CHAPTER 3

最初の手順

この章では、ACE XML Manager Web コンソールの概要を説明します。内容は次のとおりです。

Manager の Web コンソールへのログイン

ネットワークに ACE XML Manager がインストールされると、ACE XML Gateway ポリシーを作成するためのブラウザベースの環境である ACE XML Manager の Web コンソールにログインできます。

ACE XML Manager の Web コンソールは、ほとんどのブラウザの最近のバージョンで利用できます。特に、Mozilla Firefox 1.5.0.*x* と 2.0.0.*x*、および Microsoft Internet Explorer 5.5 と 6 をサポートします。ACE XML Managerの多くの Web コンソール機能を適切に動作させるため、ブラウザの JavaScript 機能が有効になっている必要があります。

ACE XML Manager の Web コンソールにログインするには、次の手順に従います。

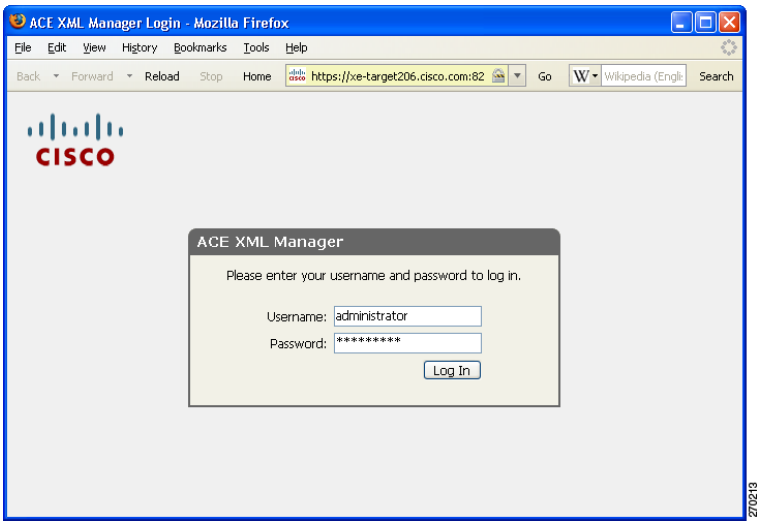
ステップ 1 ネットワーク経由で ACE XML Manager アプライアンスにアクセスできるコンピュータで、ブラウザを開き、次のアドレスに移動します。

https://<*hostname*>:8243

ここで、<*hostname*> は、ACE XML Manager の IP アドレスまたはホスト名です。接続にはセキュアな HTTP（HTTPS）が使用されます。ACE XML Manager がコンソールの要求をリッスンするデフォルト ポートは 8243 です。

ブラウザがログイン ページを表示します（図 3-1 を参照）。

図 3-1　ACE XML Manager の Web コンソールのログイン



ACE XML Manager のホスト名は、最初のインストール時に設定されます。インストールのためのログイン ページへのパスがわからない場合は、管理者に問い合せてください。

ログイン ページには、すでに Web コンソール にログインしている他のユーザがリスト表示されます。他のユーザがいつコンソールにログインしたかに注意する必要があります。ACE XML Manager では、ユーザ相互の変更の上書きを防ぐことができません（複数のユーザが 1 つの設定ページを同時に編集すると、最後に行われた変更が保存されます）。このため、作業を注意深くチェックし、新しいポリシーを導入して生成する前に、ポリシーを試験的環境でテストすることが重要です。

ステップ 2　この ACE XML Manager を使用して ACE XML Gateway の複数のクラスタを管理する場合、アクセスしたいクラスタ ポリシーを選択できるメニューが表示されることがあります。この場合、編集するクラスタの名前をメニューから選択します。

ステップ 3　[Username] フィールドに、ユーザ名を入力します。たとえば、管理者の場合、このフィールドに `administrator` と入力します。これはあらかじめ設定されたユーザ アカウントで、コンソールに対するすべての権限を持っています。

（注）　ACE XML Manager の Web コンソールへのユーザ アカウントの追加に関する詳細については、第 33 章「Web コンソール ユーザの管理」を参照してください。

ステップ 4　[Password] フィールドに、パスワードを入力します。

（注）　Administrator ユーザのデフォルトのパスワードは、「swordfish」です。セキュリティ上の理由から、デフォルトのパスワードは必ず変更してください。

