクセスできます。複数のコンテキストへのアクセス権を持つコンテキスト管理者は、アクセス権を持つ他のコンテキストに明示的にログインする必要があります。

表 15-4　管理コンテキストおよびユーザ コンテキストの事前定義されたロール ルール

事前定義されたロール / コンテキスト	説明	操作	機能
Admin ロール			
管理コンテキスト	管理コンテキストで作成された場合、ユーザは、すべてのコンテキストに完全にアクセスでき、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。	• デバッグ • 作成 • 修正 • 監視	• すべて（コンテキスト サービス設定） • ユーザ アクセス（ロール、ドメイン、およびユーザ） • システム（コンテキスト管理） • **changeto** コマンド（すべてのコンテキストへのアクセス） • **exec** コマンド（すべてのデフォルト カスタム ロール コマンドをイネーブル化）
ユーザ コンテキスト	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。	作成	• すべて • ユーザ アクセス
Network-Admin ロール			
管理コンテキスト	L3（IP およびルート）および L4 VIP の Admin	作成	• 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 • 設定のコピー[1] • **changeto** コマンド • **exec** コマンド
ユーザ コンテキスト	L3（IP およびルート）および L4 VIP へのアクセス	作成	• 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 • 設定のコピー[1]
Network-Monitor ロール			
管理コンテキスト	すべての機能のモニタリング	監視	• すべての **show** コマンド • **changeto** コマンド • **exec** コマンド
ユーザ コンテキスト	すべての機能のモニタリング	監視	• すべての **show** コマンド

表 15-4　管理コンテキストおよびユーザ コンテキストの事前定義されたロール ルール （続き）

事前定義されたロール/コンテキスト	説明	操作	機能
Security-Admin ロール			
管理コンテキスト	セキュリティ機能	作成	• アクセス コントロール リスト（ACL） • アプリケーション インスペクション • 接続パラメータ • 認証、許可、アカウンティング（AAA） • NAT • 設定のコピー[1] • **changeto** コマンド • **exec** コマンド
		修正	インターフェイス
ユーザ コンテキスト	セキュリティ機能	作成	• アクセス コントロール リスト（ACL） • アプリケーション インスペクション • 接続パラメータ • 認証、許可、アカウンティング（AAA） • NAT • 設定のコピー[1]
		修正	インターフェイス
Server-Appln-Maintenance ロール			
管理コンテキスト	サーバ メンテナンスおよび L7 ポリシー アプリケーション	作成	• 実サーバ • サーバ ファーム • ロード バランシング • 設定のコピー[1] • 実サーバ稼働中 • **changeto** コマンド • **exec** コマンド
ユーザ コンテキスト	サーバ メンテナンスおよび L7 ポリシー アプリケーション	作成	• 実サーバ • サーバ ファーム • ロード バランシング • 設定のコピー[1] • 実サーバ稼働中

表 15-4　管理コンテキストおよびユーザ コンテキストの事前定義されたロール ルール （続き）

事前定義されたロール / コンテキスト	説明	操作	機能
Server-Maintenance ロール			
管理コンテキスト	サーバ メンテナンス、モニタリング、およびデバッグ	デバッグ	• サーバ ファーム • VIP • プローブ • ロード バランシング
		作成	• **changeto** コマンド • **exec** コマンド
		修正	• 実サーバ • 実サーバ稼働中
ユーザ コンテキスト	サーバ メンテナンス、モニタリング、およびデバッグ	デバッグ	• サーバ ファーム • VIP • プローブ • ロード バランシング
		修正	• 実サーバ • 実サーバ稼働中
SLB-Admin ロール			
管理コンテキスト	ロードバランシング機能	作成	• 実サーバ • サーバ ファーム • VIP • プローブ • ロードバランス • NAT • 設定のコピー[1] • 実サーバ稼働中 • **changeto** コマンド • **exec** コマンド
		修正	インターフェイス

