CHAPTER 7

スティッキ機能の設定

この章では、スティッキ機能の動作と ACE アプライアンスでのスティッキ機能の設定方法を説明します。

（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。

この章の内容は、次のとおりです。

スティッキ機能の概要

e- コマース サイトを訪問するクライアントは、サイトをブラウズすることからインターネット上のウィンドウ ショッピングを始めます。サイトのアプリケーションによって、接続確立後にクライアントが 1 つのサーバに固定されることが必要な場合もあれば、クライアントがショッピング カートの確立を開始するまで、サーバへの固定を必要としない場合もあります。

いずれにしても、クライアントがショッピング カートに品物を入れてからは、そのクライアントのすべての要求が同じサーバに送信され、すべての品が 1 つのサーバ上の 1 つのショッピング カートに入るようにすることが重要です。お客様のショッピング カートのインスタンスは通常、特定の Web サーバ上にあり、複数のサーバに重複してはいません。

このようなスティッキ性が必要とされるのは、e- コマース アプリケーションだけではありません。バンキング アプリケーションやオンライン取引など、クライアントの情報を維持するような Web アプリケーションはスティッキ性を必要とする可能性があります。FTP および HTTP のファイル転送にも、スティッキが使用されます。

スティッキ機能を使用すると、1 つのセッション中、同じクライアントが、複数の同時 TCP または IP 接続、あるいは後続の複数の TCP または IP 接続を同一サーバとの間で維持できます。ここでの説明で使用する「セッション」とは、クライアントとサーバの間の一定期間（数分から数時間まで）における

連続したトランザクションです。スティッキは、オンライン ショッピング、特に HTTP を使用したショッピング カートの確立や HTTPS を使用したチェックアウト プロセス中など、クライアントが同じサーバとの間で複数の接続を維持する必要があるような e-コマース アプリケーションに便利な機能です。

ACE アプライアンスは、設定済みのサーバ ロード バランシング（SLB）ポリシーに応じて、使用するロード バランシング方式を判断してから、適切なサーバにクライアントを固定します。ACE アプライアンスは、クライアントが特定のサーバにすでに固定されていると判断した場合、一致ポリシーに指定されているロード バランシング基準に関係なく、そのクライアントの要求をそのサーバに送信します。クライアントが特定のサーバに固定されていないと判断した場合、ACE アプライアンス はそのコンテンツ要求に通常のロード バランシング規則を適用します。

サーバ ファームに関連付けられた実サーバへのスティッキ性を設定できます。または、*バディ スティッキ グループ*機能を使用して、複数のサーバ ファームにおける実サーバまたは実サーバ グループへの持続性を有効にできます（「バディ スティッキ グループ」（P.7-6）を参照）。

スティッキ性の概要については、次のトピックを参照してください。

- スティッキ タイプ
- スティッキ グループ
- スティッキ テーブル
- バディ スティッキ グループ

関連トピック

- 「仮想サーバ レイヤ 7 のロード バランシングの設定」（P.5-31）
- 「スティッキ グループの設定」（P.7-12）

スティッキ タイプ

ACE アプライアンスは次に基づくスティッキ機能をサポートしています。

- HTTP cookie
- HTTP ヘッダー
- IP アドレス
- HTTP コンテンツ
- IP ネットマスク
- IPv6 プレフィックス
- レイヤ 4 ペイロード
- RADIUS 属性
- RTSP ヘッダー
- SIP ヘッダー
- SSL セッション ID

関連トピック

- 「HTTP コンテンツに基づくスティッキ」（P.7-3）
- 「HTTP cookie に基づくスティッキ」（P.7-3）
- 「HTTP ヘッダーに基づくスティッキ」（P.7-4）

- 「IP ネット マスクおよび IPv6 プレフィックスに基づくスティッキ性」（P.7-4）
- 「レイヤ 4 ペイロードに基づくスティッキ」（P.7-4）
- 「RADIUS に基づくスティッキ」（P.7-5）
- 「RTSP ヘッダーに基づくスティッキ」（P.7-5）
- 「SIP ヘッダーに基づくスティッキ」（P.7-5）
- 「SSL に基づくスティッキ性」（P.7-5）

HTTP コンテンツに基づくスティッキ

HTTP コンテンツ スティッキ機能を使用すると、HTTP パケットのコンテンツに基づきクライアントをサーバに固定できます。開始パターンと終了パターン、解析するバイト数、データの始点から無視するバイト数を指定するオフセットを指定できます。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

HTTP cookie に基づくスティッキ

クライアントの *cookie* によって、ACE およびコンテンツ提供サーバに接続するクライアントを一意に識別できます。cookie は、HTTP ヘッダー内の小さなデータ構造であり、サーバはこれを使用して Web クライアントにデータを送信し、クライアントがその情報を保存するように要求します。一部のアプリケーションでは、クライアントは情報をサーバに返し、クライアントとサーバの間の接続状態または固定状態を維持します。

ACE は、コンテンツ要求を検証し、ポリシーの一致によってそのコンテンツがスティッキ状態であると判断すると、そのコンテンツ要求の cookie または URL を調べます。ACE は、cookie または URL 内の情報を使用して、該当するサーバにコンテンツ要求を転送します。

ACE がサポートする cookie スティッキには次のタイプがあります。

- ダイナミック cookie ラーニング

  クライアント要求の HTTP ヘッダーまたはサーバの応答内の server Set-Cookie メッセージで特定の cookie 名を探し、自動的にその値を学習するように ACE を設定できます。ダイナミック cookie ラーニングは、同じ cookie 内のセッション ID またはユーザ ID だけでなくその他の情報も保存するようなアプリケーションを扱う場合に適しています。スティッキに使われるのは、cookie 内の特定のバイト値だけです。

  デフォルトでは、ACE は cookie 値全体を学習します。オプションとして、オフセットと長さを指定し、cookie 値の一部だけを学習するように ACE に指示することもできます。

  あるいは、HTTP 要求内の URL ストリングに示される第 2 の cookie 値を指定することもできます。このオプションでは、ACE は URL の一部として cookie 情報を探索します（最終的には学習または固定します）。URL ラーニングは、HTTP URL の一部として cookie 情報を挿入するアプリケーションに適しています。場合によっては、この機能を使用して cookie を拒否するクライアントに対処することもできます。

- cookie 挿入

サーバの代わりに ACE がリターン要求に cookie を挿入し、サーバが cookie を入れるように設定されていなくても、ACE が cookie スティッキを実行できるようにします。この cookie には、ACE が特定の実サーバへの固定を確実に実行するために使用する情報が入っています。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

HTTP ヘッダーに基づくスティッキ

HTTP ヘッダー情報を使用してスティッキを提供することも可能です。HTTP ヘッダー スティッキ方式では、ヘッダーのオフセットを指定して、HTTP ヘッダーの一意の部分に基づいてスティッキを提供できます。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

IP ネット マスクおよび IPv6 プレフィックスに基づくスティッキ性

IP ネットマスクまたは IPv6 プレフィックスに基づいて送信元 IP アドレス、宛先 IP アドレス、またはその両方を使用すると、スティッキ性を目的として個々のクライアントとその要求を識別できます。ただし、企業やサービス プロバイダーがメガプロキシを使用してインターネットへのクライアント接続を確立している場合、送信元 IP アドレスは、要求の真の送信元として信頼できるインジケータにはなりません。このような場合は、セッションの持続性を確実にするために cookie またはその他のいずれかのスティッキ方式を使用します。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

