CHAPTER 5

仮想サーバの設定

この章では、サーバ ロード バランシングの概要、および ACE アプライアンス上でのロード バランシング用に仮想サーバを構成するための手順について説明します。

（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。

この章は、次の内容で構成されています。

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 ページを求める HTTP GET またはファイルのダウンロードを求める FTP GET から構成することができます。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。

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 アプライアンス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 アプライアンスは、負荷に対して接続数が最小のサーバ、送信元または宛先アドレス、cookie、URL、HTTP ヘッダーなど、いくつかの要因に基づいてサーバを選択します。

ACE アプライアンス Device Manager では、次のトピックで説明するように、ロード バランシングを設定できます。

- 仮想サーバ：「仮想サーバの設定」（P.5-2）を参照してください。
- 実サーバ：「実サーバの設定」（P.6-5）を参照してください。
- サーバ ファーム：「サーバ ファームの設定」（P.6-18）を参照してください。

- スティッキ グループ：「スティッキ グループの設定」（P.7-12）を参照してください。
- パラメータ マップ：「パラメータ マップの設定」（P.8-1）を参照してください。

ACE アプライアンスによって設定および実行される SLB の詳細については、次のトピックを参照してください。

- 「仮想サーバの設定」（P.5-2）
- 「ロード バランシング プレディクタ」（P.6-2）
- 「実サーバ」（P.6-3）
- 「サーバ ファーム」（P.6-5）
- 「ヘルス モニタリングの設定」（P.6-38）
- 「TCL スクリプト」（P.6-39）
- 「スティッキ グループの設定」（P.7-12）

仮想サーバの設定

ロード バランシング環境では、仮想サーバは、複数の物理サーバをロード バランシング用の 1 つのサーバに見えるようにする構成要素です。仮想サーバは、サーバ ファーム内の実サーバ上で稼働する物理サービスに結合されており、IP アドレスとポート情報を使用して、指定のロード バランシング アルゴリズムに従い、着信クライアント要求をサーバ ファーム内のサーバに分散します。

クラス マップを使用して、仮想サーバのアドレスおよび定義を設定します。ロード バランシング プレディクタ アルゴリズム（ラウンドロビンや最小接続など）は、ACE の接続要求の送信先のサーバを決定します。

仮想サーバおよび ACE アプライアンス Device Manager の詳細については、次のトピックを参照してください。

- 「仮想サーバの設定および ACE アプライアンス Device Manager の理解」（P.5-2）
- 「Device Manager を使用した仮想サーバの設定に関する情報」（P.5-5）
- 「仮想サーバの設定手順」（P.5-7）

仮想サーバの設定および ACE アプライアンス Device Manager の理解

ACE アプライアンス Device Manager Virtual Server コンフィギュレーション インターフェイスであるモジュラ ポリシー CLI（コマンドライン インターフェイス）の抽象化は、機能ロード バランシング環境の設定および配置を簡素化し、並べ替え、さらにアトミックにします。簡素化または抽象化によって、いくつかの制約または制限が必ず伴います。ここでは、仮想サーバ設定用に ACE アプライアンス Device Manager によって使用される制約およびフレームワークについて説明します。

ACE アプライアンス Device Manager では、存続可能な仮想サーバは次の属性を備えています。

- 1 つのレイヤ 3/ レイヤ 4 の一致条件

  これは、1 つのポート（またはポート範囲）とともに指定できるのは 1 つの IP アドレス（または IPv4 ネットマスクまたは IPv6 プレフィックス長が使用されている場合は 1 つの IP アドレス範囲）だけであるということです。一致条件が 1 つということにより、仮想サーバの設定が大幅に簡素化され、促進されます。
- デフォルトのレイヤ 7 アクション
- レイヤ 7 ポリシー マップ

- レイヤ 3/ レイヤ 4 クラス マップ
- マルチマッチ ポリシー マップ、クラスマップ一致、およびアクション

また、次の点に注意してください。

- 仮想サーバのマルチマッチ ポリシー マップは、インターフェイスに関連付けられているか、またはグローバルです。
- 仮想サーバの名前は、レイヤ 3/ レイヤ 4 クラス マップの名前から派生しています。

例 5-1 に、仮想サーバに必要な最小設定文を示します。

例 5-1　　仮想サーバに必要な最小設定

IPv4

```
class-map match-all Example_VIP
   2 match virtual-address 10.10.10.10 tcp eq www
policy-map type loadbalance first-match Example_VIP-l7slb
   class class-default
      forward
policy-map multi-match int10
   class Example_VIP
      loadbalance policy Example_VIP-l7slb

interface vlan 10
   ip address 192.168.65.37 255.255.255.0
   service-policy input int10
   no shutdown
```

IPv6

```
class-map match-all Example2_VIP
   2 match virtual-address 2001:DB8:10::5 tcp eq www
policy-map type loadbalance first-match Example2_VIP-l7slb
   class class-default
      forward
policy-map multi-match int11
   class Example2_VIP
      loadbalance policy Example2_VIP-l7slb

interface vlan 10
   ip address 2001:DB8:10::21/64
   service-policy input int11
   no shutdown
```

ACE アプライアンス Device Manager および仮想サーバに関する次の項目にも注意してください。

- 追加の設定オプション

  [Virtual Server] 設定画面では、機能バーチャル IP（VIP）用の追加項目を設定できます。これらの項目には、サーバ ファーム、スティッキ グループ、実サーバ、プローブ、パラメータ マップ、インスペクション、クラス マップ、インライン一致条件などがあります。項目が多すぎると画面に収まらないことがあるため、スティッキ統計情報やバックアップ実サーバなど、すべての設定オプションが [Virtual Server] 設定画面に表示されるわけではありません。これらのオプションは、[Virtual Server] 設定画面の代わりに、ACE アプライアンス Device Manager インターフェイスの他の箇所で利用できます。

- 設定オプションおよびロール

  ロールの分離をサポートおよび維持するために、一部のオブジェクトは、[Virtual Server] 設定画面からは設定できません。これらのオブジェクトには、SSL 認証、SSL キー、ネットワーク アドレス変換（NAT）プール、インターフェイス IP アドレス、ACL などがあります。ACE アプライアンス Device Manager インターフェイスでこれらの設定オプションを別のオプションとして提示することにより、仮想サーバまたは仮想サーバの各面を表示または変更できるユーザは、仮想サーバの作成または削除ができなくなります。

- RBAC ロールおよびドメイン要件

  仮想サーバを作成、修正、または削除する場合、事前に定義されている Admin ロールを使用することをお勧めします（表 15-4 を参照してください）。事前に定義されている Admin ロールを使用した場合だけ、ACE appliance Device Manager から機能仮想サーバを正常に配置できます。

  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。

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。

背景説明については、第 15 章「ACE アプライアンスの管理」の「ユーザ ロールの管理」の項を参照してください。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「Device Manager を使用した仮想サーバの設定に関する情報」（P.5-5）
- 「仮想サーバの設定手順」（P.5-7）

Device Manager を使用した仮想サーバの設定に関する情報

ACE アプライアンス Device Manager を使用して仮想サーバを設定する場合、次のことを理解することが重要です。

- **[Virtual Server] 設定画面**

  ACE アプライアンス Device Manager の [Virtual Server] 設定画面は、選択に関連する設定オプションを提示することによって仮想サーバの設定を支援するように設計されています。たとえば、Properties 設定サブセットで選択するプロトコルによって、表示される他の設定サブセットが決まります。

- **適した仮想サーバ設定方式の使用**

  ACE アプライアンス Device Manager の [Virtual Server] 設定画面では、最も使用されそうなオプションを表示することによって、仮想サーバの作成、変更、および配置プロセスを簡素化しています。また、プロトコルなど、仮想サーバの属性を指定するときに、インターフェイスは、プロトコル インスペクション、アプリケーション アクセラレーション、最適化など関連の設定オプションによってリフレッシュされることにより、仮想サーバの設定および配置の時間が短縮されます。

  [Virtual Server] 設定画面では一部の設定の複雑さは解消されていますが、この画面には [Expert] 設定オプションにはないいくつかの制約があります。CLI を使い慣れている場合は、[Expert] オプション（[Config] > [Virtual Contexts] > [*context*] > [Expert] > [Class Maps or Policy] または [Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Parameter Map] など）を使用すると、仮想サーバの複雑な属性、トラフィック ポリシー、およびパラメータ マップを設定できます。

- **仮想サーバ設定の同期化**

  CLI を使用して、ACE アプライアンスの仮想コンテキストの設定を変更する場合、ACE アプライアンス Device Manager は定期的に CLI に対してポーリングを行い（約 2 分間に 1 回）、設定の変更がないかどうかを調べます。コンテキスト内でアウトオブバンド設定変更が検出されると、変更は、ACE アプライアンス Device Manager によって維持されている設定に適用されます。ACE アプライアンス Device Manager の下部にあるステータス バーは、各種の同期化状態にあるコンテキストの概略数を示しています。

  CLI を使用して仮想サーバを設定し、[CLI Sync] オプション（[Config] > [Virtual Contexts] > [CLI Sync]）を使用して設定を手動で同期化する場合、仮想サーバ用の ACE アプライアンス Device Manager に表示される設定には、この仮想サーバ用のすべての設定オプションが表示されるわけではありません。ACE アプライアンス Device Manager に表示される設定は、クラス マップに設定されているプロトコルやポリシー マップに定義されているルールなど項目によって異なります。

  たとえば、どのプロトコルにも一致するクラス マップを含む仮想サーバを CLI で設定する場合、仮想サーバの Application Acceleration and Optimization 設定サブセットは、ACE アプライアンス Device Manager には表示されません。

- **共有オブジェクトの変更**

  サーバ ファーム、実サーバ、パラメータ マップなど複数の仮想サーバで使用されているオブジェクトを変更すると、他の仮想サーバに影響を与えることがあります。複数の仮想サーバで使用されているオブジェクトの変更については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバの設定および ACE アプライアンス Device Manager の理解」（P.5-2）
- 「仮想サーバの設定手順」（P.5-7）

仮想サーバ使用上のガイドライン

[Virtual Server] 設定ウィンドウでは、多くの設定オプションが提供されます。ただし、1 本のパスのすべてのオプションを設定する代わりに、ステージの仮想サーバを設定します。最初のステージは、単純なロード バランシングの基本的な「パススルー」接続を確立し、最小限の追加機能を含むようにする必要があります。セット アップのこのレベルでは、ポート、VLAN、インターフェイス、SSL 終了（該当する場合）、および実サーバが正しく設定されていることを確認し、基本的な接続をイネーブルにします。

このレベルの接続を確立すると、追加の仮想サーバ機能の設定およびトラブルシューティングが容易になります。

動作する基本的な仮想サーバに追加する一般的な機能は次のとおりです。

- ヘルス モニタリング プローブ
- セッションの持続性（スティッキ）
- サーバ ファームへの追加実サーバ
- アプリケーション プロトコル インスペクション
- アプリケーション アクセラレーションおよび最適化

表 5-1 に、設定情報用の関連項目へのリンクが設定されている、仮想サーバの設定サブセットを示します。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「Device Manager を使用した仮想サーバの設定に関する情報」（P.5-5）
- 「仮想サーバのテストとトラブルシューティング」（P.5-6）
- 「仮想サーバの設定手順」（P.5-7）

仮想サーバのテストとトラブルシューティング

「仮想サーバ使用上のガイドライン」（P.5-6）に説明されているように、2 台の実サーバ間のラウンドロビンなど、接続および単純ロード バランシングのみをイネーブルにする基本的な仮想サーバを最初にセット アップします。次に、ネットワーク クライアントから仮想サーバ VIP アドレスに要求を送信するためにクライアント（Web ブラウザなど）を使用します。要求が成功した場合、変更を加えたり、仮想サーバ機能を追加したりできます。

要求が成功しない場合、次の手順に説明する仮想サーバのトラブルシューティングを開始します。

1. 特に既存の ACE の設定が大きい場合は、1 ～ 2 分待ち、要求を再度実行してください。トラフィックが ACE で処理方法に影響を与えるような設定変更の場合は数秒または数分かかることがあります。
2. [Virtual Server] ページの右下の [Details] ボタンをクリックします。[Details] ボタンは、**show service-policy** の CLI コマンドの出力を表示します。
3. **show service-policy** の CLI コマンド出力の VIP 状態が INSERVICE であることを確認します。VIP 状態が INSERVICE でない場合は、次の内容を示す可能性があります。
   - 仮想サーバは、設定中に手動で無効にされました。
   - 実サーバはすべて ACE から到達不能または手動でディセーブルになりました。仮想サーバのすべての実サーバがそれらの原因の 1 つにより停止状態の場合は、仮想サーバ自体が Out Of Service とマークされます。

4. **show service-policy** の CLI コマンド出力で Hit Count を確認します。Hit Count は、ACE で受信された要求の数を示します。この値は、クライアントによる要求ごとに増加する必要があります。ヒット カウントが要求ごとに増加していない場合は、要求が仮想サーバ設定に到達していないことを示します。

   これは、次のいずれかの問題である可能性があります。

   - 物理接続。
   - VLAN または VLAN インターフェイスの設定。
   - 欠落していたり不適切な ACL がクライアント インターフェイスに適用されている。
   - 不正な IP アドレス（仮想サーバ用に選択した VLAN で無効な VIP、またはクライアントにはアクセスできない VIP）。

   Hit Count 値は増加するが応答を受信しない（Server Pkt Count が増加しない）場合、問題は ACE とバック エンドの実サーバ間の接続にある場合が多いです。この問題は、通常、次の問題の 1 つまたは複数が原因となります。

   - ワンアーム型構成（つまり、実サーバのルーティングを変更することを計画しない）で作業し、仮想サーバが送信元 NAT で使用できるよう、適切な NAT プールを選択しなかった。
   - 別のルーティングの問題（たとえば、サーバ トラフィックが ACE に戻る方法を認識しない）。
   - アドレス指定の問題（たとえば、不正な実サーバ アドレス、あるいはネットワーク トポロジにより実サーバが ACE にアクセスできない）。

（注） 一般的な Web ページを取得するには、クライアントからサーバに多くのリクエストをするため、Web ブラウザから 1 つの要求だけを行っても、ヒット カウントは、1 つ以上増加します。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「Device Manager を使用した仮想サーバの設定に関する情報」（P.5-5）
- 「仮想サーバ使用上のガイドライン」（P.5-6）
- 「仮想サーバの設定手順」（P.5-7）

仮想サーバの設定手順

仮想サーバをロード バランシング用に ACE アプライアンス Device Manager に追加するには、次の手順を使用します。

前提

- 仮想サーバに使用するプロトコルに応じて、パラメータ マップを定義しておく必要があります。
- SSL サービスのために、SSL 認証、キー、チェーン グループ、およびパラメータ マップを設定しておく必要があります。

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Virtual Servers] を選択します。

[Virtual Servers] 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仮想サーバを追加するか、または既存の仮想サーバを選択して [Edit] をクリックし、その仮想サーバを変更します。

[Virtual Server] 設定画面が表示され、数多くの設定サブセットが表示されます。表示されるサブセットは、[Basic View] または [Advanced View] のいずれを使用しているかにより、また、Properties サブセットで行っている設定エントリによって異なります。設定ペインの上部にある View オブジェクト セレクタを使用して、ビューを変更します。

表 5-1 に、設定情報用の関連項目へのリンクが設定されている、仮想サーバの設定サブセットを示します。

表 5-1　仮想サーバの設定サブセット

設定サブセット	説明	関連トピック
Properties	このサブセットでは、仮想サーバ名、IP アドレス、プロトコル、ポート、Virtual LAN（VLAN）など、仮想サーバの基本特性を指定できます。	「仮想サーバのプロパティの設定」（P.5-11）
[1]SSL Termination	このサブセットは、TCP が選択されたプロトコルであり、Other または HTTPS がアプリケーション プロトコルの場合に表示されます。 このサブセットでは、仮想サーバを SSL プロキシ サーバとして動作させ、SSL プロキシ サーバとそのクライアントとの SSL セッションを終了させるように設定することができます。	「仮想サーバの SSL 終了の設定」（P.5-19）
Protocol Inspection	このサブセットは、次の [Advanced View] に表示されます。 • FTP、HTTP、HTTPS、RTSP、または SIP とともに使用する場合の TCP • DNS または SIP とともに使用する場合の UDP このサブセットは、FTP とともに使用する場合の TCP の [Basic View] に表示されます。 このサブセットでは、仮想サーバを設定して、プロトコルの動作を確認し、選択したアプリケーション プロトコル上で ACE アプライアンスを通過する不要なまたは悪意のあるトラフィックを特定することができます。	「仮想サーバのプロトコル インスペクションの設定」（P.5-21）
L7 Load-Balancing	このサブセットは、次の [Advanced View] のみに表示されます。 • Generic、HTTP、HTTPS、RTSP、または SIP とともに使用する場合の TCP • Generic、RADIUS、または SIP とともに使用する場合の UDP このサブセットでは、SSL 開始など、レイヤ 7 ロードバランシング オプションを設定できます[1]。	「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）

表 5-1　仮想サーバの設定サブセット （続き）

設定サブセット	説明	関連トピック
Default L7 Load-Balancing Action	このサブセットでは、指定した一致条件に一致しないすべてのネットワーク トラフィックに対して、デフォルトのレイヤ 7 ロード バランシング動作を確立できます。 また、SSL 開始を設定することもできます[1]。SSL 開始は、[Advanced View] にだけ表示されます。	「仮想サーバのデフォルトのレイヤ 7 ロード バランシングの設定」（P.5-56）
Application Acceleration And Optimization	このサブセットは、HTTP または HTTPS が選択したアプリケーション プロトコルになっている場合に、[Advanced View] にだけ表示されます。 このサブセットでは、HTTP または HTTPS トラフィック用のアプリケーション アクセラレーションおよび最適化オプションを設定できます。	「アプリケーション アクセラレーションおよび最適化の設定」（P.5-59）
NAT	このサブセットは、[Advanced View] にだけ表示されます。 このサブセットでは、仮想サーバ用に Network Address Translation（NAT）を設定できます。	「仮想サーバ NAT の設定」（P.5-63）

1. SSL 開始と終了の設定オプションは、ACE NPE のソフトウェア バージョンに適用されません（「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）。

ステップ 3　仮想サーバのプロパティの設定が完了したら、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適用します。
- [Cancel] をクリックすると、エントリを保存しないで手順を終了し、[Virtual Servers] テーブルに戻ります。

ステップ 4　（任意）既存の仮想サーバの統計情報とステータス情報を表示するには、[Virtual Servers] テーブルで仮想サーバを選択し、[Details] をクリックします。

詳細な仮想サーバ情報を表示するポップアップ ウィンドウが表示されます（「仮想サーバの統計情報およびステータス情報の表示」（P.5-64）を参照）。

（注）　この機能は、ACE ソフトウェア バージョン A3（2.1）以降が必要です。以前のソフトウェア バージョンを使用するとエラーが表示されます。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバの設定および ACE アプライアンス Device Manager の理解」（P.5-2）
- 「Device Manager を使用した仮想サーバの設定に関する情報」（P.5-5）
- 「共有およびオブジェクト仮想サーバ」（P.5-10）
- 「ACE アプライアンス Device Manager でのロール マッピング」（P.15-20）

