CHAPTER 14

宛先サーバ設定の指定

この章では、保護バックエンド システムの設定を管理する方法について説明します。内容は次のとおりです。

宛先サーバについて

ACE XML Gateway ポリシーでは、トラフィックを処理し、検証するバックエンド システムの設定は、HTTP サーバ オブジェクトに含まれます。サーバ オブジェクトは、新しい仮想 Web アプリケーションを定義するときか、または Web Services Description Language（WSDL）インポート プロセスを介して仮想 Web サービスを定義するときに、作成されます。ただし、手作業で宛先 HTTP サーバを作成したり、既存の定義を変更したりすることもできます。

宛先サーバ設定は、主に、バックエンド システムに要求を転送するために ACE XML Gateway で使用される接続設定で構成されています。宛先 HTTP サーバ定義によって指定される実際のエンドポイントは、サーバ ファームまたは仮想サーバを表すアプリケーションまたは論理サーバをホストするサーバである場合があります。

（注） 宛先 HTTP サーバ オブジェクトは、HTTP ベースの通信が使用されるシステム用です。Java Message Service（JMS）、Tibco RV（Rendezvous）、または MQSeries トラフィックがサポートされるバックエンド システムでトラフィックを処理するには、代わりに、メッセージング サーバ定義を使用します。

エコー サーバは、外部バックエンド システムの代わりに ACE XML Gateway 自体で応答が生成され、戻されるサーバ定義のタイプです。Gateway では、要求がエコーされるか、または、サーバ定義用に設定されている静的な応答ページが返されます。エコー サービスは、呼び出し方式でポリシーのテストやメッセージ検証を実行する場合に役に立ちます。

この章では、ACE XML Manager でサーバを設定する方法について説明します。サーバ定義は、仮想サービスまたは仮想 Web アプリケーションを定義するときに自動的に生成することができ、また、手作業で作成することもできます。

宛先 HTTP サーバに関する作業

HTTP サーバ定義には、ネットワーク アドレス、リスニング ポート、接続に SSL が必要かなど、特定のバックエンド サーバの設定が保存されます。サーバ オブジェクトを作成、編集、または削除するには、Administrator ユーザまたは Routing ロールを持つ Privileged ユーザとして Web コンソールを使用する必要があります。

宛先 HTTP サーバの追加

HTTP サーバを作成すると、トラフィック処理ルールをサーバに関連付けることができます。宛先サーバは、新しい仮想 Web アプリケーションを定義するときか、または WSDL インポート プロセスを介して仮想 Web サービスを定義するときに、作成されます。ただし、次の手順で、手作業で宛先 HTTP サーバを作成することもできます。

ステップ 1　ACE XML Manager Web コンソールで、追加する宛先 HTTP サーバ定義に、アクティブなサブポリシーを設定します。

ステップ 2　操作メニューで [Destination HTTP Servers] リンクをクリックします。

ステップ 3　[HTTP Servers] ページで [Add a New HTTP Server] をクリックします。

ステップ 4　[Name] フィールドのサーバ定義に、わかりやすい名前を入力します。この名前はコンソール内でだけ使用され、Web コンソールの他のユーザに対するサーバ定義を指定する必要があります。ポリシー内で、HTTP サーバに対して固有である必要があります。

（注）　サービスまたはアプリケーション仮想化プロセスを介して生成されたサーバ オブジェクトでは、ACE XML Manager により、server.example.com:80 などのデフォルト サーバ名のホスト名およびポート番号が使用されます。ただし、この値は識別情報としてだけ使用されるため、このサーバ定義を他と区別するために使用できる値であれば差し支えありません。

ステップ 5　[Host] フィールドに、バックエンド サーバのホスト名を入力します。

ホスト値は、バックエンド システムの DNS 名（`swan.example.com` など）またはその IP アドレス（`192.168.1.100` など）である必要があります。フィールドには、プロトコル プレフィクス（http://）を入力する必要はありません。

ステップ 6　[Port] フィールドで、サービス要求をリッスンするバックエンド サーバのポート番号を指定します。

この値を正確に指定しなかった場合、サービス記述子は、トラフィックをサービスに正しく渡すことはできません。ほとんどの HTTP サーバでは、通常の Web トラフィックにポート 80 が使用され、SSL 接続にポート 443 が使用されます。

ステップ 7　バックエンド サーバへの接続に SSL を設定するには、次の操作を実行します。

a. [SSL] チェックボックスをクリックします。SSL 接続がサーバでサポートされている場合にだけ、このオプションを選択します。

b. 双方向 SSL では、クライアントにより、サーバに対してクライアント自体を認証する必要や、その逆を行う必要があります。サーバによりクライアント認証が要求される場合（この場合は ACE XML Gateway）、Gateway では、[If requested, use client public/private keypair] とラベルが記されているフィールドに、指定した証明書を提示できます。

