CHAPTER 1

概要

この章では、Cisco Application Control Engine（ACE）モジュールで実装されているサーバ ロード バランシング（SLB）について説明します。この章の内容は次のとおりです。

サーバ ロード バランシングの概要

サーバ ロード バランシング（SLB）とは、ロード バランシング デバイスが、サービスを求めるクライアント要求の送信先サーバを決定することです。たとえば、クライアント要求は、Web ページを取得する HyperText Transport Protocol（HTTP; ハイパーテキスト転送プロトコル）の GET、またはファイルをダウンロードする File Transfer Protocol（FTP; ファイル転送プロトコル）の GET で設定されたりします。ロード バランサのジョブは、クライアント要求に対応できるサーバを選択し、サーバにもサーバ ファーム全体にも過負荷を与えずに、できるだけ短時間に選択を行うことです。

ACE は、次のプロトコルのロード バランシングをサポートします。

- 汎用プロトコル
- HTTP
- Remote Authentication Dial-In User Service（RADIUS）
- Reliable Datagram Protocol（RDP）
- Real Time Streaming Protocol（RTSP）
- Session Initiation Protocol（SIP）

設定するロード バランシング アルゴリズム、つまり*プレディクタ*に応じて、ACE では一連のチェックおよび計算を実行し、各クライアント要求に最良に対応できるサーバを決定します。ACE は、送信元または宛先のアドレス、cookie、URL、HTTP ヘッダー、負荷に対して接続数が最小のサーバなど、いくつかの要因に基づいてサーバを選択します。

ロード バランシング プレディクタ

ACE では次のプレディクタを使用して、クライアント要求の対応に最適なサーバを選択します。

- アプリケーション応答 - 現在の接続数およびサーバの重み（設定されている場合）に基づいた指定の応答時間測定で平均応答時間が最小であるサーバを選択します。
- ハッシュ アドレス - 送信元 IP アドレスまたは宛先 IP アドレス、あるいはその両方に基づいたハッシュ値を使用してサーバを選択します。Firewall Load Balancing（FWLB; ファイアウォール ロード バランシング）のプレディクタを使用します。FWLB の詳細については、第 6 章「ファイアウォール負荷分散の設定」を参照してください。
- ハッシュ コンテンツ - Trusted Third Parties（TTP）のパケット本体のコンテンツ ストリングに基づくハッシュ値を使用してサーバを選択します。
- ハッシュ cookie - cookie 名に基づいたハッシュ値を使用してサーバを選択します。
- ハッシュ ヘッダー - HTTP ヘッダー名に基づいたハッシュ値を使用してサーバを選択します。

- ハッシュ URL - 要求された URL に基づいたハッシュ値を使用してサーバを選択します。URL で一致する開始パターンと終了パターンを指定することができます。このプレディクタ方式を使用して、キャッシュ サーバに負荷を分散させます。
- 最小帯域幅 - 指定サンプル数にサーバが使用した平均帯域幅に基づき、処理したネットワーク トラフィック量が最小であるサーバを選択します。
- 最小接続 - サーバの重みに基づいてアクティブ接続数が最小のサーバを選択します。最小接続プレディクタの場合、稼動させたばかりのサーバに対して高い割合で新規接続を送信することを避けるために、スロースタート メカニズムを設定できます。
- 最小負荷 - Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）プローブから取得された情報に基づき、最小負荷のサーバを選択します。このプレディクタを使用するには、SNMP プローブをこれに関連付ける必要があります。
- ラウンドロビン - サーバの重み（Weighted Round-Robin（[WRR; 重み付けラウンドロビン]）に基づいて実サーバのリストから次のサーバを選択します。大きい重み値を持つサーバは、受け取る接続の割合も大きくなります。これがデフォルトのプレディクタです。

（注）　ハッシュ プレディクタ方式では、実サーバに設定する重み値を認識しません。ACE では、最小接続、アプリケーション応答、ラウンドロビンのプレディクタ方式の場合にだけ、実サーバに割り当てる重みを使用します。