共有およびオブジェクト仮想サーバ

共有オブジェクトとは、複数の仮想サーバによって使用されるオブジェクトのことです。共有オブジェクトの例は、次のとおりです。

- アクション リスト
- クラス マップ
- パラメータ マップ
- 実サーバ
- サーバ ファーム
- SSL サービス
- スティッキ グループ

これらのオブジェクトは共有されるため、1 つの仮想サーバでオブジェクトの設定を変更すると、このオブジェクトを使用している他の仮想サーバに影響することがあります。

共有オブジェクトの設定

ACE アプライアンス Device Manager は、Virtual Server 設定画面に共有オブジェクト用の次のオプションを備えています（[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Virtual Servers]）。

- [View]：オブジェクトの設定を確認する場合に [View] をクリックします。画面がリフレッシュされ、読み取り専用フィールドと次の 3 つのボタンが表示されます。
- [Cancel]：読み取り専用ビューを閉じ、前の画面に戻る場合に [Cancel] をクリックします。
- [Edit]：選択したオブジェクトの設定を変更する場合に [Edit] をクリックします。画面がリフレッシュされ、読み取り専用のままの [Name] フィールド以外のフィールドが変更可能として表示されます。

（注） 共有オブジェクトの設定を変更する前に、同じオブジェクトを使用している他の仮想サーバにもたらされる変更の影響について理解してください。別の手段としては、[Duplicate] オプションの使用を検討してください。

- [Duplicate]：選択したオブジェクトと同じ設定を持つ新しいオブジェクトを作成する場合に、[Duplicate] をクリックします。画面がリフレッシュされて、設定可能なフィールドが表示されます。[Name] フィールドに新しいオブジェクトの一意の名前を入力し、目的どおりに設定を変更します。このオプションでは、同じオブジェクトを使用している他の仮想サーバに影響を与えずに新しいオブジェクトを作成することができます。

共有オブジェクトを備えた仮想サーバの削除

仮想サーバを作成し、その設定に共有オブジェクトを含める場合は、仮想サーバを削除しても、関連付けられた共有オブジェクトは削除されません。これにより、同じ共有オブジェクトを使用している他の仮想サーバに影響はありません。

関連トピック

- 「仮想サーバの管理」（P.5-65）
- 「仮想サーバのプロパティの設定」（P.5-11）
- 「仮想サーバの SSL 終了の設定」（P.5-19）
- 「仮想サーバのプロトコル インスペクションの設定」（P.5-21）

- 「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）
- 「仮想サーバのデフォルトのレイヤ 7 ロード バランシングの設定」（P.5-56）
- 「アプリケーション アクセラレーションおよび最適化の設定」（P.5-59）

仮想サーバのプロパティの設定

仮想サーバのプロパティを設定するには、次の手順を使用します。

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Virtual Servers] を選択します。[Virtual Servers] 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仮想サーバを追加するか、または既存の仮想サーバを選択して [Edit] をクリックし、その仮想サーバを変更します。[Virtual Server] 設定画面が表示されます。[Properties] 設定サブセットはデフォルトで開いています。

[Properties] 設定サブセットに表示されるフィールドは、[Advanced View] または [Basic View] のいずれを使用しているかによって異なります。

- [Advanced View] プロパティを設定するには、ステップ 3 に進みます。
- [Basic View] プロパティを設定するには、ステップ 4 に進みます。

ステップ 3　[Advanced View] で仮想サーバのプロパティを設定するには、表 5-2 の情報を入力します。

表 5-2　仮想サーバのプロパティ – [Advanced View]

フィールド	説明
Virtual Server Name	仮想サーバの名前を入力します。
IP Address Type	仮想サーバのアドレス タイプに、IPv4 または IPv6 を選択します。
Virtual IP Address	仮想サーバの IP アドレスを入力します。
Virtual IP Mask	(IPv4 アドレス タイプのみ) 仮想サーバ IP アドレスに適用するサブネット マスクを選択します。
Virtual IP Prefix Length	(IPv6 アドレス タイプのみ) 仮想サーバ IP アドレスに適用するプレフィックス長を入力します。プレフィックスのデフォルトの長さは 128 です。
Transport Protocol	仮想サーバがサポートするプロトコルを選択します。 • [Any]：任意の IP プロトコルを使用して、仮想サーバが接続を受け入れます。 • [TCP]：仮想サーバが、TCP を使用している接続を受け入れることを示しています。 • [UDP]：仮想サーバが、UDP を使用している接続を受け入れることを示しています。 **(注)**　このフィールドは、既存の仮想サーバを編集しているときは読み取り専用になります。Device Manager では、レイヤ 7 サーバのロード バランシング ポリシー マップを必要とするプロトコル間の変更はできません。仮想サーバを削除し、目的のプロトコルを備えた新しい仮想サーバを作成する必要があります。

表 5-2　仮想サーバのプロパティ – [Advanced View]（続き）

フィールド	説明
Application Protocol	このフィールドは、TCP または UDP が選択されているときに表示されます。仮想サーバでサポートされるアプリケーション プロトコルを選択します。 （注）　このフィールドは、既存の仮想サーバを編集しているときは読み取り専用になります。Device Manager では、レイヤ 7 サーバのロード バランシング ポリシー マップを必要とするプロトコル間の変更はできません。仮想サーバを削除し、目的のアプリケーション プロトコルを備えた新しい仮想サーバを作成する必要があります。 TCP の場合、オプションは次のとおりです。 • [FTP]：File Transfer Protocol • [Generic]：汎用プロトコル解釈 • [HTTP]：Hyper Text Transfer Protocol • [HTTPS]：HTTP over SSL [HTTPS] を選択する場合、[SSL Termination] 設定サブセットが表示されます。「仮想サーバの SSL 終了の設定」（P.5-19）を参照してください。 • [Other]：指定されている以外の任意のプロトコル • [RDP]：Remote Desktop Protocol • [RTSP]：Real Time Streaming Protocol • [SIP]：Session Initiation Protocol • Unterminated HTTPS （注）　このオプションは、ACE が NPE のソフトウェア バージョンを使用する場合は有効ではありません（「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）。 UDP の場合、オプションは次のとおりです。 • [DNS]：Domain Name System • [Generic]：汎用プロトコル解釈 • [Other]：指定されている以外の任意のプロトコル • [RADIUS]：Remote Authentication Dial-In User Service • [SIP]：Session Initiation Protocol 特定のアプリケーション プロトコルを選択すると、[Protocol Inspection] 設定サブセットが表示されます。「仮想サーバのプロトコル インスペクションの設定」（P.5-21）を参照してください。

表 5-2　仮想サーバのプロパティ – [Advanced View]（続き）

フィールド	説明
Port	デフォルトでは、このフィールドに指定したプロトコルのデフォルト ポート番号が示されます。 ポート番号を変更するには、指定したプロトコルに使用するポートを入力します。有効な値は、10-20 など、0 ～ 65535 の整数または整数の範囲です。すべてのポートを指定するには、0（ゼロ）を入力します。 プロトコルおよびポートの完全なリストについては、www.iana.org/numbers/ にある『Internet Assigned Numbers Authority』を参照してください。
All VLANs	すべての VLAN からの着信トラフィックをサポートするには、このチェックボックスをオンにします。特定の VLAN だけからの着信トラフィックをサポートするには、このチェックボックスをクリアします。

表 5-2　仮想サーバのプロパティ – [Advanced View]（続き）

フィールド	説明
VLAN	このフィールドは、[All VLANs] チェックボックスがクリアされると表示されます。 [Available] リストで、着信トラフィックに使用する VLAN を選択し、[Add to Selection] をクリックします。項目が [Selected] リストに表示されます。 VLAN を削除するには、[Selected] リストで選択し、[Remove from Selection] をクリックします。項目が [Available] リストに表示されます。 （注）　VLAN を仮想サーバに指定すると、VLAN を変更することはできません。仮想サーバを削除し、目的の VLAN を備えた新しい仮想サーバを作成する必要があります。
HTTP Parameter Map	このフィールドが表示されるのは、選択したアプリケーション プロトコルが HTTP または HTTPS の場合です。 既存の HTTP パラメータ マップを選択するか、または [*New*] をクリックして新しいパラメータ マップを作成します。 • 既存のパラメータ マップを選択する場合、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。 • [*New*] をクリックすると、[HTTP Parameter Map] 設定ペインが表示されます。表 8-2 の説明に従って、HTTP パラメータ マップを設定します。
Connection Parameter Map	このフィールドが表示されるのは、選択したプロトコルが TCP の場合です。 既存の接続パラメータ マップを選択するか、または [*New*] をクリックして新しいパラメータ マップを作成します。 • 既存のパラメータ マップを選択する場合、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。 • [*New*] をクリックすると、[Connection Parameter Map] 設定ペインが表示されます。表 8-3 の説明に従って、接続パラメータ マップを設定します。 （注）　[More Settings] をクリックして、別の [Connection Parameter Maps] 設定属性にアクセスします。デフォルトでは、Device Manager は、デフォルトの [Connection Parameter Maps] 設定属性と、あまり使用されない属性を非表示にします。

表 5-2　仮想サーバのプロパティ – [Advanced View]（続き）

フィールド	説明
KAL-AP-TAG Name	KAL-AP-TAG 機能を使用すると、Cisco Global Site Selector（GSS）独自の KAL-AP プロトコルにより、ファイアウォールを GSS と ACE の間に配置した場合に、ACE から負荷およびアベイラビリティの情報を抽出できます。この機能により、ACE の最大 4,096 個のタグに対して、VIP ごとのタグ（名前）を設定することができます。この機能では、ドメイン機能ごとのタグは置き換えられません。この機能に関する詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』の「Configuring Health Monitoring」の章を参照してください。 [KAL-AP-TAG Name] フィールドには、引用符で囲まずにスペースを入れないで、76 文字以内の英数字で名前を入力します。 次の場合はサポートされていないため、エラーになります。 • 別のポリシー設定の一部としてすでにタグ設定がある VIP のタグ名は設定できません。 • 複数の VIP に同じタグ名を関連付けることはできません。 • ドメインと VIP に同じタグ名を関連付けることはできません。 • VIP が同じで、ポート番号が異なる 2 つのレイヤ 3 クラス マップに、2 つの異なるタグを割り当てることはできません。KAL-AP プロトコルは、これらのクラス マップの VIP が同じであると見なし、GSS が VIS 問い合わせた際に、両方のレイヤ 3 の規則の負荷を合わせて計算します。
Kal-AP Primary Out of Service	バックアップ サーバ ファームの使用中にプライマリ サーバ ファームが停止していることを Global Site Selector (GSS) に通知するには、ACE のこのボックスをオンにします。 デフォルトでは、ACE 上でバックアップ サーバ ファームとしてリダイレクト サーバ ファームを設定している場合、バックアップ サーバは別のデータセンターにクライアント要求をリダイレクトします。ただし、VIP は INSERVICE 状態のままになります。 GSS と通信するように ACE を設定するとサーバのアベイラビリティに関する情報を提供します。プライマリ サーバ ファームが停止後にバックアップ サーバが使用中でこの機能が有効の場合、ACE は 255 の負荷値を返すことによって、プライマリ サーバ ファームの VIP が非稼働状態であることを GSS に通知します。GSS は、プライマリ サーバ ファームがダウンしていると認識し、他のデータセンターの IP アドレスを使用して以降の DNS 要求を送信します。 この機能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。

表 5-2　仮想サーバのプロパティ – [Advanced View]（続き）

フィールド	説明
DNS Parameter Map	このフィールドが表示されるのは、UDP 上で選択したプロトコルが DNS の場合です。 既存の DNS パラメータ マップを選択するか、または [*New*] をクリックして新しい DNS パラメータ マップを作成します。 • 既存のパラメータ マップを選択する場合、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。 • [*New*] をクリックすると、[DNS Parameter Map] 設定ペインが表示されます。表 8-11 の説明に従って、DNS パラメータ マップを設定します。
Generic Parameter Map	このフィールドが表示されるのは、TCP または UDP 上で選択したアプリケーション プロトコルが汎用の場合です。 既存の汎用パラメータ マップを選択するか、または [*New*] をクリックして新しい汎用パラメータ マップを作成します。 • 既存のパラメータ マップを選択する場合、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。 • [*New*] をクリックすると、[Generic Parameter Map] 設定ペインが表示されます。表 8-7 の説明に従って、汎用パラメータ マップを設定します。
RTSP Parameter Map	このフィールドが表示されるのは、TCP 上で選択したアプリケーション プロトコルが RTSP の場合です。 既存の RTSP パラメータ マップを選択するか、または [*New*] をクリックして新しい RTSP パラメータ マップを作成します。 • 既存のパラメータ マップを選択する場合、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。 • [*New*] をクリックすると、[RTSP Parameter Map] 設定ペインが表示されます。表 8-8 の説明に従って、RTSP 接続パラメータ マップを設定します。

表 5-2　仮想サーバのプロパティ – [Advanced View]（続き）

フィールド	説明
ICMP Reply	ICMP ECHO 要求に対する仮想サーバの応答方法を指定します。 • [None]：仮想サーバが ICMP ECHO-REPLY 応答を ICMP 要求に対して送信しないことを示します。 • [Active]：設定済みの VIP がアクティブの場合にだけ、仮想サーバが ICMP ECHO-REPLY 応答を送信することを示しています。 • [Always]：仮想サーバが ICMP ECHO-REPLY 応答を ICMP 要求に対して常に送信することを示しています。 • [Primary Inservice]：バックアップ サーバ ファームの状態に関係なく、プライマリ サーバ ファームの状態が UP の場合だけ ACE が ICMP ping に応答することを示しています。このオプションが選択されていて、プライマリ サーバ ファームの状態が DOWN の場合、ACE は ICMP 要求を廃棄し、この要求はタイムアウトになります。
Status	仮想サーバが稼働しているか、稼働していないかを示します。 • [In Service]：ロード バランシング処理のために仮想サーバをイネーブルにします。 • [Out-of-Service]：ロード バランシング処理のために仮想サーバをディセーブルにします。

ステップ 4　[Basic View] で仮想サーバのプロパティを設定するには、表 5-3 の情報を入力します。

表 5-3　仮想サーバのプロパティ - [Basic View]

フィールド	説明
Virtual Server Name	仮想サーバの名前を入力します。
IP Address Type	仮想サーバのアドレス タイプに、IPv4 または IPv6 を選択します。
Virtual IP Address	仮想サーバの IP アドレスを入力します。
Transport Protocol	仮想サーバがサポートするプロトコルを選択します。 • [Any]：任意の IP プロトコルを使用して、仮想サーバが接続を受け入れることを示しています。 • [TCP]：仮想サーバが、TCP を使用している接続を受け入れることを示しています。 • [UDP]：仮想サーバが、UDP を使用している接続を受け入れることを示しています。

表 5-3　仮想サーバのプロパティ - [Basic View]（続き）

フィールド	説明
Application Protocol	仮想サーバでサポートされるアプリケーション プロトコルを選択します。 TCP の場合、オプションは次のとおりです。 • [FTP]：File Transfer Protocol • [HTTP]：Hyper Text Transfer Protocol • [HTTPS]：HTTP over SSL [HTTPS] を選択する場合、[SSL Termination] 設定サブセットが表示されます。「仮想サーバの SSL 終了の設定」（P.5-19）を参照してください。 （注）　このオプションは、ACE が NPE のソフトウェア バージョンを使用する場合は有効ではありません（「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）。 • [Generic]：汎用プロトコル解釈 • [Other]：指定されている以外の任意のプロトコル • [RTSP]：Real Time Streaming Protocol • [RDP]：Remote Desktop Protocol • [SIP]：Session Initiation Protocol UDP の場合、オプションは次のとおりです。 • [DNS]：Domain Name System • [Generic]：汎用プロトコル解釈 • [Other]：指定されている以外の任意のプロトコル • [RTSP]：Real Time Streaming Protocol • [RADIUS]：Remote Authentication Dial-In User Service • [SIP]：Session Initiation Protocol
Port	デフォルトでは、このフィールドに指定したプロトコルのデフォルト ポート番号が示されます。 ポート番号を変更するには、指定したプロトコルに使用するポートを入力します。有効な値は、10-20 など、0 ～ 65535 の整数または整数の範囲です。すべてのポートを指定するには、0（ゼロ）を入力します。 すべてのプロトコルおよびポートの完全なリストについては、www.iana.org/numbers/ にある『Internet Assigned Numbers Authority』を参照してください。

表 5-3　仮想サーバのプロパティ - [Basic View]（続き）

フィールド	説明
All VLANs	すべての VLAN からの着信トラフィックをサポートするには、このチェックボックスをオンにします。特定の VLAN だけからの着信トラフィックをサポートするには、このチェックボックスをクリアします。
VLAN	このフィールドは、[All VLANs] チェックボックスがクリアされると表示されます。 [Available] リストで、着信トラフィックに使用する VLAN を選択し、[Add to Selection] をクリックします。項目が [Selected] リストに表示されます。 VLAN を削除するには、[Selected] リストで選択し、[Remove from Selection] をクリックします。項目が [Available] リストに表示されます。 （注）　VLAN を仮想サーバに指定すると、VLAN を変更することはできません。仮想サーバを削除し、目的の VLAN を備えた新しい仮想サーバを作成する必要があります。

ステップ 5　仮想サーバのプロパティの設定が完了したら、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適用します。
- [Cancel] をクリックすると、エントリを保存しないで手順を終了します。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバの SSL 終了の設定」（P.5-19）

仮想サーバの SSL 終了の設定

（注）　このセクションの情報は、ACE NPE のソフトウェア バージョンに適用されません（「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）。

SSL 終了サービスでは、仮想サーバは SSL プロキシ サーバとして機能し、仮想サーバとそのクライアントの間の SSL セッションを終了し、HTTP サーバに対して TCP 接続を確立することができます。SSL 接続を終了すると、ACE はクライアントからの暗号文を復号化し、データをクリア テキストとして HTTP サーバに送信します。

仮想サーバの SSL 終了サービスを設定するには、次の手順を使用します。

前提

[Properties] 設定サブセットで、仮想サーバを HTTPS over TCP 用または Other over TCP 用に設定しておきます。詳細については、「仮想サーバのプロパティの設定」（P.5-11）を参照してください。

手順

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

ステップ 2　SSL 終了を設定する仮想サーバを選択し、[Edit] をクリックします。[Virtual Server] 設定画面が表示されます。

ステップ 3　[SSL Termination] をクリックします。[Proxy Service Name] フィールドが表示されます。

ステップ 4　[Proxy Service Name] フィールドで、既存の SSL 終了サービスを選択するか、または [*New*] を選択して新しい SSL プロキシ サービスを作成します。

- 既存の SSL サービスを選択する場合、画面がリフレッシュされ、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。
- [*New*] を選択すると、[Proxy Service] 設定サブセットが表示されます。