レイヤ 4 ペイロードに基づくスティッキ

レイヤ 4 ペイロード スティッキ機能を使用すると、レイヤ 4 フレームのデータに基づきクライアントをサーバに固定できます。開始パターンと終了パターン、解析するバイト数、データの始点から無視するバイト数を指定するオフセットを指定できます。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）

- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

RADIUS に基づくスティッキ

次の RADIUS 属性に基づく RADIUS スティッキが可能です。

- 発信側ステーション ID
- ユーザ名

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

RTSP ヘッダーに基づくスティッキ

RTSP スティッキは RTSP セッション ヘッダーに基づいて機能します。RTSP ヘッダー スティッキ方式では、ヘッダーのオフセットを指定して、RTSP ヘッダーの一意の部分に基づいてスティッキを提供できます。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

SIP ヘッダーに基づくスティッキ

SIP ヘッダー スティッキは、SIP Call-ID ヘッダー フィールドに基づいて機能します。SIP ヘッダー スティッキ方式では、SIP ヘッダー全体が必要であるため、オフセットは指定できません。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

SSL に基づくスティッキ性

SSL のスティッキ性により、SSL セッション ID に基づいてクライアントをサーバに固定することができます。HTTPS サーバ ロード バランシング ポリシー マップに SSL スティッキ グループを関連付けることができます。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ グループ」（P.7-6）
- 「スティッキ テーブル」（P.7-11）

スティッキ グループ

スティッキ グループを使用すると、ACE はクライアントをサーバ ファーム内の実サーバまたは実サーバのグループに固定したままにできます。ACE ではスティッキ グループの考え方を利用してスティッキ機能を設定します。スティッキ グループを使用することによって、スティッキ属性を指定できます。スティッキ グループとその属性の設定後、そのスティッキ グループを、レイヤ 7 SLB ポリシー マップのレイヤ 7 ポリシー マップ アクションと関連付けます。各コンテキストに最大 4096 のスティッキ エントリを作成できます。ACE アプライアンス に設定された各スティッキ グループには、次の事項を決定する一連のパラメータが含まれています。

- スティッキ方式
- タイムアウト
- レプリケーション
- cookie のオフセットおよびその他の cookie 関連属性
- HTTP ヘッダーのオフセットおよびその他のヘッダー関連属性
- バディ グループ名

関連トピック

- 「スティッキ機能の概要」（P.7-1）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ テーブル」（P.7-11）
- 「スティッキ グループの設定」（P.7-12）

バディ スティッキ グループ

バディ スティッキ グループを使用すると、クライアント要求が異なるサーバ ファームによって処理される場合でも、ACE はクライアントを実サーバまたは実サーバのグループに固定したままにできます。

バディ スティッキ グループ機能を使用するには、次の手順を実行します。

1. サーバ ファームの実サーバを指定する際に、実サーバのバディ グループを作成します（「サーバ ファームの設定」（P.6-18）を参照）。
2. サーバ ファームをスティッキ グループで指定する際に、スティッキ サーバ ファームのバディ グループを作成します（「スティッキ グループの設定」（P.7-12）を参照）。グループ メンバとして合わせてバディ化される各スティッキ サーバ ファームを作成します。

ここでは、次のバディ スティッキ グループの用途について説明します。

- 1 対 1 の関連付け：2 つの異なるサーバ ファーム内の同じ物理サーバ インスタンスにクライアントを固定します。
- 非対称の関連付け：クライアントが非 HTTP 要求または異なる HTTP ヘッダーにより復旧した場合であっても、異なるサーバ ファーム間で構成された実サーバにクライアントを固定します。

- 多対 1 の関連付け：より少ない数のサーバを含む第 2 階層にある 1 台の実サーバに、第 1 階層の複数の実サーバを固定します。

この項では、次のトピックについて取り上げます。

- 「注意事項および制約事項」（P.7-7）
- 「1 対 1 の関連付けの例」（P.7-8）
- 「非対称の関連付けの例」（P.7-9）
- 「多対 1 の関連付けの例」（P.7-10）

注意事項および制約事項

バディ スティッキ グループ機能を使用する場合は、次のガイドラインと制約事項に従ってください。

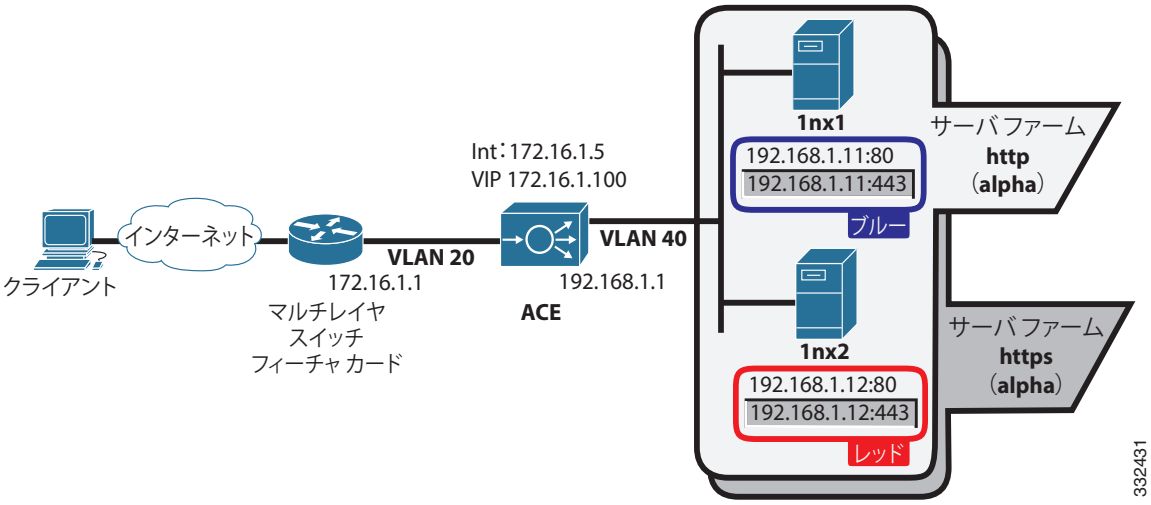
- 異なるタイムアウト値の 2 つのスティッキ グループを合わせてバディ化した場合、ACE はバディ グループに対して最も短いタイムアウト値を使用します。
- 合わせてバディ化されるスティッキ グループは、同じタイプ（すべてが IP-sticky、すべてが http-cookie など）である必要があります。ACE は、バディ化された異なるタイプのスティッキ グループをサポートしません。
- 2 つのスティッキ グループを合わせてバディ化し、これらの一方をタイムアウト アクティブ接続用に設定した場合、メンバ グループもまた、タイムアウト アクティブ接続用に設定されます。
- 2 つのスティッキ グループが異なる IP ネットマスク（IPv4）またはプレフィックス長（IPv6）を使用して設定されている場合、ACE は、最も粒度の高いネットマスクまたはプレフィックス長を持つスティッキ グループを使用します。
- バディ スティッキ グループ内にスタティック エントリを作成した場合、その動作は変更されず、実サーバが関連付けられるバディ グループに関係なく、設定された同じ実サーバに固定されます。
- メンバとしてスティッキ グループを設定する前に、そのスティッキ グループ内でサーバ ファームが設定されており、そのサーバ ファームに属するすべての実サーバにおいて、そのスティッキ グループ内でバディ グループが設定されている必要があります。この要件により、無効な設定が防止されます。
- ACE では、バディ スティッキ グループのメンバとして、次のタイプのスティッキ グループの設定はサポートされません。
  - SSL
  - RTSP Header
- ACE は SIP スティッキなどの PTMP スティッキ グループをサポートしています。ただし、バディ スティッキ グループ機能が動作するためには、両方のスティッキ グループ間での設定が同じであることを確認する必要があります。
- 実サーバのバックアップ用途の場合
  - バディ スティッキによる 1 レベルのみの backup-rserver の使用をお勧めします。
  - プライマリ実サーバにバディ グループを追加した場合は、バックアップ サーバがこのバディ グループを継承します。ただし、プライマリ実サーバからバディ グループを削除した場合、バディ グループはバックアップ実サーバから削除されません（その逆の場合も同様です）。