使用するキーペアがメニューに表示されていない場合、[Upload] をクリックし、ポリシーに対するリソースとして追加します。

c. これらのオプションから、バックエンド HTTP サーバが提示した証明書が ACE XML Gateway で検証される方法を指定します。

- サーバから提示された証明書を受け付けるには、[Require remote server certificate signed by this CA certificate] オプションを、そのデフォルト値の [none] のままにします。この設定は、デフォルトです。
- 指定された Certificate Authority（CA; 認証局）によって認証された証明書を受け付けるには、メニューから、[Require remote server certificate signed by this CA certificate] オプションを選択し、CA 証明書を選択します。証明書がメニューに表示されない場合、[Upload] を選択し、Trusted Certificate Authority（Trusted CA）の ACE XML Manager のリストに証明書を追加します。
- 指定された証明書と同等の証明書がサーバによって提示される必要があることを指定するには、[Require a certificate from the remote server that is identical to this certificate] ボタンをクリックし、メニューから証明書を選択します。証明書がメニューに表示されない場合、[Upload] を選択し、リモート サーバ証明書の ACE XML Manager のリストに証明書を追加します。

ステップ 8　オプションで、このバックエンド サーバへの SSL 接続のネゴシエーションを受け付ける暗号を、[SSL Cipher Suite] メニューで指定します。接続を使用するには、セキュア接続のネゴシエーションで、ACE XML Gateway およびサーバによって暗号スイートで合意できる必要があります。ここで指定された暗号がサーバでサポートされていない場合、接続は許可されません。

接続では、デフォルトで、[System Management] > [I/O Settings] ページで設定されているように、ACE XML Gateway の HTTP クライアント プロセスに対して、SSL 暗号スイート設定が使用されます。このオプションを使用すると、このサーバに対して、より詳細な設定を適用できます。

http://www.openssl.org/docs/apps/ciphers.html に説明されているように、[SSL Cipher Suite] メニューからカスタム設定を選択して暗号スイートを指定し、表示されるフィールドで、OpenSSL 暗号文字列形式で受け付けられる暗号スイートを入力します。

（注）　暗号スイート文字列を入力する際には、注意してください。ACE XML Manager Web コンソール インターフェイスでは、入力値は検証されません。無意味な値を誤って入力した場合、ACE XML Gateway では、サーバとの SSL 接続をオープンできないことがあります。

ステップ 9　このサーバに対するメッセージ処理で、Reactor プロセスを回避する場合、[Flex Path] オプションを選択します。Reactor は、ACE XML Gateway で、メッセージ処理が飛躍的に高速化される、高性能でストリーム型の XML エンジンです。ただし、Gateway で実行されるすべての処理タスクが、Reactor によってサポートされるわけではありません。仮想サービスの機能が Reactor によってサポートされない場合（プロトコル メディエーションなど）、Reactor では、メッセージが自動的に Flex Path 処理に渡されます。外部システムとの互換性を保つため、このオプションを使用することによって、サーバに対して Reactor をディセーブルにする必要が生じることがあります。一般的には、クライアントおよびサーバとの相互運用性について注意深くテストした後でだけ、実稼動システムで Reactor を使用することを推奨します。

ステップ 10　[Save Changes] をクリックし、サーバの設定を終了します。

終了すると、ポリシーにある仮想サービスおよび仮想 Web アプリケーションで、サーバを使用できます。

プーリング バックエンド サーバ

サーバ プールは、サービスのセットへのアクセスが合同で提供される、バックエンド サービス プロバイダーのグループです。ACE XML Gateway でバックエンド サービス プロバイダーのサーバ プーリングを設定でき、これによって、ACE XML Gateway を介して発生するサービス アクセスのスケーラビリティおよび信頼性が向上します。

サーバ プールを作成するには、プールに対してプライマリ サーバを設定し、次に、プールを構成するサーバを、ホスト名または IP アドレスを使用して指定します。

サーバ プールは、次の 2 つのモードの 1 つで動作できます。

- フェールオーバーのみ。プライマリ サーバに障害が発生した場合にだけ、プライマリ サーバによってすべてのサービス プロビジョニング機能が実行され、プールの他のサーバによってトラフィックが処理されます。
- 負荷分散型フェールオーバー。要求が、ラウンドロビン方式でプールにあるサーバに分散されます。

サーバへの要求によってエラー応答が発生した場合か、サーバ ヘルス チェックに対する応答に失敗した場合、サーバに障害が発生したと見なされます。サーバに障害は発生した場合（または何らかの理由でサーバに到達不能な場合）、ACE XML Gateway では、設定可能なバックオフ期間と呼ばれる期間、アクティブなサーバ プールからサーバが削除されます。バックオフ期間が終了すると、ACE XML Gateway では、障害が発生したサーバへの通信を試行します。正常に実行された場合、サーバは回復されます。

フェールオーバーのみのモードでは、プールにある 1 つのサーバがプライマリと見なされます。プライマリでは、何らかの理由で障害が発生するか、または、管理者によってディセーブルにされるまで、すべてのトラフィックが処理されます。このイベントでは、プールにある別の応答可能なサーバがプライマリになり、そのプライマリによって、障害イベントが発生するかディセーブルにされるまで、トラフィックが処理されます。

サーバ プーリングの設定

サービス プロバイダーに対してサーバ プーリングを設定するには、次の操作を実行します。

ステップ 1　[HTTP Servers] ページがすでに開かれていない場合、（メニューの [Message Routing] セクションにある [Policy] リンク内の）操作メニューで [Destination HTTP Servers] リンクをクリックします。