ステップ 5　表 5-4 の指示に従って、SSL サービスを設定します。

表 5-4　仮想サーバの SSL 終了の属性

フィールド	説明
Name	この SSL プロキシ サービスの名前を入力します。有効な入力は英数値ストリングで、最大 64 文字です。
Keys	データ暗号化のための SSL ハンドシェイク時に使用する SSL キー ペアを選択します。
Certificates	SSL ハンドシェイク時に使用する SSL 認証を選択します。
Chain Groups	SSL ハンドシェイク時に使用するチェーン グループを選択します。
Auth Groups	このプロキシ サーバ サービスに関連付ける SSL 認証グループを選択します。
CRL Best-Effort	このオプションが表示されるのは、[Auth Group Name] フィールドで認証グループを選択した場合です。 CRL がエクステンションに含まれているかどうかを判別し、値が存在する場合にその値を取得するサービスを求めて、ACE がクライアント証明書を調べることができるようにする場合に、このチェックボックスを選択します。 この機能をディセーブルにするには、チェックボックスをクリアします。
CRL Name	このオプションが表示されるのは、[CRL Best-Effort] チェックボックスがクリアされている場合です。 ACE でこのプロキシ サービスを使用する場合は、[CRL] を選択します。
Parameter Maps	このプロキシ サーバ サービスに関連付ける SSL パラメータ マップを選択します。

SSL の詳細については、「SSL の設定」（P.9-1）を参照してください。

ステップ 6　仮想サーバのプロパティの設定が完了したら、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この手順を終了します。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバのプロパティの設定」（P.5-11）

仮想サーバのプロトコル インスペクションの設定

プロトコル インスペクションを設定すると、仮想サーバは、プロトコルの動作を確認し、ACE アプライアンスを通過する不要なまたは悪意のあるトラフィックを特定することができます。

[Advanced View] では、プロトコル インスペクションの設定は、次の仮想サーバのプロトコル設定に利用できます。

- FTP、HTTP、HTTPS、RTSP、または SIP とともに使用する場合の TCP
- DNS または SIP とともに使用する場合の UDP

[Basic View] では、プロトコル インスペクションの設定は、FTP とともに使用する場合の TCP で利用できます。

仮想サーバでプロトコル インスペクションを設定するには、この手順を使用します。

前提

仮想サーバは、[Properties] 設定サブセットでプロトコル インスペクションをサポートしているプロトコルの 1 つを使用するように設定しておきます。これらのプロトコルの設定の詳細については、「仮想サーバのプロパティの設定」（P.5-11）を参照してください。

手順

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

ステップ 2　プロトコル インスペクションを設定する仮想サーバを選択し、[Edit] をクリックします。[Virtual Server] 設定画面が表示されます。

ステップ 3　[Protocol Inspection] をクリックします。[Enable Inspect] チェックボックスが表示されます。

ステップ 4　指定したトラフィックにインスペクションをイネーブルにするには、[Enable Inspect] チェックボックスを選択します。このトラフィックでのインスペクション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。デフォルトでは、ACE アプライアンスではすべての要求方式が可能になっています。

ステップ 5　[Enable Inspect] チェックボックスを選択する場合、仮想サーバのアプリケーション プロトコル設定に応じて、追加のインスペクション オプションを設定します。

- DNS の場合、[Length] フィールドに、DNS パケットの最大長をバイト単位で入力します。有効な入力は、512 ～ 65535 バイトです。このフィールドに値を入力しない場合は、DNS パケット サイズは確認されません。
- FTP の場合、ステップ 6 に進みます。
- HTTP および HTTPS の場合、ステップ 7 に進みます。
- SIP の場合、ステップ 9 に進みます。

（注）　RTSP には、プロトコル固有のインスペクション オプションはありません。

ステップ 6　FTP プロトコル インスペクションの場合、次の手順を実行します。

a. 仮想サーバで FTP トラフィックの拡張インスペクションの実行および RFC 標準への準拠の確認を実施する場合は、[Use Strict] チェックボックスを選択します。仮想サーバが拡張 FTP インスペクションを実行しないようにするには、このチェックボックスをクリアします。

b. [Use Strict] チェックボックスを選択する場合は、[Blocked FTP Commands] フィールドに、仮想サーバによって拒否されるようにするコマンドを指定します。FTP コマンドの詳細については、表 12-13 を参照してください。

- [Available] リストで、仮想サーバによってブロックされるようにするコマンドを選択し、[Add] をクリックします。コマンドが [Selected Items] リストに表示されます。
- ブロックされたくないコマンドを削除するには、[Selected] リストで目的のコマンドを選択し、[Remove] をクリックします。コマンドが [Available] リストに表示されます。

ステップ 7　HTTP または HTTPS インスペクションの場合、次の手順を実行します。

a. レイヤ 3 およびレイヤ 4 トラフィックの監視をイネーブルにするには、[Logging Enabled] チェックボックスをオンにします。イネーブルの場合、送信元または宛先 IP アドレスやアクセス対象の URL を含め、指定したクラスのトラフィックで送信される各 URL 要求がログに記録されます。レイヤ 3 およびレイヤ 4 トラフィックの監視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。

b. [Policy] サブセットで、[Add] をクリックして新しい一致条件およびアクションを追加するか、または既存の一致条件およびアクションを選択し、[Edit] をクリックしてそれを変更します。[Policy] 設定ペインが表示されます。

c. [Matches] フィールドで、既存のクラス マップまたは [*New*] または [*Inline Match*] を選択し、プロトコル インスペクション用の新しい一致条件を設定します。

既存のクラス マップを選択すると、画面がリフレッシュされ、選択したクラス マップの設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

d. 表 5-5 のステップに従って、一致条件および関連アクションを設定します。

表 5-5　プロトコル インスペクションの一致条件の設定

選択項目	アクション
Existing class map	**1.** [View] をクリックし、選択したクラス マップの一致条件情報を確認します。 **2.** 次の手順を実行します。 – [Cancel] をクリックすると、変更しないで続行し、前の画面に戻ります。 – [Edit] をクリックすると、既存の設定が変更されます。 – [Duplicate] をクリックすると、同じクラス マップを使用している他の仮想サーバに影響を与えずに、同じ属性で新しいクラス マップを作成します。 共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。 **3.** [Action] フィールドに、指定した一致条件と一致する場合にトラフィックに対して仮想サーバが実行するアクションを指定します。 – [Permit] : 指定したディープ インスペクション一致条件と一致する場合、指定したトラフィックは仮想サーバで受信されます。 – [Reset] : 指定したトラフィックは仮想サーバで拒否され、接続を終了するために TCP リセット メッセージがクライアントまたはサーバに送信されます。

表 5-5　プロトコル インスペクションの一致条件の設定 （続き）

選択項目	アクション
New	1. [Name] フィールドに、このクラス マップの一意な名前を指定します。 2. 複数の一致条件が存在する場合、[Match] フィールドに、複数の一致文の評価に使用する方式を選択します。 – [All]：すべての一致条件が満たされる場合にだけ一致することになります。 – [Any]：一致条件の少なくとも 1 つが満たされる場合に一致することになります。 3. [Conditions] テーブルで、[Add] をクリックして新しい条件を追加するか、または既存の条件を選択し、[Edit] をクリックしてそれを変更します。[Type] フィールドが表示されます。 4. [Type] フィールドで、プロトコル インスペクション用に満たす条件のタイプを選択し、表 5-6 の情報に従ってプロトコル固有の条件を設定します。 5. [Action] フィールドに、指定した一致条件と一致する場合にトラフィックに対して仮想サーバが実行するアクションを指定します。 – [Permit]：指定したディープ インスペクション一致条件と一致する場合、指定したトラフィックは仮想サーバで受信されます。 – [Reset]：指定したトラフィックは仮想サーバで拒否され、接続を終了するために TCP リセット メッセージがクライアントまたはサーバに送信されます。
Inline Match	1. [Conditions Type] フィールドで、プロトコル インスペクション用に満たすインライン一致条件のタイプを選択します。 表 5-6 に、条件のタイプおよび関連の設定オプションを示します。 2. 表 5-6 の情報に従って、条件固有の基準を指定します。 3. [Action] フィールドに、指定した一致条件と一致する場合にトラフィックに対して仮想サーバが実行するアクションを指定します。 – [Permit]：指定したディープ インスペクション一致条件と一致する場合、指定したトラフィックは仮想サーバで受信されます。 – [Reset]：指定したトラフィックは仮想サーバで拒否され、接続を終了するために TCP リセット メッセージがクライアントまたはサーバに送信されます。

表 5-6　HTTP および HTTPS のプロトコル インスペクションの条件およびオプション

条件	説明
Content	HTTP entity-body に含まれている特定のコンテンツは、アプリケーション インスペクションの決定に使用されます。 **1.** [Content Expression] フィールドに、照合するコンテンツを入力します。有効な入力は 1 ～ 255 文字の英数字ストリングです。 **2.** [Content Offset] フィールドに、ヘッダーとメッセージ ボディの間の空白行（CR、LF、CR、LF）より後ろにあって、メッセージ ボディの第 1 バイトから始まっていて無視するバイト数を入力します。有効な入力は、1 ～ 255 バイトです。
Content Length	コンテンツ解析長は、アプリケーション インスペクションの決定に使用されます。 **1.** [Content Length Operator] フィールドで、コンテンツ長の比較に使用するオペランドを選択します。 – [Equal To] : コンテンツ長を [Content Length Value] フィールドの数値と同一にする必要があります。 – [Greater Than] : コンテンツ長を [Content Length Value] フィールドの数値より大きくする必要があります。 – [Less Than] : コンテンツ長を [Content Length Value] フィールドの数値より小さくする必要があります。 – [Range] : コンテンツ長を [Content Length Lower Value] フィールドと [Content Length Higher Value] フィールドに指定された範囲におさめる必要があります。 **2.** 値を入力してコンテンツ長を比較します。 – [Content Length Operator] フィールドで [Equal To]、[Greater Than]、[Less Than] を選択した場合、[Content Length Value] フィールドが表示されます。[Content Length Value] フィールドに、比較に使用するバイト数を入力します。有効な入力は 0 ～ 4294967295 の整数です。 – [Content Length Operator] フィールドで [Range] を選択した場合、[Content Length Lower Value] フィールドと [Content Length Higher Value] フィールドが表示されます。 1. [Content Length Lower Value] フィールドに、一致条件の下限に使用するバイト数を入力します。有効な入力は 0 ～ 4294967295 の整数です。このフィールド内の数字は、[Content Length Higher Value] フィールドに入力した数字よりも小さい必要があります。 2. [Content Length Higher Value] フィールドに、一致条件の上限に使用するバイト数を入力します。有効な入力は 0 ～ 4294967295 の整数です。このフィールド内の数字は、[Content Length Lower Value] フィールドに入力した数字よりも大きい必要があります。
Content Type Verification	ヘッダー MIME-type を備えた MIME-type メッセージの確認は、アプリケーション インスペクションの決定に使用されます。このオプションは、ヘッダー MIME-type 値が、サポートされている MIME-types の内部リストにあること、また、ヘッダー MIME-type がメッセージのデータまたはボディ部にあるコンテンツと一致していることを確認します。

表 5-6　HTTP および HTTPS のプロトコル インスペクションの条件およびオプション （続き）

条件	説明
Header	HTTP ヘッダーの名前および値は、アプリケーション インスペクションの決定に使用されます。 1. [Header] フィールドで、一致条件に使用する定義済み HTTP ヘッダーの 1 つを選択します。または [HTTP Header] を選択して他の HTTP ヘッダーを指定します。 2. [HTTP Header] を選択した場合、[Header Name] フィールドに比較させる HTTP ヘッダー名を入力します。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）。 3. [Header Value] フィールドに、HTTP ヘッダー内の指定したフィールドの値と比較するヘッダー値式ストリングを入力します。有効な入力は英数字ストリングで、最大 255 文字です。ACE は、照合に正規表現をサポートしています。ヘッダー表現にはスペースを使用できますが、エスケープ シーケンスまたは引用符が必要です。ヘッダー マップのすべてのヘッダーは一致する必要があります。正規表現に使用できる、サポート対象文字の一覧については、表 12-33 を参照してください。
Header Length	HTTP メッセージのヘッダー長は、アプリケーション インスペクションの決定に使用されます。 1. [Header Length Type] フィールドで、アプリケーション インスペクションの判定に使用する HTTP ヘッダー要求または応答メッセージを指定します。 – [Request] : ヘッダー長について、HTTP ヘッダー要求メッセージが確認されます。 – [Response] : ヘッダー長について、HTTP ヘッダー応答メッセージが確認されます。 2. [Header Length Operator] フィールドで、ヘッダー長の比較に使用するオペランドを選択します。 – [Equal To] : ヘッダー長を [Header Length Value] フィールドの数値と同一にする必要があります。 – [Greater Than] : ヘッダー長を [Header Length Value] フィールドの数値より大きくする必要があります。 – [Less Than] : ヘッダー長を [Header Length Value] フィールドの数値より小さくする必要があります。 – [Range] : ヘッダー長を [Header Length Lower Value] フィールドと [Header Length Higher Value] フィールドに指定された範囲におさめる必要があります。 3. 値を入力してヘッダー長を比較します。 – [Header Length Operator] フィールドで [Equal To]、[Greater Than]、[Less Than] を選択した場合、[Header Length Value] フィールドが表示されます。[Header Length Value] フィールドに、比較に使用するバイト数を入力します。有効な入力は 0 ～ 255 の整数です。 – [Header Length Operator] フィールドで [Range] を選択した場合、[Header Length Lower Value] フィールドと [Header Length Higher Value] フィールドが表示されます。 1. [Header Length Lower Value] フィールドに、一致条件の下限に使用するバイト数を入力します。有効な入力は 0 ～ 255 の整数です。このフィールド内の数字は、[Header Length Higher Value] フィールドに入力した数字よりも小さい必要があります。 2. [Header Length Higher Value] フィールドに、一致条件の上限に使用するバイト数を入力します。有効な入力は 1 ～ 255 の整数です。このフィールド内の数字は、[Header Length Lower Value] フィールドに入力した数字よりも大きい必要があります。

表 5-6　HTTP および HTTPS のプロトコル インスペクションの条件およびオプション （続き）

条件	説明
Header MIME Type	Multipurpose Internet Mail Extension（MIME）メッセージ タイプは、アプリケーション インスペクションの決定に使用されます。 [Header MIME Type] フィールドで、一致条件に使用する MIME メッセージ タイプを選択します。
Port Misuse	このポート 80（または HTTP が動作している他のポート）の誤用は、アプリケーション インスペクションの決定に使用されます。 この一致条件に使用するアプリケーション カテゴリを選択します。 • [IM]：インスタント メッセージング アプリケーションが確認されます。 • [P2P]：ピアツーピア アプリケーションが確認されます。 • [Tunneling]：トンネリング アプリケーションが確認されます。
Request Method	プロトコル インスペクションの判定に、要求メソッドを使用します。デフォルトでは、ACE はすべての要求方式と拡張方式を許可します。このオプションを使用すると、RFC 2616 と HTTP 拡張メソッドに定義されている要求メソッドに準拠してプロトコル インスペクションの判定を設定できます。 1. この一致基準に使用する要求メソッドのタイプを選択します。 – [Ext]：HTTP 拡張メソッドが使用されます。 （注）　選択する使用可能な HTTP 拡張メソッドのリストは、ACE にインストールされたソフトウェアのバージョンによって異なります。 – [RFC]：RFC 2616 に規定されている要求方式が使用されます。 2. [Request Method] フィールドで、検査される要求方式を選択します。
Strict HTTP	HTTP RFC 2616 への準拠は、アプリケーション インスペクションの決定に使用されます。
Transfer Encoding	HTTP transfer-encoding タイプは、アプリケーション インスペクションの決定に使用されます。transfer-encoding general-header フィールドは、送信者と受信者の間でメッセージを安全に転送するために HTTP メッセージ ボディに適用された変換のタイプを示します（何か適用されている場合）。 [Transfer Encoding] フィールドで、確認するエンコーディングのタイプを選択します。 • [Chunked]：メッセージ本文は、一連のチャンクとして転送されます。 • [Compress]：エンコーディング フォーマットは、UNIX ファイル圧縮プログラム *compress* によって作成されます。 • [Deflate]：.zlib フォーマットは、RFC 1951 に規定されている DEFLATE 圧縮メカニズムとともに、RFC 1950 に規定されています。 • [Gzip]：エンコーディング フォーマットは、RFC 1952 に規定されているファイル圧縮プログラム GZIP（GNU zip）によって作成されます。 • [Identity]：変換の使用を必要としないデフォルトの（identity）エンコーディングです。

表 5-6　HTTP および HTTPS のプロトコル インスペクションの条件およびオプション （続き）

条件	説明
URL	URL 名はアプリケーション インスペクションの決定に使用されます。 [URL] フィールドに、照合する URL または URL の一部を入力します。有効な入力は、1 ～ 255 の英数字による URL ストリングで、www.*hostname.domain* の URL の一部だけを含めます。たとえば、URL が www.anydomain.com/latest/whatsnew.html の場合、/latest/whatsnew.html のみを含めます。
URL Length	[URL length] は、アプリケーション インスペクションの決定に使用されます。 **1.** [URL Length Operator] フィールドで、URL 長の比較に使用するオペランドを選択します。 – [Equal To] : URL 長を [URL Length Value] フィールドの数値と同一にする必要があります。 – [Greater Than] : URL 長を [URL Length Value] フィールドの数値より大きくする必要があります。 – [Less Than] : URL 長を [URL Length Value] フィールドの数値より小さくする必要があります。 – [Range] : URL 長を [URL Length Lower Value] フィールドと [URL Length Higher Value] フィールドに指定された範囲におさめる必要があります。 **2.** 値を入力して URL 長を比較します。 – [URL Length Operator] フィールドで [Equal To]、[Greater Than]、[Less Than] を選択した場合、[URL Length Value] フィールドが表示されます。[URL Length Value] フィールドに、比較に使用する値を入力します。有効な範囲は 1 ～ 65535 バイトです。 – [URL Length Operator] フィールドで [Range] を選択した場合、[URL Length Lower Value] フィールドと [URL Length Higher Value] フィールドが表示されます。 1. [URL Length Lower Value] フィールドに、一致条件の下限に使用するバイト数を入力します。有効な入力は 1 ～ 65535 の整数です。このフィールド内の数字は、[URL Length Higher Value] フィールドに入力した数字よりも小さい必要があります。 2. [URL Length Higher Value] フィールドに、一致条件の上限に使用するバイト数を入力します。有効な入力は 1 ～ 65535 の整数です。このフィールド内の数字は、[URL Length Lower Value] フィールドに入力した数字よりも大きい必要があります。

e. 次の手順を実行します。

– エントリを保存するには、[OK] をクリックします。[Conditions] テーブルは新しいエントリによってリフレッシュされます。

– [Cancel] をクリックすると、エントリを保存しないで Policy サブセットを終了します。

f. [Default Action] フィールドで、プロトコル インスペクション用に指定した一致条件が満たされない場合に、仮想サーバが実行するデフォルトのアクションを選択します。