表 15-4　管理コンテキストおよびユーザ コンテキストの事前定義されたロール ルール （続き）

事前定義されたロール/コンテキスト	説明	操作	機能
ユーザ コンテキスト	ロードバランシング機能	作成	• 実サーバ • サーバ ファーム • VIP • プローブ • ロードバランス • NAT • 設定のコピー[1] • 実サーバ稼働中
		修正	インターフェイス
SSL-Admin ロール			
管理コンテキスト	SSL 機能	作成	• SSL • PKI • 設定のコピー[1] • **changeto** コマンド • **exec** コマンド
		修正	インターフェイス
ユーザ コンテキスト	SSL 機能	作成	• SSL • PKI • 設定のコピー[1]
		修正	インターフェイス

1. **copy** コマンドの説明については、『*Command Reference, Cisco ACE Application Control Engine*』を参照してください。

関連トピック

- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）
- 「Cisco ACE アプライアンスへのアクセスの制御」（P.15-3）
- 「ユーザの管理」（P.15-7）
- 「ユーザ ロールの管理」（P.15-14）
- 「ドメインの管理」（P.15-32）

ACE アプライアンス Device Manager でのロール マッピング

ACE アプライアンス Device Manager にログインすると、アクセス権が付与されているタスクが表示されます。表 15-5 で、事前定義されたロール、およびそれらのロールで使用可能なメニュー タスクと機能について説明しています。ロールに適用されない機能とメニューは表示されません。

事前定義されたロールは、必要となることのあるすべてのロール タイプを網羅しているため、それらを使用することを推奨します。専用のロールを定義する場合は、CLI の機能と ACE アプライアンス Device Manager のメニュー タスクが 1 対 1 のマッピングではない点に注意してください。

ユーザ定義のロールに適したルールを定義するには、表 15-4 の機能と ACE アプライアンス Device Manager のメニュー タスクとのマッピングを作成する必要があります。たとえば、仮想サーバを管理するためには、ロールで 6 つのメニュー機能（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、NAT、およびインターフェイス）を選択する必要があります。

（注）　ACE アプライアンス Device Manager の機能には、CLI での対応する機能マッピングがない機能もあります。この機能の 1 例はクラス マップです。これらの機能を修正するには、修正権限を持つ機能を少なくとも 1 つは含む事前定義されたロールを選択する必要があります。

事前定義されたロールおよびそれらのデフォルトの権限の詳細については、表 15-4 を参照してください。

表 15-5　ACE アプライアンス Device Manager でのロール マッピング

メニュー タスク	使用可能な機能
Admin の事前定義されたロール	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[System] > [Syslog]
	[System] > [SNMP]
	[System] > [Global Policies]
	[System] > [Licenses]
	[System] > [Resource Class]
	[System] > [Application Acceleration and Optimization]
	[Load Balancing] > [Virtual Servers]
	[Load Balancing] > [Real Servers]
	[Load Balancing] > [Server Farms]
	[Load Balancing] > [Health Monitoring]
	[Load Balancing] > [Stickiness]
	[Load Balancing] > [Parameter Maps]
	[Load Balancing] > [Secure KAL-AP]
	[SSL] > [Certificates]
	[SSL] > [Keys]
	[SSL] > [Parameter Maps]
	[SSL] > [Chain Group Parameters]
	[SSL] > [CSR Parameters]
	[SSL] > [Proxy Service]
	[SSL] > [Auth Group Parameters]
	[SSL] > [Certificate Revocation Lists (CRL)]
	[Security] > [ACLs]
	[Security] > [Object Groups]

表 15-5　ACE アプライアンス Device Manager でのロール マッピング （続き）

メニュー タスク	使用可能な機能
	[Network] > [Port Channel Interfaces]
	[Network] > [GigabitEthernet Interfaces]
	[Network] > [VLAN Interfaces]
	[Network] > [BVI Interfaces]
	[Network] > [Static Routes]
	[Network] > [Global IP DHCP]
	[High Availability (HA)] > [Setup]
	[HA Tracking And Failure Detection] > [Interfaces]
	[HA Tracking And Failure Detection] > [Hosts]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
	[Expert] > [Action Lists]
[Config] > [Operations]	Real Servers
	Virtual Servers
[Monitor] > [Virtual Contexts]	Load Balancing
	CPU
	Application Acceleration
	Interfaces
	Real Servers
	Statistics Collection
	Probes
	Resource Usage
	ping
[Admin] > [Role-Based Access Control]	Users
	Active Users
	Roles
	Domains
[Admin] > [Device Management]	Statistics
	Statistics Collection
[Admin] > [Tools]	Lifeline Management
	File Browser