1 対 1 の関連付けの例

1 対 1 でのバディ スティッキ グループの関連付けでは、2 つの異なるサーバ ファーム内の同じ物理サーバ インスタンスにクライアントを固定するバディ スティッキ グループを作成します。図 7-1 で示したネットワークの例では、ACE は次のサーバ ファーム、関連付けられた実サーバ、および両方の項目をグループ化するバディ スティッキ グループにより設定されています。

サーバ ファーム	サーバ ファーム バディ メンバ グループ	実サーバ	実サーバ バディ グループ
http （HTTP 要求用）	alpha	1nx1:192.168.1.11:80	ブルー
		1nx2:192.168.1.12:80	レッド
https （HTTPS 要求用）	alpha	1nx1:192.168.1.11:443	ブルー
		1nx2:192.168.1.12:443	レッド

図 7-1　バディ スティッキ グループ：1 対 1 の関連付け



ACE は、1nx1:192.168.1.11:80 または 1nx2:192.168.1.12:80 のいずれかの実サーバを使用して、サーバ ファーム http に対する HTTP 要求のロード バランシングを行うように設定されています。ACE は、サーバ ファーム https および 1nx1:192.168.1.11:443 または 1nx2:192.168.1.12:443 のいずれかの実サーバを使用して、HTTPS 要求のロード バランシングを行うようにも設定されています。バディ グループにより、ACE は同じ実サーバ（たとえば 1nx1）にクライアントを固定することができ、それと同時に、HTTP 要求を使用してショッピング カートを確立してから、HTTPS を使用してチェック アウトできます。

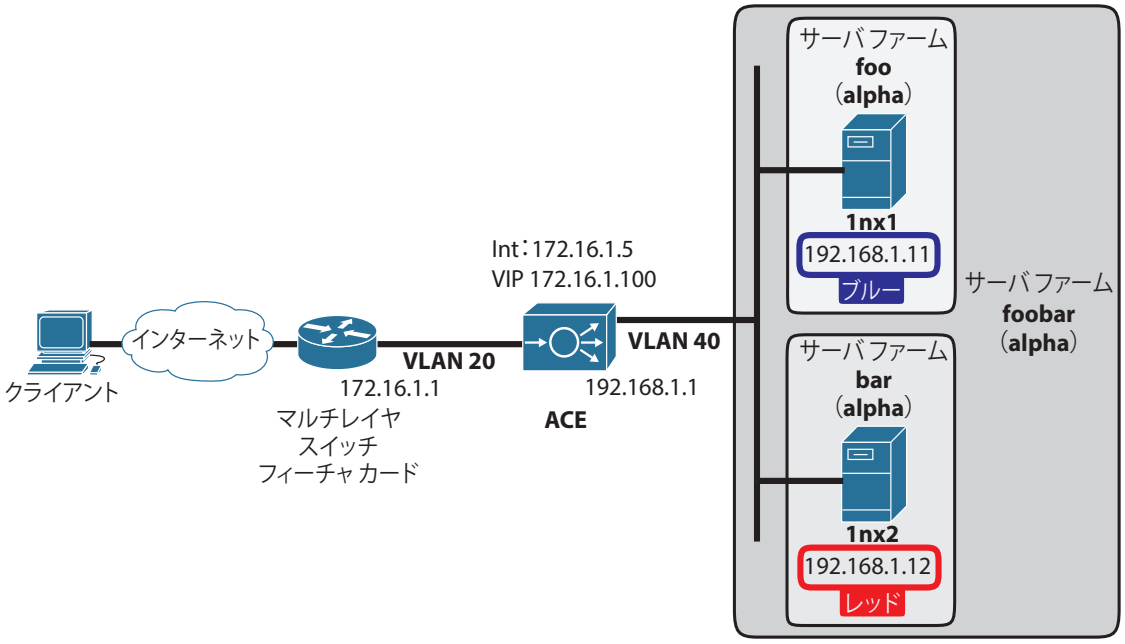
この例では、クライアントは HTTP 要求を使用して VIP 172.16.1.100 宛先ポート 80 にヒットして、ショッピング カートの確立を開始します。ACE は、サーバ ファーム http、実サーバ 1nx1:192.168.1.11:80 への要求のロード バランシングを行い、対応するスティッキ グループ（たとえば、送信元 IP アドレスなど）に基づいてスティッキ エントリを作成します。このスティッキ エントリにより、クライアントがショッピング カートを確立する間にクライアントが実サーバに固定されます。チェック アウト用の安全な接続（ポート 443）に移動すると、クライアントは宛先ポート 443 を使用して VIP にヒットし、ACE はサーバ ファーム https にクライアントを送信します。2 台の実サーバはブルーのバディ グループ内で合わせてバディ化されているため、ACE は、既存のスティッキ エントリと実サーバ Inx1:192.168.1.11:80 を検出し、クライアントを 1nx1:192.168.1.11:443 に転送します。

非対称の関連付けの例

非対称でのバディ スティッキ グループの関連付けでは、一部のトラフィックがレイヤ 7 クラス マップと一致しない場合でも、クライアントから特定の実サーバへのすべてのレイヤ 7 トラフィックを固定するバディ スティッキ グループを作成します。図 7-2 に示すネットワーク例では、次のサーバ ファーム、関連付けられた実サーバ、および実サーバのバディ スティッキ グループを含むように ACE が設定されています。

サーバ ファーム	サーバ ファーム バディ メンバ グループ	実サーバ	実サーバ バディ グループ
foo bar	alpha	1nx1	ブルー
		1nx2	レッド
foo	alpha	1nx1	ブルー
bar	alpha	1nx2	レッド

図 7-2　バディ スティッキ グループ：非対称の関連付け



ACE は、ネストされたサーバ ファーム（foo および bar）を含むサーバ ファーム foobar に、レイヤ 3 の一致を使用してクライアント トラフィックを送信するよう設定されています。ACE はレイヤ 7 クラス マップの一致に基づいて、ネストされたサーバ ファームのいずれかに対してクライアント トラフィックのロード バランシングを行います。バディ スティッキ グループを定義することによって、ACE は、同じ実サーバに一致しないクライアント トラフィックを固定することもできます。