ステップ 5　[Log In] ボタンをクリックします。

有効な組み合わせのユーザ名とパスワードを入力しなかった場合、エラー メッセージが表示されます。Administrator による Manager のアクセスの設定によって、ACE XML Manager が無条件で終了し、ユーザ アカウントがディセーブルになる前に試みることができるログイン回数が制限される場合があります（デフォルトでは 3 回）。このセキュリティ機能は、Administrator ユーザ アカウント以外のすべてのユーザ アカウントに適用されます（Administrator ユーザ タイプで作成されたユーザ アカウントには適用されます）。

この機能およびユーザ アカウントの復元に関する詳細については、「ログイン試行に失敗したユーザのログイン拒否設定」（P.35-368）を参照してください。

有効な組み合わせのユーザ名とパスワードを入力すると、次のいずれかのページが表示されます。

- ライセンスが ACE XML Manager に設定されていない場合、ライセンス エラー ページが表示されます。ACE XML Gateway および Manager でのライセンスの取得と適用に関する詳細については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。
- ACE XML Manager に有効なライセンスがあり、ポリシーがサービス ルーティングに設定されていない場合、[Welcome] ページが表示されます。[Welcome] ページから、仮想サービスの定義を開始できます。
- ポリシーに仮想サービスが含まれている場合、[Dashboard] ページが表示されます。Manager の [Dashboard] では、システム イベントおよびアクティビティの概要を示します。

パスワードを最初のログイン時に割り当てられたものから変更することを推奨します。パスワードを変更するには、ページの右上にあるユーザ名をクリックします。[User Information] ウィンドウで、[Change Password] ボタンをクリックし、新しいパスワードを指定します。

デフォルトでは、コンソールのパスワードは、最低限の複雑さの要件を満たしている必要があります。パスワードは 8 文字以上にしてください。また、辞書に載っているような言葉がパスワード全体での最小限の割合を超えて含まれておらず、社会保障番号や国民 ID 番号と似ていないものにする必要があります。一般的に、パスワードには文字、数字、および特殊文字の組み合わせを使用することを推奨します。