表 15-5　ACE アプライアンス Device Manager でのロール マッピング （続き）

メニュー タスク	使用可能な機能
Network-Admin の事前定義されたロール	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[System] > [Global Policies]
	[Load Balancing] > [Parameter Maps]
	[Network] > [VLAN Interface]
	[Network] > [BVI Interfaces]
	[Network] > [Static Routes]
	[Network] > [Global IP DHCP]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
[Config] > [Operations]	Virtual Servers
[Monitor] >	Application Acceleration
	Interfaces
	Real Servers
	Probes
	Resources
	ping
[Admin] > [Tools]	File Browser

表 15-5　ACE アプライアンス Device Manager でのロール マッピング （続き）

メニュー タスク	使用可能な機能
Network-Monitor の事前定義されたロール	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[System] > [Syslog]
	[System] > [Global Policies]
	[Load Balancing] > [Virtual Servers]
	[Load Balancing] > [Real Servers]
	[Load Balancing] > [Server Farms]
	[Load Balancing] > [Health Monitoring]
	[Load Balancing] > [Stickiness]
	[Load Balancing] > [Parameter Maps]
	[Load Balancing] > [Secure KAL-AP]
	[SSL] > [Certificates]
	[SSL] > [Keys]
	[SSL] > [Parameter Map]
	[SSL] > [Chain Group Parameters]
	[SSL] > [CSR Parameters]
	[SSL] > [Proxy Service]
	[SSL] > [Auth Group Parameters]
	[SSL] > [Certificate Revocation Lists (CRL)]
	[Security] > [ACLs]
	[Security] > [Object Groups]
	[Network] > [VLAN Interfaces]
	[Network] > [BVI Interfaces]
	[Network] > [Static Routes]
	[Network] > [Global IP DHCP]
	[HA Tracking And Failure Detection] > [Interfaces]
	[HA Tracking And Failure Detection] > [Hosts]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
	[Expert] > [Action Lists]
[Config] > [Operations]	Real Servers
	Virtual Servers

表 15-5　ACE アプライアンス Device Manager でのロール マッピング （続き）

メニュー タスク	使用可能な機能
[Monitor] >	Load Balancing
	Application Acceleration
	Interfaces
	Real Servers
	Probes
	Resource Usage
	ping
Security-Admin の事前定義されたロール	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[System] > [Global Policies]
	[Load Balancing] > [Parameter Maps]
	[Security] > [ACLs]
	[Security] > [Object Groups]
	[Network] > [VLAN Interfaces]
	[Network] > [BVI Interfaces]
	[Network] > [Global IP DHCP]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
[Monitor] > [Virtual Contexts]	Resource Usage
	ping
[Admin] > [Tools]	File Browser
Server-AppIn-Maintenance の事前定義されたロール	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[Load Balancing] > [Real Servers]
	[Load Balancing] > [Server Farms]
	[Load Balancing] > [Parameter Maps]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
	[Expert] > [Action Lists]
[Config] > [Operations]	Real Servers
[Monitor] > [Virtual Contexts]	Load Balancing
	Real Servers
	Resource Usage
	ping
[Admin] > [Tools]	File Browser

表 15-5　ACE アプライアンス Device Manager でのロール マッピング （続き）

メニュー タスク	使用可能な機能
Server-Maintenance の事前定義されたロール	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[Load Balancing] > [Real Servers]
	[Load Balancing] > [Server Farms]
	[Load Balancing] > [Health Monitoring]
	[Load Balancing] > [Parameter Maps]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
	[Expert] > [Action Lists]
[Config] > [Operations]	Real Servers
	Virtual Servers
[Monitor] > [Virtual Contexts]	Load Balancing
	Real Servers
	Probes
	Resource Usage
	ping
SLB-Admin の事前定義されたロール	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[System] > [Global Policies]
	[Load Balancing] > [Virtual Servers]
	[Load Balancing] > [Real Servers]
	[Load Balancing] > [Server Farms]
	[Load Balancing] > [Health Monitoring]
	[Load Balancing] > [Parameter Maps]
	[Network] > [VLAN Interfaces]
	[Network] > [BVI Interfaces]
	[Network] > [Global IP DHCP]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
	[Expert] > [Action Lists]
[Config] > [Operations]	Real Servers
	Virtual Servers
[Monitor] > [Virtual Contexts]	Load Balancing
	Real Servers
	Probes
	Resource Usage
	ping

