CHAPTER 1

概要

Cisco Application Control Engine（ACE）モジュールは、1 つまたは複数のコンテキストで操作できます。複数のコンテキストでは、仮想化を使用して、ACE を複数の仮想デバイスまたは仮想コンテキストに分割します。各コンテキストには、それぞれ一連のポリシー、インターフェイス、リソース、および管理者が含まれます。この機能では、ACE のシステム リソースおよびユーザだけでなく、顧客に提供するサービスもさらに緊密かつ効率的に管理できるようなツールを提供しています。

ACE にはデフォルトで、Admin コンテキストおよび 5 つのユーザ コンテキストが提供されており、それらを設定すると、複数のコンテキストを使用できます。ユーザ コンテキストを追加する（最大 250 まで）には、シスコ システムズから別売のライセンスを入手する必要があります。ライセンスの詳細については、*Cisco Application Control Engine Module Administration Guide* を参照してください。

この章では、仮想化に関連する基本的概念の概要を説明します。主な内容は次のとおりです。

- コンテキスト
- ドメイン
- ロールベース アクセス コントロール
- リソース クラス

コンテキスト

仮想化された環境は、コンテキストと呼ばれるオブジェクトに分割されます。各コンテキストは、それぞれのポリシー、インターフェイス、ドメイン、サーバファーム、実サーバ、および管理者を持つ、独立した ACE のように動作します。各コンテキストでは管理 VLAN も設定でき、この VLAN には、Telnet または Secure Shell（SSH; セキュア シェル）を使用してアクセスできます。管理ポリシーを定義してインターフェイスに適用する方法については、『*Cisco Application Control Engine Module Administration Guide*』を参照してください。

グローバル管理者（Admin）は、各仮想デバイスまたはコンテキストの基本設定を含む Admin コンテキストから、すべてのコンテキストを設定および管理できます。スーパーバイザ エンジン経由でコンソールまたは Telnet を使用して ACE にログインすると、Admin コンテキストで認証されます。

Admin コンテキストは、他のコンテキストとほぼ同じです。相違点は、Admin コンテキストに（SSH などを使用して）ログインすると、ACE 全体および、その中のすべてのコンテキストおよびオブジェクトへの、システム管理者としての完全なアクセス権が付与されるということです。Admin コンテキストでは、Syslog サーバまたはコンテキスト設定サーバなどのネットワーク全体のリソースにアクセスできます。ACE 設定、コンテキスト、リソース クラスなどのグローバル コマンドはすべて、Admin コンテキストでのみ使用可能です。