ステップ 2　サーバ プーリングを設定するサーバの横にある [view] リンクをクリックします。

フェールオーバーだけに設定されている場合、サーバ プーリングを設定するサーバは、デフォルトで、クラスタのプライマリ サーバです。プライマリ サーバは、通常の条件で要求に応答します。

ステップ 3　[Server Pooling] という見出しの横の [Edit] リンクをクリックします。

[Edit Server Pooling] ページが表示されます。

ステップ 4　[Use pooled servers for failover] チェックボックスを選択します。

ステップ 5　オプションで、[Rotate requests among pooled servers] を選択します。このオプションには、次の影響があります。

- 選択されていない場合、プールはフェールオーバー モードのみで動作します。ホスト リストにある最初のサーバにより、設定されているサーバのすべての要求に対して応答が行われ、プライマリに障害が発生するまで、プールの他のサーバは非アクティブのままになります。
- 他方で、このオプションを選択すると、プール メンバの中でラウンドロビン方式での要求の割り当てがイネーブルになります。

ステップ 6　[Suspend requests to a failed host for at least] の横にあるフィールドで、応答のないプール メンバに対する要求を ACE XML Gateway が一時停止する秒数を指定します。

この値は、障害が発生したサーバのバックオフ期間です。ACE XML Gateway により、ユーザが指定した回数、障害が発生したサーバへの通信が試行されます。回数が超過すると、ヘルス チェック メッセージがサーバに送信され、応答を受信すると、サーバがプールに回復されます。この間、サービスの要求はプールにある残りのサーバに対して送信されます。

この値は、現在のプールにあるサーバに対してだけではなく、ヘルス チェックをイネーブルにしたすべてのサーバに適用されます。

ステップ 7　[Primary Hosts] フィールドで、プールに追加する各サーバの IP アドレスまたはホスト名およびリスニング ポートを入力します。

各サーバのアドレスは、次のように、それぞれの行に記載する必要があります。

```
primary.example.com:80
pool-member1.example.com:80
pool-member2.example.com:80
192.168.10.1:8080
```

各行は固有である必要があります。サーバをポリシーで使用するには、ポリシーでサーバを HTTP サーバとして設定する必要があります。

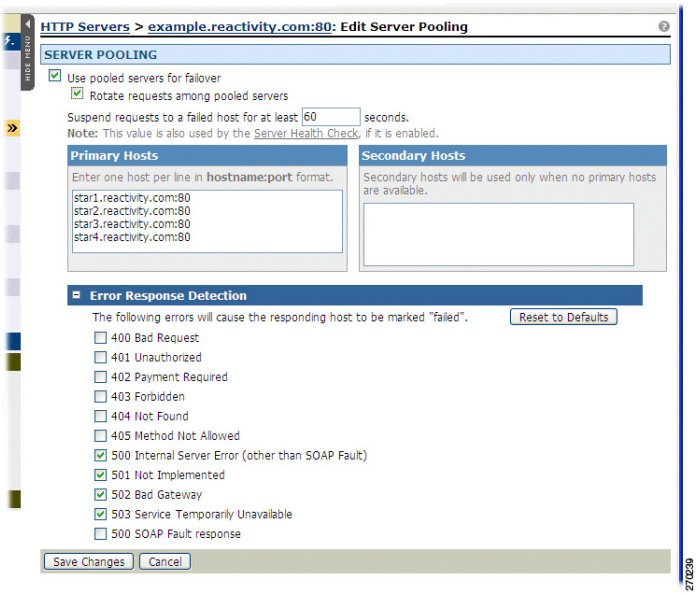
ステップ 8　オプションで、セカンダリ プールについての追加アドレスを入力します。プライマリ プールにあるすべてのサーバに障害が発生した場合、ACE XML Gateway では、セカンダリ プールに対してだけメッセージがルーティングされます。

ステップ 9　エラー応答に基づいて ACE XML Gateway でサーバ障害が解釈される方法を設定するには、ページの [Error Response Detection] エリアを拡張し、エラー応答選択を変更します。

実際にサーバ障害を示すエラー コードだけを選択するようにしてください。つまり、サーバによってホストされているアプリケーションにより、SOAP 障害応答など、アプリケーション特有のステータスを示す応答の 1 つを返す場合は、選択する必要はありません。

設定ページは 図 14-1 のようになります。

図 14-1　サーバ プーリング設定



ステップ 10　完了したら [Save Changes] をクリックします。

[HTTP Server] 情報ページが再度表示されますが、プールされているサーバのリストが [Server Pooling] エリアに表示されます。

（注）　新たに追加されたサーバのステータスのリストは、未導入として表示されます。ACE XML Gateway では、ユーザがポリシーを導入するまで、プールにあるサーバ宛てに送信されません。ポリシーの導入後、プールのリストにより、サーバがイネーブルであることが表示されます。