ロード バランシング プレディクタの詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。

実サーバおよびサーバ ファーム

ここでは、実サーバとサーバ ファーム、および ACE でこれらを実装する方法について簡単に説明します。具体的な内容は次のとおりです。

- 実サーバ
- サーバ ファーム
- ヘルス モニタリング

実サーバ

クライアントにサービスを提供するには、ACE 上で*実サーバ*（実際の物理サーバ）を設定します。実サーバは、HTTP や XML コンテンツなどのクライアント サービス、Web サイトのホスティング、FTP ファイルのアップロードやダウンロード、別の場所に移された Web ページへのリダイレクションなどを提供します。ACE では、サーバが何らかの理由で稼動しなくなった場合に備えて、バックアップ サーバを設定することもできます。

ACE での実サーバの作成および名前の指定後、接続制限、ヘルス プローブ、重みなど、いくつかのパラメータを指定することができます。サーバ ファーム内の他のサーバとの相対重要度に基づいて、各実サーバに重みを割り当てることができます。ACE では、重み付きラウンドロビンのサーバの重み値、および最小接続ロード バランシング プレディクタを使用します。ACE プレディクタのリストおよび簡単な説明については、「ロード バランシング プレディクタ」を参照してください。ACE ロード バランシング プレディクタおよびサーバ ファームの詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。

サーバ ファーム

データセンターでは通常、サーバは、*サーバ ファーム*と呼ばれる関連グループに編成されています。多くの場合、サーバ ファーム内のサーバには同じコンテンツ（ミラー化されたコンテンツと呼ばれる）が格納されているため、1 つのサーバが動作しなくなると、別のサーバが直ちに処理を引き継ぎます。また、ミラー コンテンツを使用すると、複数のサーバで、オリンピックなどの地元または国際的なイベントの間に増加する要求の負荷を分散することができます。コンテンツに対するこの急激な要求の増加は、*フラッシュ クラウド*と呼ばれます。

サーバ ファームの作成および名前の指定後、サーバ ファームに既存の実サーバを追加したり、ロード バランシング プレディクタ、サーバの重み、バックアップ サーバ、ヘルス プローブなど、サーバ ファームの他のパラメータを指定することができます。ACE プレディクタの詳細については、「ロード バランシング プレディクタ」を参照してください。ACE ロード バランシング プレディクタおよびサーバ ファームの詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。

ヘルス モニタリング

ヘルス プローブ（*キープアライブ*とも呼ばれる）を設定することによって、サーバおよびサーバ ファームのヘルスをチェックするように ACE に指示することができます。プローブを作成したら、プローブを実サーバまたはサーバ ファームに割り当てます。プローブは、TCP、ICMP、Telnet、HTTP など、多くのタイプのいずれかにすることができます。TCL スクリプト言語を使用して、スクリプト化されたプローブを設定することもできます。

ACE は、プローブを定期的に送信してサーバのステータスを調べ、サーバの応答を確認し、クライアントがサーバにアクセスできなくなるようなネットワークの他の問題がないかどうかをチェックします。ACE は、サーバの応答に基づいてサーバの稼動と非稼動の切り替えを行うことができ、また、サーバ ファーム内のサーバのステータスに基づいて、ロード バランシングに関する信頼性の高い決定を行うことができます。アウトオブバンド ヘルス モニタの詳細については、第 4 章「ヘルス モニタリングの設定」を参照してください。

トラフィック分類およびポリシーの設定

ACE では、いくつかの設定要素を使用して対象のトラフィックを分類（フィルタ）して、ロード バランシングの決定を行う前にトラフィックに対して各種のアクションを実行します。これらのフィルタ要素および後続のアクションは、SLB の基礎となっています。ここでは、次の内容について説明します。

- ACL によるトラフィックのフィルタ
- レイヤ 3 およびレイヤ 4 トラフィックの分類
- レイヤ 7 トラフィックの分類
- パラメータ マップの設定
- トラフィック ポリシーの作成
- サービス ポリシーを使用したインターフェイスへのトラフィック ポリシーの適用