– [Permit] : 指定した HTTP トラフィックは仮想サーバによって受信されます。

– [Reset] : 指定した HTTP トラフィックは仮想サーバによって拒否されます。

– [N/A] : この属性は設定されません。

ステップ 8　SIP インスペクションの場合、次の手順を実行します。

a. [Actions] サブセットで、[Add] をクリックして新しい一致条件およびアクションを追加するか、または既存の一致条件およびアクションを選択し、[Edit] をクリックしてそれを変更します。[Actions] 設定ペインが表示されます。

b. [Matches] フィールドで、既存のクラス マップまたは [*New*] または [*Inline Match*] を選択し、プロトコル インスペクション用の新しい一致条件を設定します。

既存のクラス マップを選択すると、画面がリフレッシュされ、選択したクラス マップの設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

c. 表 5-7 の情報に従って、一致条件および関連アクションを設定します。

表 5-7　SIP プロトコル インスペクションの条件およびオプション

条件	説明
Called Party	SIP To ヘッダーの URI に指定した宛先つまり着信側は、SIP プロトコル インスペクションの決定に使用されます。 [Called Party] フィールドに、この一致条件に対応する SIP To ヘッダーの URI の着信側を特定する正規表現を入力します。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 255 文字）。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。
Calling Party	SIP From ヘッダーの URI に指定した送信元つまり発信側は、SIP プロトコル インスペクションの決定に使用されます。 [Calling Party] フィールドに、この一致条件に対応する SIP From ヘッダーの URI の発信側を特定する正規表現を入力します。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 255 文字）。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。
IM Subscriber	IM（インスタント メッセージング）サブスクライバは、アプリケーション インスペクションの決定に使用されます。 [IP Subscriber] フィールドに、この一致条件に対応する IM サブスクライバを特定する正規表現を入力します。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 255 文字）。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。
Message Path	SIP インスペクションにより、特定の SIP プロキシ サーバから発信されたり、これを通過したりするメッセージをフィルタすることができます。ACE は、不正な SIP プロキシ IP アドレスまたは URI を正規表現形式のリストにして維持し、このリストと各 SIP パケット内の [VIA header] フィールドを照合します。 [Message Path] フィールドに、この一致条件に対応する SIP プロキシ サーバを特定する正規表現を入力します。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 255 文字）。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。
SIP Content Type	SIP メッセージ ボディのコンテンツ タイプは、SIP プロトコル インスペクションの決定に使用されます。 [Content Type] フィールドに、この一致条件に使用する SIP メッセージ ボディのコンテンツ タイプを特定する正規表現を入力します。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 255 文字）。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 5-7　SIP プロトコル インスペクションの条件およびオプション （続き）

条件	説明
SIP Content Length	SIP メッセージ ボディのコンテンツ長は、SIP プロトコル インスペクションの決定に使用されます。 SIP メッセージ ボディ長に基づいて SIP トラフィックを指定するには、次の手順を実行します。 1. [Content Operator] フィールドで、[Greater Than] が選択されていることを確認します。 2. [Content Length] フィールドに、SIP プロトコル インスペクションを実行しないで ACE が許可する SIP メッセージ ボディの最大サイズをバイト単位で入力します。SIP メッセージが指定値を超えると、ACE は、関連付けられたポリシー マップの定義に従って、SIP プロトコル インスペクションを実行します。有効な入力は 0 ～ 65534 の整数バイトです。
SIP Request Method	SIP 要求方式は、アプリケーション インスペクションの決定に使用されます。 [Request Method] フィールドで、検査される要求方式を選択します。
Third Party	SIP を使用し、From や To のヘッダー フィールドに異なる値を指定した REGISTER メッセージを送信することにより、別のユーザに代わって登録を行うことができます。このプロセスは、REGISTER メッセージが実際は DEREGISTER メッセージである場合、セキュリティ上の脅威になることがあります。悪意のあるユーザが、すべてのユーザになり代わってこれらのユーザの登録を解除すると、DoS 攻撃（サービス拒絶攻撃）を仕掛けることができるからです。こうしたセキュリティ上の脅威を避けるために、登録の実行や解除を代行できる特権ユーザのリストを指定できます。ACE では、このリストが regex テーブルとして保持されます。このポリシーを設定すると、ACE では、From と To ヘッダーが一致しない REGISTER メッセージや、いずれの特権ユーザ ID とも一致しない From ヘッダー値を含むメッセージがドロップされます。 [Third Party Registration Entities] フィールドに、第三者の登録権限を持つ特権ユーザを特定する正規表現を入力します。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 255 文字）。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。
URI Length	ACE は、SIP URI または Tel URI の長さを確認できます。SIP URI は、発信側（送信元）が着信側（宛先）に連絡を取るときに使用するユーザ ID です。Tel URI は、SIP 接続のエンドポイントを識別する電話番号です。SIP URI および Tel URI の詳細については、RFC 2534 および RFC 3966 をそれぞれ参照してください。 URI に基づいて SIP トラフィックをフィルタするには、次の手順を実行します。 1. [URI Type] フィールドに、使用する URI のタイプを指定します。 – [SIP URI]：この一致条件に使用する発信側の URI – [Tel URI]：この一致条件に使用する電話番号 2. [URI Operator] フィールドで、[Greater Than] が選択されていることを確認します。 3. [URI Length] フィールドに、SIP URI または Tel URI の最大長をバイト単位で入力します。有効な入力は 0 ～ 254 の整数バイトです。

d. [Action] フィールドで、指定した一致条件が満たされる場合に、仮想サーバが実行するアクションを選択します。

- [Drop]：指定した SIP トラフィックは仮想サーバによって廃棄されます。
- [Permit]：指定した SIP トラフィックは仮想サーバによって受信されます。
- [Reset]：指定した SIP トラフィックは仮想サーバによって拒否されます。

e. 次の手順を実行します。

- エントリを保存するには、[OK] をクリックします。[Conditions] テーブルは新しいエントリによってリフレッシュされます。
- [Cancel] をクリックすると、エントリを保存しないで [Conditions] サブセットを終了し、[Conditions] テーブルに戻ります。

f. [SIP Parameter Map] フィールドで、既存のパラメータ マップを選択するか、または [*New*] を選択して新しいパラメータ マップを設定します。

既存のパラメータ マップを選択すると、画面がリフレッシュされ、選択したパラメータ マップの設定の表示、変更、または削除ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

g. 表 8-9 の情報に従って、SIP パラメータ マップ オプションを設定します。

h. [Secondary Connection Parameter Map] フィールドで、既存のパラメータ マップを選択するか、または [*New*] を選択して新しいパラメータ マップを設定します。

既存のパラメータ マップを選択すると、画面がリフレッシュされ、選択したパラメータ マップの設定の表示、変更、または削除ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

i. 表 8-3 の情報に従って、セカンダリ接続パラメータ マップ オプションを設定します。

j. [Default Action] フィールドで、SIP プロトコル インスペクション用に指定した一致条件が満たされない場合に、仮想サーバが実行するデフォルトのアクションを選択します。

- [Drop]：指定した SIP トラフィックは仮想サーバによって廃棄されます。
- [Permit]：指定した SIP トラフィックは仮想サーバによって受信されます。
- [Reset]：指定した SIP トラフィックは仮想サーバによって拒否されます。

k. レイヤ 3 およびレイヤ 4 トラフィックの監視をイネーブルにするには、[Logging Enabled] チェックボックスをオンにします。イネーブルの場合、送信元または宛先 IP アドレスやアクセス対象の URL を含め、指定したクラスのトラフィックで送信される各 URL 要求がログに記録されます。レイヤ 3 およびレイヤ 4 トラフィックの監視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。

ステップ 9　仮想サーバのプロパティの設定が完了したら、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この手順を終了します。

関連トピック

- 「仮想サーバのプロパティの設定」（P.5-11）
- 「仮想サーバの SSL 終了の設定」（P.5-19）
- 「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）

仮想サーバ レイヤ 7 のロード バランシングの設定

レイヤ 7 ロード バランシングは、次のいずれか 1 つのプロトコルの組み合わせで利用できます。

- Generic、HTTP、HTTPS、RTSP、または SIP とともに使用する場合の TCP
- Generic、RADIUS、または SIP とともに使用する場合の UDP

これらのプロトコルの設定の詳細については、「仮想サーバのプロパティの設定」（P.5-11）を参照してください。

仮想サーバでレイヤ 7 ロード バランシングを設定するには、この手順を使用します。

前提

次のいずれか 1 つのプロトコルの組み合わせを使用して仮想サーバを設定しておきます。

- Generic、HTTP、HTTPS、RTSP、または SIP とともに使用する場合の TCP
- Generic、RADIUS、または SIP0 とともに使用する場合の UDP

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Virtual Servers] を選択します。

[Virtual Servers] テーブルが表示されます。

ステップ 2　レイヤ 7 ロード バランシングを設定する仮想サーバを選択し、[Edit] をクリックします。

[Virtual Server] 設定画面が表示されます。

ステップ 3　[L7 Load-Balancing] をクリックします。[Layer 7 Load-Balancing Rule Match] テーブルが表示されます。

ステップ 4　[Rule Match] テーブルで、[Add] をクリックして新しい一致条件およびアクションを追加するか、または既存の一致条件およびアクションを選択し、[Edit] をクリックしてそれを変更します。

[Rule Match] 設定ペインが表示されます。

ステップ 5　[Rule Match] フィールドで、既存のクラス マップまたは [*New*] または [*Inline Match*] を選択し、レイヤ 7 ロード バランシング用の新しい一致条件を設定します。

- 既存のクラス マップを選択する場合、既存の設定の確認、変更、または複製を行うには、[View] をクリックします。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。
- [*New*] または [*Inline Match*] をクリックする場合、[Rule Match] 設定サブセットが表示されます。

ステップ 6　表 5-8 のステップに従って、一致条件を設定します。

表 5-8　レイヤ 7 ロード バランシングの一致条件の設定

選択項目	アクション
Existing class map	1. [View] をクリックし、選択したクラス マップの一致条件情報を確認します。 2. 次の手順を実行します。 – [Cancel] をクリックすると、変更しないで続行し、前の画面に戻ります。 – [Edit] をクリックすると、既存の設定が変更されます。 – [Duplicate] をクリックすると、同じクラス マップを使用している他の仮想サーバに影響を与えずに、同じ属性で新しいクラス マップを作成します。 共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。
New	1. [Name] フィールドに、このクラス マップの一意な名前を入力します。 2. 複数の一致条件が存在する場合、[Matches] フィールドに、複数の一致文の評価に使用する方式を選択します。 – [Any]：一致条件の少なくとも 1 つが満たされる場合に一致することになります。 – [All]：すべての一致条件が満たされる場合にだけ一致することになります。 3. [Conditions] テーブルで、[Add] をクリックして新しい条件を追加するか、または既存の条件を選択し、[Edit] をクリックしてそれを変更します。 4. [Type] フィールドで一致条件を選択し、プロトコル固有のオプションを設定します。 – Generic プロトコル オプションの場合、表 12-8 を参照してください。 – HTTP および HTTPS プロトコル オプションの場合、表 5-9 を参照してください。 – RADIUS プロトコル オプションの場合、表 12-9 を参照してください。 – RTSP プロトコル オプションの場合、表 12-10 を参照してください。 – SIP プロトコル オプションの場合、表 12-11 を参照してください。 5. 表 5-9 の情報に従って、条件固有のオプションを設定します。 6. 次の手順を実行します。 – [OK] をクリックして、エントリを確定し、[Conditions] テーブルに戻ります。 – [Cancel] をクリックすると、エントリを保存しないでこの手順を終了し、[Conditions] テーブルに戻ります。
Inline Match	[Conditions Type] フィールドで、インライン一致条件のタイプを選択し、プロトコル固有のオプションを設定します。 • Generic プロトコル オプションの場合、表 12-8 を参照してください。 • HTTP および HTTPS プロトコル オプションの場合、表 5-9 を参照してください。 • RADIUS プロトコル オプションの場合、表 12-9 を参照してください。 • RTSP プロトコル オプションの場合、表 12-10 を参照してください。 • SIP プロトコル オプションの場合、表 12-11 を参照してください。

表 5-9　レイヤ 7 HTTP/HTTPS ロード バランシング ルールの一致設定

一致条件	説明
Class Map	このルールは、既存のクラス マップを使用して一致条件を確立します。 この方式を選択する場合、[Class Map] フィールドで、使用するクラス マップを選択します。 **（注）**　このオプションは、インライン一致条件では使用できません。
HTTP Content	HTTP entity-body に含まれている特定のコンテンツは、一致条件の確立に使用されます。 **1.** [Content Expression] フィールドに、照合するコンテンツを入力します。有効な入力は 1 ～ 255 文字の英数字ストリングです。 **2.** [Content Offset] フィールドに、ヘッダーとメッセージ ボディの間の空白行（CR、LF、CR、LF）より後ろにあって、メッセージ ボディの第 1 バイトから始まっていて無視するバイト数を入力します。有効な入力は 1 ～ 255 の整数です。
HTTP Cookie	HTTP cookie がこのルールに使用されます。 この方式を選択する場合 **1.** [Cookie Name] フィールドに、一意な cookie 名を入力します。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）。 **2.** [Cookie Value] フィールドに、一意な cookie 値式を入力します。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 255 文字）。ACE アプライアンス 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。 **3.** この一致条件を満たすために ACE アプライアンスが cookie 名と cookie 値を使用させるには、[Secondary Cookie Matching] チェックボックスを選択します。この一致条件を満たすために ACE アプライアンスが cookie 名と cookie 値のいずれかを使用させるには、このチェックボックスをクリアします。
HTTP Header	HTTP ヘッダーおよび対応する値をこのルールに使用します。 この方式を選択する場合 **1.** [Header Name] フィールドに、HTTP ヘッダーの汎用フィールドの名前を入力します。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）。 **2.** [Header Value] フィールドに、HTTP ヘッダー内の指定したフィールドの値と比較するヘッダー値式ストリングを入力します。有効な入力は英数字ストリングで、最大 255 文字です。ACE アプライアンスは、照合に正規表現をサポートしています。ヘッダー表現にはスペースを使用できますが、エスケープ シーケンスまたは引用符が必要です。ヘッダー マップのすべてのヘッダーは一致する必要があります。表 12-33 は、正規表現で使用できるサポート対象文字の一覧です。

表 5-9　レイヤ 7 HTTP/HTTPS ロード バランシング ルールの一致設定 （続き）

一致条件	説明
HTTP URL	このルールは、HTTP URL ストリングに基づき、特定の接続から受信したパケット データに対して正規表現照合を実行します。 この方式を選択する場合 1. [URL Expression] フィールドに、照合する URL または URL の一部を入力します。有効な入力は 1 ～ 255 文字の英数字の URL ストリングです。照合文には、www.hostname.domain に続く URL の一部だけを含めます。たとえば、URL が www.anydomain.com/latest/whatsnew.html の場合、/latest/whatsnew.html のみを含めます。www.anydomain.com 部分と一致させる場合は、URL 文字列を URL 正規表現の形式にすることができます。ACE アプライアンスは、URL 文字列の一致条件に正規表現をサポートしています。表 12-33 は、正規表現で使用できるサポート対象文字の一覧です。 2. [Method Expression] フィールドに、照合する HTTP メソッドを入力します。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）。方式は、標準 HTTP 1.1 方式名（OPTIONS、GET、HEAD、POST、PUT、DELETE、TRACE、または CONNECT）の 1 つにすることも、または厳密に一致しなければならないテキスト ストリング（CORVETTE など）にすることもできます。
Source Address	このルールは、クライアントの送信元 IP アドレスを使用して一致条件を確立します。 この方式を選択する場合 1. [Source Address] 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。ドット付き 10 進表記で IP アドレスを入力します（例：192.168.11.2）。 2. [Netmask] フィールドで、送信元 IP アドレスに適用するサブネット マスクを選択します。

表 5-9　レイヤ 7 HTTP/HTTPS ロード バランシング ルールの一致設定 （続き）

一致条件	説明
SSL	（注）　SSL オプションは、ACE NPE のソフトウェア バージョンに適用されません（「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）。 特定の SSL 暗号または暗号強度に基づいてロード バランシングの決定を定義します。ACE が、SSL 終了時に ACE との間でネゴシエートされる SSL 暗号化レベルに基づいて、各サーバ ファームにクライアント トラフィックを分散できるようにします。 この方式を選択する場合 1. [SSL Cipher Match Type] フィールドで、照合タイプを選択します。オプションは次のとおりです。 – [Equal To]：ロード バランシング決定用に SSL 暗号を指定します。 – [Less Than]：ロード バランシング決定用に SSL 暗号強度を指定します。 2. [Equal To] を選択した場合、[Cipher Name] フィールドには、ロード バランシング決定用の SSL 暗号を指定します。表示される値は次のとおりです。 – RSA_EXPORT1024_WITH_DES_CBC_SHA – RSA_EXPORT1024_WITH_RC4_56_MD5 – RSA_EXPORT1024_WITH_RC4_56_SHA – RSA_EXPORT_WITH_DES40_CBC_SHA – RSA_EXPORT_WITH_RC4_40_MD5 – RSA_WITH_3DES_EDE_CBC_SHA – RSA_WITH_AES_128_CBC_SHA – RSA_WITH_AES_256_CBC_SHA – RSA_WITH_DES_CBC_SHA – RSA_WITH_RC4_128_MD5 – RSA_WITH_RC4_128_SHA 3. [Less Than] を選択した場合、[Specify Minimum Cipher Strength] フィールドで、非包含最小 SSL 暗号ビット強度を指定します。たとえば、暗号強度に 128 を指定すると、128 に満たない SSL 暗号にはトラフィック ポリシーが適用されます。SSL 暗号が 128 ビット以上の場合、接続にはポリシーは適用されません。 表示される値は次のとおりです。 – [128]：128 ビット強度 – [168]：168 ビット強度 – [256]：256 ビット強度 – [56]：56 ビット強度

ステップ 7　[Primary Action] フィールドに、指定した一致条件と一致する場合にトラフィックに対して仮想サーバが実行するアクションを指定します。

- [Drop]：一致条件が満たされると、コンテンツに対するクライアント要求は廃棄されます。ステップ 10 に進みます。
- [Forward]：一致条件が満たされると、要求に対するロード バランシングを実行しないで、コンテンツに対するクライアント要求は転送されます。ステップ 10 に進みます。
- [Load Balance]：一致条件が満たされると、コンテンツに対するクライアント要求は、サーバ ファームに転送されます。ステップ 8 に進みます。
- [Sticky]：一致条件が満たされると、コンテンツに対するクライアント要求は、スティッキ グループによって処理されます。ステップ 8 に進みます。

ステップ 8　[Load Balance] をプライマリ アクションとして選択すると、サーバ ファーム、サーバ ファーム/バックアップ サーバ ファームのペア、既存のスティッキ グループ、または新しいスティッキ グループを使用してロード バランシングを設定できます。

上記のいずれかのシナリオで既存のオブジェクトを選択する場合、選択したオブジェクトの既存の設定の表示、変更、または複製ができます。仮想サーバでの共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

（注）　既存のサーバ ファームの統計情報とステータス情報を表示するには、リストのサーバ ファームを選択し、[Details] をクリックします。DM は、**show serverfarm** *name* **detail** CLI コマンドにアクセスして、詳細なサーバ ファーム情報を表示します。「サーバ ファームの統計情報およびステータス情報の表示」（P.6-38）を参照してください。