プール メンバの手作業での削除

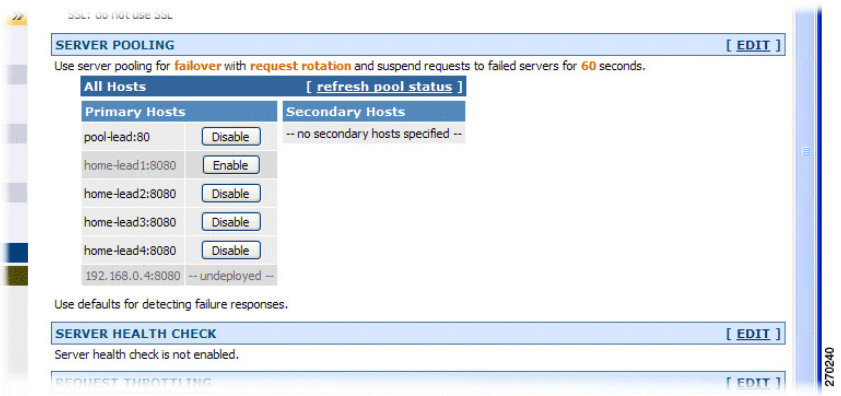
ACE XML Gateway では、バックオフ期間中にメッセージ トラフィックまたはヘルス チェックに対して応答がないサーバ プール メンバは、自動的に非アクティブに設定されます。さらに、たとえば、サーバでメンテナンスを実行する場合などに、プール メンバを手作業で取り消せます。

ここで説明されているようにサーバをイネーブルまたはディセーブルにすると、ただちにその状況が反映されます。この変更を有効にするために、ポリシーを導入する必要はありません。

次の手順で、プール メンバを非アクティブまたはアクティブにできます。

- [Disable] ボタンをクリックすると、プールでサーバ メンバが非アクティブになります。ACE XML Gateway では、ディセーブルにされたプール メンバにトラフィックは送信されず、ヘルス チェック メッセージの送信も試行されません。
- ディセーブルにされたサーバは、コンソールでイネーブルにすることによってのみ、プールに回復できます。[Enable] ボタンを使用すると、サーバを再度アクティブにできます。

図 14-2　　サーバ プール リスト



サービス プロバイダーヘルス チェック

ヘルス チェックは、使用可能であることを確認するために、ACE XML Gateway によって定期的な間隔でサービス プロバイダーに送信される、HTTP メッセージです。サーバがヘルス チェックに対して応答しない場合、（バックオフ期間と呼ばれる）設定可能な時間の間、サービス トラフィックはサーバに送信されません。

（注）　サービス プロバイダーのヘルス チェックを Gateway のヘルス チェックと混同しないよう注意します。サービス プロバイダーのヘルス チェックは、ACE XML Gateway がそれ自体のヘルス チェックを行う前に、ロード バランサまたはルータによって使用されます。これらのタイプのヘルス チェックの設定の詳細については、「静的コンテンツ応答の設定」（P.15-168）を参照してください。

ヘルス チェックは、1 つのホストまたはサーバ プールで構成されているサーバ定義に対して設定できます。プールのプライマリ サーバに設定されているヘルス チェックは、プールのすべてのメンバで実行されます。使用不可能なサーバがサーバ プールのメンバの場合、このサーバは、バックオフ期間の間、サーバ プールから除外されます。バックオフ期間が期限切れになると、ACE XML Gateway では、サーバへの通信を試行します。サーバが応答可能な場合、サーバはプールに戻されます。

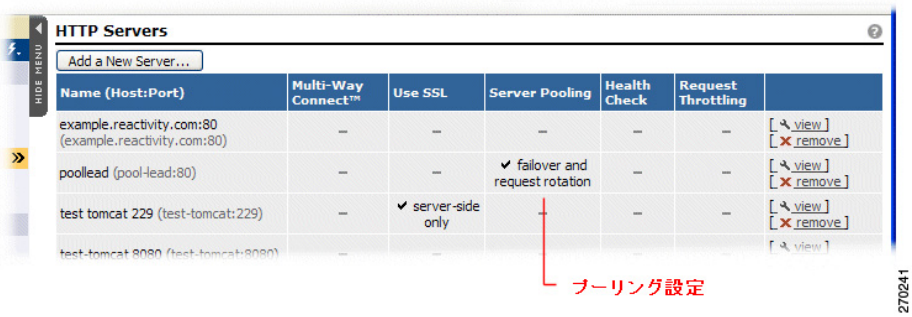
ユーザは、送信するメッセージ コンテンツ、（パスによって）ヘルス チェックが要求されるサーバでのリソース、サーバ応答の解釈方法について、設定することができます。ヘルス チェックの間隔は秒単位でも指定できます。ヘルス チェック間隔の期間中、サーバとやり取りされるサービス トラフィックがある場合、ACE XML Gateway により、ヘルス チェック メッセージだけが送信されます。この結果、トラフィックが高負荷のときには、ACE XML Gateway によってサーバのステータスはチェックされません。

起動前に、ヘルス チェックの一部として呼び出すサーバのリソースを決定します。

サーバ ヘルス チェックを設定するには、次の操作を実行します。

ステップ 1　[HTTP Servers] ページでサーバの横にある [view] リンクをクリックし、プーリング設定が含まれたサーバの設定ページを開きます。プーリング設定が含まれているサーバは、サーバ リストの [Server Pooling] 情報フィールドによって示されます。

図 14-3　　[Server Pooling] ページ



ステップ 2　[Server Health Check] という見出しの横の [Edit] リンクをクリックします。

ステップ 3　[Server Health Check] ページで、[Send the following HTTP request to each host (including any pooled hosts) every] とラベルが記されている 1 つ目のチェックボックスを選択してサーバのヘルス チェックをイネーブルにし、隣接フィールドにヘルス チェックの間隔を秒単位で入力します。