Manager の Web コンソールの操作

図 3-2 に、ACE XML Manager の Web コンソールで利用するインターフェイスの主要な構成を示します。

図 3-2　ACE XML Manager Dashboard

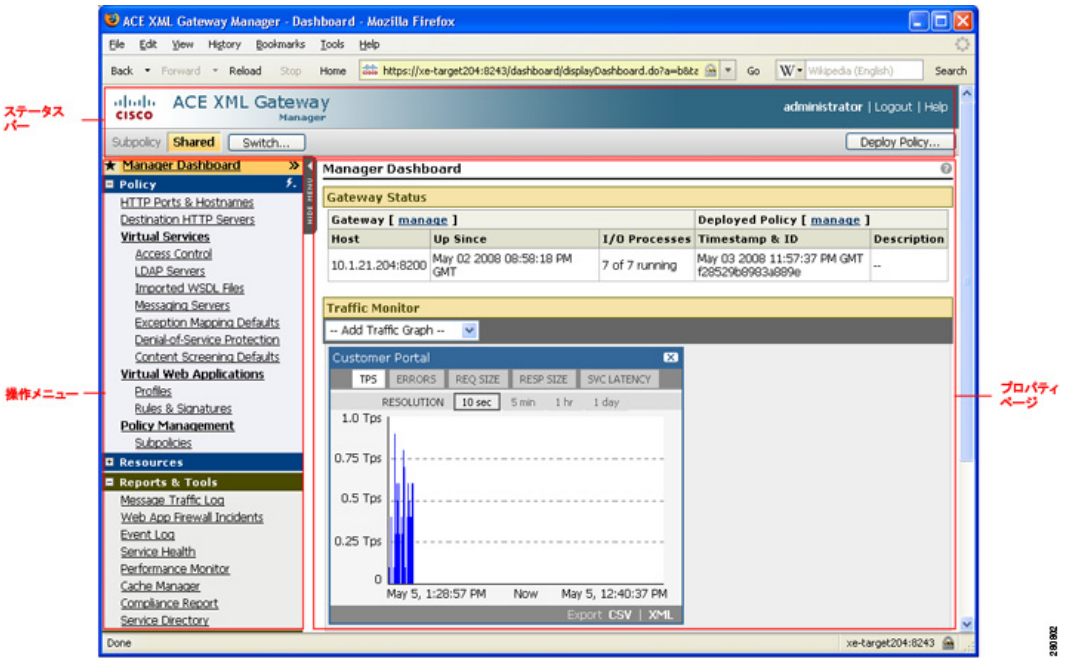


図 3-2 に示すように、ACE XML Manager の Web コンソールは、次のエリアで構成されています。

- ナビゲーション メニュー
- ステータスバー
- プロパティ ページ

ナビゲーション メニュー

ナビゲーション メニューは、コンソールの左側に表示されます。コンソールの主な設定およびモニタリングのページへのリンクが表示されており、次のカテゴリに分類されます。

- [Policy] セクションには、ルールを定義し、ACE XML Gateway で処理されるトラフィックに適用できる操作を処理するページへのリンクが含まれています。
- [Resources] セクションには、ポリシーで使用されるリソース ファイルを管理するページへのリンクが含まれています。詳細については、第 28 章「リソース ファイルの管理」を参照してください。
- [Reports & Tools] には、ACE XML Gateway とネットワークの状態をモニタリングするページへのリンクが含まれています。
- [Administration] には、コンソール管理者が ACE XML Manager 自体を制御できるページ（ライセンス、ユーザ アカウント、監査ロギング、診断など）へのリンクが含まれています。

ナビゲーション メニューの [Policy] の見出しの横に、[Quick Links] ボタン（）が表示されます。このボタンを使用すると、Web Services Description Language（WSDL）ファイルのインポート、仮想サービスの作成、およびオーセンティケータ（サービスへのアクセスを制御するために使用するポリシー オブジェクト）の作成などの共通タスクにアクセスできます。

ステータスバー

ステータスバーは、コンソールのすべてのページの上部に表示されます。現在アクティブなサブポリシー、およびコンソールに現在アクセスしているユーザ アカウントのユーザ名を表示します。ポリシーの導入やログアウトなど、コンソールで共通の操作を行うためのボタンがあります。

Administrator ユーザは、ステータスバーに表示されるバナー テキストを設定し、他のコンソール ユーザに通知またはその他のタイプの情報を発表したりできます。

サブポリシーは、ポリシー内のオブジェクトを組織化するためのコンテナです。*Shared* サブポリシーは、サブポリシーを使用して作業を組織化しているかどうかにかかわらず存在している組み込みサブポリシーです。すべてのサブポリシーで使用される共通のオブジェクトが含まれています。

ご使用の環境でポリシー内に「Shared」以外のサブポリシーがある場合、サブポリシー ラベルの横に [Switch] ボタンが表示されます。作業コンテキストを別のサブポリシーに変更するには、[Switch] ボタンをクリックします。

サブポリシーの詳細については、「サブポリシーの使用」（P.30-306）を参照してください。

プロパティ ページ

プロパティ ページでは、システムの操作の特定のエリアの情報または設定を表示します。一般的に、プロパティ ページでは、機能に関連する変更可能な設定に対する制御手段にアクセスできます。

サブポリシーを使用したポリシーの組織化

*サブポリシー*を使用して、ポリシー内の関連オブジェクトを組織化できます。サブポリシーは、特定のポリシーにあるオブジェクトのサブセットです。サブポリシーへのアクセスは、サブポリシーに対する特権を持つコンソール ユーザだけがサブポリシーを変更できるように制御できます。

システムには、*Shared* と呼ばれる組み込みサブポリシーが含まれています。新しくインストールされた ACE XML Manager の Web コンソールに最初にログインすると、「Shared」サブポリシーがアクティブになります。「Shared」サブポリシーは、そのオブジェクトに他のサブポリシーからアクセスできる唯一のサブポリシーです。その他のサブポリシーでは、異なるサブポリシー間で設定およびオブジェクトを使用できません。

サブポリシーの最良の組織化対策（特定のサブポリシーまたは「Shared」で作成するオブジェクトを選択する方法）は、実装によって異なる可能性があります。ただし、一般的に、「Shared」サブポリシーには、ポート設定、認証局、共通バックエンド HTTP サーバなど、すべてのプロジェクトで必要なリソースが含まれている必要があります。一方、サブポリシーには、通常、仮想サービスや認証オブジェクトなどのアプリケーション固有のオブジェクトが含まれています。