ACL によるトラフィックのフィルタ

特定の IP アドレスまたはネットワーク全体との間で送受信するトラフィックを許可または拒否するには、Access Control List（ACL; アクセス コントロール リスト）を設定します。ACL では、特定のインターフェイスまたはすべてのインターフェイスで明示的に許可したトラフィックにだけアクセスを許可することによって、ACE およびデータセンターにセキュリティの対策手段を提供します。ACL は、送信元アドレス、宛先アドレス、プロトコル、ポートなどの特別な基準を備えた一連の許可または拒否エントリから設定されています。すべての ACL には暗黙的な拒否（deny）ステートメントが含まれているため、ACE との間でトラフィックの送受信を許可するには、明示的な許可（permit）エントリを追加する必要があります。ACL の詳細については、『*Cisco Application Control Engine Module Security Configuration Guide*』を参照してください。

レイヤ 3 およびレイヤ 4 トラフィックの分類

レイヤ 3 およびレイヤ 4 ネットワーク トラフィックを分類するには、アプリケーション要件に応じてクラス マップを設定し、一致基準を指定します。トラフィック フローが特定の一致基準と一致すると、ACE では、クラス マップが関連付けられているポリシー マップに指定されたアクションを適用します。ポリシー マップは、（コンテキスト内でのすべての VLAN インターフェイスまたは単一の VLAN インターフェイスに対してグローバルな）サービス ポリシーによってポリシー マップを適用したインターフェイスに入るトラフィックに適用されます。

SLB 用にレイヤ 3 およびレイヤ 4 で動作するクラス マップでは通常、Virtual IP（VIP; 仮想 IP）アドレスを一致基準として使用します。SLB 用のレイヤ 3 およびレイヤ 4 クラス マップの詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。

レイヤ 7 トラフィックの分類

レイヤ 3 およびレイヤ 4 クラス マップ以外に、HTTP cookie、HTTP ヘッダー、URL 設定など高度なロード バランシング一致基準に対して、レイヤ 7 クラス マップを設定することもできます。レイヤ 7 クラス マップを設定したら、このクラス マップをレイヤ 7 ポリシー マップに関連付けます。レイヤ 7 ポリシー マップは、インターフェイスに直接適用できません（「トラフィック ポリシーの作成」

を参照)。SLB 用のレイヤ 7 クラス マップの詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。

パラメータ マップの設定

パラメータ マップでは、レイヤ 3 およびレイヤ 4 ポリシー マップで使用する関連 HTTP または RTSP のアクションを組み合わせます。パラメータ マップは、ACE インターフェイスに入るトラフィックに対し、特定の基準に基づいてアクションを実行するための手段です。基準としては、HTTP ヘッダーや cookie の設定、サーバ接続の再使用、HTTP ヘッダーや cookie や URL が設定済み最大長を超えると実行されるアクションなどが使用されます。パラメータ マップの設定後、そのパラメータ マップをレイヤ 3 およびレイヤ 4 ポリシー マップに関連付けます。HTTP または RTSP のロード バランシング パラメータ マップの設定に関する詳細は、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。

トラフィック ポリシーの作成

ACE ではポリシー マップを使用することによって、クラス マップとパラメータ マップを組み合わせてトラフィック ポリシーにし、ポリシーに設定された基準と一致するトラフィックに対して特定の設定済みアクションを実行します。ポリシー マップは、レイヤ 3 とレイヤ 4、およびレイヤ 7 で動作します。ACE ではレイヤ 7 ポリシー マップが子マップと見なされるため、サービス ポリシーを使用してトラフィック ポリシーをインターフェイスに適用するには、各レイヤ 7 ポリシー マップをレイヤ 3 およびレイヤ 4 ポリシー マップに関連付ける必要があります。SLB トラフィック ポリシーの設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。