ここで設定する間隔に加え、サービス プロバイダーの応答時間が、チェック間での実際の時間の間隔に影響を及ぼす可能性があることに、注意してください。たとえば、ヘルス チェック間隔が 1 分で、サーバからの通常の応答時間が 5 秒であるとします。プールに 10 のサーバがある場合、ヘルス チェック間の実際の間隔は、1 分と 50 秒になります。

ステップ 4　メッセージの送信に HTTP の GET 方式を使用するか POST 方式を使用するかを選択します。

ステップ 5　[Request Path] フィールドで、ヘルス チェックで呼び出されるサーバのリソースへのパスを入力します。

ステップ 6　[Response Checking] セクションのコントロールを使用するとサーバが使用可能であることを示す応答を指定します。

秒単位でタイムアウト期間を指定し、ポジティブ テスト（応答基準として [meets] を選択）またはネガティブ テスト（応答基準として [does not meet] を選択）のいずれかを、次の応答の値またはアトリビュートの 1 つとして指定します。

- HTTP 応答コード（デフォルトで 200）
- 応答での HTTP ヘッダーの存在と、オプションで、ヘッダー フィールドの値
- 正規表現で示され、XPath による応答によって指定される、応答の本文にある特定の値

ステップ 7　オプションで、[If a server fails (does not send a healthy response), suspend requests for at least] とラベルが記されているフィールドに新しい値を入力することによって、バックオフ期間を変更します。

使用可能であると断定された後は、この回数分の、ACE XML Gateway によるサーバへの通信は試行されません。

ステップ 8　完了したら [Save Changes] をクリックします。

ユーザが行った設定の変更は、サーバの情報ページの [Server Health Check] セクションに反映されます。

バックエンド サーバ トラフィックのスロットリング

Denial-of-Service（DoS; サービス拒絶）攻撃は、サービス プロバイダーが適切な時間内に応答できないようにするため、サービス プロバイダーに問題を生じさせることを意図した、広く知られているネットワーク攻撃のタイプです。攻撃には、次のように、いくつかの形式があります。

- メッセージが大きすぎて、サービスで処理できない場合。
- メッセージの配信速度が速すぎて、サービスで応答できない場合。
- 非常に大きな処理能力を使用するよう、メッセージが設計されている可能性がある場合。たとえば、多くのレベルでネストされたエンティティがある（エンティティが他のエンティティを参照する）XML が、メッセージ含まれている場合などがあります。

ACE XML Gateway では、次のものに制限を加えることにより、このような攻撃を防ぐことができます。

- 添付ファイルのサイズを含む、サービスに配信されるメッセージのサイズ
- メッセージが配信可能なレート
- バックエンド サービスがメッセージの処理に消費できる最大時間

ACE XML Gateway でこれらの制限の 1 つに違反するトラフィックのパターンが検出された場合、この制限に該当する場合に、その後のバックエンド サービスへの配信が、一定時間の間、ディセーブルにされます。メッセージの処理は、レート制限を超過せずにその後の配信が許可される十分な時間が経過した後で、回復されます。

ACE XML Gateway では、無効なスロットリング制限を超えるメッセージが拒否されます。要求は、その後の処理のためにキューに追加されるわけではないことに、注意することが重要です。Gateway により、応答コード HTTP 500（デフォルト）でクライアントに対してエラー メッセージが返されます。必要に応じ、例外マッピング ページで、無効なメッセージのエラー マッピングを変更することによって、ACE XML Gateway が異なる応答を送信するよう設定できます。

バックエンド スロットリングの設定

バックエンド スロットリングの設定は、バックエンド サーバによって指定可能です。値を設定しているリソースが実際のサーバ プールの場合、個々の各サーバではなくプール全体に送信されるトラフィックに対して、設定が適用されます。

バックエンド サーバにトラフィック スロットリングを設定するには、次の操作を実行します。

ステップ 1　`Administrator` ユーザまたはコンソールの `Operations` ロールを持つ `Privileged` ユーザとして ACE XML Manager にログイン中に、編集するリソースを提供するものに対してアクティブなサブポリシーを設定します。

ステップ 2　操作メニューで [Destination HTTP Servers] リンクをクリックします。

ステップ 3　[HTTP Servers] ページで、設定するサーバの横にある [view] リンクをクリックします。

ステップ 4　[Request Throttling] セクションの [Edit] リンクをクリックし、ACE XML Gateway によってメッセージがサーバに送信されるレートを制限します。

[Edit Request Throttling] ページが表示されます。

ステップ 5　要求スロットリングをイネーブルにするには、[Throttle the rate of requests] オプションを選択します。

[Request rate] フィールド、[Request burst] フィールド、[Average request size] フィールド、および [Average latency] フィールドが、イネーブルになります。

ステップ 6　次のフィールドを設定することによって、受信可能なサーバ負荷の上限を指定します。

- [Request rate]。ACE XML Gateway が保護サーバに送信可能な、サーバで 1 秒当たりに受信可能な要求メッセージの数。デフォルトは、1 秒当たり 50 の要求です。
- [Request burst]。ACE XML Gateway が一度にサーバに送信可能な、サーバで受信可能な要求メッセージの数。デフォルトは、一度に 15 の要求です。