表 15-5　ACE アプライアンス Device Manager でのロール マッピング （続き）

メニュー タスク	使用可能な機能
[Admin] > [Tools]	File Browser
SSL-Admin	
[Config] > [Virtual Contexts] >	[System] > [Primary Attributes]
	[System] > [Global Policies]
	[Load Balancing] > [Parameter Maps]
	[SSL] > [Certificates]
	[SSL] > [Keys]
	[SSL] > [Parameter Maps]
	[SSL] > [Chain Group Parameters]
	[SSL] > [CSR Parameters]
	[SSL] > [Proxy Service]
	[SSL] > [Auth Group Parameters]
	[SSL] > [Certificate Revocation Lists (CRL)]
	[Network] > [VLAN Interfaces]
	[Network] > [BVI Interfaces]
	[Network] > [Global IP DHCP]
	[Expert] > [Class Maps]
	[Expert] > [Policy Maps]
[Monitor] > [Virtual Contexts]	Resource Usage
	ping
[Admin] > [Tools]	File Browser

関連トピック

- 「管理コンテキストおよびユーザ コンテキストの事前定義されたロール ルール」
- 「Cisco ACE アプライアンスへのアクセスの制御」（P.15-3）
- 「ユーザ ロールの管理上の注意事項」（P.15-15）
- 「ユーザの管理」（P.15-7）
- 「ユーザ ロールの管理」（P.15-14）
- 「ドメインの管理」（P.15-32）

仮想サーバに関連する RBAC ユーザ ロール要件

仮想サーバの作成、修正、または削除が必要な場合、事前定義された Admin ロールの使用をお勧めします（表 15-4 を参照）。ACE appliance Device Manager から機能する仮想サーバを正常に導入する能力をサポートしているのは、事前定義された Admin ロールだけです。

ユーザがカスタム ロールの割り当てを希望し、仮想サーバを作成、修正、または削除する権限を必要としている場合、管理者はこのユーザに対して、このような仮想サーバ アクティビティの実行に適したロールへの権限を定義する必要があります。

（注）　仮想サーバを構成できるようにするには、ユーザにデフォルト ドメイン（default-domain）を割り当てる必要があります。ドメインはユーザが操作を行う名前空間です。

（注）　カスタマイズされたロールのユーザに ACE Appliance Device Manager から設定と操作変更を実行する場合、config-copy および exec コマンド機能に対する作成操作を許可するルールのロールを設定する必要があります。

仮想サーバを作成、修正、または削除するためにユーザが必要な RBAC 権限の一覧は次のとおりです。

```
-----------------------------------------
 Rule    Type    Permission      Feature
 ----------------------------------------
  1.   Permit    Create                real
  2.   Permit    Create           serverfarm
  3.   Permit    Create                 vip
  4.   Permit    Create               probe
  5.   Permit    Create          loadbalance
  6.   Permit    Create                 nat
  7.   Permit    Create           interface
  8.   Permit    Create          connection
  9.   Permit    Create                 ssl
 10.   Permit    Create                 pki
 11.   Permit    Create              sticky
 12.   Permit    Create             inspect
```

ただし、特定の設定済み仮想サーバはこれらの機能の一部だけをカバーしており、上記の権限をすべて必要としているわけではありませんので注意してください。一般に、ユーザが仮想サーバのすべての要素を設定できるようにするには上記の権限が必要です。

ユーザ ロールの表示

既存のユーザ ロールを表示するには、このオプションを使用します。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Roles] を選択します。定義済みのロールとそれらの設定値のテーブルが表示されます。

ステップ 2　この画面のオプションを使用して、新規ロールの作成、ストリングに基づくロールのフィルタ、またはアクセス権を持つ既存のロールの修正や削除を実行できます。