この例では、クライアントはレイヤ 3 の一致を使用してトラフィックを送信し、ACE は（IP スティッキを使用して）そのトラフィックをサーバ ファーム foobar に転送および固定します。ACE はレイヤ 7 クラス マップを使用して HTTP URL（ある場合）を確認し、サーバ ファーム foo にトラフィックを送信し、送信元 IP アドレスに基づくスティッキを使用してそのサーバにクライアント トラフィックを固定します。バディ スティッキ グループを使用することにより、ACE はスティッキ エントリを使用して、他のすべてのトラフィックをクライアントから同じ実サーバに送信します。たとえば、ACE がレ

イヤ 7 クラス マップの一致に基づいてサーバ ファーム foo の実サーバ lnx1 にクライアントの HTTP トラフィックを固定する場合は、バディ スティッキ グループを使用することにより、ACE はクライアントから同じ実サーバに非 HTTP トラフィックを送信できます。

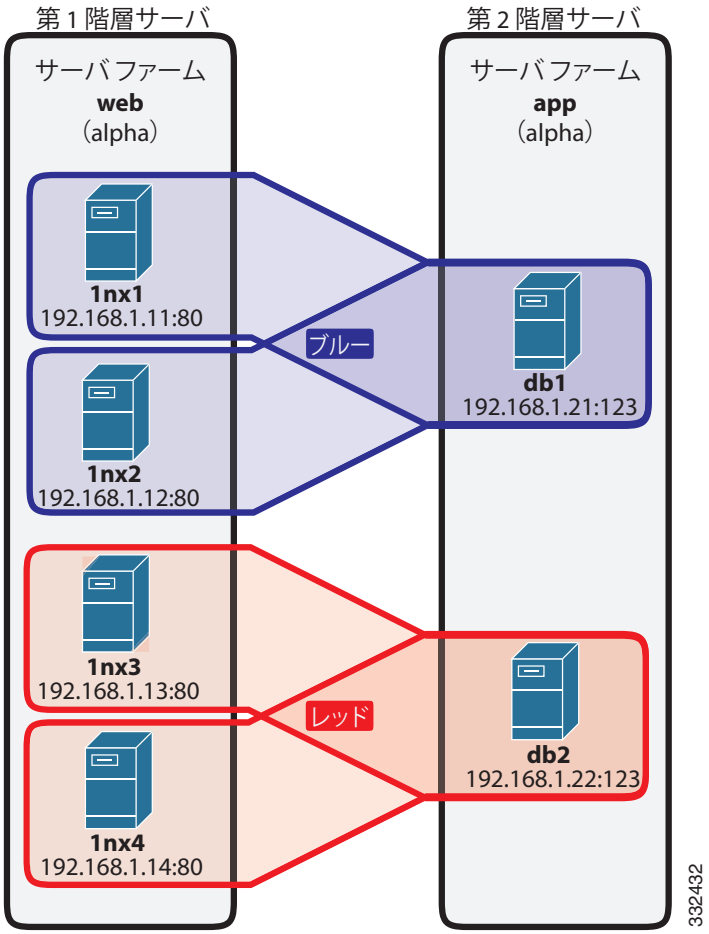
多対 1 の関連付けの例

多対 1 でのバディ スティッキ グループの関連付けでは、実サーバのグループを特定の実サーバに固定するバディ スティッキ グループを作成します。これは、多くの実サーバを含む第 1 階層のサーバ ファームに対してクライアントのロード バランシングを行い、より少ない実サーバを含む第 2 階層のサーバ ファームに転送する場合に役立ちます。このような用途では、第 1 階層の各実サーバ グループを第 2 階層の特定の実サーバに固定するバディ スティッキ グループを作成します。

図 7-3 に示すネットワーク例では、次のサーバ ファーム、関連付けられた実サーバ、および関連付けられた実サーバのバディ スティッキ グループにより ACE が設定されています。

サーバ ファーム	サーバ ファーム バディ メンバ グループ	実サーバ	実サーバ バディ グループ
web（第 1 階層）	alpha	1nx1:192.168.1.11:80	ブルー
		1nx2:192.168.1.12:80	ブルー
		1nx3:192.168.1.13:80	レッド
		1nx4:192.168.1.14:80	レッド
app（第 2 階層）	alpha	db1:192.168.1.21:123	ブルー
		db1:192.168.1.22:123	レッド

図 7-3　バディ スティッキ グループ：多対 1 の関連付け



ブルーとレッドのバディ スティッキ グループにより、第 1 階層の実サーバがグループに分割され、これらの各グループが特定の第 2 階層の実サーバに固定されます。

この例では、ACE が実サーバ 1nx1 または 1nx2 に対してクライアントのロード バランシングを行う場合に、サーバ ファーム app に移行する準備ができると、クライアントが実サーバ db1 にのみ転送されます。ACE が 1nx3 または 1nx4 に対してロード バランシングを行うクライアントは、サーバ ファーム app に移行する準備ができると、実サーバ db2 にのみ転送されることにも注意してください。

スティッキ テーブル

スティッキ接続のトラックを維持するために、ACE アプライアンス はスティッキ テーブルを使用します。テーブルのエントリには、次の項目が含まれています。

- スティッキ グループ
- スティッキ方式
- スティッキ接続
- 実サーバ

スティッキ テーブルには最大 400 万のエントリを保存できます（同時に 400 万のユーザ）。テーブルが最大エントリ数に達してから、スティッキ接続が追加されると、テーブルが循環して最初のユーザとその該当サーバとのスティッキが解除されます。

ACE アプライアンス は設定可能なタイムアウト メカニズムによってスティッキ テーブルのエントリをエージング アウトします。エントリがタイムアウトになると、そのエントリは再利用できる状態になります。接続率が高ければ、スティッキ エントリがタイムアウトになる前にエージング アウトされることもあります。このような場合、ACE アプライアンス は有効期限に最も近いエントリを再利用します。

スティッキ エントリには、ダイナミック（動作時に ACE アプライアンスが生成）とスタティック（ユーザ設定）があります。スタティック スティッキ エントリを作成すると、ACE アプライアンス はスティッキ テーブル内に即座にそのエントリを置きます。スタティック エントリは、ユーザが設定から削除するまで、スティッキ データベース内に残ります。各コンテキストに最大 4096 のスタティック スティッキ エントリを作成できます。

なんらかの理由（プローブ エラー、no inservice コマンド、または ARP タイムアウト）で ACE アプライアンスが実サーバを非稼働状態にした場合、ACE アプライアンスはそのサーバに関連付けられているスティッキ エントリをすべてデータベースから削除します。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ タイプ」（P.7-2）
- 「スティッキ テーブル」（P.7-11）

スティッキ グループの設定

スティッキ（またはセッションの持続性）は、同じクライアントが 1 つのセッション中に、複数の同時 TCP 接続、または後続の複数の TCP 接続を同一サーバとの間で維持できるようにする機能です。ここでの説明で使用する「セッション」とは、クライアントとサーバの間の一定期間（数分から数時間まで）における連続したトランザクションです。スティッキは、オンライン ショッピング、特にショッピング カートの確立やチェックアウト プロセス中など、クライアントが同じサーバとの間で複数の TCP 接続を維持する必要があるような e- コマース アプリケーションに便利な機能です。

