CHAPTER 34

Gateway クラスタの管理

この章では、ACE XML Gateway クラスタ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。

複数のクラスタの管理について

ACE XML Manager によって管理される ACE XML Gateway インスタンスは、クラスタによる Manager の設定によって組織化されます。管理対象クラスタの 1 つに追加することによって、ACE XML Gateway を ACE XML Manager の管理コントロール下に置きます。

設定で、ACE XML Manager には常に少なくとも 1 つのクラスタがあります。しかし、複数ある場合もあります。クラスタ内の Gateway すべてに同じポリシー バージョンを適用する必要がありますが、1 つの Manager に管理された別のクラスタには、別のポリシーを適用できます。この機能は、通常、別のビジネス ユニット向けに異なるトラフィック処理ルールを適用する場合に使用されますが、開発、テスト、および実稼動の環境など、特定のポリシーのライフ サイクルの異なる段階を表す異なる Gateway 環境を一元管理することもできます。

Default Cluster とは

Manager Web コンソールは、特定の Gateway クラスタのポリシーのコンテキストでだけ開くことができます。インストール後、すべての Managers には、Default Cluster という名前のクラスタが 1 つ含まれます。これは、作業のデフォルトの開始点として機能します。

スタンドアロン モードで設定されたアプライアンスでは、Default Cluster はこのアプライアンスをクラスタ メンバとするようあらかじめ設定されています。Manager 専用アプライアンスには、Gateway を追加する空の Default Cluster があります。必要に応じてデフォルト クラスタの名前を変更したり、クラスタに Gateway を追加できます。

Manager で少なくとも 1 つのクラスタを定義する必要のあることに注意してください。唯一のクラスタを削除すると新しい "Default Cluster" が次のログイン時に自動的に作成されます。

複数のクラスタを使用する場合の考慮事項

クラスタは、[Cluster Management] ページでこの Manager のコントロールに追加できます。このページには、操作メニューの [Administration] セクションの [Cluster Management] リンクをクリックするとアクセスできます。クラスタ設定ページでクラスタ内の Gateway を IP アドレスで指定します。

（注）　クラスタの追加については、「Manager の制御下への Gateway の追加」（P.3-18）を参照してください。

ACE XML Manager の管理者は、いくつかの方法でクラスタのポリシーへのアクセスを提供できます。

- ログイン ページのメニュー選択肢として。[Cluster] メニューには、この Manager 用に設定されたクラスタの名前が表示されます。
- 特定の管理ポートで。Web コンソールはデフォルトでポート 8243 を使用します。追加クラスタのコンソールは別のポート番号を使用できます。
- 特定の IP アドレスで。ポート番号は、クラスタ マネージャを区別するためのメカニズムの 1 つです。しかし、別の IP アドレスを使用すると、クラスタ マネージャはコンソール ユーザに完全に区別して表示されます。たとえば、クラスタ A のマネージャを 192.168.1.1、クラスタ B のマネージャを 192.168.1.2 に置けます。その後、ネットワークの DNS インフラストラクチャを使用して、一方の IP アドレスに gateway-prod、もう一方に gateway-test など、説明的なホスト名を設定できます。ユーザは、https://gateway-prod:8243 または https://gateway-test:8243 と指定して、2 つの完全に別個のアプライアンスであるように、各クラスタにログインできるようになります。

クラスタ設定ページでは、クラスタの IP アドレスを選択できます。使用できるアドレスは、Manager ネットワーク インターフェイスが設定されたものです。

（注）　インターフェイス上で IP アドレス エイリアスを設定する詳細については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。

ユーザが特定のクラスタにログインすると、そのクラスタの Manager Web コンソール環境が、独自のポリシー、ユーザ アカウント、ログ情報を持つもう 1 つのクラスタとは完全に別の環境として表示されます。

コンソール ユーザ アカウントはクラスタのコンテキストに存在するため、各ユーザ（組み込み `administrator` ユーザ アカウント以外）は、追加されたクラスタのポリシーにしかアクセスできません。別のクラスタにアクセスするには、ユーザがもう 1 つのクラスタ ポリシーで有効なアカウントを持っている必要があります。

クラスタ間でポリシーを移動するには、「サブポリシー間でのオブジェクトのコピー」（P.30-309）で説明している Portable Policy Format（PPF）メカニズムを使用する必要があります。具体的には、ソース クラスタのコンソールでポリシーを PPF ファイルとしてエクスポートしてから、もう 1 つのクラスタのコンソールにログインして、PPF をインポートします。