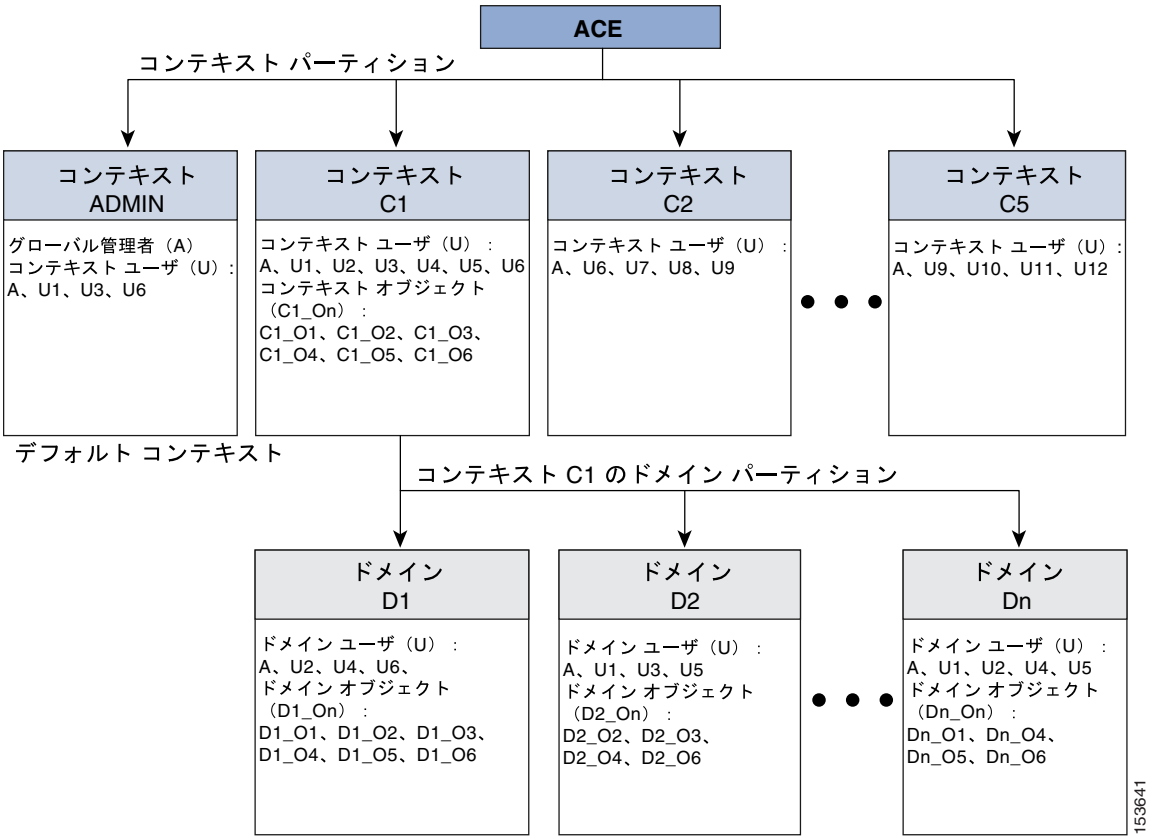
Admin コンテキストを含む各コンテキストには、それぞれのコンフィギュレーション ファイルおよびローカル ユーザ データベースがあります。これらは、フラッシュ ディスク上のローカル ディスク パーティションに格納されていますが、File Transfer Protocol（FTP; ファイル転送プロトコル）サーバ、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ、または HTTP（S）サーバからダウンロードすることもできます。各コンテキストの startup-config ファイルは、フラッシュ ディスク上にスタートアップ コンフィギュレーション ファイルとして格納されています。

Admin コンテキストでは、EXEC モードで **changeto** コマンドを、またはコンフィギュレーション モードで **do changeto** コマンドを使用して、コンテキスト間を移動できます。**changeto** コマンドを使用できるのは、Admin コンテキストで認証されたユーザのみです。

コンテキストの設定の詳細については、第 2 章「仮想化の設定」を参照してください。

図 1-1 は、仮想化を使用して、ACE が複数の仮想デバイスとして機能するようパーティションを作成する方法を示しています。

図 1-1　ACE 仮想化チャート



作成した各コンテキストは、仮想デバイスを表します。各コンテキストは、コンテキストへのアクセスを管理するためのドメインに分割できます。表 1-1 で、図 1-1 内に示したコンポーネントについて説明します。

表 1-1　ACE 仮想化要素

要素	説明
コンテキスト（**C*n***）	1 つの ACE に *コンテキスト*と呼ばれるパーティションを作成することで、複数の仮想化デバイスとして動作するよう設定できます。各コンテキストは、それぞれ一連のユーザ、オブジェクト、および割り当てられたリソースを持つ独立したデバイスとして機能します。ACE にはデフォルトで、Admin コンテキストおよび 5 つの設定可能なユーザ コンテキストが設定されています。ユーザ コンテキストを 250 まで作成できるようアップグレードするには、シスコ システムズから別売のライセンスを購入する必要があります。コンテキストの詳細については、「コンテキスト」を参照してください。
ドメイン（**D*n***）	各コンテキストは、*ドメイン*と呼ばれる複数のパーティションに分割でき、これを使用して、コンテキスト内のオブジェクトへのユーザのアクセスを管理できます。ドメインを作成する場合は、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の間の関連付けを作成します。ドメインの詳細については、「ドメイン」を参照してください。
ユーザ（**A**、**U*n***）	ACE にはデフォルトのグローバル システム管理者が設定されており、この管理者は、すべての ACE 機能にアクセスしたり、追加のユーザを作成したりできます。Admin コンテキスト内で作成したユーザはすべて、デフォルトで、ACE のすべてのリソースにアクセスできます。ユーザ定義のコンテキスト内で作成したユーザはすべて、そのコンテキスト内のリソースにのみアクセスできます。各ユーザにはロールを割り当てます。このロールにより、そのユーザが使用可能なコマンドおよびリソースが決定されます。ユーザおよびユーザ ロールの詳細については、第 2 章「仮想化の設定」を参照してください。