このようなスティッキ性が必要とされるのは、e- コマース アプリケーションだけではありません。バンキング アプリケーションやオンライン取引など、クライアントの情報を維持するような Web アプリケーションはスティッキ性を必要とする可能性があります。FTP および HTTP のファイル転送にも、スティッキが使用されます。

ACE アプライアンス ではスティッキ グループの考え方を利用してスティッキ機能を設定します。スティッキ グループを使用することによって、スティッキ属性を指定できます。スティッキ グループとその属性の設定後、そのスティッキ グループを、レイヤ 7 SLB ポリシー マップのレイヤ 7 ポリシー マップ アクションと関連付けます。

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Stickiness] を選択します。[Sticky Groups] テーブルが表示されます。

ステップ 2　[Add] をクリックして新しいスティッキ グループを追加するか、変更するスティッキ グループを選択してから [Edit] をクリックします。

ステップ 3　スティッキ グループの属性を入力します（表 7-1 を参照）。

表 7-1　スティッキ グループの属性

フィールド	説明
Group Name	スティッキ グループの識別子。有効な値は、スペースを含まない引用符抜きの英数字です（最大 64 文字）。
Type	スティッキ接続確立時に使用される方式 • [HTTP Content] : ACE は、HTTP パケットのデータ部分の文字列に基づいて、クライアント接続を同じ実サーバに固定します。設定オプションの詳細については、表 7-2 を参照してください。 • [HTTP Cookie] : ACE アプライアンスは、クライアント要求の HTTP ヘッダーから cookie を学習するか、サーバからクライアントへの応答の Set-Cookie ヘッダーに cookie を挿入し、トランザクションの間、その cookie を使用してクライアントとサーバの間の接続を固定します。 • [HTTP Header] : ACE アプライアンスは HTTP ヘッダーに基づいて、クライアント接続を同じ実サーバに固定します。 • [IP Netmask] : ACE アプライアンスは、トランザクションの完了に必要な場合、IP ネットマスクに基づくクライアントの送信元 IP アドレス、宛先 IP アドレス、またはその両方を使用して、後続の複数の接続に関して、クライアントを同じサーバに固定します。このスティッキ タイプと共に IPv6 プレフィックス長を任意で設定できます。 （注）　クライアントがインターネットに接続している場合、組織がメガプロキシを使用して複数のプロキシ サーバにわたってクライアント要求のロード バランシングを行うときは、送信元 IP アドレスは、要求の本当の送信元であることを示している信頼性の高い指標ではありません。このような場合は、セッションの持続性を確実にするために cookie またはその他のスティッキ方式を使用します。 • [IPv6 Prefix] : ACE アプライアンスは、トランザクションの完了に必要な場合、IPv6 プレフィックスに基づくクライアントの送信元 IP アドレス、宛先 IP アドレス、またはその両方を使用して、後続の複数の接続に関して、クライアントを同じサーバに固定します。このスティッキ タイプと共に IPv4 ネットマスクを任意で設定できます。 • [Layer 4 Payload] : ACE は、レイヤ 4 プロトコル パケットのペイロード部分の文字列に基づいて、クライアント接続を同じ実サーバに固定します。設定オプションの詳細については、表 7-6 を参照してください。 • [RADIUS] : ACE は、RADIUS 属性に基づいて、クライアント接続を同じ実サーバに固定します。設定オプションの詳細については、表 7-7 を参照してください。 • [RTSP Header] : ACE は、RTSP Session ヘッダー フィールドに基づいて、クライアント接続を同じ実サーバに固定します。設定オプションの詳細については、表 7-8 を参照してください。 • [SIP Header] : ACE は、SIP Call-ID ヘッダー フィールドに基づいて、クライアント接続を同じ実サーバに固定します。 • [SSL] : ACE は、SSL セッション ID に基づいて、クライアント接続を同じ実サーバに固定します。 （注）　このオプションは、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）。

表 7-1　スティッキ グループの属性 （続き）

フィールド	説明
Cookie Name	このオプションは、スティッキ タイプの HTTP Cookie に表示されます。 cookie の一意な識別子を入力します。有効な値は、スペースを含まない引用符抜きの英数字です（最大 64 文字）。
Enable Insert	このオプションが表示されるのは、スティッキ タイプが HTTP Cookie の場合だけです。 ACE アプライアンスがサーバからクライアントへの応答の Set-Cookie ヘッダーに cookie を挿入するように設定する場合は、このチェックボックスをオンにします。このオプションが有用なのは、サーバが適切な cookie を設定しない場合にセッション cookie による固定を実行する場合です。このチェックボックスを選択すると、ACE アプライアンスは、クライアントが受信する応答の送信元サーバを識別できるように cookie 値を選択します。同じトランザクションの後続の接続については、クライアントは cookie を使用して同じサーバに固定します。 cookie の挿入をディセーブルにするには、このチェックボックスをクリアします。
Browser Expire	このオプションは、スティッキ タイプの HTTP Cookie で [Enable Insert] を選択したときに表示されます。 セッションの終了時にクライアント ブラウザが cookie を期限切れにできるようにするには、このチェックボックスをオンにします。ブラウザによる期限切れをディセーブルにするには、このチェックボックスをクリアします。
Offset (Bytes)	このオプションは、スティッキ タイプの HTTP Cookie および HTTP ヘッダーに表示されます。 cookie の最初のバイトを始点として、ACE アプライアンスが無視するバイト数を入力します。有効な入力は 0 ～ 999 の整数です。デフォルト値は 0（ゼロ）です。デフォルトの設定では、ACE アプライアンスは cookie のどの部分も除外しません。
Length (Bytes)	このオプションは、スティッキ タイプが HTTP Cookie、HTTP Header、および SSL の場合に表示されます。 ACE アプライアンスがクライアントをサーバに固定するために使用する cookie 部分の長さ（オフセット値の後ろのバイトからの長さ）を入力します。SSL スティッキ タイプの場合は、解析する必要がある SSL セッション ID の長さを入力します。有効な入力は 1 ～ 1000 の整数です。
Secondary Name	このオプションが表示されるのは、スティッキ タイプが HTTP Cookie の場合だけです。 サーバ上の Web ページの URL ストリングに示されている代替 cookie 名を入力します。ACE アプライアンス は、クライアントとサーバのスティッキ接続を維持するためにこの cookie を使用し、スティッキ テーブルにセカンダリ エントリを追加します。有効な入力は、スペースを含まず引用符なしの最大 64 文字です。
Header Name	このオプションは、スティッキ タイプの HTTP ヘッダーに表示されます。 クライアント接続の固定に使用する HTTP ヘッダーを選択します。
IPv4 Netmask	このオプションが表示されるのは、スティッキ タイプが IP Netmask または IPv6 Prefix の場合だけです。このオプションは、スティッキ タイプ IP Netmask の場合は必須、スティッキ タイプ IPv6 Prefix の場合は任意です。 送信元 IP アドレス、宛先 IP アドレス、またはその両方に適用するネットマスクを選択します。
IPv6 Prefix Length	このオプションが表示されるのは、スティッキ タイプが IPv6 Prefix または IP Netmask の場合だけです。このオプションは、スティッキ タイプ IPv6 Prefix の場合は必須、スティッキ タイプ IP Netmask の場合は任意です。 送信元 IP アドレス、宛先 IP アドレス、またはその両方に適用する IPv6 プレフィックス長を入力します。