表 5-10 の情報に従って、ロード バランシングを設定します。

表 5-10　仮想サーバのロード バランシング オプション

設定内容	手順
サーバ ファームを使用したロード バランシング	[Server Farm] フィールドで、この仮想サーバのロード バランシングに使用するサーバ ファーム[1] を選択するか、または [*New*] を選択して新しいサーバ ファームを設定します（表 5-11 を参照）。
サーバ ファーム/バックアップ サーバ ファームのペアを使用したロード バランシング	1. [Server Farm] フィールドで、ロード バランシングに使用するプライマリ サーバ ファーム[1] を選択するか、または [*New*] を選択して新しいサーバ ファームを設定します（表 5-11 を参照）。 2. [Backup Server Farm] フィールドで、プライマリ サーバ ファームが利用できない場合にロード バランシング用のバックアップ サーバ ファームとして使用するサーバ ファーム[1] を選択するか、または [*New*] を選択して新しいバックアップ サーバ ファームを設定します（表 5-11 を参照）。

表 5-10　仮想サーバのロード バランシング オプション （続き）

設定内容	手順
既存のスティッキ グループを使用したロード バランシング	1. [Server Farm] フィールドで、ロード バランシングに使用するプライマリ サーバ ファーム[1]を選択します。これは、既存のスティッキ グループで指定したプライマリ サーバ ファームである必要があります。 2. [Backup Server Farm] フィールドで、ロード バランシングに使用するバックアップ サーバ ファーム[1]を選択します。これは、既存のスティッキ グループで指定したバックアップ サーバ ファームである必要があります。 3. [Sticky Group] フィールドで、使用するスティッキ グループを選択します。 （注）　スティッキ グループが [Sticky Group] フィールドに表示されるのは、設定済みのプライマリおよびバックアップ サーバ ファームがそれぞれ選択されている場合**だけ**です。スティッキ グループを選択し、別のプライマリまたはバックアップ サーバ ファームを選択すると、[Sticky Group] フィールドで選択したスティッキ グループは表示されなくなります。既存のスティッキ グループの設定を変更するには、[Stickiness] 設定画面でその変更を行います（[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Stickiness]）。
新しいスティッキ グループを使用したロード バランシング	1. [Server Farm] フィールドで、ロード バランシングに使用するプライマリ サーバ ファーム[1]を選択するか、または [*New*] を選択して新しいサーバ ファームを設定します（表 5-11 を参照）。 2. [Backup Server Farm] フィールドで、プライマリ サーバ ファームが利用できない場合にロード バランシング用のバックアップ サーバ ファームとして使用するサーバ ファーム[1]を選択するか、または [*New*] を選択して新しいバックアップ サーバ ファームを設定します（表 5-11 を参照）。 3. [Sticky Group] フィールドで、[*New*] を選択し、表 5-13 の情報に従って新しいスティッキ グループを設定します。 （注）　スティッキ グループを設定するコンテキストは、ACE アプライアンス リソースの一部をスティッキ性に割り当てるリソース クラスと関連付ける必要があります。リソース クラスの詳細については、「リソース クラスの管理」（P.4-36）を参照してください。

1. 既存のサーバ ファームを選択するときに、表示される機能ボタンを使用して次のことが実行できます。

- 表示される機能ボタンを使用して編集または複製できるサーバ ファームの設定を表示するには、[View] をクリックします。
- ポップアップ ウィンドウで、**show serverfarm** *sf_name* **detail** コマンドの出力を表示するには、[Details] をクリックします。このコマンドの出力は、サーバ ファームの設定情報を提供します。
- ポップアップウィンドウで **show buddy group** コマンドの出力を表示するには、[Buddy Group] をクリックします。このコマンドの出力では、仮想コンテキストで設定されたバディ グループのリストが表示されます（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）。

表 5-11　サーバ ファームの新しい属性

フィールド	説明
Name	このサーバ ファームの一意な名前を入力します。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。
Type	サーバ ファームのタイプを選択します。 • [Host]：コンテンツおよびサービスをクライアントに提供する実サーバから構成された標準的なサーバ ファームです。 デフォルトでは、バックアップ サーバ ファームを設定している場合で、プライマリ サーバ ファーム内のすべての実サーバが停止したときは、プライマリ サーバ ファームはバックアップ サーバ ファームにフェールオーバーします。フェールオーバーのしきい値を指定し、サービスに戻るには、次のオプションを使用します。 a. [Partial-Threshold Percentage] フィールドに、サーバ ファームの稼働状態を維持するためにアクティブにしておく必要のある、プライマリ サーバ ファーム内の実サーバの最小パーセンテージを入力します。アクティブな実サーバのパーセンテージがこのしきい値を下回ると、ACE はそのサーバ ファームを非稼働状態にします。有効な入力は 0 ～ 99 の整数です。 b. ACE がサーバ ファームを再稼働するために、[Back Inservice] フィールドで、アクティブにしておく必要のあるプライマリ サーバ ファーム内の実サーバの最小パーセンテージを入力します。有効な入力は 0 ～ 99 の整数です。このフィールドの値は、[Partial Threshold Percentage] フィールドの値より大きくする必要があります。 • [Redirect]：クライアント要求を、実サーバの設定で指定した代わりの場所にリダイレクトする実サーバだけから構成されたサーバ ファーム。
Fail Action	サーバ ファーム内の実サーバに障害が発生した場合に、ACE アプライアンスが接続に対して実行するアクションを選択します。 • [N/A]：サーバ ファーム内のサーバに障害が発生しても、ACE アプライアンスはアクションを実行しません。 • [Purge]：サーバ ファーム内の実サーバに障害が発生した場合、ACE アプライアンスは実サーバへの接続を解除します。ACE アプライアンスは、リセット コマンドをクライアント、および障害が発生したサーバの両方に送信します。 • [Reassign]：このコマンドの入力後に実サーバで障害が発生した場合、バックアップ用の実サーバ（設定されている場合）に ACE がその既存サーバ接続を再割り当てすることを示します。障害が発生したサーバにバックアップ用の実サーバが設定されていない場合に [Reassign] を選択すると、既存の接続は障害が発生した実サーバに接続できない状態となります。

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Failaction Reassign Across Vlans	このフィールドは、[L7 Load-Balancing Action] パラメータが次のように設定されている場合のみ表示されます。[Primary Action] : LoadBalance、[ServerFarm] : New、[Fail Action] : Reassign。 実サーバで障害が発生した場合、ACE が別の VLAN インターフェイス（一般にバイパス VLAN と呼ばれます）のバックアップ用の実サーバに既存サーバ接続を再割り当てするよう指定する場合は、このチェックボックスをオンにします。障害が発生したサーバにバックアップ用の実サーバが設定されていない場合、このオプションを設定しても無効になり、既存の接続は障害が発生した実サーバに接続できない状態となります。 このオプションをイネーブルにする場合は、次の設定要件と制約事項に注意してください。 • ACE の VIP アドレスをサーバの IP アドレスに変換する際に NAT を使用しないよう ACE に指示するには、[Transport] オプションをイネーブルにします（次のフィールドを参照）。[Failaction Reassign Across Vlans] オプションは、ACE で処理状態を把握するファイアウォール ロード バランシング（FWLB）に使用することを目的としています。ここで、ACE への接続用の宛先 IP アドレスはエンドポイントの実サーバで、ACE は、別のネクスト ホップで転送されるように接続を割り当てます。 • フロー内の同じサーバから出入りするパケットが同じファイアウォールまたはステートフル デバイスを通過するようにするため、すべてのサーバ側インターフェイスで [MAC Sticky] オプションをイネーブルにします（「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10）を参照）。 • [Predictor Hash Address] オプションを設定します。サポートされているプレディクタ方式、および各プレディクタ方式の設定可能な属性の詳細については、表 5-12 を参照してください。 • プライマリ インターフェイスとバックアップサーバのインターフェイスに対して同じポリシーを設定する必要があります。バックアップ インターフェイスは、プライマリ インターフェイスと同じ機能が設定されていることが必要です。 • プライマリサーバのインターフェイスのポリシーとは異なるポリシーをバックアップサーバのインターフェイスで設定した場合、そのポリシーは新しい接続に対してのみ有効になります。再割り当てされた接続には、プライマリサーバのインターフェイス ポリシーだけが常に設定されます。 • インターフェイス固有の機能（NAT、アプリケーション プロトコル インスペクション、アウトバウンド ACL、または SYN クッキーなど）はサポートされていません。 • 障害が発生した実サーバが復旧した後は、このサーバへの接続を再割り当てできません。この制約は、同じ VLAN バックアップ サーバにも適用されます。 • 実サーバは、ACE に直接接続する必要があります。この要件は、同じ VLAN バックアップ サーバにも適用されます。 • ファイアウォールのシーケンス番号のランダム化をディセーブルにする必要があります（「接続パラメータ マップの設定」（P.8-5）を参照）。 • プローブ設定は、両方の ACE で同一とする必要があり、インターバル値は低く設定する必要があります。たとえば、ACE-1 で高いインターバル値、ACE-2 で低いインターバル値を設定すると、再割り当てされた接続はプローブ設定の不一致により停止する場合があります。インターバル値が低い ACE-2 は、最初にプライマリ サーバの障害を検出し、着信接続をすべてバックアップサーバのインターフェイス VLAN に再割り当てします。インターバル値が高い ACE-1 は、プライマリ サーバが復旧する前に障害を検出しない場合があるので、プライマリ サーバを指し示し続けます。 パケット損失を最小限に抑えるために、両方の ACE で次に示すプローブ パラメータ値を推奨します。Interval : 2、Faildetect : 2、Passdetect interval : 2、Passdetect count : 5

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Transparent	このフィールドは、ホスト サーバとして特定されている実サーバにだけ表示されます。 VIP アドレスからサーバ IP アドレスへのネットワーク アドレス変換を指定するには、このチェックボックスをオンにします。VIP アドレスからサーバ IP アドレスへのネットワーク アドレス変換が行われないように指定するには、このチェックボックスをオフにします（デフォルト）。
Dynamic Workload Scaling	このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。 ローカル VM の平均 CPU 使用率、メモリ使用率、またはその両方が指定された最大しきい値に達すると、ACE はリモート VM にトラフィックをバーストさせることができます。ローカル VM の平均 CPU 使用率またはメモリ使用率が設定された最小しきい値まで低下すると、ACE はリモート VM へのトラフィックのバーストを停止します。このオプションは、Nexus 7000、VM Controller および VM プローブを使用して、ACE が動的ワークロード拡張用に設定されていることが必要です（「動的ワークロード拡張の設定」（P.6-14）を参照）。 次のオプション ボタンのオプションのいずれかをクリックします。 • [N/A]：適用しない（デフォルト）。 • [Local]：ACE は、ロード バランシングにのみ VM Controller ローカル VM を使用できます（バーストは使用できません）。 • [Burst]：ACE はリモート VM Controller VM にトラフィックをバーストさせることができます。 [Burst] を選択すると、[VM Probe Name] フィールドが使用可能な VM プローブの一覧とともに表示されます。使用可能な VM のプローブを選択するか、または [Add] をクリックするとヘルス モニタリングのポップアップ ウィンドウが表示され、新しい VM プローブを作成するか、または既存の VM プローブを編集できます（「ヘルス モニタリングの設定」（P.6-38）を参照）。
Fail-On-All	このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。 デフォルトでは、サーバ ファーム内に設定される実サーバは、そのサーバ ファーム上で直接設定されたプローブを継承します。1 つのサーバ ファームに複数のプローブを設定している場合、そのサーバ ファームの実サーバでは、これらのプローブに対して OR ロジックが使用されます。つまり、サーバ ファームに設定されているプローブの 1 つにエラーが発生した場合、このサーバ ファームにある実サーバすべてがエラーとなり、PROBE-FAILED 状態になります。 AND ロジックを使用すると、サーバ ファーム プローブの 1 つがエラーとなっても、サーバ ファーム内の実サーバは OPERATIONAL 状態を維持します。そのサーバ ファームに関連付けられているすべてのプローブがエラーになると、そのサーバ ファームのすべての実サーバがエラーとなり、PROBE-FAILED 状態になります。サーバ ファーム内の実サーバに直接設定するプローブにも AND ロジックを設定できます。 サーバ ファームの実サーバが複数のサーバ ファーム プローブに対して AND ロジックを使用させるには、このチェックボックスをオンにします。 Fail On All 関数はすべてのプローブ タイプに適用できます。

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Inband-Health Check	このフィールドが表示されるのは、ホスト サーバ ファームの場合だけです。 デフォルトでは、ACE は ARP およびヘルス プローブを使用して設定のすべての実サーバの状態を監視します。ただし、実サーバがダウンしたときと、ACE がその状態を認識したときとの間には遅延時間が生じます。インバンド ヘルス モニタリング機能では、ACE は次の接続障害からサーバ ファーム内の実サーバの状態を監視できます。 • TCP の場合、サーバまたは SYN タイムアウトからのリセット（RST）。 • UDP の場合、ICMP ホスト、ネットワーク、ポート、プロトコル、およびソース ルートの到達不能メッセージ。 障害カウントのしきい値を設定していて、障害の数がリセット時間内にしきい値を超えた場合、ACE はただちにそのサーバを [failed] のマークを付けて非稼働にし、ロード バランシングから除外します。サーバは、オプションの再開サービス期限が切れるまで、ロード バランシングの対象と見なされません。 次のいずれかを選択します。 • [Count] : TCP または UDP エラーの合計数を追跡し、**show serverfarm** *name* **inband** CLI コマンドで表示されるカウンタを増分します。 • [Log] : イベントの数が設定されている接続障害のしきい値に達すると、syslog エラー メッセージをログに記録します。 • [Remove] : ：イベントの数がしきい値に到達し、サーバをサービスから除外した場合、syslog エラー メッセージをログに記録します。 **（注）** サーバを監視するためにこの機能およびヘルス プローブを設定できます。設定を行う場合、サーバ ファーム内で実サーバを稼働状態に維持する必要があります。いずれかの機能がサーバが非稼働であることを検出した場合、ACE はこのサーバをロード バランシングの対象として選択しません。
Connection Failure Threshold Count	このフィールドは、[Inband-Health Check] が [Log] または [Remove] に設定されている場合にだけ表示されます。 ACE が実サーバに [failed] のマークを付ける前に、実サーバがリセット時間間隔を示すことができる接続の最大数を入力します。有効な値は 1 ～ 4294967295 の整数です。
Reset Timeout (Milliseconds)	このフィールドは、[Inband-Health Check] が [Log] または [Remove] に設定されている場合にだけ表示されます。 リセット時間間隔をミリ秒単位で入力します。有効な値は 100 ～ 300000 の整数です。デフォルトの間隔は、100 です。 この間隔は、ACE が接続障害を検出した時点で開始します。この間隔の間に接続障害のしきい値に到達すると、ACE は Syslog メッセージを生成します。[Inband-Health Check] が [Remove] に設定されている場合、ACE は、サービスからも実サーバを除外します。 このオプションの設定を変更すると、次の示すとおり実サーバの動作に影響します。 • 実サーバが OPERATIONAL 状態になると、一部の接続障害が発生していても、新しいリセット時間間隔は、次回接続エラーが発生したときに有効になります。 • 接続エラーが INBAND-HM-FAILED 状態の場合は、サーバが OPERATIONAL 状態に移行した後、次回接続エラーが発生したときに有効になります。

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Resume Service (Seconds)	このフィールドは、[Inband-Health Check] が [Remove] に設定されている場合にだけ表示されます。 [failed] とマークされたサーバが、アクティブな接続を送信することを再試行するまでの秒数を入力します。有効な値は 30 ～ 3600 の整数です。デフォルトの設定は 0 です。このオプションの設定は、次のとおり、インバンド障害状態の実サーバの動作に影響します。 • このフィールドが設定されず、デフォルト設定が 0 になっている場合、実サーバは、手動で一時停止され再びアクティブ化されるまで障害状態になります。 • このフィールドが設定されず、デフォルト設定が 0 で、このオプションを 30～3,600 の整数で設定した場合、障害が発生した実サーバはただちに動作状態に移行します。 • このフィールドを設定しており、値が大きくなると、実サーバは、以前設定した値の期間中障害状態のままになります。新しい値は、次回実サーバが障害状態に移行したときに有効になります。 • このフィールドを設定しており、値が小さくなると、障害が発生した実サーバはただちに動作状態に移行します。 • 30～3,600 の整数でこのフィールドを設定し、デフォルトの 0 にリセットした場合、実サーバは、以前設定した値の期間中障害状態のままになります。デフォルト設定は、次回実サーバが障害状態に移行したときに有効になります。その実サーバは、手動で一時停止され再びアクティブ化されるまで障害状態になります。 • リセット時間間隔内でこのフィールドを変更し、実サーバが複数の接続障害により OPERATIONAL 状態になると、新しいしきい値の間隔は、たとえ現在のリセット期間内にエラーが発生した場合でも、次回接続エラーが発生したときに有効になります。
Predictor	クライアント要求に応答する、サーバ ファーム内の次のサーバの選択方式を指定します。サーバ ファームのデフォルトのプレディクタ方式は、ラウンドロビンです。 サポートされているプレディクタ方式、および各プレディクタ方式の設定可能な属性の詳細については、表 5-12 を参照してください。

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Probes	使用するヘルス モニタリング用のプローブを指定します。 • ヘルス モニタリングに使用するプローブを含めるには、[Available] リストで目的のプローブを選択し、[Add] をクリックします。プローブが [Selected] リストに表示されます。 リダイレクト実サーバ プローブのリストに表示されるのは、タイプが Is Routed に設定されたプローブのみです。これは ACE が、ACE の内部ルーティング テーブルに従ってプローブのアドレスをルーティングすることを意味します（「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照）。 **（注）** サーバ ファームに IPv6 と IPv4 の両方のプローブを関連付けることができます。 **（注）** 使用可能なプローブのリストには VM のヘルス モニタリング プローブは含まれません。ローカル VM の使用率を監視するための VM プローブを選択するには、[Dynamic Workload Scaling] フィールドを参照してください。 • ヘルス モニタリングに使用しないプローブを削除するには、[Selected] リストで目的のプローブを選択し、[Remove] をクリックします。プローブが [Available] リストに表示されます。 • 使用するプローブの順序を指定するには、[Selected] リストでプローブを選択し、[Up] または [Down] をクリックして目的の順序にします。 • 既存のプローブの設定を表示するには、右側のリストでプローブを選択し、[View] をクリックします。 • 既存のプローブの統計情報とステータス情報を表示するには、右側のリストでプローブを選択し、[Details] をクリックします。DM は、**show probe** *name* **detail** CLI コマンドにアクセスして、詳細なプローブ情報を表示します。「ヘルス モニタリング統計情報およびステータス情報の表示」（P.6-67）を参照してください。 新しいプローブを追加するには、[Create] をクリックします。新しいヘルス モニタリング プローブの追加および特定のプローブ タイプの属性の定義の詳細については、「実サーバに対するヘルス モニタリングの設定」（P.6-40）を参照してください。また、[Server Farm] の [Probes] セクションで次のプローブ設定パラメータを設定します。 • [Expect Addresses] : [Expect Addresses] 設定画面で DNS プローブの予期アドレスを設定するには、[IPv4/IPv6 Address] フィールドに、ACE アプライアンス が DNS 要求へのサーバ応答として予期する IP アドレスを入力します。このフィールドに複数のアドレスを入力できます。ただし、IPv4 と IPv6 アドレスを混在させることはできません。 • [Probe Headers] : HTTP または HTTPS プローブのいずれかのプローブ ヘッダーを設定するには、[Probe Headers] フィールドに、*header_name=header_value* というフォーマットで、HTTP ヘッダーの名前と照合対象の値を入力します。 – *header_name* は、プローブが使用する HTTP ヘッダーです。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）。最大長の限界を超えないかぎり、定義済みのヘッダーまたは他のカスタム ヘッダー名を指定できます。 – *header_value* ヘッダー フィールドに割り当てる文字列です。有効な入力は、255 文字以下のテキスト文字列です。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。