（注）　トラフィックの負荷のしきい値の設定に関する詳細は、「トラフィック レートのしきい値について」（P.23-224）を参照してください。

- [Average request size]。ACE XML Gateway がサーバに送信可能な、サーバで受信可能な要求の平均サイズ。平均メッセージ サイズのデフォルト値は 1024 キロバイト（KB）です。このサイズよりも大きな個々のメッセージは、性能測定の目的で複数のメッセージとして数えられます。
- [Average latency]。バックエンド サービスから受信可能な、秒数で表される平均応答時間。この値よりも長い個々の応答時間は、性能測定の目的で複数のメッセージとして数えられます。

ステップ 7　受信可能な個々のメッセージの最大サイズを指定するには、[Never send any request that is larger than] チェックボックスを選択し、該当するフィールドに、受信可能なメッセージの最大サイズを表す整数をキロバイト（KB）単位で入力します。

ACE XML Gateway では、指定されたキロバイト数より大きな要求は拒否されます。

ステップ 8　サービスによってコード 503（Server Busy）応答が返された場合に後続の要求を遅延させるには、[If the server returns code 503 (Server Busy)] を選択します。

[wait at least ... seconds] フィールドがイネーブルになります。

ステップ 9　サーバによってコード 503（Server Busy）の応答が返された後に ACE XML Gateway によって追加要求を遅延させる秒数を指定するには、[wait at least ... seconds] フィールドに数を入力します。

ACE XML Gateway でサーバから 503 エラー応答を受信した場合、指定された秒数が経過するまで、要求は送信されません。

ステップ 10　[Save Changes] をクリックし、現在の作業ポリシーに新しい設定をコミットします。

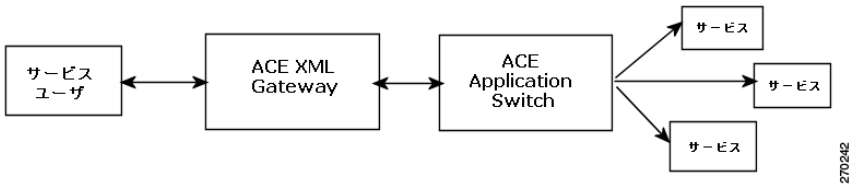
ACE XML Gateway で新しいスロットリング設定を有効にするため、ポリシーを導入します。

ACE アプリケーション スイッチとの統合

実稼動中のネットワークでは、アプリケーション サーバがクライアント アプリケーションによって直接アクセスされることはほとんどありません。代わりに、通常、1 つまたは複数のロード バランサによって、プロキシされます。ACE XML Manager には、Cisco Application Control Engine（ACE）アプリケーション スイッチによってプロキシされているバックエンド サービスを迅速に統合する機能が含まれています。ACE アプリケーション スイッチは、ネットワーク上のアプリケーションの可用性、パフォーマンス、セキュリティを最大限に活用する高性能アプリケーション スイッチです。

ACE アプリケーション スイッチ設定を検査することにより、ACE XML Manager では、ACE アプリケーション スイッチの後にあるアプリケーション サーバにサービス トラフィックをルーティングする必要があるポリシー設定を迅速に生成できます。

図 14-4　ダウンストリーム ACE アプライアンスの設定



ACE 設定の用語で、ACE アプリケーション スイッチでは、*Virtual IP*（VIP; バーチャル IP）を介して外部ネットワークに対してバックエンド サーバ ファームが公開されます。ACE XML Manager では、ACE アプリケーション スイッチ仮想デバイス コンテキストにクエリーを送信し、公開されている VIP が検出されます。

VIP 検出の実行後、ACE XML Manager により、Cisco ACE 仮想デバイスで見つけられた VIP が公開されます。HTTP サーバ オブジェクトを生成する VIP を選択できます。これは、仮想サービスのバックエンド サービス宛先として使用できます。

ACE XML Manager は、ACE アプリケーション スイッチの次のバージョンで動作します。

- Cisco ACE アプライアンス、ソフトウェア バージョン A1(7) およびそれ以降
- Cisco ACE モジュール、ソフトウェア バージョン A1(0)、A2(0)、およびそれ以降

ACE アプリケーション スイッチと ACE XML Gateway 設定との統合は、次のように 2 段階で発生します。

1. VIP のインポート元となる ACE アプリケーション スイッチ仮想デバイスへの接続を設定します。
2. ACE 仮想デバイス接続の設定後、Cisco ACE 仮想デバイスを検査し、選択した VIP からサーバ オブジェクトを生成するよう、ACE XML Manager を指定します。

ACE XML Manager によって特定の ACE 仮想デバイスで VIP 検出を実行するたびに、ACE XML Manager では、検出が新しいイベントとして処理されます。つまり、HTTP サーバ オブジェクトを設定済みの VIP が検索され、レポートされます。ただし、ACE XML Manager により、前にインポートされた VIP から重複するサーバ オブジェクトが生成されることは防止されます。すでにインポートされた VIP に対しては、いかなるタイプの設定のアップデートも試行されません。

（注）　ACE アプリケーション スイッチで設定されているバックエンド サーバに対する SSL 接続要求は、ACE XML Gateway ポリシーへの VIP インポートによって生成された HTTP サーバ オブジェクトには反映されません。バックエンド SSL サーバに VIP をインポート後、オブジェクト設定で手作業で SSL 接続の暗号化をイネーブルにする必要があります。