ポリシーでサブポリシーを使用する場合、設定の変更またはポリシー オブジェクトの追加を行う前に、ACE XML Manager の Web コンソールでどのサブポリシーがアクティブになっているのかを認識することが重要です。特定のサブポリシーにポリシー オブジェクトを作成すると、ポリシー オブジェクトは、そのサブポリシーのコンテキストで、そのサブポリシーを修正する特権を持つユーザだけが編集できるようになります。

サブポリシーは、ポリシーの作成環境の管理およびセキュリティ保護に役立ちます。承認ベースの導入にも、同様の利点があります。承認ベースの導入では、コンソール管理者は、ACE XML Gateway に反映させるために、ポリシーの導入を承認する必要があります。この機能は、ポリシーの変更および導入のプロセスの制御と管理に役立ちます。

サブポリシーはポリシー内でオブジェクトを組織化する手段を提供しますが、大規模な実装では、パーティション作業に異なるポリシーを使用しなければならない場合があります。ACE XML Manager の複数クラスタ管理機能では、特定の ACE XML Manager インスタンスで異なるポリシーを作成し、これらのポリシーを異なる ACE XML Gateway クラスタに導入できます。

Manager の制御下への Gateway の追加

『*Cisco ACE XML Gateway Administration Guide*』で説明されているように、ACE XML アプライアンスは、Gateway モード、Manager モード、または独立型モード（このモードでは、アプライアンスは Gateway と Manager の両方のモードで動作します）の 3 つのモードのいずれかで動作が可能です。

独立型アプライアンスの場合、初期設定後、ACE XML Manager は、すでに自己管理用に設定されています（アプライアンスのためのエントリが Manager の管理された Gateway リストにあります）。設定に Gateway を追加する必要はなく、すぐにポリシーで作業を開始できます。

ただし、アプライアンスが Manager 専用モードの場合、ここで説明しているように、ポリシーを導入してテストする前に、Manager の管理制御下に Gateway を追加する必要があります。

（注）　独立型アプライアンスでは、ACE XML Manager は、他の Gateway アプライアンスと自身の Gateway インスタンスを制御できます。したがって、これらの手順は、独立型アプライアンスの Manager の管理制御下に Gateway を追加したい場合にも適用できます。

ACE XML Gateway は、一度に複数の ACE XML Manager の制御下に設定できません。この制限は、複数クラスタ管理機能で作成された実際の Manager アプライアンスまたは Manager インスタンスによる管理に適用されます。

Gateway を Manager の制御下に追加する一般的な手順は、次のとおりです。

1. アプライアンスのシェル インターフェイスから Gateway の動作モードを設定する場合、この Gateway を制御する Manager の IP アドレスを指定します。

（注）　詳細については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。

2. ACE XML Manager の Web コンソールで、Gateway を Manager のクラスタ プールの 1 つ（そのデフォルトのクラスタなど）に追加します。
3. Web コンソールで、追加された ACE XML Gateway のライセンスのステータスをチェックします。必要な場合、ライセンスを要求して適用します。

ここでは、手順 2（Gateway を Manager のクラスタの 1 つに追加する方法）について説明します。Gateway がクラスタ グループに追加されると、Manager からポリシーの導入を受信できるようになります。次に、Gateway はアクティビティに関するレポートを Manager に返信し、Manager はすべての Gateway のロギング情報をその制御下に集約します。手順 1 および 3 の詳細については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。

（注）　ACE XML Manager は、Gateway の複数のクラスタを制御できます。単一クラスタ内のすべての Gateway は同じポリシー バージョンである必要がありますが、Manager の制御下にある複数のクラスタでは異なるポリシー バージョンを適用できます。詳細については、第 34 章「Gateway クラスタの管理」を参照してください。

デフォルト クラスタへの Gateway の追加

ACE XML Gateway を Manager の制御下に追加するには、Gateway を Manager の設定にあるクラスタに追加します。前に述べたように、独立型アプライアンスでは、これらの手順を行う必要はありません。これらの手順が必要なのは、Manager 専用アプライアンスを設定する場合または Gateway を独立型アプライアンスの管理制御下に追加する場合だけです。