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Probes （続き）	• [Probe Expect Status] : FTP、HTTP、HTTPS、RTSP、SIP-TCP、SIP-UDP、または SMTP プローブのプローブ予期ステータスを設定する場合は、[Probe Expect Status] フィールドで、次の情報を入力します。 – 単一の予期ステータス コードを設定する場合は、このプローブの最小の予想ステータス コードを入力し、次に最小値として入力したものと同じ予想ステータス コードを入力します。有効な入力は 0 ～ 999 の整数です。 – 予期ステータス コードの範囲を設定する場合は、ステータス コードの範囲の下限を入力し、次にステータス コードの範囲の上限を入力します。最大予想ステータス コードは、最小予想ステータス コードの数値以上にする必要があります。有効な入力は 0 ～ 999 の整数です。 • [SNMP OID Table] : SNMP プローブの SNMP OID を設定するには、「SNMP プローブの OID の設定」（P.6-66）を参照してください。 プローブを追加したら、「実サーバに対するヘルス モニタリングの設定」（P.6-40）の説明に従って、[Health Monitoring] テーブル（[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Health Monitoring]）からヘルス プローブの属性を変更できます。[Health Monitoring] テーブルから既存のヘルス プローブを削除することもできます。

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Real Servers	[Real Servers] テーブルでは、実サーバの追加、変更、削除、または順序変更ができます。 1. 既存のサーバを選択するか、または [Add] をクリックして実サーバをサーバ ファームに追加します。 – 既存のサーバを選択すると、サーバの既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。 – [Add] をクリックすると、テーブルはリフレッシュされ、サーバ情報を入力できるようになります。 2. [IP Address Type] に、[IPv6] または [IPv4] を選択します。 3. [IP Address] フィールドに、IP アドレスを入力します。 4. [Name] フィールドに、実サーバの名前を入力します。 5. [Port] フィールドに、サーバのポート アドレス変換（PAT）に使用するポート番号を入力します。有効な入力は 1 ～ 65535 の整数です。 6. [Weight] フィールドに、サーバ ファーム内のこのサーバに割り当てる重みを入力します。有効な入力は 1 ～ 100 の整数で、デフォルトは 8 です。 7. [Redirection Code] フィールドで、適切なリダイレクション コードを選択します。このフィールドが表示されるのは、実サーバがリダイレクト サーバとして指定された場合だけです。 – [N/A] : Web ホスト リダイレクション コードは定義されていないことを示します。 – [301] : 要求されたリソースは完全に移動されたことを示します。クライアントは、今後このリソースを参照する場合、返された URI のいずれかを使用する必要があります。 – [302] : 要求されたリソースは検出されましたが、一時的に別の場所に移されていることを示します。リソースは別の場所に移されることもあるため、クライアントは、今後このリソースを参照する場合、引き続き、要求 URI を使用する必要があります。 8. [Web Host Redirection] フィールドに、別のサーバへのリダイレクト要求に使用される URL ストリングを入力します。このフィールドが表示されるのは、実サーバがリダイレクト サーバとして指定された場合だけです。要求を別のサーバにリダイレクトする際に使用する URL とポートを入力します。有効な値は、http://host.com:port の形式です（host はサーバの名前、port は使用されるポート）。有効なホスト エントリは、引用符で囲まずスペースを含まない 255 文字以下のテキスト文字列です。有効なポート番号は 1 ～ 65535 です。 リロケーション文字列は、次の特殊文字をサポートしています。 – %h : 要求のホスト ヘッダーからホスト名を挿入します。 – %p : 要求から URL パス文字列を挿入します。 9. [Rate Bandwidth] フィールドで、実サーバの帯域幅の制限をバイト / 秒で指定します。有効な入力は 1 ～ 300000000 の整数です。 10. [Rate Connection] フィールドで、1 秒あたりの接続の制限を指定します。有効な入力は 1 ～ 350000 の整数です。 11. [State] フィールドで、このサーバの管理ステートを選択します。 – [In Service] : サーバは、サーバのロード バランシング用の宛先として使用されます。 – [In Service Standby] : サーバはバックアップ サーバとなり、プライマリ サーバに障害が発生しないかぎり非アクティブのままです。プライマリ サーバに障害が発生すると、バックアップ サーバはアクティブになり、接続の受信を開始します。 – [Out Of Service] : サーバは、クライアント接続用の宛先として、サーバ ロード バランサによって使用されることはありません。

表 5-11　サーバ ファームの新しい属性 （続き）

フィールド	説明
Real Servers（続き）	**12.** [Buddy Real Group] フィールドで、バディ実サーバ グループを作成または既存のグループから選択して、実サーバとバディ グループを関連付けます（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）。 **13.** [Fail-On-All] フィールドでこのチェックボックスをオンにすると、関連付けられているプローブすべてでエラーが発生しない限り、実サーバは OPERATIONAL 状態のままになるように設定されます（AND ロジック）。[Fail-On-All] 機能はすべてのプローブ タイプに適用できます。 [Fail-On-All] は、ホスト実サーバにだけ適用できます。 **14.** [Cookie String] フィールドに、実サーバの cookie 文字列値を入力します。これは、スティッキ接続を確立するときの HTTP cookie 挿入に使用されます。有効な入力は英数字ストリングで、最大 32 文字です。cookie 文字列値にはスペースや特殊文字を入力できます。HTTP cookie スティッキ接続の詳細については、第 7 章「スティッキ機能の設定」を参照してください。 [Cookie String] は、ホスト実サーバにだけ適用できます。 **15.** 次の手順を実行します。 – [OK] をクリックして、エントリを確定し、この実サーバをサーバ ファームに追加します。テーブルは最新の情報でリフレッシュされます。 – エントリを保存せずに手順を終了し、[Real Servers] テーブルに戻るには、[Cancel] をクリックします。 既存の実サーバの統計情報とステータス情報を表示するには、リストの実サーバを選択し、[Details] をクリックします。DM は、**show rserver** *name* **detail** CLI コマンドにアクセスして、詳細な実サーバ情報を表示します。「実サーバの統計情報およびステータス情報の表示」（P.6-9）を参照してください。

表 5-12　プレディクタ方式および属性

プレディクタ方式	説明 / 処理
Hash Address	ACE は、送信元または宛先 IP アドレスに基づいてハッシュ値を使用して、サーバを選択します。 ハッシュ アドレス プレディクタ方式を設定するには、次の手順を実行します。 1. [Mask Type] フィールドで、送信元 IP アドレスと宛先 IP アドレスのどちらを基にしてサーバを選択するかを指定します。 – [N/A]：このオプションは定義されていません。 – [Destination]：宛先 IP アドレスに基づいてサーバが選択されます。 – [Source]：送信元 IP アドレスに基づいてサーバが選択されます。 2. [IP Netmask] フィールドで、アドレスに適用するサブネット マスクを選択します。指定しない場合、デフォルトは 255.255.255.255 です。
Hash Content	ACE は、HTTP パケット本体の指定したコンテンツ ストリングに基づきハッシュ値を使用して、サーバを選択します。 1. [Begin Pattern] フィールドに、コンテンツ ストリングの開始パターン、およびハッシュ前に一致させるパターン ストリングを入力します。開始パターンを指定しないと、ACE はオフセット バイトの直後の HTTP ボディの解析を開始します。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）。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。 2. [End Pattern] フィールドに、ハッシュの終了を示すパターンを入力します。長さも終了パターンも指定しないと、ACE はフィールドの最後またはパケットの最後に到達するか、あるいは最大ボディ解析長に到達するまで、データを解析します。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）。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。 3. [Length] フィールドに、ACE がクライアントをサーバに固定するために使用するコンテンツ部分の長さ（オフセット値の後ろのバイトからの長さ）をバイト単位で入力します。有効な入力は 1 ～ 1000 の整数バイトです。 オフセットと長さは 0 ～ 1000 バイトまで変更できます。ペイロード値がオフセットよりも長く、オフセット + ペイロードの長さの値よりも短い場合、ACE は、オフセット値の後ろのバイトを始点とし、オフセット + 長さで指定されるバイトを終点とするペイロード部分に基づいて接続を固定します。オフセットと長さの合計は、1000 バイト以下にする必要があります。 ハッシュ コンテンツ プレディクタには、長さと終了パターン オプションの両方を指定することはできません。 4. [HTTP Content Offset] フィールドに、ペイロードの最初のバイトから無視するバイト数を示すことにより、ACE が特定のサーバにクライアントを固定するために使用するコンテンツ部分を入力します。有効な入力は 0 ～ 999 の整数バイトです。デフォルトは 0 です。デフォルトでは、ACE はコンテンツのどの部分も除外しません。
Hash Cookie	ACE は、cookie 名に基づくハッシュ値を使用してサーバを選択します。 [Cookie Name] フィールドに、スペースを入れない引用符なしのテキスト ストリングの形式で、最大 64 文字で cookie 名を入力します。

表 5-12　プレディクタ方式および属性 （続き）

プレディクタ方式	説明 / 処理
Hash Secondary Cookie	ACE は、cookie ヘッダーではなく、URL クエリー ストリングで指定された cookie 名に基づくハッシュ値を使用して、サーバを選択します。 [Cookie Name] フィールドに、スペースを入れない引用符なしのテキスト ストリングの形式で、最大 64 文字で cookie 名を入力します。
Hash Header	ACE は、ヘッダー名に基づくハッシュ値を使用してサーバを選択します。 [Header Name] フィールドで、サーバの選択に使用する HTTP ヘッダーを選択します。 • 標準 HTTP ヘッダーの 1 つではない HTTP ヘッダーを指定するには、1 番めのオプション ボタンを選択し、[Header Name] フィールドに HTTP ヘッダー名を入力します。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。 • 標準 HTTP ヘッダーの 1 つを指定するには、2 番めのオプション ボタンを選択し、リストから HTTP ヘッダーの 1 つを選択します。
Hash Layer 4	ACE は、レイヤ 4 汎用プロトコル ロード バランシング方式を使用してサーバを選択します。ACE の正式なサポート対象ではないプロトコルからのパケットのロード バランシングを行う場合は、このプレディクタを使用します。 **1.** [Begin Pattern] フィールドに、レイヤ 4 ペイロードの開始パターン、およびハッシュ前に一致させるパターン ストリングを入力します。開始パターンを指定しないと、ACE はオフセット バイトの直後の HTTP ボディの解析を開始します。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）。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。 **2.** [End Pattern] フィールドに、ハッシュの終了を示すパターンを入力します。長さも終了パターンも指定しないと、ACE はフィールドの最後またはパケットの最後に到達するか、あるいは最大ボディ解析長に到達するまで、データを解析します。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）。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。 **3.** [Length] フィールドに、ACE がクライアントをサーバに固定するために使用するペイロード部分の長さ（オフセット値の後ろのバイトからの長さ）をバイト単位で入力します。有効な入力は 1 ～ 1000 の整数バイトです。 オフセットと長さは 0 ～ 1000 バイトまで変更できます。ペイロード値がオフセットよりも長く、オフセット + ペイロードの長さの値よりも短い場合、ACE は、オフセット値の後ろのバイトを始点とし、オフセット + 長さで指定されるバイトを終点とするペイロード部分に基づいて接続を固定します。オフセットと長さの合計は、1000 バイト以下にする必要があります。 ハッシュ レイヤ 4 プレディクタには、長さと終了パターン オプションの両方を指定することはできません。 **4.** [HTTP Content Offset] フィールドに、ペイロードの最初のバイトから無視するバイト数を示すことにより、ACE が特定のサーバにクライアントを固定するために使用するコンテンツ部分を入力します。有効な入力は 0 ～ 999 の整数バイトです。デフォルトは 0 です。デフォルトでは、ACE はコンテンツのどの部分も除外しません。

表 5-12　プレディクタ方式および属性 （続き）

プレディクタ方式	説明/処理
Hash URL	ACE は、URL に基づくハッシュ値を使用してサーバを選択します。ファイアウォールに対してロード バランシングを行うには、この方式を使用します。 パターン フィールドの一方または両方に値を入力します。 • [URL Begin Pattern] フィールドに、URL の開始パターン、および解析するパターン ストリングを入力します。 • [URL End Pattern] フィールドに、URL の終了パターン、および解析するパターン ストリングを入力します。 これらのフィールドには、設定するパターンごとに、引用符で囲まずにスペースを入れないで 255 文字以内で英数字を入力します。
Least Bandwidth	ACE は指定サンプル期間のネットワーク トラフィックが最小のサーバを選択します。 1. [Assess Time] フィールドに、ACE がトラフィック情報を収集する秒数を入力します。有効な入力は 1 ～ 10 の整数秒です。 2. [Least Bandwidth Samples] フィールドに、最終負荷値を計算するためにプローブ クエリーの結果を加重平均するサンプル数を入力します。有効な入力は 1、2、4、8、および 16（2 のべき乗でもある 1 ～ 16 の整数）です。
Least Connections	ACE は接続数の最も少ないサーバを選択します。 [Slowstart Duration] フィールドに、このプレディクタ方式に適用する slow-start 値を入力します。有効な入力は 1 ～ 65535 の整数で、1 は最も遅い ramp-up 値です。 稼働させたばかりのサーバに高い割合で新規接続を送信することを避けるには、スロースタート メカニズムを使用します。
Least Loaded	ACE は SNMP プローブからの情報に基づいて、負荷が最小のサーバを選択します。 1. [SNMP Probe Name] フィールドで、使用する SNMP プローブの名前を選択します。 2. [Auto Adjust] フィールドで、負荷が 0 に達した実サーバに対して 16000 の最大負荷を適用するか、またはデフォルトの動作を上書きするよう ACE に指示する自動調整機能を設定します。デフォルトでは、ACE は負荷が 0 になった実サーバに、サーバ ファームの平均負荷を適用します。ACE は、サーバの SNMP プローブと設定されたその他のオプションからのフィードバックに基づいて、この負荷の値を定期的に調整します。 オプションは次のとおりです。 – [Average]：負荷が 0 になった実サーバに、サーバ ファームの平均負荷を適用します。この設定により、サーバがロード バランシングに参加できると同時に、そのサーバに新規の接続があふれるのを防ぎます。これがデフォルト設定です。 – [Maxload]：負荷が 0 になった実サーバに、16000 の最大負荷を適用するように ACE に指示します。 – [Off]：このサーバに対する次回の負荷更新が SNMP プローブから届くまで、負荷が 0 になったサーバにすべての新規接続を送信するよう ACE に指示します。2 つのサーバの負荷値が同一で、しかも最小（ゼロまたはゼロ以外）である場合、ACE は接続の負荷をラウンドロビン方式で 2 つのサーバに分散させます。 3. ACE で実サーバの最終負荷計算に現在の接続数が使用されるようにするには、[Weight Connection] フィールドで、このチェックボックスをオンにします。このオプションを設定した場合、ACE でサーバ ファームの個々の実サーバに対する総負荷計算に現在の接続数が含まれるようになります。ACE の動作をリセットして、負荷の計算から現在の接続数が除外されるようにする（デフォルト）には、このチェックボックスをオフにします。

表 5-12　プレディクタ方式および属性 （続き）

プレディクタ方式	説明 / 処理
Response	ACE は、要求された応答時間の測定に対して、応答時間が最小のサーバを選択します。 1. [Response Type] フィールドで、使用する測定タイプを選択します。 – [App-Req-To-Resp] : ACE がサーバに HTTP 要求を送信してから、ACE がその要求に対する応答をサーバから受信するまでの応答時間です。 – [Syn-To-Close] : ACE がサーバに TCP SYN を送信してから、ACE がそのサーバから CLOSE を受信するまでの応答時間です。 – [Syn-To-Synack] : ACE がサーバに TCP SYN を送信してから、ACE がそのサーバから SYN-ACK を受信するまでの応答時間です。 2. [Response Samples] フィールドに、応答時間の測定結果を平均するサンプル数を入力します。有効な入力は 1、2、4、8、および 16（2 のべき乗でもある 1 ～ 16 の整数）です。 3. ACE で実サーバの最終負荷計算に現在の接続数が使用されるようにするには、[Weight Connection] フィールドで、このチェックボックスをオンにします。このオプションを設定した場合、ACE でサーバ ファームの個々の実サーバに対する総負荷計算に現在の接続数が含まれるようになります。ACE の動作をリセットして、負荷の計算から現在の接続数が除外されるようにする（デフォルト）には、このチェックボックスをオフにします。
Round Robin	ACE はサーバの重みに基づいて、サーバのリストから次のサーバを選択します。これはデフォルトのプレディクタ方式です。

表 5-13　スティッキ グループの属性

フィールド	説明
Group Name	このスティッキ タイプの一意な識別子を入力します。自動的に 1 ずつ増える値で確定するか、または自分で値を入力します。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）。
Type	スティッキ接続を確立する場合に使用する方式を選択します。 • [HTTP Content]：仮想サーバは、HTTP パケットのデータ部のストリングに基づき、クライアント接続を同じ実サーバに対して固定します。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]：仮想サーバは、cookie をクライアント要求の HTTP ヘッダーから学習するか、または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、学習済みの cookie を使用してトランザクション中のクライアントとサーバの間のスティッキ性を得ます。 • [HTTP Header]：仮想サーバは、HTTP ヘッダーに基づき、同じ実サーバに対してクライアント接続を固定します。 • [IPv4 Netmask]：トランザクションの完了の必要に応じて、仮想サーバは、クライアントの送信元 IPv4 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対してクライアントを同じサーバに固定します。 **（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。 • [V6 Prefix]：トランザクションの完了の必要に応じて、仮想サーバは、クライアントの送信元 IPv6 アドレス、宛先 IPv6 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対してクライアントを同じサーバに固定します。 • [Layer 4 Payload]：仮想サーバは、レイヤ 4 プロトコル パケットのペイロード部のストリングに基づき、クライアント接続を同じ実サーバに対して固定します。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]：仮想サーバは、RADIUS 属性に基づき、同じ実サーバに対してクライアント接続を固定します。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]：仮想サーバは、[RTSP Session] ヘッダー フィールドに基づき、同じ実サーバに対してクライアント接続を固定します。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]：仮想サーバは、[SIP Call-ID] ヘッダー フィールドに基づき、同じ実サーバに対してクライアント接続を固定します。
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）。