ACE XML Gateway によって用意されたサーバ管理機能は、手作業で作成された HTTP サーバ オブジェクトと VIP インポートによって生成されたオブジェクトとでは異なります。要求スロットリングは ACE ベースのサーバ オブジェクトに対して設定可能ですが、（ACE アプリケーション スイッチは、通常、ロード バランシングのバックエンド サーバでのタスクの実行に依存するため）サーバ プーリングは設定可能ではありません。

Cisco ACE 仮想デバイス接続の設定

ACE アプリケーション スイッチから VIP をインポートするには、まず、ACE アプリケーション スイッチで仮想デバイスへの接続を指定します。この接続は、ACE XML Manager でのポリシー作成でだけ使用できることに注意してください。サービス トラフィックは、Cisco ACE 仮想デバイスで見つけられた VIP から生成された接続に送信されます。また、ACE XML Manager では、この接続によって指定された ACE デバイスの設定は変更されません。つまり、ACE XML Manager では、Cisco ACE デバイスでだけ、読み取りのみの操作が実行されます。

Cisco ACE 仮想デバイスへの接続を設定するには、次の操作を実行します。

ステップ 1　ACE XML Manager Web コンソールの操作メニューで、[Destination HTTP Servers] リンクをクリックします。

ステップ 2　[Configure Integrated ACE Management] ボタンをクリックします。

ステップ 3　[Add ACE Application Switch] ボタンをクリックします。

ステップ 4　次のフィールドに値を入力します。

- [ACE VLAN Address]：インポートする VIP がある ACE アプリケーション スイッチ仮想デバイスの IP アドレス。このアドレスは、ACE 設定の特定の VLAN アドレスに対応させる必要があります。
- [HTTP(S) Port]：この Cisco ACE 仮想デバイスが HTTP 要求をリッスンするポート番号。
- [Use HTTPS]：ACE アプリケーション スイッチに接続して、VIP を検査し、インポートするときに、ACE XML Gateway が SSL を使用する必要があるかどうか。ACE XML Gateway では、セキュア ソケット レイヤ セキュリティを使用して ACE デバイスにアクセスできますが、（証明書は ACE XML Gateway にインポートできないため）ACE アプリケーションの証明書を検証できません。

  SSL を使用して ACE アプライアンスにアクセスする場合、通常は、ポート 10443 に接続する必要があります（ポート 443 は ACE アプライアンスで他の用途に予約されています）。
- [Username]：この ACE アプリケーション スイッチ仮想デバイスの管理アカウントのユーザ名。
- [Password]：指定されたユーザ アカウントのパスワード。

- [Connection Timeout] : Manager が、接続を検証し、Cisco ACE アプリケーション スイッチから VIP を検出する試行を放棄する必要がある、経過時間の長さ。この値は、検査に要する全体的な時間ではなく、検証イベント内個々の要求に対して適用されることに、注意してください。

ステップ 5　[Save Changes] をクリックします。

ACE XML Manager では、Cisco ACE 仮想デバイスへの接続が検証され、その設定の初期検査が実行されます。正常に終了した場合、新たに定義された接続が ACE テーブルに表示されます。

該当する接続の [Import VIPs] リンクをクリックし、続くセクションでの説明に従うことによって、Cisco ACE 仮想デバイスから VIP をインポートできるようになります。

VIP からのサーバ定義の生成

ACE アプリケーション スイッチ仮想デバイス接続の設定後、任意の時点で、VIP 情報をインポートできます。このプロセスでは、Manager により、公開される VIP の ACE 仮想デバイスが検査され、Web コンソールで提示されます。次の手順で説明されているように、Manager が HTTP サーバ オブジェクトを生成する VIP を選択できます。

ステップ 1　まだ開かれていない場合、操作メニューで [Destination HTTP Servers] リンクをクリックすることによって、[HTTP Servers] ページを開きます。

設定済みの Cisco ACE デバイス接続は、HTTP Servers リストの ACE の部分に表示されます。接続の設定に関する詳細は、「Cisco ACE 仮想デバイス接続の設定」（P.14-161）を参照してください。

ステップ 2　VIP のインポート元となる ACE 仮想デバイスの横にある [import VIPs] リンクをクリックします。

ACE XML Manager では、ACE アプリケーション スイッチが検査されます。完了すると、IP アドレスとポート番号のリストが、ACE 仮想デバイスにある VIP で表示されます。

（注）　ACE XML Gateway では、ACE アプリケーション スイッチ ポリシーの IP アドレスの範囲に一致するすべての VIP のインポートはサポートされません。

ステップ 3　チェックボックスを選択することによって、サーバ オブジェクトを作成する VIP を選択します。

VIP にあるポート番号が（ACE ポリシーで選択されているポートのように）範囲にある場合、バックエンド ACE アプリケーション スイッチに要求を送信する特定のポート番号を、VIP の横にあるテキスト フィールドに入力します。

（注）　バックエンド VIP のいくつかのポートの 1 つにメッセージを送信する場合、異なる各ポートについて、サーバ オブジェクトを作成する必要があります。追加ポートについて、VIP インポート プロセスを繰り返してバックエンド サーバ オブジェクトを作成する必要があります。