表 7-1　スティッキ グループの属性 （続き）

フィールド	説明
Address Type	このオプションが表示されるのは、スティッキ タイプが IP Netmask または IPv6 Prefix の場合だけです。 このスティッキ タイプを、クライアントの送信元 IP アドレス、宛先 IP アドレス、またはその両方のいずれに適用するかを指定します。 • [Both]：このスティッキ タイプを送信元 IP アドレスと宛先 IP アドレスの両方に適用します。 • [Destination]：このスティッキ タイプを宛先 IP アドレスにだけ適用します。 • [Source]：このスティッキ タイプを送信元 IP アドレスにだけ適用します。
Enable Sticky For Response	このチェックボックス オプションは、スティッキ タイプが Layer 4 Payload および SSL の場合に表示されます。 ACE がサーバからの応答バイトを解析し、スティッキ ラーニングを実行するよう指示するには、このチェックボックスをオンにします。ACE においてこの操作を実行しない場合は、チェックボックスをオフにします。
Sticky Server Farm	このスティッキ グループに関連付けるサーバ ファームを選択します。
Backup Server Farm	このフィールドは、サーバ ファームを選択した場合に表示されます。 このスティッキ グループに関連付けるバックアップ サーバ ファームを選択します。プライマリ サーバ ファームが停止した場合、ACE アプライアンスはバックアップ サーバ ファームを使用します。
Aggregate State	このフィールドは、サーバ ファームとバックアップ サーバ ファームを選択した場合に表示されます。 バックアップ サーバ ファームの状態を仮想サーバの状態と結合する場合は、このチェックボックスをオンにします。バックアップ サーバ ファームの状態を仮想サーバの状態と結合しない場合は、このチェックボックスの選択を解除します。
Enable Sticky on Backup Server Farm	このフィールドは、サーバ ファームとバックアップ サーバ ファームを選択した場合に表示されます。 バックアップ サーバ ファームをスティッキにする場合は、このチェックボックスをオンにします。バックアップ サーバ ファームをスティッキにしない場合は、このチェックボックスをクリアします。
Buddy Group	このフィールドは、サーバ ファームを選択した場合に表示されます。 サーバ ファームを既存のバディ スティッキ グループに関連付けるか、バディ スティッキ グループを作成します。同じバディ グループに複数のサーバ ファームを関連付けた場合は、要求が異なるサーバ ファームによって処理されると、クライアント要求は同じ実サーバに固定されます。詳細については、「バディ スティッキ グループ」（P.7-6）を参照してください。 **（注）** ACE は SSL または RTSP のスティッキ タイプのバディ グループ機能をサポートしていません。
Replicate on HA Peer	ACE アプライアンスがスタンバイ ACE アプライアンスにスティッキ テーブル エントリを複製するように指定する場合は、このチェックボックスをオンにします。フェールオーバーが発生した場合、このオプションが選択されていれば、新しいアクティブ ACE アプライアンスで既存のスティッキ接続を維持できます。 ACE アプライアンスがスタンバイ ACE アプライアンスにスティッキ テーブル エントリを複製しないように指定する場合は、このチェックボックスの選択を解除します。
Timeout (Minutes)	最後のクライアント接続の終了後、ACE アプライアンスがスティッキ テーブル内のそのクライアント接続のスティッキ情報を維持する時間を分単位で入力します。有効な入力は 1 ～ 65535 の整数で、デフォルトは 1440 分（24 時間）です。

表 7-1　スティッキ グループの属性 （続き）

フィールド	説明
Timeout Active Connections	スティッキ タイマーの満了後、アクティブ接続が存在しても、ACE アプライアンスがスティッキ テーブル エントリをタイムアウトにするように指定する場合は、このチェックボックスをオンにします。 スティッキ タイマーの満了後、アクティブ接続が存在する場合は、ACE アプライアンスがスティッキ テーブル エントリをタイムアウトにしないように指定する場合は、このチェックボックスの選択を解除します。これはデフォルトの動作です。

ステップ 4　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。スティッキ スタティックを設定する場合は、「スティッキ スタティックの設定」（P.7-22）を参照してください。
- [Cancel] をクリックして、エントリを保存せずに手順を終了し、[Sticky Groups] テーブルに戻ります。
- [Next] をクリックして、エントリを保存し、別のスティッキ グループを設定します。

関連トピック

- 「スティッキ スタティックの設定」（P.7-22）
- 「仮想コンテキスト クラス マップの作成」（P.12-9）
- 「仮想コンテキスト ポリシー マップの作成」（P.12-35）
- 「実サーバの設定」（P.6-5）
- 「サーバ ファームの設定」（P.6-18）

スティッキ グループ 属性テーブル

スティッキ グループ タイプ固有の属性を設定する際には、次の各項を参照してください。

- 「HTTP Content スティッキ グループの属性」（P.7-17）
- 「HTTP Cookie スティッキ グループの属性」（P.7-18）
- 「HTTP Header スティッキ グループの属性」（P.7-18）
- 「IP Netmask スティッキ グループの属性」（P.7-19）
- 「Layer 4 Payload スティッキ グループの属性」（P.7-19）
- 「RADIUS スティッキ グループの属性」（P.7-20）
- 「RTSP Header スティッキ グループの属性」（P.7-21）
- 「SSL Header スティッキ グループの属性」（P.7-21）

HTTP Content スティッキ グループの属性

表 7-2　HTTP Content スティッキ グループの属性

フィールド	説明
HTTP Content	HTTP コンテンツは時間の経過とともに変化し、クライアントとサーバ間のトランザクション全体を通じて変化しないのはごくわずかな部分だけです。 ACE が特定サーバに接続を固定するために、HTTP コンテンツの変化しない部分を使用するように設定する場合は、このチェックボックスをオンにします。[Offset]、[Length]、[Begin Pattern]、[End Pattern] のフィールドでスティッキに使用する特定のコンテンツを識別する場合は、このチェックボックスの選択を解除します。
Offset (Bytes)	cookie の 1 番めのバイトから始まっていて仮想サーバが無視するバイト数を入力します。有効な入力は 0 ～ 999 の整数です。デフォルト値は 0（ゼロ）です。デフォルトの設定では、仮想サーバは cookie のどの部分も除外しません。
Length (Bytes)	ACE がクライアントをサーバに固定するために使用する cookie 部分の長さ（オフセット値の後ろのバイトからの長さ）を入力します。有効な入力は 1 ～ 1000 の整数です。
Begin Pattern	HTTP コンテンツ ペイロードの開始パターンと、ハッシュを行う前に照合するパターン文字列を入力します。開始パターンを指定しない場合、ACE はオフセット バイトの直後に解析を開始します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません 有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ストリング全体を引用符（"）で囲むことによって、スペースを含むテキスト文字列を入力することもできます。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。
End Pattern	ハッシュの終点を示すパターンを入力します。終了パターンまたは長さを指定しない場合、ACE はフィールドまたはパケットの終了に到達するか、あるいは最大本体解析長に到達するまでデータの解析を継続します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません 有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ストリング全体を引用符（"）で囲むことによって、スペースを含むテキスト文字列を入力することもできます。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。