ほとんどの場合、単一の Manager での各クラスタの設定は、他のクラスタとは完全に別に維持されます。つまり、ポリシー設定はクラスタ間で共有されません。このルールにはいくつか例外があります。主に、コンソール システム管理設定で行う必要があります。次のような例外があります。

- 監査ログ設定
- SDK 開発モード
- SDK 拡張モジュール
- Manager ログレベル

これらのいずれかの設定が変更されると、変更はクラスタ環境全体に影響します。Manager Web コンソール（特に、[System Management] > [Manager Settings] ページ）は、クラスタ全体に適用される設定を示しています。

複数のクラスタがイネーブルの場合も同様にログインの際に考慮すべき事項があります。Gateway に生成されたログ イベントと Manager に生成されたログ イベント間には、次の違いがあることに注意してください。

- Gateway イベントは、Manager Web コンソールが現在アクセスしているクラスタ内の Gateway のイベント ログだけに表示されます。
- クラスタ全体で、Manager イベントはすべてイベント ログに表示されます。わかりやすいように、イベントにはクラスタの名前が付けられます。たとえば、次のようになります。

  User "administrator" has logged in to cluster "Default Cluster" from IP address 10.0.4.5.

また、ACE XML Gateway 実装のモニタリング ポイントとして、Manager は実行ベースで ACE XML Gateway アクティビティの情報を受信します。高負荷の Gateway は膨大な量のイベント トラフィックを生成する可能性があります。イベント情報は、syslog 経由で Manager に渡されます。syslog は UDP プロトコルとしてベストエフォート型配送だけを提供します。高負荷のネットワークでは、イベント ログ情報を失う可能性があります。システムのクラスタ トポロジを設計する場合は、この動作を考慮することが重要です。特に、パフォーマンス テストを行うテスト クラスタとともに実稼動クラスタを 1 つの Manager を使用して管理することは避けてください。これを行うと、実稼動クラスタを監視する Manager の機能に影響する場合があります。

1 つの ACE XML Gateway を複数の ACE XML Manager で同時に管理しないでください。つまり、Gateway を複数のクラスタに入れないでください。この制限は、クラスタが単一の Manager 上にあるか、別の ACE XML Manager アプライアンス上にあるかに関係なく適用されます。

クラスタに関する作業

ここでは、Manager のクラスタ 定義を追加、修正、および削除する方法について説明します。

クラスタの作成

ほとんどの実装で、必要なクラスタは 1 つだけです。具体的には、別の Gateway 上や、単一の Manager からの Gateway のグループで独立したポリシーを管理する場合にだけ、これらの手順を使用して、追加のクラスタを作成する必要があります。

ACE XML Manager の新しいクラスタを定義するには、次の手順に従います。

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

クラスタ管理ページには、"Default Cluster" という名前のクラスタが表示されます。スタンドアロン モードのアプライアンスの Manager で、Default Cluster はこのアプライアンスを唯一のメンバ Gateway としてリストします。これ以外の場合、デフォルト クラスタは空です。

ステップ 2　[Manage a New Cluster] をクリックして新しいクラスタを定義し、Gateway を新しいクラスタに追加します。

ステップ 3　新しいクラスタにこれらの設定を行います。

- [Cluster Name] フィールドにクラスタの名前を入力します。この Manager の同じポートを複数のクラスタが使用している場合は、Manager Web コンソールにアクセスしようとしているユーザのログイン ページにその名前が表示されます。このため、クラスタ名で一意であり、コンソール ユーザにとって意味のある名前にする必要があります。
- [Manager HTTPS Port] では、Manager がこのクラスタのポリシーにアクセスするための Web コンソールを提供する HTTP ポートを指定します。デフォルト ポートの 8243 を受け入れるか、別のポートを入力できます。

  複数のクラスタが同じ Manager ポートを使用できます。同じ IP アドレスも使用する場合は、アクセスするクラスタのメニュー選択肢がログイン ページに表示されます。
- IP アドレス メニューでは、このクラスタの Web コンソールを提供するアドレスを選択できます。メニューは、アプライアンス上の物理イーサネット インターフェイスに設定されるアドレスをリストします。クラスタ マネージャはすべて同じ IP アドレスを使用できます。ただし、別の IP アドレスを使用すると、コンソール ユーザに対してクラスタ環境をより良く区別できます。別の IP アドレスを使用し、さらに自分の DNS インフラストラクチャを使用して、各クラスタの Web コンソールに意味のあるホスト名を関連付けられます。これによって、ユーザは https://gateway-prod:8243 や https://gateway-test:8243 のような URL でクラスタにアクセスできます。
- このページに表示される [SSL Certificate] は、Manager Web コンソールからブラウザへの接続を保護するために使用されます。メニューに示されているように、Manager では一時的な証明書が提供されます。この証明書を目的に応じて生成した証明書に置き換える必要があります。[Manage Certificates] ボタンをクリックすると、CSR を作成できます。