ステップ 4　HTTP サーバ オブジェクトを作成する VIP を選択した後で、[Create HTTP Servers] ボタンをクリックします。

HTTP Servers テーブルに VIP が表示されます。これで、ポリシーにある仮想サービスのバックエンド サービス設定で、VIP を使用できます。

HTTP エコー サーバの設定

仮想サービスで、そのバックエンド サービスとしてエコー サーバが使用される場合、外部サーバの代わりに ACE XML Gateway によって応答が生成されます。応答は、（ポリシーで設定されている HTML ページまたは SOAP 応答のような）固定応答の場合も、クライアントに反映される元の要求の場合もあります。

エコー サーバは、次のような場合に役に立ちます。

- バックエンド システムが開発中で、要求を受信する準備が整っていない場合に、使用できます。エコー サービスを使用すると、バックエンド サービスの準備が整うまで、クライアント側のアプリケーションのテストを行うことができます。
- ACE XML Gateway により、メイン トラフィック ストリームの外側にあるメッセージを検証できます。

エコー サーバは、HTTP ベースの仮想サービスでだけ動作できます。MQ シリーズなどのメッセージング サーバでは動作しません。

エコー サーバを設定するには、次の手順を実行します。

ステップ 1　操作メニューで [Destination HTTP Servers] リンクをクリックし、[Add a New HTTP Echo Server] ボタンを押します。

ステップ 2　[New Server] ページで、エコー サーバ定義として識別可能な名前を、[Name] フィールドに入力します。名前は、ポリシー内のエコー サーバ定義で固有である必要があります。

ステップ 3　次のオプションから、応答の生成方法を選択します。

- [Echo] には、クライアントに戻される要求が反映されます。ポリシーで指定されているすべての処理または検証の設定は、Gateway を経由するにつれてメッセージに適用されます。必要に応じた HTTP ヘッダーの調整を除いて、エコー サーバ自体によるメッセージの処理は行われません。つまり、応答処理でメッセージが Gateway に反映される前に、要求固有の HTTP ヘッダーが削除され、応答固有の HTTP ヘッダーが追加されます。
- [Fixed] により、[Status Code] フィールド、[Content-Type] フィールド、[Other Headers] フィールド、[Body] フィールドで設定した応答が返されます（ここで設定されたヘッダーに加え、エコー サーバにより、メッセージ サイズに応じた適切な値で、`Content-length` HTTP ヘッダーが戻されるメッセージに加えられます）。
- [Asynchronous] により、返信コード 202 の HTTP 応答が常に戻されます。このオプションは、機能的に、[Fixed] 応答を選択し、[Status Code] を [202 Accepted] に設定するのと同等です。

（注）　これらのオプションについての詳細は、これらの手順の後の説明を参照してください。

ステップ 4　[Save Changes] をクリックして作業ポリシーに変更を保存します。

ステップ 5　メッセージをエコーするサービス定義の [Backend Service] 設定で、エコー サーバ定義をホスト サーバとして選択します。新しいオブジェクトでは、サービス インターフェイスで使用可能なサーバのリストで、エコー サーバが使用可能です。

トラフィック ストリームの外側の処理エンジンとして ACE XML Gateway を使用する場合は、次の点に注意します。

- ACE XML Gateway で（たとえば、XSLT またはコンテンツの置き換えによって）メッセージを変換する場合、エコー モードを使用します。変換に失敗した場合、変換されたメッセージの代わりに HTTP 500 応答が返されます。
- （XSD、SOAP 添付ファイル チェック、コンテンツ スクリーニングなどの）さまざまな形式を含む読み取りのみの各操作について、エコー応答または固定応答のいずれかを使用できます。帯域幅の観点からより効率的で、受信アプリケーションによって簡単にパースされるため、固定応答がほとんどの場合に適しています。

いずれの場合でも、応答のステータス コード 200 は、呼び出しアプリケーションに対して、メッセージが検証に渡されたことを示します。他のすべてのエラー コードは、検証の障害と解釈されます。

メッセージング サーバに関する作業

ACE XML Gateway により、TIBCO Rendezvous（TIB/RV）または Message Queue（MQ）シリーズ サーバからメッセージ トラフィックをルーティングできます。Java Messaging Service（JMS）サーバも、オプションの SDK ベースの拡張モジュールの使用を介してサポートされます。

[Messaging Servers] ページに、ACE XML Gateway ポリシーで現在定義されているメッセージング サーバ プロファイルのリストが表示されます。メッセージング サーバ定義を作成できるページで、既存のサーバ定義を編集または削除できます。

メッセージング サーバの詳細については、第 16 章「JMS トラフィックに関する作業」、および
第 16 章「JMS トラフィックに関する作業」を参照してください。

サーバ定義の削除

コンソールの操作メニューで [Destination HTTP Servers] または [Messaging Servers] リンクをクリックすると、サーバ定義を削除できます。サーバ リストで、サーバのエントリの横にある [remove] リンクをクリックして、サーバを削除します。プロンプトが表示されたら、操作を確認します。

サーバを使用するサービス定義がない場合にだけ、サーバを削除できます。この場合にサーバを削除するには、サーバに依存するオブジェクトを削除するか、または、それを別のサーバに変更します。