ステップ 3　ロールに割り当てられたユーザを表示するには、[Admin] > [Role-Based Access Control] > [Users] を選択します。

関連トピック

- 「操作権限について」（P.15-6）
- 「ユーザ ロールの管理」（P.15-14）

ユーザ ロールの作成

新しいユーザ定義のロールを作成できます。新しいロールを作成するときは、新しいロールの名前と説明を指定し、その後、各タスクの操作権限を選択します。また、このロールは 1 人以上のユーザに割り当てることができます。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Roles] を選択します。定義済みのロールとそれらの設定値のテーブルが表示されます。

ステップ 2　[Add] をクリックします。[New Role] 設定画面が表示されます。

ステップ 3　次の属性を入力します。

表 15-6　ロールの属性

属性	説明
Name	ロールの名前
Description	ロールの簡単な説明

ステップ 4　この設定を展開するには、[Deploy Now] をクリックします。新しいロールがユーザ ロールのリストに追加され、コンテンツ エリアの [Roles] フォームの下に [Rules] テーブルが表示されます。

ステップ 5　[Add] をクリックし、このロールのルールを作成します。このロールは、それを作成したユーザのロールを継承します。

ステップ 6　ルールを変更するには、次の属性から変更を加える属性を選択します。

（注）　カスタマイズされたロールのユーザに ACE Appliance Device Manager から設定と操作変更を実行する場合、config-copy および exec コマンド機能に対する作成操作を許可するルールのロールを設定する必要があります。

表 15-7　ルールの属性

属性	説明
Rule Number	このルールに割り当てられた番号。
Permission	指定した操作を許可または拒否します。
Operation	指定した機能を作成、デバッグ、修正[1]、および監視します。
Feature	AAA、Access List、Change To Context、Config Copy、Connection、DHCP、Exec コマンド、Fault Tolerant、Inspect、Interface、Load Balance、NAT、PKI[2]、Probe、Real Inservice、Routing、Real Server、Server Farm、SSL[2,3]、Sticky、Syslog、および VIP。 Changeto 機能を使用すると、管理コンテキストから別の仮想コンテキストに移動し、新しいコンテストでも、仮想コンテキストと同じ権限、同じロールを維持し続けることができます。 Exec コマンドの機能は、ACE でデフォルトのカスタム ロール コマンドをすべてイネーブル化します。デフォルトのカスタム ロール コマンドは、capture、debug、gunzip、mkdir、move、rmkdir、tac-pac、untar、write、および undebug です。

1. 機能の中には、特定の操作で使用できないものがあります。修正する場合、Change To Context、Config-Copy、DHCP、Exec コマンド、NAT、Real Inservice、Routing、および Syslog の機能は使用できません。
2. PKI 機能および SSL 機能は ACE NPE ソフトウェア バージョンでは使用できません（「ACE No Payload Encryption ソフトウェア バージョン関する情報」（P.1-2）を参照）。
3. SSL に関連するすべての操作において、カスタム ロールを持つユーザは SSL 機能を含むルールと、PKI 機能を含むルールの 2 つのルールが必要です。

ステップ 7　[Deploy Now] をクリックして、このロールのルールを更新します。

関連トピック

- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）
- 「操作権限について」（P.15-6）
- 「ユーザ ロールの管理」（P.15-14）

ユーザ ロールの修正

任意のユーザ定義のロールを修正できます。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Roles] を選択します。定義済みのロールとそれらの設定値のテーブルが表示されます。

ステップ 2　修正するロールを選択します。

ステップ 3　[Edit] をクリックします。

ステップ 4　変更を加えます。

ステップ 5　[Deploy Now] をクリックして、この設定を展開し、[Roles] テーブルに戻ります。

関連トピック

- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）
- 「操作権限について」（P.15-6）
- 「ユーザ ロールの管理」（P.15-14）

ユーザ ロールの削除

任意のユーザ定義のロールを削除できます（ユーザによって使用されていないかぎり）。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Roles] を選択します。定義済みのロールとそれらの設定値のテーブルが表示されます。