HTTP Cookie スティッキ グループの属性

表 7-3　HTTP Cookie スティッキ グループの属性

フィールド	説明
Cookie Name	cookie の一意な識別子を入力します。有効な値は、スペースを含まない引用符抜きの英数字です（最大 64 文字）。
Enable Insert	仮想サーバが、サーバからクライアントへの応答の Set-Cookie ヘッダーに cookie を挿入するようにするには、このチェックボックスをオンにします。このオプションが有用なのは、サーバが適切な cookie を設定しない場合にセッション cookie による固定を実行する場合です。このチェックボックスを選択すると、サーバは、クライアントが受信する応答の送信元サーバを特定する cookie 値を選択します。同じトランザクションの後続の接続については、クライアントは cookie を使用して同じサーバに固定します。 cookie 挿入をディセーブルにする場合は、このチェックボックスの選択を解除します。
Browser Expire	このオプションは、スティッキ タイプの HTTP Cookie で [Enable Insert] を選択したときに表示されます。 セッションの終了時にクライアント ブラウザが cookie を期限切れにできるようにするには、このチェックボックスをオンにします。ブラウザによる期限切れをディセーブルにするには、このチェックボックスをクリアします。
Offset (Bytes)	cookie の 1 番めのバイトから始まっていて仮想サーバが無視するバイト数を入力します。有効な入力は 0 ～ 999 の整数です。デフォルト値は 0（ゼロ）です。デフォルトの設定では、仮想サーバは cookie のどの部分も除外しません。
Length (Bytes)	ACE がクライアントをサーバに固定するために使用する cookie 部分の長さ（オフセット値の後ろのバイトからの長さ）を入力します。有効な入力は 1 ～ 1000 の整数です。
Secondary Name	サーバ上の Web ページの URL ストリングに示されている代替 cookie 名を入力します。仮想サーバは、クライアントとサーバの間のスティッキ接続を維持するためにこの cookie を使用し、スティッキ テーブルにセカンダリ エントリを追加します。有効な入力は、スペースを含まず引用符なしの最大 64 文字です。

HTTP Header スティッキ グループの属性

表 7-4　HTTP Header スティッキ グループの属性

フィールド	説明
Header Name	クライアント接続の固定に使用する HTTP ヘッダーを選択します。
Offset (Bytes)	cookie の 1 番めのバイトから始まっていて仮想サーバが無視するバイト数を入力します。有効な入力は 0 ～ 999 の整数です。デフォルト値は 0（ゼロ）です。デフォルトの設定では、仮想サーバは cookie のどの部分も除外しません。
Length (Bytes)	ACE がクライアントをサーバに固定するために使用する cookie 部分の長さ（オフセット値の後ろのバイトからの長さ）を入力します。有効な入力は 1 ～ 1000 の整数です。

IP Netmask スティッキ グループの属性

表 7-5　IP Netmask スティッキ グループの属性

フィールド	説明
Netmask	送信元 IP アドレス、宛先 IP アドレス、またはその両方に適用するネットマスクを選択します。
Address Type	このスティッキ タイプを、クライアントの送信元 IP アドレス、宛先 IP アドレス、またはその両方のいずれに適用するかを指定します。 • [Both]: 送信元 IP アドレスと宛先 IP アドレスの両方にこのスティッキ タイプが適用されます。 • [Destination]：このスティッキ タイプは、宛先 IP アドレスだけに適用されます。 • [Source]：このスティッキ タイプは、送信元 IP アドレスだけに適用されます。

Layer 4 Payload スティッキ グループの属性

表 7-6　Layer 4 Payload スティッキ グループの属性

フィールド	説明
Offset (Bytes)	cookie の 1 番めのバイトから始まっていて仮想サーバが無視するバイト数を入力します。有効な入力は 0 ～ 999 の整数です。デフォルト値は 0（ゼロ）です。デフォルトの設定では、仮想サーバは cookie のどの部分も除外しません。
Length (Bytes)	ACE がクライアントをサーバに固定するために使用する cookie 部分の長さ（オフセット値の後ろのバイトからの長さ）を入力します。有効な入力は 1 ～ 1000 の整数です。
Begin Pattern	レイヤ 4 ペイロードの開始パターンと、ハッシュを行う前に照合するパターン文字列を入力します。開始パターンを指定しない場合、ACE はオフセット バイトの直後に解析を開始します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません 有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ストリング全体を引用符（"）で囲むことによって、スペースを含むテキスト文字列を入力することもできます。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。

表 7-6　Layer 4 Payload スティッキ グループの属性 （続き）

フィールド	説明
End Pattern	ハッシュの終点を示すパターンを入力します。終了パターンまたは長さを指定しない場合、ACE はフィールドまたはパケットの終了に到達するか、あるいは最大本体解析長に到達するまでデータの解析を継続します。同じトラフィック分類に属する異なるサーバ ファームには、異なる開始パターンと終了パターンを設定できません 有効な値は、スペースを含まない引用符抜きの英数字です（最大 255 文字）。ストリング全体を引用符（"）で囲むことによって、スペースを含むテキスト文字列を入力することもできます。ACE は、文字列式の一致条件に正規表現をサポートしています。表 12-33 は、文字列式の照合に使用できるサポート対象文字の一覧です。
Enable Sticky For Response	ACE でサーバ応答を解析し、スティッキ学習を実行できるようにするには、このチェックボックスをオンにします。ACE は、スティッキ データベースにデータを入力するために、サーバ応答バイトのハッシュを使用します。次に、ACE がこれらと同じバイトを持つクライアント要求を受信したときに、このクライアントは同じサーバに固定されます。 ACE の動作をリセットして、サーバ応答の解析とスティッキ学習が行われないようにする（デフォルト）には、このチェックボックスをオフにします。

RADIUS スティッキ グループの属性

表 7-7　RADIUS スティッキ グループの属性

フィールド	説明
RADIUS Types	クライアント接続の固定に使用する RADIUS 属性を選択します。 • [N/A]：このオプションは設定されません。 • [RADIUS Calling ID]：RADIUS フレーム化 IP 属性および発信側ステーション ID 属性に基づいてスティッキ機能が実行されます。 • [RADIUS User Name]：RADIUS フレーム化 IP 属性およびユーザ名属性に基づいてスティッキ機能が実行されます。
Enter User IPv6Prefix Length	IPv6 RADIUS 属性を使用する場合に、IPv6 エンド ユーザ パケットの IPv6 プレフィックスの長さを入力します。IPv6 を使用した RADIUS フレーム化 IP スティッキの場合、スティッキ エントリは、RADIUS パケット内のフレーム化された IPv6 プレフィックスおよび IPv6 プレフィックス長に基づきます。エンド ユーザ パケットのスティッキ ルックアップの一致するプレフィックス長を使用してください。 1 ～ 128 のプレフィックス長を入力します。デフォルトは 64 です。
Wait For Acknowledgement	アカウンティング開始が応答を受信しない場合に、フレーム化 IP スティッキ エントリ（スティッキ エントリの実サーバを除く）にヒットする RADIUS 要求のリロード バランシングを行うように ACE を設定するには、このチェックボックスをオンにします。この機能は、アカウンティング フェーズ中にスティッキ エントリが作成される場合のために設計されています。 確認応答のための待機を使用しないように ACE を設定するには、このチェックボックスをオフにします。