表 1-1　ACE 仮想化要素（続き）

要素	説明
オブジェクト（**C*n*_O*n***、**D*n*_O*n***）	以下のオブジェクトは、ユーザが設定可能な項目です。 • アクセス リスト • 定義済みインターフェイス • ポリシー マップ • ヘルス プローブ • 実サーバ • サーバ ファーム • スクリプト • スティッキ グループ 作成したオブジェクトは、作成時のコンテキストに固有のオブジェクトです。コンテキストが複数のドメインに分割されている場合は、各ドメイン内でオブジェクトを割り当てます。

ドメイン

管理しやすいように、コンテキストは *ドメイン*と呼ばれるオブジェクトに分割され、各ドメインは、その全体が 1 つのコンテキスト内に含まれます。ドメインには、ユーザが動作する場所となる名前空間があり、各ユーザは、少なくとも 1 つのドメインに関連付けられています。ユーザに割り当てられたロールにより、そのユーザがドメイン内のオブジェクトに対して実行可能な動作および使用可能なコマンド セットが決定されます。コンテキストを作成すると、ACE により自動的に、そのコンテキストのデフォルト ドメインが作成されます。

グローバル管理者（Admin）またはコンテキスト管理者は、追加のドメインを作成できます。ドメイン名は、関連付けられたコンテキスト内で一意である必要があります。

作成可能なオブジェクト（サーバ ファーム、実サーバ、プローブ、VLAN など）はどれでも、ドメインに追加でき、複数のドメインに同じオブジェクトを追加できます。他のオブジェクトが関連付けられているオブジェクト（実サーバが設定されているサーバ ファームなど）をドメインに追加した場合、関連付けられているオブジェクトは、自動的にはそのドメインの一部になりません。各オブジェクトを個別に追加する必要があります。オブジェクトを作成すると、ACE により自動的にドメインに追加されます。

（注）　**show running-config** コマンドで表示できるコンテキスト設定が、ドメインにより制限されることはありません。ただし、ACE 内の設定可能なオブジェクトへのユーザのアクセスは、ドメインによって制限されます。ユーザにロールを割り当てることで、それらの設定可能なオブジェクトに対してユーザが実行できる動作をさらに制限できます。ユーザ ロールの詳細については、「ロールベース アクセス コントロール」を参照してください。

ドメインの設定の詳細については、第 2 章「仮想化の設定」を参照してください。

ロールベース アクセス コントロール

ACE では、各ユーザが使用可能なコマンドおよびリソースを決定するメカニズムであるロールベース アクセス コントロール（RBAC）が提供されています。ロールにより一連の権限が定義され、コンテキスト内のオブジェクトとリソース、およびそれらを実行する動作にアクセスできるようになります。グローバル管理者またはコンテキスト管理者は、ユーザのネットワーク機能およびユーザにアクセスを許可するリソースに基づいて、ユーザにロールを割り当てます。

ACE では以下の定義済みロールが提供されており、これらは、削除することも変更することもできません。

- Admin — Admin コンテキスト内で作成した場合は、ACE 全体のすべてのコンテキスト、ドメイン、ロール、リソース、およびオブジェクトに対して完全なアクセスと制御が可能となります。ユーザ コンテキスト内でユーザを作成した場合、そのユーザはこのロールにより、そのコンテキスト内のすべてのオブジェクトに対する完全なアクセスと制御が可能となります。コンテキスト管理者は、ポリシー、ロール、ドメイン、サーバ ファーム、実サーバなど、そのコンテキスト内のあらゆるオブジェクトの作成、設定、および変更を実行できます。
- Network Admin — 以下の機能に対する完全なアクセスと制御が可能です。
  - 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
- Network-Monitor — すべての **show** コマンドおよび **changeto** コマンドのみにアクセスできます。これは、**username** コマンドで明示的にユーザにロールを割り当てていない場合のデフォルトのロールです。
- Security-Admin — コンテキスト内の以下のセキュリティ関連機能に対する完全なアクセスと制御が可能です。
  - 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