Manager には、ACE XML Gateway を追加できる「Default Cluster」というあらかじめ設定されたクラスタがあります。デフォルト クラスタの名前は変更できます。また、設定の他の点も変更できます。特に別個の ACE XML Gateway 環境を維持する意図がない限り、Manager の設定に新しいクラスタを追加しないようにしてください。詳細については、第 34 章「Gateway クラスタの管理」を参照してください。

デフォルト クラスタに ACE XML Gateway を追加するには、次の手順に従います。

ステップ 1　Administrator 特権を持つユーザとして、Manager の Web コンソールで、ナビゲーション メニューから [Cluster Management] リンクをクリックします。

クラスタ管理ページに、「Default Cluster」という名前のクラスタが表示されます。独立型モードのアプライアンスの Manager では、[Default Cluster] に、このアプライアンスが唯一のメンバとして表示されます。その他のモードでは、新しくインストールした場合、デフォルト クラスタは空のクラスタとして表示されます。

ステップ 2　[Default Cluster] の横にある [edit] リンクをクリックして、クラスタに Gateway を追加します。

ステップ 3　必要に応じて、デフォルト クラスタにあらかじめ設定された内容（名前と HTTPS ポート、Manager の Web コンソールへの SSL アクセスで使用されるセキュリティ証明書など）を修正します。

このページに表示される [SSL Certificate] は、ブラウザから Manager の Web コンソールへの接続に適用されます。メニューが示すように、Manager では、デフォルトで使用される一時的な証明書が提供されます。組み込みの証明書を生成したサーバ証明書に置き換えることを推奨します。Manager と開発ワークステーションをセキュアなネットワーク内で動作させる場合、自己署名証明書を使用するように選択できます。ただし、セキュリティを強化するため、特にクラスタを実稼動環境に導入する場合は、CA 署名証明書を使用することを推奨します。

[Cluster Management] ページで [Manage SSL Certificates] ボタンをクリックして、ブラウザ接続で使用する新しい証明書を生成できます。そのページから [Generate CSR] ボタンを使用して、証明書署名要求を生成します。詳細については、「CSR の生成」（P.28-290）を参照してください。サーバ証明書が生成されて Manager にアップロードされたら、このページのメニューから証明書を選択し、ブラウザ接続に適用します。

ステップ 4　[Cluster Members] テキスト フィールドで、このクラスタに追加したい各 ACE XML Gateway の IP アドレスおよび管理ポートを入力します。各 Gateway のアドレスは、次のように、テキスト フィールドに 1 行ずつ入力する必要があります。

10.0.5.12
10.0.5.22

ログ イベントなどの管理情報を交換するために Manager および Gateway が使用する管理ポートは 8200 です。8200 を使用できない特定のネットワークの前提条件がある場合、IP アドレスに 8200 を付加し、別のポートを指定できます。

ステップ 5　[Save Changes] をクリックします。

ステップ 6　クラスタに追加後、通常、Gateway にライセンスを設定する必要があります。Gateway のライセンスのステータスをチェックするには、Web コンソールの [License Management] ページを開きます。Gateway でライセンスが必要な場合、アプライアンスでの製品ライセンスの取得と適用に関する詳細については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。

[Cluster Management] ページに、ACE XML Gateway がクラスタのメンバとして表示されます。これで、ポリシーを ACE XML Manager から ACE XML Gateway の制御下に導入できます。

クラスタの使用に関する詳細については、第 34 章「Gateway クラスタの管理」を参照してください。

コンソールからの安全なログアウト

セキュリティ上の理由から、ACE XML Manager の Web コンソールが無人の状態でユーザ セッションから離れないようにしてください。Web コンソールを使用した後、ログアウトし、使用したすべてのブラウザ ウィンドウを閉じる必要があります。この操作を行わない場合、ユーザ セッション中にブラウザにキャッシュされたページを他のユーザに見られる可能性があります。

ACE XML Manager から安全にログアウトするには、次の手順に従います。

ステップ 1　[Logout] ボタンをクリックします。

ステップ 2　確認ダイアログで [OK] ボタンをクリックして、ログアウトします。

ステップ 3　コンソール セッションで使用したすべてのブラウザ ウィンドウを閉じます。

セキュリティを強化するために、ACE XML Manager からログアウトした後、ブラウザのキャッシュをクリアします。