  クラスタ マネージャを区別するために IP アドレスを使用している場合は、各クラスタ マネージャのホスト名に対応したサブジェクト CN を持つ証明書が、クラスタごとに必要です。

ステップ 4　[Cluster Members] テキスト フィールドに、このクラスタに追加する Gateway の IP アドレスを入力します。各 Gateway IP は、次のように、テキスト フィールドのそれぞれの行に記述する必要があります。

10.0.5.12
10.0.5.22

Gateway の IP アドレスを入力する場合は注意が必要です。Web コンソール インターフェイスは、入力した値が実際に ACE XML Gateway アプライアンスのアドレスであることを確認する検証は行いません。ホスト IP が間違っている場合、ターゲットの Gateway への導入が試行され、導入に失敗するまでエラーが検出されない可能性があります。

ステップ 5　[Save Changes] をクリックします。

（注）　各 ACE XML Gateway は、それを管理する ACE XML Manager の IP アドレスで設定する必要があります。これがまだ実行されていない場合、各クラスタ メンバのシェル インターフェイスにアクセスし、Manager アドレスを設定します。詳細については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。

現在のクラスタ名がコンソール ページの上部に表示されます。

ステップ 6　ポート設定の変更など、Manager の再起動が必要な変更を行った場合は、Manager を再起動するように求めるプロンプトが表示されます。これを実行するには、[Cluster Management] ページの最上部にある [Restart the ACE XML Manager] ボタンをクリックします。

ステップ 7　多くの場合、追加された Gateway にはライセンスを設定する必要があります。ポリシーはライセンスが付与されるまで ACE XML Gateway に導入できません。ライセンスの設定については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。

クラスタの設定はこれで完了です。新しいクラスタのポリシーにアクセスするには、Manager からログアウトして、クラスタの設定に応じてログイン ページの [Cluster] メニューから選択するか、適切なポートまたは IP アドレスに移動して、新しいクラスタの Web コンソールにログインします。新しいクラスタにログインするには、組み込みの `administrator` ユーザ アカウントを使用します。

クラスタの編集

クラスタを作成した後、いつでもその設定（名前や管理ポート番号など）を修正できます。クラスタの設定を修正するには、変更するクラスタの Web コンソールが Web コンソールでアクティブである必要があります。Manager が別のクラスタの設定にアクセスしている間は、クラスタの設定を変更できません。

クラスタの Manager Web コンソールにアクセスしている間に、次の手順でそのクラスタ特有の設定を修正します。

ステップ 1　操作メニューで [Cluster Management] リンクをクリックします。

ステップ 2　ページ上にリストされたクラスタの横にある [edit] リンクをクリックします。

ステップ 3　[Edit Cluster Configuration] ページで必要に応じてクラスタの設定を変更します。設定の詳細については、「クラスタに関する作業」（P.34-361）を参照してください。

ステップ 4　変更をクラスタ設定にコミットするには、[Save Changes] をクリックします。

ステップ 5　ポート設定の変更など、Manager の再起動が必要な変更を行った場合は、Manager を再起動するように求めるプロンプトが表示されます。これを実行するには、[Cluster Management] ページの最上部にある [Restart the ACE XML Manager] ボタンをクリックします。

クラスタの削除

クラスタを削除すると、ポリシーを含むそのクラスタの設定がすべて削除されます。このため、クラスタを削除する場合は、誤ってポリシー作成作業が無駄にならないように注意する必要があります。

クラスタを削除するには、まず Manager Web コンソールからクラスタ設定にアクセスします。別のクラスタのコンテキストで Manager Web コンソールにアクセスしている間はクラスタ定義を削除できません。

[Cluster Management] ページでクラスタの [remove] リンクをクリックします。現在のクラスタが削除され、Web コンソールからログアウトされます。

Manager には少なくとも 1 つのクラスタが必要であることに注意してください。Manager から唯一のクラスタを削除すると、次のログイン時に新しいデフォルト クラスタが作成されます。