  - インターフェイス
  - Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）
  - NAT
  - コピー設定
  - **changeto** コマンド
- Server-Appln-Maintenance — 以下の機能に対する完全なアクセスと制御が可能です。
  - 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
- Server-Maintenance — 以下の機能に対する実サーバのメンテナンス、監視、デバッグが可能です。
  - 実サーバ — 変更権限
  - 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
- SLB-Admin — コンテキスト内の以下の ACE 機能に対する完全なアクセスと制御が可能です。
  - 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
- SSL-Admin — すべての Secure Sockets Layer（SSL）機能の管理者です。
  - SSL — 作成権限
  - Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）— 作成権限
  - インターフェイス — 変更権限
  - コピー設定 — 作成権限
  - **changeto** コマンド — 作成権限

あらゆるコンテキストの Admin は、これらの定義済みロールの他に新しいロールを定義できます。詳細については、第 2 章「仮想化の設定」を参照してください。

リソース クラス

リソース クラスで、同時接続または帯域幅レートなどの ACE リソースへのコンテキスト アクセスを管理できます。ACE には、Admin コンテキストおよび、作成したあらゆるユーザ コンテキストに適用されるデフォルト リソース クラスが設定されています。デフォルト リソース クラスは、リソース アクセスなし（0%）から完全なリソース アクセス（100%）までのいずれかの範囲内でコンテキストが動作できるよう設定されています。

デフォルト リソース クラスを複数のコンテキストで使用すると、ACE により先着順で、すべてのコンテキストにすべてのリソースへのフル アクセスが許可されるため、ACE リソースをオーバーサブスクライブするおそれがあります。リソースがその最大限まで使用されると、そのリソースのあらゆるコンテキストからの追加要求は、ACE により拒否されます。

リソースのオーバーサブスクライブを避け、あらゆるコンテキストが確実にリソースにアクセスできるようにするために、ACE では、カスタマイズされたリソース クラスを作成して、1 つ以上のコンテキストに関連付けることができます。関連付けたコンテキストは、リソース クラスの*メンバ*となります。リソース クラスを作成すると、メンバ コンテキストが使用できる各 ACE リソースの量の最小値と最大値を制限できます。最小値と最大値は、全体に対するパーセンテージで定義します。たとえば、リソース クラスを作成して、ACE がサポートする SSL 接続の総数の 25% 以上へのアクセスをメンバ コンテキストに許可することができます。

以下の ACE リソースの割り当ての制限および管理が可能です。

- ACL メモリ
- Syslog メッセージおよび TCP out-of-order（OOO）セグメント用のバッファ
- 同時接続（ACE 経由のトラフィック）
- 管理接続（ACE へのトラフィック）
- プロキシ接続
- リソースの制限をレート（秒単位の数）で設定
- 正規表現（regexp）メモリ
- SSL 接続
- スティッキ エントリ

- スタティックまたはダイナミック ネットワーク アドレス変換（Xlates）

デフォルトでは、コンテキストの作成時に、ACE によりコンテキストにデフォルト リソース クラスが関連付けられます。デフォルト リソース クラスにより、スティッキ エントリを除くすべてのリソースに対する 0 という最小値および無制限という最大値がリソースに設定されます。スティッキ性が正常に機能するためには、**limit-resource** コマンドを使用して、スティッキ エントリに明示的に最小リソース制限を設定する必要があります。

リソースの設定および制限の詳細については、第 2 章「仮想化の設定」を参照してください。スティッキ性の詳細については、『*Cisco Application Control Engine Module Server Load-Balancing Guide*』を参照してください。