ステップ 2　削除するロールを選択します。

ステップ 3　[Delete] をクリックします。この処理の確定を求めるプロンプトが表示されます。ロールを削除するには、[OK] をクリックします。または、ロールを削除せずに手順を終了するには、[Cancel] をクリックします。

[OK] をクリックすると、ウィンドウは [Roles] テーブルとともにリフレッシュされ、削除したロールの表示は消えます。削除したロールを持つユーザは、そのロールに該当するアクセス権を失います。

関連項目

「ユーザ ロールの管理」（P.15-14）

ルールの追加、編集、または削除

ルールを変更または削除し、特定のロールに含まれる機能へのアクセス権を定義し直すことができます。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Roles] を選択します。定義済みのロールとそれらの設定値のテーブルが表示されます。

ステップ 2　変更するロールを選択します。ペインでロールが 1 つだけ選択されている場合は、ルールの変更だけが実行できます。

ステップ 3　次のタスクのいずれかを実行します。

- [Add] をクリックし、新しいルールを作成します。ルールの情報を入力し（表 15-7（P.15-30）を参照）、[Deploy Now] をクリックします。
- ルールを選択して、[Edit] をクリックし、既存のルールを変更します。[Deploy Now] をクリックして、このエントリを保存します。
- このロールから削除するルールを選択し、[Delete] をクリックします。[OK] をクリックして、削除を確定します。

関連項目

- 「ユーザ ロールの管理」（P.15-14）
- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）
- 「ユーザ ロールの管理上の注意事項」（P.15-15）

ドメインの管理

ネットワーク ドメインは、ネットワーク内のデバイスおよびそれらのコンポーネント（物理および論理）を編成し、サイトの編成方法に従ってアクセスを許可する手段を提供します。

ここでは、ドメインを管理する方法について説明します。

- 「ドメインの管理上の注意事項」（P.15-33）
- 「ネットワーク ドメインの表示」（P.15-33）
- 「ドメインの作成」（P.15-34）
- 「ドメインの修正」（P.15-35）
- 「ドメインの削除」（P.15-35）

ドメインの管理上の注意事項

- デバイスおよびそれらのコンポーネントをドメインに追加するには、事前にそれらが ACE アプライアンス Device Manager に設定されている必要があります。
- ドメインは、*「論理」*コンセプトです。ドメインを削除しても、ドメインのメンバーは削除*されません*。
- 事前定義されたドメインは、修正または削除できません。
- 通常、ユーザはデフォルトのドメインに関連付けられます。デフォルトのドメインでは、ユーザはコンテキスト内のすべての設定を表示できます。ユーザがカスタマイズされたドメインに設定されると、そのユーザはそのドメイン内のものしか表示できません。

（注） オブジェクトをカスタマイズしたドメインに追加するには、CLI を使用し、その後、ACE アプライアンス Device Manager の同期機能を使用して、このオブジェクトを ACE アプライアンス Device Manager のカスタマイズしたドメインに追加します。ACE アプライアンス Device Manager 内でオブジェクトをカスタマイズしたドメインに直接追加すると、オブジェクトはデフォルト ドメインに追加されます。

関連トピック

- 「ネットワーク ドメインの表示」（P.15-33）
- 「ドメインの作成」（P.15-34）
- 「ドメインの修正」（P.15-35）
- 「ドメインの削除」（P.15-35）

ネットワーク ドメインの表示

（注） ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Domains] を選択します。[Domains] テーブルが表示されます。

ステップ 2　すべてのネットワーク ドメインが表示されるまで、テーブルを拡大します。

ステップ 3　[Domains] テーブルからドメインを選択し、そのドメインの設定を表示します。

ステップ 4　また、このペインで、次のタスクを実行することもできます。

- 「ドメインの作成」（P.15-34）
- 「ドメインの修正」（P.15-35）
- 「ドメインへのドメイン オブジェクトの追加またはドメインからのドメイン オブジェクトの削除」（P.15-36）
- 「ドメインの削除」（P.15-35）

関連項目

- 「ドメインの管理」（P.15-32）
- 「ドメインの管理上の注意事項」（P.15-33）

ドメインの作成

新しいドメインを作成するには、このオプションを使用します。

（注） ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Domains] を選択します。[Domains] テーブルが表示されます。