RTSP Header スティッキ グループの属性

表 7-8　RTSP Header スティッキ グループの属性

フィールド	説明
Offset (Bytes)	cookie の 1 番めのバイトから始まっていて仮想サーバが無視するバイト数を入力します。有効な入力は 0 ～ 999 の整数です。デフォルト値は 0（ゼロ）です。デフォルトの設定では、仮想サーバは cookie のどの部分も除外しません。
Length (Bytes)	ACE がクライアントをサーバに固定するために使用する cookie 部分の長さ（オフセット値の後ろのバイトからの長さ）を入力します。有効な入力は 1 ～ 1000 の整数です。

SSL Header スティッキ グループの属性

表 7-9　SSL スティッキ グループの属性

フィールド	説明
Enable Sticky For Response	ACE がサーバからの応答バイトを解析し、スティッキ ラーニングを実行するよう指示するには、このチェックボックスをオンにします。ACE においてこの操作を実行しない場合は、チェックボックスをオフにします。
Length (Bytes)	解析する必要がある SSL セッション ID の長さ。有効な入力は 1 ～ 1000 の整数です。

Viewing All Sticky Groups by Context

特定の仮想コンテキストに関連付けられているすべてのスティッキ グループを表示するには、次の手順を行います。

手順

ステップ 1　[Config] > [Virtual Contexts] を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　表示するスティッキ グループが関連付けられている仮想コンテキストを選択し、[Load Balancing] > [Stickiness] をクリックします。[Sticky Groups] テーブルが表示され、選択したコンテキストに関連付けられているスティッキ グループが表示されます。

関連トピック

- 「スティッキ グループの設定」（P.7-12）
- 「スティッキ スタティックの設定」（P.7-22）

スティッキ スタティックの設定

スティッキ スタティックを設定するには、次の手順を行います。

前提

スティッキ グループが設定されている必要があります。詳細については、「スティッキ グループの設定」（P.7-12）を参照してください。

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Stickiness] を選択します。[Sticky Groups] テーブルが表示されます。

ステップ 2　スティッキ スタティックを設定するスティッキ グループを選択し、[Sticky Statics] タブを選択します。[Sticky Groups] テーブルの下に [Sticky Statics] タブが表示されない場合は、[Switch between Configure and Browse Modes] ボタンをクリックしてください。

ステップ 3　[Add] をクリックしてテーブルに新しいエントリを追加するか、既存のエントリを選択してから [Edit] をクリックして、そのエントリを変更します。[Sticky Statics] 設定画面が表示されます。

ステップ 4　[Sequence Number] フィールドで、このエントリの自動増分番号を受け入れるか、新しいシーケンス番号を入力します。このシーケンス番号は、複数のスティッキ スタティック設定の適用順序を示します。

ステップ 5　[Type] フィールドで、正しいスティッキ グループ タイプが選択されていることを確認します。複数のスティッキ グループを選択していて、新しいスタティック スティッキ エントリを作成する場合は、表 7-10 に示すように、使用するスティッキ グループ タイプを選択します。

表 7-10　スティッキ グループのタイプ

スティッキ グループ	説明
HTTP Content	ACE アプライアンスは HTTP パケットのコンテンツに基づいてクライアントをサーバに固定することを示します。開始パターンと終了パターン、解析するバイト数、データの始点から無視するバイト数を指定するオフセットを指定できます。
HTTP Cookie	ACE アプライアンスは、クライアント要求の HTTP ヘッダーから cookie を学習するか、サーバからクライアントへの応答の Set-Cookie ヘッダーに cookie を挿入し、トランザクションの間、その cookie を使用してクライアントとサーバの間の接続を固定することを示します。
HTTP Header	ACE アプライアンスは HTTP ヘッダーに基づいて、クライアント接続を同じ実サーバに固定することを示します。
IP Netmask	ACE アプライアンスは、トランザクションの完了に必要な場合、IPv4 ネットマスクに基づくクライアントの送信元 IP アドレス、宛先 IP アドレス、またはその両方を使用して、後続の複数の接続に関して、クライアントを同じサーバに固定します。このスティッキ タイプと共に IPv6 プレフィックス長を任意で設定できます。 **（注）**　クライアントがインターネットに接続している場合、組織がメガプロキシを使用して複数のプロキシ サーバにわたってクライアント要求のロード バランシングを行うときは、送信元 IP アドレスは、要求の本当の送信元であることを示している信頼性の高い指標ではありません。このような場合は、セッションの持続性を確実にするために cookie またはその他のスティッキ方式を使用します。

表 7-10　スティッキ グループのタイプ （続き）

スティッキ グループ	説明
IPv6 Prefix	ACE アプライアンスは、トランザクションの完了に必要な場合、IPv6 プレフィックス長に基づくクライアントの送信元 IP アドレス、宛先 IP アドレス、またはその両方を使用して、後続の複数の接続に関して、クライアントを同じサーバに固定します。このスティッキ タイプと共に IPv4 ネットマスクを任意で設定できます。
Layer 4 Payload	ACE アプライアンスは、レイヤ 4 フレームのデータに基づいてクライアントをサーバに固定することを示します。開始パターンと終了パターン、解析するバイト数、データの始点から無視するバイト数を指定するオフセットを指定できます。
RADIUS	ACE アプライアンスは、クライアント接続の固定に、RADIUS 属性（発信側ステーション ID またはユーザ名）を使用することを示します。
RTSP Header	ACE アプライアンスは RTSP セッション ヘッダー内の情報に基づいて、クライアント接続を固定することを示します。RTSP ヘッダー スティッキ方式では、ヘッダーのオフセットを指定して、RTSP ヘッダーの一意の部分に基づいてスティッキを提供できます。
SIP Header	ACE アプライアンスは SIP Call-ID ヘッダー フィールドに基づいて、クライアント接続を固定することを示します。SIP ヘッダー スティッキ方式では、SIP ヘッダー全体が必要であるため、オフセットは指定できません。

ステップ 6　[HTTP Cookie]、[HTTP Header]、[HTTP Content]、[Layer 4 Payload]、[RTSP Header]、または [SIP Header] のいずれかのスティッキ タイプを選択した場合、[Static Value] フィールドに cookie ストリング値を入力します。有効な入力は、引用符なしの最大 255 文字の英数字です。文字列にスペースが含まれている場合は、文字列を引用符で囲みます。

ステップ 7　スティッキ タイプとして [IP Netmask] または [IPv6 Prefix] を選択する場合

a.　[IP Address Type] で、[IPv4] または [IPv6] を選択します。

b.　[Static Source] フィールドに、クライアントの送信元 IP アドレスを入力します。

c.　[Static Destination] フィールドに、クライアントの宛先 IP アドレスを入力します。

ステップ 8　[Named Real Server] フィールドで、このスタティック スティッキ エントリに関連付ける実サーバを選択します。

ステップ 9　Port フィールドに、実サーバのポート番号を入力します。有効な入力は 1 ～ 65535 の整数です。

ステップ 10　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- [Cancel] をクリックして、エントリを保存せずに手順を終了し、[Sticky Statics] テーブルに戻ります。
- [Next] をクリックして、エントリを保存し、別のスティッキ スタティック エントリを設定します。

関連項目

「スティッキ グループの設定」（P.7-12）