サービス ポリシーを使用したインターフェイスへのトラフィック ポリシーの適用

トラフィック ポリシーを 1 つまたは複数のインターフェイスに適用するには、サービス ポリシーを使用します。サービス ポリシーは、個々のインターフェイスに対して、または入力方向だけのコンテキストにおけるすべてのインターフェイスに対してグローバルに使用できます。インターフェイスでサービス ポリ

シーを使用する場合は、クラス マップ、パラメータ マップ、およびレイヤ 7 ポリシー マップが関連付けられていて一致基準を備えたレイヤ 3 およびレイヤ 4 ポリシー マップを適用して有効にします。サービス ポリシーを使用して、トラフィック ポリシーをインターフェイスに適用する方法の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。

接続制限およびレート制限

システム リソースを保護するために、ACE は次の項目を制限できるようになっています。

- 最大接続数
- 接続レート（1 秒あたりの接続数。実サーバを宛先とした新規接続に適用される）
- 帯域幅レート（1 秒当たりのバイト数。ACE と実サーバの間の双方向のネットワーク トラフィックに適用される）

詳細については、第 2 章「実サーバおよびサーバ ファームの設定」および『*Cisco Application Control Engine Module Security Configuration Guide*』を参照してください。

ロード バランサとしての ACE の厳密な使用

ACE を SLB デバイスとして厳密に動作させることができます。SLB だけを使用する場合は、特定のパラメータを設定し、ACE セキュリティ機能の一部をディセーブルにする必要があります。デフォルトでは ACE は、ACE インターフェイスに入るトラフィックに対して、TCP/IP 正規化チェックおよび ICMP セキュリティ チェックを実行します。次の設定を使用すると、ネットワーク アプリケーションでの必要に応じて非対称ルーティングを行うこともできます。

主な設定項目は次のとおりです。

- ACL をグローバルにすべて許可するよう設定します。コンテキスト内のすべてのインターフェイスに適用してすべてのポートを開くようにします。
- TCP/IP 正規化のディセーブル化
- ICMP セキュリティ チェックのディセーブル化
- SLB の設定

SLB 専用に ACE を動作させるには、次の手順を実行します。

ステップ 1　グローバルにすべて許可するように ACL を設定し、この ACL をコンテキスト内のすべてのインターフェイスに適用します。このアクションによって、現在のコンテキスト内のすべてのポートが開かれます。

```
host1/Admin(config)# access-list ACL1 extended permit ip any any
host1/Admin(config)# access-group input ACL1
```

ステップ 2　ロード バランシング サービス ポリシーを使用して VIP を設定する各インターフェイスに対して、デフォルトの TCP/IP 正規化チェックをディセーブルにします。TCP 正規化の詳細については、『*Cisco Application Control Engine Module Security Configuration Guide*』を参照してください。

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# no normalization
```

注意　TCP 正規化をディセーブルにすると、ACE およびデータセンターがセキュリティ リスクにさらされるおそれがあります。TCP 正規化では、トラフィックに奇妙なまたは悪意のあるセグメントを検出する厳密なセキュリティ ポリシーを実施することによって、ACE およびデータセンターを攻撃者から防御します。

ステップ 3　ロード バランシング サービス ポリシーを使用して VIP を設定する各インターフェイスに対して、デフォルトの ICMP セキュリティ チェックをディセーブルにします。ICMP セキュリティ チェックの詳細については、『*Cisco Application Control Engine Module Security Configuration Guide*』を参照してください。

```
host1/Admin(config-if)# no icmp-guard
```

注意　ACE ICMP セキュリティ チェックをディセーブルにすると、ACE およびデータセンターがセキュリティ リスクにさらされるおそれがあります。また、**no icmp-guard** コマンドの入力後、ACE は、エラー パケット内の ICMP ヘッダーおよびペイロードに Network Address Translation（NAT; ネットワーク アドレス変換）を実行しないため、実際のホスト IP アドレスが攻撃者にさらされるおそれがあります。

ステップ 4　SLB を設定します。詳細については、このガイドの残りの章を参照してください。

次の作業

ACE で SLB の設定を開始するには、第 2 章「実サーバおよびサーバ ファームの設定」に進んでください。