ステップ 2　[Add] をクリックします。

ステップ 3　新しいドメインの名前を入力し、[Deploy Now] をクリックします。

ステップ 4　Domain フォームの下に表示された [Domain Object] テーブルで [Add] をクリックします。

ステップ 5　表 15-8 に表示された属性を入力します。

表 15-8　ドメインの属性

フィールド	説明
Object Type	このドメインを構成するオブジェクトの集合。仮想コンテキストに応じて、次のオプションが使用できます。 • All • Access List Ethertype • Access List Extended • Class Map • Interface VLAN • Interface BVI • Parameter Map • Policy Map • Probe • Real Server • Script • Server Farm • Sticky
Object Name	このフィールドは、特定のオブジェクト タイプが選択されている場合に表示されます。定義されている既存のオブジェクトの名前。

ステップ 6　この設定を展開するには、[Deploy Now] をクリックします。

関連項目

- 「ドメインの管理」（P.15-32）
- 「ドメインの管理上の注意事項」（P.15-33）

ドメインの修正

ドメイン内の設定を変更するには、このオプションを使用します。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Domains] を選択します。

ステップ 2　変更するドメインを選択します。

ステップ 3　[Edit] をクリックします。

ステップ 4　変更を加えます。

ステップ 5　この設定を展開するには、[Deploy Now] をクリックします。

関連トピック

- 「ドメインの管理」（P.15-32）
- 「ドメインの管理上の注意事項」（P.15-33）

ドメインの削除

ネットワーク ドメイン、およびそのネットワーク ドメインに含まれるすべてのデバイスとドメイン オブジェクトをシステムから削除するには、このオプションを使用します。削除できるのは、ユーザに関連付けられていないドメインだけです。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Domains] を選択します。

[Domains] テーブルには、既存のドメインのリストが含まれます。

ステップ 2　削除するドメインを選択します。

ステップ 3　[Delete] をクリックします。

この処理の確定を求めるプロンプトが表示されます。

ステップ 4　[OK] をクリックします。

ドメインは、ACE アプライアンス から削除されます。

関連トピック

- 「ドメインの管理」（P.15-32）
- 「ドメインの管理上の注意事項」（P.15-33）

ドメインへのドメイン オブジェクトの追加またはドメインからのドメイン オブジェクトの削除

ネットワーク ドメイン、およびそのネットワーク ドメインに含まれるすべてのデバイスとドメイン オブジェクトをシステムに追加、またはシステムから削除するには、このオプションを使用します。削除できるのは、ユーザに関連付けられていないドメインだけです。

（注）　ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。

手順

ステップ 1　[Admin] > [Role-Based Access Control] > [Domains] を選択します。

[Domains] テーブルには、既存のドメインのリストが含まれます。

ステップ 2　[Domains] テーブルから、処理を実行するドメインを選択します。

ステップ 3　その後、次の操作を実行できます。

- [Domain Object] テーブルで [Add] をクリックし、オブジェクト タイプとオブジェクト名（必要な場合）を入力して、ドメイン オブジェクトを追加します。その後、[Deploy Now] をクリックします。
- [Domain Object] テーブルで削除する行を選択し、[Delete] をクリックします。

  この処理の確定を求めるプロンプトが表示されます。[OK] をクリックします。ドメイン オブジェクトは、ACE アプライアンスから削除されます。

関連トピック

- 「ドメインの管理」（P.15-32）
- 「ドメインの管理上の注意事項」（P.15-33）

ACE アプライアンス統計情報のモニタリング

次のメニューを使用して、ACE アプライアンス プラットフォーム統計情報データを表示および設定できます。

- [Statistics]：ACE アプライアンス統計情報を表示します。それらをグラフィカルに表示できます。「ACE アプライアンス サーバ統計情報の表示」（P.15-37）を参照してください。
- [Statistics Collection]：ACE アプライアンス統計情報の収集を有効または無効にします。「ACE アプライアンス サーバの統計情報収集の設定」（P.15-37）を参照してください。