表 5-13　スティッキ グループの属性 （続き）

フィールド	説明
Enable Insert	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。 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 を挿入させるには、このチェックボックスを選択します。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 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 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)	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。 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。有効な入力は 1 ～ 1000 の整数です。
Secondary 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。 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。
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。
Netmask	このフィールドは、スティッキ タイプの IP Netmask に表示されます。このフィールドは、スティッキ タイプ V6 のプレフィックスに対して任意選択です。 送信元 IPv4 アドレス、宛先 IPv4 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。
Prefix Length	このフィールドは、スティッキ タイプの V6 Prefix に表示されます。このフィールドは、スティッキ タイプ IP Netmask に対して任意選択です。 送信元 IPv6 アドレス、宛先 IPv6 アドレス、またはその両方に適用するプレフィックス長を入力します。
Address Type	このフィールドは、スティッキ タイプの IP Netmask に表示されます。 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。

表 5-13　スティッキ グループの属性 （続き）

フィールド	説明
Sticky Server Farm	このスティッキ グループのプライマリ サーバとして使用する既存のサーバ ファームを選択するか、[*New*] を選択した新しいサーバ ファームを作成します。[*New*] を選択する場合、表 5-11 の指示に従ってサーバ ファームを設定します。
Backup Server Farm	このスティッキ グループのバックアップ サーバとして使用する既存のサーバ ファームを選択するか、[*New*] を選択した新しいサーバ ファームを作成します。[*New*] を選択する場合、表 5-11 の指示に従ってサーバ ファームを設定します。
Aggregate State	プライマリ サーバ ファームのステートを、（設定されている場合）サーバ ファーム内およびバックアップ サーバ ファーム内のすべての実サーバのステートに結び付けるには、このチェックボックスを選択します。ACE アプライアンスは、プライマリ サーバ ファーム内のすべての実サーバおよびバックアップ サーバ ファーム内のすべての実サーバがダウンしている場合、プライマリ サーバ ファームのダウンを宣言します。 プライマリ サーバ ファームのステートを、サーバ ファーム内およびバックアップ サーバ ファーム内のすべての実サーバのステートに結び付けない場合は、このチェックボックスをクリアします。
Enable Sticky On Backup Server Farm	バックアップ サーバ ファームをスティッキに指定する場合は、このチェックボックスをオンにします。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	バディ スティッキ グループを作成するか、既存のグループを選択して、バディ メンバ グループとサーバ ファームを関連付けます（詳細情報については、「バディ スティッキ グループ」（P.7-6）を参照）。
Replicate On HA Peer	仮想サーバがバックアップ サーバ ファームのスティッキ テーブル エントリを複製させるには、このチェックボックスを選択します。フェールオーバーが実行され、このオプションが選択されている場合、新しいアクティブなサーバ ファームは既存のスティッキ接続を維持できます。 仮想サーバがバックアップ サーバ ファームのスティッキ テーブル エントリを複製しないようにするには、このチェックボックスをクリアします。
Timeout (Minutes)	最新のクライアント接続の終了後に、仮想サーバがスティッキ テーブルにクライアント接続のスティッキ情報を維持しておく分数を入力します。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。
Timeout Active Connections	スティッキ タイマーの期限切れ後にアクティブな接続が存在する場合であっても、仮想サーバがスティッキ テーブル エントリをタイムアウトにさせるには、このチェックボックスを選択します。 スティッキ タイマーの期限切れ後にアクティブな接続が存在する場合であっても、仮想サーバがスティッキ テーブル エントリをタイムアウトにしないようにするには、このチェックボックスをクリアします。これはデフォルトの動作です。

ステップ 9　[Compression Method] フィールドで、クライアント ブラウザがパケット圧縮に対応できることをクライアント要求が示している場合に、ACE アプライアンスがパケットを圧縮する方法を示す HTTP 圧縮方式を選択します。デフォルトでは、ACE の HTTP 圧縮はディセーブルです。ACE で HTTP 圧縮を設定すると、ACE は実サーバからの HTTP GET 応答内のデータを圧縮します。ACE は、クライアントからの HTTP 要求、またはサーバ応答内の HTTP ヘッダーを圧縮しません。

（注）　デフォルトでは、ACE は 100 メガビット/秒（Mbps）のレートで HTTP 圧縮をサポートしています。オプションの HTTP 圧縮ライセンスをインストールすると、この値を最大 2 Gbps まで大きくすることができます。ACE ライセンス オプションの詳細については、『*Administration Guide, Cisco ACE Application Control Engine*』を参照してください。

オプションは次のとおりです。

- [Deflate] : クライアント ブラウザが deflate および gzip 圧縮方式をサポートしている場合に使用する方式として deflate 圧縮フォーマットを指定します。deflate は、RFC1951 に記載されているデータの圧縮フォーマットです。
- [Gzip] : クライアント ブラウザが deflate および gzip 圧縮方式をサポートしている場合に使用する方式として gzip 圧縮フォーマットを指定します。gzip は、RFC1952 に記載されているファイルの圧縮フォーマットです。
- [N/A] : HTTP 圧縮はディセーブルです。

HTTP 圧縮を設定する場合、HTTP 圧縮から次の MIME タイプを除外することを推奨します。「.*gif」、「.*css」、「.*js」、「.*class」、「.*jar」、「.*cab」、「.*txt」、「.*ps」、「.*vbs」、「.*xsl」、「.*xml」、「.*pdf」、「.*swf」、「.*jpg」、「.*jpeg」、「.*jpe」、「.*png」。

HTTP 圧縮をイネーブルにすると、ACE は次のデフォルトの圧縮パラメータ値を使用してパケットを圧縮します。

- [Mime type] : あらゆるテキスト フォーマット（text/*）
- [Minimum size] : 512 バイト
- [User agent] : なし

ステップ 10　[SSL Initiation] フィールドで、既存のサービスを選択するか、または [*New*] を選択して新しいサービスを作成します。

（注）　[SSL Initiation] フィールドは、[Advanced View] にだけ表示され、選択されたプロトコルが TCP であって、Other、HTTP、または HTTPS がアプリケーション プロトコルの場合に表示されます。

（注）　SSL 開始オプションは、ACE NPE のソフトウェア バージョンに適用されません（「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）。

SSL 開始では仮想サーバは、自身と SSL サーバとの SSL 接続を開始および維持する SSL プロキシ クライアントとして機能させることができます。この特定の用途では、ACE はクリア テキストを HTTP クライアントから受け取り、そのデータを暗号化して暗号文として SSL サーバに送信します。一方、ACE は SSL サーバから受け取った暗号文を復号化し、そのデータをクリア テキストとしてクライアントに送信します。

- 既存の SSL サービスを選択すると、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。
- [*New*] を選択する場合、表 5-14 の指示に従ってサービスを設定します。

表 5-14　仮想サーバの SSL 開始の属性

フィールド	説明
Name	この SSL プロキシ サービスの名前を入力します。有効な入力は英数値ストリングで、最大 26 文字です。
Keys	データ暗号化のための SSL ハンドシェイク時に使用する SSL キー ペアを選択します。
Certificates	SSL ハンドシェイク時に使用する SSL 認証を選択します。

表 5-14　仮想サーバの SSL 開始の属性 （続き）

フィールド	説明
Chain Groups	SSL ハンドシェイク時に使用するチェーン グループを選択します。
Auth Groups	このプロキシ サーバ サービスに関連付ける SSL 認証グループを選択します。
CRL Best-Effort	このオプションが表示されるのは、[Auth Group Name] フィールドで認証グループを選択した場合です。 CRL がエクステンションに含まれているかどうかを判別し、値が存在する場合にその値を取得するサービスを求めて、ACE がクライアント証明書を調べることができるようにする場合に、このチェックボックスを選択します。 この機能をディセーブルにするには、チェックボックスをクリアします。
CRL Name	このオプションが表示されるのは、[CRL Best-Effort] チェックボックスがクリアされている場合です。 ACE でこのプロキシ サービスを使用する場合は、[CRL] を選択します。
Parameter Maps	このプロキシ サーバ サービスに関連付ける SSL パラメータ マップを選択します。

SSL の詳細については、「SSL の設定」（P.9-1）を参照してください。

ステップ 11　[Insert HTTP Headers] フィールドに、***header_name=header_value*** というフォーマットで、HTTP ヘッダーの名前と照合対象の値を入力します。

- ***header_name*** は、クライアント HTTP 要求に挿入する HTTP ヘッダーの名前です。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）。最大長の限界を超えないかぎり、定義済みのヘッダーまたは他のカスタム ヘッダー名を指定できます。
- ***header_value*** は、HTTP ヘッダー内に指定したフィールドの値と照合する式ストリングです。有効な入力は英数字ストリングで、最大 255 文字です。ACE アプライアンスは、照合に正規表現をサポートしています。ヘッダー表現にはスペースを使用できますが、エスケープ シーケンスまたは引用符が必要です。ヘッダー マップのすべてのヘッダーは一致する必要があります。表 12-33 は、正規表現で使用できるサポート対象文字の一覧です。

たとえば、`Host=www.cisco.com` と入力できます。

ステップ 12　次の手順を実行します。

- [OK] をクリックすると、エントリを保存し、[Rule Match] テーブルに戻ります。
- [Cancel] をクリックすると、エントリを保存せずに作業を終了し、[Rule Match] テーブルに戻ります。

ステップ 13　新しい仮想サーバに対する [Rule Match] エントリを追加し、[Virtual Server] 設定ページの [L7 Load Balancing] セクション内のルールの順序を変更する場合は、[Up] または [Down] をクリックして、[Rule Match] テーブルのエントリの順序を変更します。

（注）　[Up] ボタンと [Down] ボタンは新しい仮想サーバでのみ利用可能です。既存の仮想サーバでは利用可能ではありません。既存の仮想サーバに対する [Rule Match] テーブルのエントリの順序を変更するには、[Config] > [Expert] > [Policy Maps] に移動し、レイヤ 7 ロード バランシング ポリシー マップを選択し、順序を変更するエントリを削除し、[Insert Before] オプションを使用してもう一度エントリを追加し、正しい順序に移します。詳細については、「ポリシー マップの規則およびアクションの設定」（P.12-37）を参照してください。

ステップ 14　仮想サーバのプロパティの設定が完了したら、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この手順を終了します。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバのプロパティの設定」（P.5-11）
- 「仮想サーバの SSL 終了の設定」（P.5-19）
- 「仮想サーバのプロトコル インスペクションの設定」（P.5-21）

仮想サーバのデフォルトのレイヤ 7 ロード バランシングの設定

指定済みの一致条件に一致しないすべてのネットワーク トラフィックに対して、デフォルトのレイヤ 7 ロード バランシング動作を設定するには、この手順を使用します。

前提

仮想サーバを設定しておきます。仮想サーバの設定の詳細については、「仮想サーバの設定」（P.5-2）を参照してください。

手順

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

ステップ 2　デフォルトのレイヤ 7 ロード バランシングを設定する仮想サーバを選択し、[Edit] をクリックします。[Virtual Server] 設定画面が表示されます。

ステップ 3　[Default L7 Load-Balancing Action] をクリックします。[Default L7 Load-Balancing Action] 設定ペインが表示されます。

ステップ 4　[Primary Action] フィールドで、指定した一致条件が満たされない場合に、コンテンツに対するクライアント要求に応じて仮想サーバが実行するデフォルトのアクションを指定します。

- [Drop]：指定した一致条件を満たさないクライアント要求は廃棄されます。ステップ 7 に進みます。
- [Forward]：指定した一致条件を満たさないクライアント要求は、要求に対してロード バランシングを実行しないで転送されます。ステップ 7 に進みます。
- [Load Balance]：コンテンツに対するクライアント要求は、サーバ ファームに転送されます。[Load Balance] を選択すると、サーバ ファーム、バックアップ サーバ ファーム、およびスティッキ設定オプションが表示されます。ステップ 5 に進みます。
- [Sticky]：一致条件が満たされると、コンテンツに対するクライアント要求は、スティッキ グループによって処理されます。ステップ 6 に進みます。

ステップ 5　[Load Balance] をプライマリ アクションとして選択すると、サーバ ファーム、サーバ ファーム/バックアップ サーバ ファームのペア、既存のスティッキ グループ、または新しいスティッキ グループを使用してロード バランシングを設定できます。

（注） 上記のいずれかのシナリオで既存のオブジェクトを選択する場合、選択したオブジェクトの既存の設定の表示、変更、または複製ができます。仮想サーバでの共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

表 5-10 の情報に従って、ロード バランシングを設定します。

ステップ 6　（任意）[Sticky] をプライマリ アクションとして選択する場合、[Sticky Group] フィールドで、既存のスティッキ グループを選択するか、[*New*] をクリックして新しいスティッキ グループを追加します（表 5-13 を参照）。

（注） 既存のサーバ ファームの統計情報とステータス情報を表示するには、リストのサーバ ファームを選択し、[Details] をクリックします。DM は、**show serverfarm** *name* **detail** CLI コマンドにアクセスして、詳細なサーバ ファーム情報を表示します。「サーバ ファームの統計情報およびステータス情報の表示」（P.6-38）を参照してください。

（注） 既存のスティッキ グループを選択すると、選択したオブジェクトの既存の設定の表示、変更、または複製ができます。仮想サーバでの共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。

ステップ 7　[Compression Method] フィールドで、クライアント ブラウザがパケット圧縮に対応できることをクライアント要求が示している場合に、ACE アプライアンスがパケットを圧縮する方法を示す HTTP 圧縮方式を選択します。デフォルトでは、ACE の HTTP 圧縮はディセーブルです。ACE で HTTP 圧縮を設定すると、ACE は実サーバからの HTTP GET 応答内のデータを圧縮します。ACE は、クライアントからの HTTP 要求、またはサーバ応答内の HTTP ヘッダーを圧縮しません。

（注） デフォルトでは、ACE は 100 メガビット / 秒（Mbps）のレートで HTTP 圧縮をサポートしています。オプションの HTTP 圧縮ライセンスをインストールすると、この値を最大 2 Gbps まで大きくすることができます。ACE ライセンス オプションの詳細については、『*Administration Guide, Cisco ACE Application Control Engine*』を参照してください。

オプションは次のとおりです。

- [Deflate] : クライアント ブラウザが deflate および gzip 圧縮方式をサポートしている場合に使用する方式として deflate 圧縮フォーマットを指定します。deflate は、RFC1951 に記載されているデータの圧縮フォーマットです。
- [Gzip] : クライアント ブラウザが deflate および gzip 圧縮方式をサポートしている場合に使用する方式として gzip 圧縮フォーマットを指定します。gzip は、RFC1952 に記載されているファイルの圧縮フォーマットです。
- [N/A] : HTTP 圧縮はディセーブルです。

HTTP 圧縮を設定する場合、HTTP 圧縮から次の MIME タイプを除外することを推奨します。「.*gif」、「.*css」、「.*js」、「.*class」、「.*jar」、「.*cab」、「.*txt」、「.*ps」、「.*vbs」、「.*xsl」、「.*xml」、「.*pdf」、「.*swf」、「.*jpg」、「.*jpeg」、「.*jpe」、「.*png」。

（注） [Gzip] または [Deflate] 圧縮フォーマットをイネーブルにした場合、DM GUI は自動的に L7 Load Balance Primary Action を挿入し、上に示されている MIME タイプを除外します。ただし、HTTP 圧縮を後で無効にすると、自動挿入された Load Balance Primary Action を排除する必要があります。

HTTP 圧縮をイネーブルにすると、ACE は次のデフォルトの圧縮パラメータ値を使用してパケットを圧縮します。

- [Mime type]：あらゆるテキスト フォーマット（text/*）
- [Minimum size]：512 バイト
- [User agent]：なし

ステップ 8　[SSL Initiation] フィールドで、既存のサービスを選択するか、または [*New*] を選択して新しいサービスを作成します。

（注） [SSL Initiation] フィールドは、[Advanced View] にだけ表示され、選択されたプロトコルが TCP であって、Other、HTTP、または HTTPS がアプリケーション プロトコルの場合に表示されます。

（注） SSL 開始オプションは、ACE NPE のソフトウェア バージョンに適用されません（「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）。

SSL 開始では仮想サーバは、自身と SSL サーバとの SSL 接続を開始および維持する SSL プロキシ クライアントとして機能させることができます。この特定の用途では、ACE はクリア テキストを HTTP クライアントから受け取り、そのデータを暗号化して暗号文として SSL サーバに送信します。一方、ACE は SSL サーバから受け取った暗号文を復号化し、そのデータをクリア テキストとしてクライアントに送信します。

- 既存の SSL サービスを選択すると、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。
- [*New*] を選択する場合、表 5-14 の指示に従ってサービスを設定します。

SSL の詳細については、「SSL の設定」（P.9-1）を参照してください。

ステップ 9　[Insert HTTP Headers] フィールドに、***header_name*=*header_value*** というフォーマットで、HTTP ヘッダーの名前と照合対象の値を入力します。

- ***header_name*** は、クライアント HTTP 要求に挿入する HTTP ヘッダーの名前です。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）。最大長の限界を超えないかぎり、定義済みのヘッダーまたは他のカスタム ヘッダー名を指定できます。
- ***header_value*** は、HTTP ヘッダー内に指定したフィールドの値と照合する式ストリングです。有効な入力は英数字ストリングで、最大 255 文字です。ACE アプライアンスは、照合に正規表現をサポートしています。ヘッダー表現にはスペースを使用できますが、エスケープ シーケンスまたは引用符が必要です。ヘッダー マップのすべてのヘッダーは一致する必要があります。表 12-33 は、正規表現で使用できるサポート対象文字の一覧です。

たとえば、`Host=www.cisco.com` と入力できます。

ステップ 10　仮想サーバのプロパティの設定が完了したら、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] をクリックすると、エントリを保存しないでこの手順を終了し、[Virtual Servers] テーブルに戻ります。

関連トピック

- 「仮想サーバのプロパティの設定」（P.5-11）
- 「仮想サーバの SSL 終了の設定」（P.5-19）
- 「仮想サーバのプロトコル インスペクションの設定」（P.5-21）
- 「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）

アプリケーション アクセラレーションおよび最適化の設定

ACE アプライアンスは、エンタープライズ アプリケーションを加速化できる設定オプションを備えているため、従業員の生産性が向上し、顧客の定着率が伸び、オンライン収益が増大します。ACE アプライアンスのアプリケーション アクセラレーション機能は、Web アプリケーションのパフォーマンスを加速化するためのいくつかの最適化技術を利用しています。ACE アプライアンス のアプリケーション アクセラレーション機能によって、企業はネットワーク パフォーマンスを最適化し、重要なビジネス情報へのアクセスを改善することができます。この機能によって、顧客関係管理（CRM）、ポータル、オンライン コラボレーションなど、Web アプリケーションのパフォーマンスは最大 10 倍にまで加速化されます。

アプリケーション アクセラレーションおよび最適化の詳細については、「アプリケーション アクセラレーションおよび最適化の設定」（P.13-1）または『*Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance*』を参照してください。