ACE アプライアンス サーバ統計情報の表示

ACE アプライアンス統計情報（たとえば、CPU、ディスク、およびメモリ使用状況）を表示し、それらをグラフィカルに表示するには、次の手順を使用します。

デフォルトでは、統計情報の収集は有効になっており、デバイス SNMP 証明書設定が検証に成功し保存された後、5 分ごとに統計情報が収集され、データベースに保存されます。新たに作成された仮想コンテキストの場合、統計情報収集を開始するために入力する必要のある情報は、[Config] > [SNMP] 画面で入力する SNMP コミュニティ情報だけです。

ACE アプライアンス統計情報収集を有効または無効にするには、「ACE アプライアンス サーバの統計情報収集の設定」（P.15-37）を参照してください。

手順

[Admin] > [Device Management] > [Statistics] を選択します。表 15-9 に示す ACE アプライアンス統計情報が表示されます。

表 15-9　ACE アプライアンス サーバの統計情報

名前	説明
Owner	統計情報を収集するプロセス。
Statistic	次の統計情報が含まれます。 • [CPU Usage]：最新 5 分間の ACE アプライアンス CPU 全体に対する使用された CPU のパーセンテージ • [Disk Usage]：ACE アプライアンスによって使用されているディスク容量 • [Memory Usage]：ACE アプライアンスによって使用されているメモリ量 • [Process Uptime]：このシステムが最後に初期化されてからの経過時間、またはシステムのネットワーク管理部分が最後に再初期化されてからの経過時間
Value	統計情報の値
Description	収集した統計情報に関する情報。

関連トピック

- 「ACE アプライアンス統計情報のモニタリング」（P.15-36）
- 「ACE アプライアンス サーバの統計情報収集の設定」（P.15-37）

ACE アプライアンス サーバの統計情報収集の設定

[Monitor] メニューから ACE アプライアンス統計情報ポーリングを有効にするには、次の手順を使用します。収集される統計情報には、次の情報が含まれます。

- [CPU Usage]：最新 5 分間の ACE アプライアンス CPU 全体に対する使用された CPU のパーセンテージ

- [Disk Usage]：ACE アプライアンスによって使用されているディスク容量
- [Memory Usage]：ACE アプライアンスによって使用されているメモリ量
- [Process Uptime]：このシステムが最後に初期化されてからの経過時間、またはシステムのネットワーク管理部分が最後に再初期化されてからの経過時間

仮想コンテキストごとにインターフェイス、CPU、ロード バランシング、およびその他の統計情報の収集を設定する場合は、「仮想コンテキスト統計情報収集のセットアップ」（P.14-33）を参照してください。

手順

ステップ 1　[Admin] > [Device Management] > [Statistics Collection] を選択します。[Statistics Collection] 画面が表示されます。

ステップ 2　[Polling Stats] フィールドでは、[Enable] を選択するとバックグラウンド ポーリングが開始し、[Disable] を選択するとバックグラウンド ポーリングが停止します。

ステップ 3　[Background Polling Interval] フィールドで、ネットワーク環境に適したポーリング インターバルを選択します。インターバルの範囲は、1 分間～ 6 時間です。

ステップ 4　エントリを保存するには、[OK] をクリックします。

（注）　アプライアンスをリブートした場合、これらの設定値は保存されません。システムのデフォルト値が復元されます。

関連トピック

- 「ACE アプライアンス統計情報のモニタリング」（P.15-36）
- 「ACE アプライアンス サーバ統計情報の表示」（P.15-37）

Admin ツールの使用

トラブルシューティングおよび診断タスクを実行するには、Admin ツールを使用します。

- 「診断パッケージの生成」（P.16-1）：クリティカルな問題を Cisco サポート ラインに報告し、診断パッケージを生成するには、ライフライン機能が提供するトラブルシューティングおよび診断ツールを使用します。
- 「ACE アプライアンス ファイルの操作」（P.16-6）：表示したり追跡したりするために、ACE アプライアンスに対してファイルをダウンロードまたはアップロードするには、ファイル ブラウザを使用します。

これらの管理ツールの詳細については、「ACE アプライアンス Device Manager トラブルシューティング ツールの使用」（P.16-1）を参照してください。