仮想サーバでアクセラレーションおよび最適化を設定するには、この手順を使用します。

前提

仮想サーバを設定しておきます。仮想サーバの設定の詳細については、「仮想サーバの設定」（P.5-2）を参照してください。

考慮事項

アプリケーション アクセラレーションおよび最適化は IPv4 サーバ ロードバランシング設定への IPv4 のみでサポートされます。

手順

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

ステップ 2　最適化を設定する仮想サーバを選択し、[Edit] をクリックします。[Virtual Server] 設定画面が表示されます。

ステップ 3　[Application Acceleration And Optimization] をクリックします。[Application Acceleration And Optimization] 設定ペインが表示されます。

ステップ 4　[Configuration] フィールドで、アプリケーション アクセラレーションおよび最適化を設定する場合に使用する方式を指定します。

- [EZ]：標準のアプリケーション アクセラレーションおよび最適化オプションを使用します。ステップ 5 に進みます。

- [Custom]：この仮想サーバのアプリケーション アクセラレーションおよび最適化用の特定の一致条件、アクション、およびパラメータ マップを関連付けます。このオプションを選択する場合、ステップ 6 に進みます。

ステップ 5　[EZ] を選択すると、[Latency Optimization (FlashForward)] フィールドおよび [Bandwidth Optimization (Delta)] フィールドが表示されます。

a. ACE アプライアンスが帯域幅削減を使用し、HTML ページに組み込まれているオブジェクトにアクセラレーション手法をダウンロードさせるには、[Latency Optimization (FlashForward)] チェックボックスを選択します。ACE アプライアンスが HTML ページに組み込まれているオブジェクトにこれらの手法を使用しないようにするには、このチェックボックスをクリアします。遅延最適化は、FlashForward 機能に対応しています。FlashForward 機能の詳細については、「最適化の概要」（P.13-2）を参照してください。

b. ACE アプライアンスがクライアント ブラウザのキャッシュをコンテンツの差分（デルタ）で動的に更新させるには、[Bandwidth Optimization (Delta)] チェックボックスを選択します。ACE アプライアンスがクライアント ブラウザのキャッシュを動的に更新しないようにするには、このチェックボックスをクリアします。帯域幅最適化は、アクション リスト デルタ最適化に対応しています。デルタ最適化の詳細については、「最適化の概要」（P.13-2）および「HTTP 最適化アクション リストの設定」（P.13-3）を参照してください。

c. ステップ 11 に進みます。

ステップ 6　[Custom] を選択すると、[Actions] 設定ペインが表示され、一致条件およびアクションがリストされたテーブルが表示されます。[Add] をクリックしてこのテーブルにエントリを追加するか、または既存のエントリを選択して [Edit] をクリックし、そのエントリを変更します。設定サブセットは、利用可能な設定オプションによってリフレッシュされます。

ステップ 7　[Apply Template] フィールドで、設定する最適化のタイプ用に設定テンプレートの 1 つを選択するか、またはテンプレートなしで最適化を設定する場合は空白のままにします。

- [Bandwidth Optimization]：Web ベースのトラフィックの帯域幅を最大化します。
- [Latency Optimization For Embedded Objects]：Web ベースのトラフィックに組み込まれたオブジェクトに伴う遅延を短縮します。
- [Latency Optimization For Embedded Images]：Web ベースのトラフィックに組み込まれたイメージに伴う遅延を短縮します。
- [Latency Optimization For Containers]：Web コンテナに伴う遅延を短縮します。

テンプレートを選択しないで、[Rule Match] フィールドおよび [Actions] フィールドで [*New*] を選択する場合は、独自の最適化およびアクションを作成することになります。

ステップ 8　[Rule Match] フィールドで、既存のクラス マップを選択するか、または [*New*] をクリックして新しい一致条件を指定します。

- 既存のクラス マップを選択すると、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。
- [*New*] をクリックすると、選択したテンプレートに対応したデフォルトの設定によって画面はリフレッシュされます。デフォルトの設定で確定するか、または表 5-15 の指示に従ってその設定を変更します。

表 5-15　最適化ルール一致の設定オプション

フィールド	説明
Name	この一致条件ルールの一意な名前を入力します。
Matches	複数の一致条件が存在する場合、複数の一致文の評価に使用する方式を選択します。 • [Any]：一致条件の少なくとも 1 つが満たされる場合に一致することになります。 • [All]：すべての一致条件が満たされる場合にだけ一致することになります。
Conditions	[Add] をクリックして新しい一連の条件を追加するか、または既存のエントリを選択して [Edit] をクリックし、そのエントリを変更します。 1. [Type] フィールドで、使用する一致条件を選択し、表 5-9 の指示に従って条件固有のオプションを設定します。 2. エントリを保存するには、[OK] をクリックします。エントリを保存しないで手順を終了するには、[Cancel] をクリックします。

ステップ 9　[Actions] フィールドで、最適化に使用する既存のアクション リストを選択するか、または [*New*] をクリックして新しいアクション リストを作成します。

- 既存の最適化アクション リストを選択すると、既存の設定の表示、変更、または複製ができます。共有オブジェクトの変更の詳細については、「共有およびオブジェクト仮想サーバ」（P.5-10）を参照してください。
- [*New*] をクリックすると、選択したテンプレートに対応したデフォルトの設定によって画面はリフレッシュされます。デフォルトの設定で確定するか、または表 5-16 の指示に従ってその設定を変更します。

表 5-16　最適化アクション リストの設定オプション

フィールド	説明
Action List Name	最適化アクション リストの一意な名前を入力します。有効な入力は、引用符なしの最大 64 文字の英数字です。
Enable Delta	デルタ最適化は、クライアント ブラウザのキャッシュをコンテンツの差分（デルタ）で直接動的に更新するため、ページのダウンロードが高速になります。 指定した URL のデルタ最適化をイネーブルにするには、このチェックボックスをオンにします。 指定した URL のデルタ最適化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。 **（注）** あらかじめ、Cache Dynamic または Dynamic Entity Tag でデルタ最適化を指定している場合、ACE によりデルタ最適化のイネーブル化は制限されます。
Enable AppScope	AppScope はオプションの Cisco AVS 3180A Management Station の Management Console で動作し、エンドツーエンドのアプリケーション パフォーマンスを測定します。 ACE アプライアンスでの AppScope パフォーマンス モニタリングの使用をイネーブルにするには、このチェックボックスをオンにします。ACE アプライアンスでの AppScope パフォーマンス モニタリングの使用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。

表 5-16　最適化アクション リストの設定オプション （続き）

フィールド	説明
Flash Forward	FlashForward 機能は、ローカル オブジェクト ストレージと組み込みオブジェクトの動的名前変更を組み合わせることによって、帯域幅の使用率を削減し、組み込みオブジェクトのダウンロードを加速させ、これにより親 HTML ページ内でのオブジェクトの新しさを実現します。 ACE アプライアンスでの FlashForward の実施方法を指定します。 • [N/A]：この機能はイネーブルではありません。 • [FlashForward]：指定した URL に対して FlashForward はイネーブルになり、組み込みオブジェクトは変換されます。 • [Flash Forward Object]：対応する URL が参照している Cascading Style Sheet（CSS）、JPEG、GIF ファイルなどのオブジェクトに対して、FlashForward 静的キャッシングはイネーブルになります。
Cache Dynamic	応答内の期限切れ設定のコンテンツが動的であることを示している場合でも、指定した URL の Adaptive Dynamic Caching をイネーブルにするには、このチェックボックスをオンにします。キャッシュ オブジェクトの期限切れは、時間またはサーバの負荷に基づいて、キャッシュの期限切れ設定によって制御されます。 この機能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。 **（注）** あらかじめ、Enable Delta または Dynamic Entity Tag でデルタ最適化を指定している場合、ACE により Cache Dynamic のイネーブル化は制限されます。
Cache Forward	対応する URL のキャッシュ転送機能をイネーブルにするには、このチェックボックスをオンにします。キャッシュ転送を使用すると、最大 TTL が経過していない場合にオブジェクトの期限が切れたときでも、ACE はキャッシュ（静的または動的）からのオブジェクトに対応することができます（Optimization パラメータ マップ内の [Cache Time-To-Live Duration (%):] フィールドを指定することによって設定）。同時に、ACE は非同期要求を発信元サーバに送信し、そのオブジェクトのキャッシュをリフレッシュします。 この機能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。
Dynamic Entity Tag	この機能では、キャッシュ不可能な組み込みオブジェクトのアクセラレーションが有効になり、アプリケーションの応答時間が向上します。イネーブルの場合、キャッシュ不可能なオブジェクトを要求ごとにダウンロードする必要がなくなります。 ACE アプライアンスでキャッシュ不可能な組み込みオブジェクトに対して、ジャストインタイム オブジェクト アクセラレーションを実施するには、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。 **（注）** あらかじめ、Enable Delta または Cache Dynamic でデルタ最適化を指定している場合、ACE により Dynamic Entity Tag のイネーブル化は制限されます。
Fine Tune Optimization Parameters	追加の最適化属性を設定するには、このヘッダーをクリックします。展開すると、設定ペインには、設定している最適化のタイプに固有のオプションとイネーブルにする機能が表示されます。 表示されている特定のオプションの詳細については、表 8-5 を参照してください。

ステップ 10　一致基準およびアクションの設定が完了したら、次の手順を実行します。

- [OK] をクリックすると、エントリを保存し、[Rule Match and Actions] テーブルに戻ります。
- [Cancel] をクリックすると、エントリを保存しないで手順を終了し、[Rule Match and Actions] テーブルに戻ります。

ステップ 11　仮想サーバのプロパティの設定が完了したら、次の手順を実行します。

- エントリを保存するには、[Deploy Now] をクリックします。ACE アプライアンスは最適化アクション リストの設定を確認し、ACE アプライアンスに配置します。
- [Cancel] をクリックすると、エントリを保存しないでこの手順を終了し、[Virtual Servers] テーブルに戻ります。

関連トピック

- 「仮想サーバのプロパティの設定」（P.5-11）
- 「最適化トラフィック ポリシーおよび一般的な設定フロー」（P.13-2）
- 「HTTP 最適化のトラフィック ポリシーの設定」（P.13-6）
- 「仮想サーバのプロトコル インスペクションの設定」（P.5-21）
- 「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）
- 「仮想サーバのデフォルトのレイヤ 7 ロード バランシングの設定」（P.5-56）

仮想サーバ NAT の設定

仮想サーバで Name Address Translation（NAT）を設定するには、この手順を使用します。

前提

- 仮想サーバを設定しておきます。仮想サーバの設定の詳細については、「仮想サーバの設定」（P.5-2）を参照してください。
- VLAN を設定しておきます。VLAN インターフェイスの設定については、「仮想コンテキスト VLAN インターフェイスの設定」（P.10-10）を参照してください。
- VLAN インターフェイスに、少なくとも 1 つの NAT プールを設定しておきます。NAT プールの設定については、「VLAN インターフェイス NAT プールの設定および NAT 使用率の表示」（P.10-32）を参照してください。

手順

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

ステップ 2　NAT を設定する仮想サーバを選択し、[Edit] をクリックします。[Virtual Server] 設定画面が表示されます。

ステップ 3　[NAT] をクリックします。[NAT] テーブルが表示されます。

ステップ 4　[Add] をクリックしてエントリを追加するか、または既存のエントリを選択して [Edit] をクリックし、そのエントリを変更します。

ステップ 5　[VLAN] フィールドで、NAT に使用する [VLAN] を選択します。NAT の詳細については、「VLAN インターフェイス NAT プールの設定および NAT 使用率の表示」（P.10-32）を参照してください。

ステップ 6　[NAT Pool ID] フィールドで、選択した VLAN に関連付ける NAT プールを選択します。

ステップ 7　次の手順を実行します。

- [OK] をクリックすると、エントリを保存し、[NAT] テーブルに戻ります。[NAT] テーブルは新しいエントリによってリフレッシュされます。
- [Cancel] をクリックすると、エントリを保存しないで手順を終了し、[NAT] テーブルに戻ります。

ステップ 8　仮想サーバのプロパティの設定が完了したら、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] をクリックすると、エントリを保存しないでこの手順を終了し、[Virtual Servers] テーブルに戻ります。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバのプロパティの設定」（P.5-11）
- 「仮想サーバの SSL 終了の設定」（P.5-19）
- 「仮想サーバのプロトコル インスペクションの設定」（P.5-21）
- 「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）
- 「仮想サーバのデフォルトのレイヤ 7 ロード バランシングの設定」（P.5-56）

仮想サーバの統計情報およびステータス情報の表示

[Details] ボタンを使用して、特定の仮想サーバの統計情報とステータス情報を表示できます。

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Virtual Servers] を選択します。

[Virtual Servers] テーブルが表示されます。

ステップ 2　[Virtual Servers] テーブルで、仮想サーバを [Virtual Servers] テーブルから選択し、[Details] をクリックします。

show service-policy *policy_name* **class-map** *class_name* **detail** CLI コマンド出力が表示されます。表示されるフィールドの詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

（注）　この機能は、ACE ソフトウェア バージョン A3（2.1）以降が必要です。以前のソフトウェア バージョンを使用するとエラーが表示されます。

ステップ 3　（任意）ウィンドウの情報を更新するときは [Update Details] をクリックします。

ステップ 4　[Close] をクリックして、[Virtual Servers] テーブルへ戻ります。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバの管理」（P.5-65）
- 「すべての仮想サーバの表示」（P.5-67）

仮想サーバの管理

仮想サーバを作成すると、次のオプションが利用できます。

作業	関連トピック
仮想サーバの設定の変更	「仮想サーバの設定」（P.5-2）
仮想コンテキスト別の仮想サーバのリスト	「コンテキスト別の仮想サーバの表示」（P.5-65）
仮想サーバのアクティブ化	「仮想サーバのアクティブ化」（P.5-66）
仮想サーバの一時停止	「仮想サーバの一時停止」（P.5-66）
すべての仮想サーバおよびその設定済みステートを表示	「すべての仮想サーバの表示」（P.5-67）

コンテキスト別の仮想サーバの表示

仮想コンテキストに関連付けられているすべての仮想サーバを表示するには、この手順を使用します。

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　表示する仮想サーバに関連付けられているコンテキストを選択し、[Load Balancing] > [Virtual Servers] を選択します。次の情報が載った [Virtual Servers] テーブルが表示されます。

- 仮想サーバ名
- 稼働中など、設定済みステート
- 仮想 IP アドレス
- ポート
- 関連付けられている VLAN
- 関連付けられているサーバ ファーム
- 仮想コンテキスト名

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバの管理」（P.5-65）

仮想サーバの統計情報およびステータス情報の表示

[Details] ボタンを使用して、特定の仮想サーバの統計情報とステータス情報を表示できます。DM は、**show service-policy** *policy_name* **detail** CLI コマンドにアクセスして、詳細な仮想サーバ情報を表示します。

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [Load Balancing] > [Virtual Servers] を選択します。

[Virtual Servers] テーブルが表示されます。

ステップ 2　[Virtual Servers] テーブルで、仮想サーバを [Virtual Servers] テーブルから選択し、[Details] をクリックします。

show service-policy *policy_name* **detail** CLI コマンド出力が表示されます。表示される出力フィールドの詳細については、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

ステップ 3　**show service-policy** *policy_name* **detail** CLI コマンドの出力を更新するときは [Update Details] をクリックします。

ステップ 4　[Close] をクリックして、[Virtual Servers] テーブルへ戻ります。

関連トピック

- 「仮想サーバの設定」（P.5-2）
- 「仮想サーバの管理」（P.5-65）
- 「すべての仮想サーバの表示」（P.5-67）

仮想サーバのアクティブ化

仮想サーバをアクティブ化するには、次の手順を使用します。

手順

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

ステップ 2　アクティブ化するサーバを選択し、[Activate] をクリックします。サーバがアクティブ化し、画面の [Configured State] カラムは最新情報によってリフレッシュされます。

関連トピック

- 「仮想サーバの管理」（P.5-65）
- 「すべての仮想サーバの表示」（P.5-67）
- 「仮想サーバの一時停止」（P.5-66）

仮想サーバの一時停止

仮想サーバを一時停止するには、次の手順を使用します。

手順

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

ステップ 2　一時停止する仮想サーバを選択し、[Suspend] をクリックします。[Suspend Virtual Server] 画面が表示されます。

ステップ 3　[Reason] フィールドに、このアクションの理由を入力します。トラブル チケット、オーダー チケット、またはユーザ メッセージを入力できます。

注意　**[Reason] フィールドにパスワードを入力しないでください。**

ステップ 4　次の手順を実行します。

- この設定を展開するには、[Deploy Now] をクリックします。仮想サーバが稼働を停止し、Device Manager が [Virtual Servers] テーブルに戻ります。画面の [Oper State] カラムは最新情報によってリフレッシュされます。
- [Cancel] をクリックすると、仮想サーバを一時停止せずに手順を終了し、[Virtual Servers] テーブルに戻ります。

関連トピック

- 「仮想サーバの管理」（P.5-65）
- 「すべての仮想サーバの表示」（P.5-67）
- 「仮想サーバのアクティブ化」（P.5-66）

すべての仮想サーバの表示

すべての仮想サーバを表示するには、[Config] > [Operations] > [Virtual Servers] を選択します。サーバごとに次の情報が載った [Virtual Servers] テーブルが表示されます。表 5-17 には [Virtual Servers] テーブルの情報が記載されています。

表 5-17　仮想サーバのテーブル フィールド

項目	説明
Name	仮想コンテキスト別にソートされたサーバ ファーム名。
Policy Map	関連するポリシー マップ。
IP Address/Protocol/Port	通信に使用するサーバ ファームの IP アドレス、プロトコル、およびポート番号。
Context	サーバ ファームに関連付けられている仮想コンテキスト。
Admin	仮想サーバの管理ステート：[UP] または [DOWN]。
Oper	仮想サーバの動作状態：[UP] または [DOWN]。 ポップアップ ウィンドウの仮想サーバに関する詳細情報を表示するには、このカラムのリンク状態値をクリックします。 **（注）** 仮想サーバ表示の詳細機能は、ACE ソフトウェア バージョン A3（2.1）以降が必要です。以前のソフトウェア バージョンを使用するとエラーが表示されます。

表 5-17　仮想サーバのテーブル フィールド （続き）

項目	説明
DWS	次のような仮想サーバの動的ワークロード拡張の動作状態。 • [N/A] : 適用されない。仮想サーバに関連付けられたサーバ ファームは、動的ワークロード拡張を使用するように設定されていません。 • [Local] : 仮想サーバに関連付けられた最低 1 台のサーバ ファームで動的ワークロード拡張を使用するように設定されていますが、その ACE は VM のコントローラのローカル VM のみにトラフィックを送信します。 • [Expanded] : 仮想サーバに関連付けられた最低 1 台のサーバ ファームで動的ワークロード拡張を使用するように設定されていて、その ACE は VM のコントローラのローカルおよびリモートの VM にトラフィックを送信します。
Conn	アクティブな接続の数
Stat Age	SNMP 値をポーリング後、そのページのロード時間。
Server farms	関連付けられているサーバ ファーム。
VLANs	関連付けられている VLAN。

このテーブルから仮想サーバのアクティブ化または一時停止ができ、また、仮想サーバの状態に関する詳細情報を取得することができます。

関連トピック

- 「仮想サーバのアクティブ化」（P.5-66）
- 「仮想サーバの一時停止」（P.5-66）