CHAPTER 4

Fabric Manager の認証

Fabric Manager には、ファブリック内のスイッチと通信する相互依存ソフトウェア コンポーネントが含まれています。これらのコンポーネントはさまざまな方法を使用して、ほかのコンポーネントおよびスイッチに対する認証を行います。この章では、これらの認証ステップとファブリックおよびコンポーネントの認証設定のベスト プラクティスについて説明します。

この章の内容は、次のとおりです。

Fabric Manager の認証概要

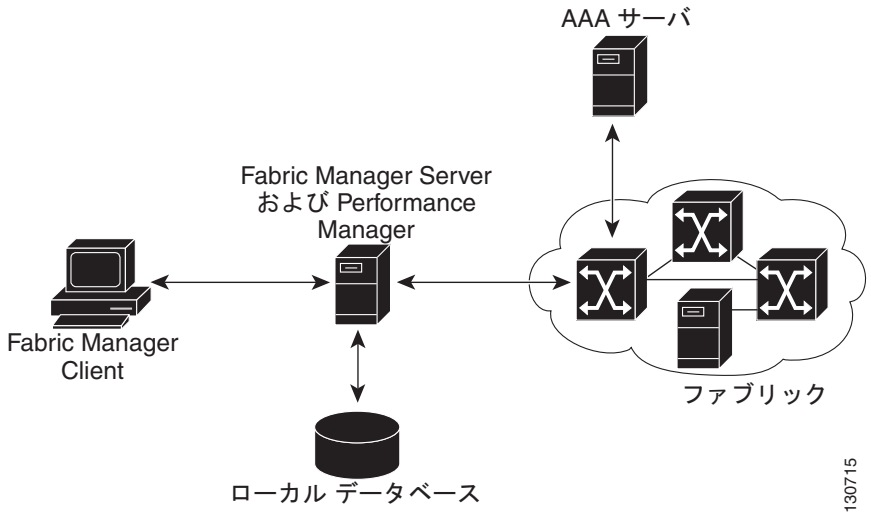
Fabric Manager には、ファブリックを管理するために相互作用する複数のコンポーネントが含まれています。

次のコンポーネントが含まれます。

- Fabric Manager Client
- Fabric Manager Server
- Performance Manager
- Cisco MDS 9000 スイッチおよびストレージ デバイスが内部接続されたファブリック
- AAA サーバ（オプション）

図 4-1 に、これらのコンポーネントの構成例を示します。

図 4-1　Fabric Manager の認証例



管理者は Fabric Manager Client を起動して、ファブリックの検出に使用されるシード スイッチを選択します。使用するユーザ名およびパスワードが Fabric Manager Server に渡され、シード スイッチの認証に使用されます。このユーザ名およびパスワードが、認識された SNMP（簡易ネットワーク管理プロトコル）ユーザ名およびパスワードと異なる場合、Fabric Manager Client か Fabric Manager Server が、スイッチに対する CLI（コマンドライン インターフェイス）セッションを開き（Secure Shell [SSH; セキュア シェル] または Telnet）、ユーザ名およびパスワードのペアを再試行します。ローカル スイッチ認証データベースまたはリモート Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバで、スイッチがユーザ名とパスワードを認識した場合、スイッチは Fabric Manager Client および Server で使用される一時的な SNMP ユーザ名を作成します。

（注）　リモート AAA サーバ認証を使用して Fabric Manager または Device Manager を認証する場合は、認証が遅くなることがあります。

（注）　CLI セッションが、Fabric Manager Client と Fabric Manager Server 間のファイアウォールを通過できるようにする必要があります。「ファイアウォールの背後での Fabric Manager の稼動」（P.2-42）を参照してください。

（注）　SNMPv3 ユーザ名認証のパスワードとプライバシ パスワード、および CLI ユーザ名とパスワードの照合には、同じパスワードを使用することを推奨します。

ファブリックの検出のベスト プラクティス

Fabric Manager Server は同じユーザ インターフェイスで複数の物理ファブリックを監視します。この機能により、冗長ファブリックの管理が容易になります。ライセンスが付与された Fabric Manager Server では、すべての設定済みファブリックに関する最新の検出情報が維持されるため、Fabric Manager Client を起動すると、デバイス ステータスおよび相互接続をすぐに使用できます。

注意　Fabric Manager Server の CPU 利用率が 50 パーセントを超える場合は、より高クラスの CPU システムに交換することを推奨します。詳細および推奨ハードウェアについては、「インストールを開始する前に」（P.2-19）を参照してください。

ネットワークの検出および Performance Manager の設定は、上記のベスト プラクティスに従うことをお勧めします。これにより、Fabric Manager Server はファブリックを詳細に表示できます。以降の Fabric Manager Client セッションでは、クライアントのログイン権限に基づいてこの詳細ビューをフィルタリングできます。たとえば、ファブリック内に複数の VSAN（仮想 SAN）があり、これらの VSAN のサブセットに制限されているユーザが作成されています。Fabric Manager Server でファブリック内のすべての VSAN を表示するために、ネットワーク管理者ロール、またはネットワーク オペレータ ロールを使用して Fabric Manager Server でファブリック検出を開始するとします。VSAN 制限のあるユーザが Fabric Manager Client を起動すると、管理が許可されている VSAN だけが表示されます。

（注）　Fabric Manager Server は、常にローカル スイッチ アカウントを使用してファブリックを監視します。AAA（RADIUS または TACACS+）サーバは使用しません。ファブリック サービスのプロビジョニングを目的としたクライアントへのログインには AAA ユーザ アカウントを使用できます。Fabric Manager Server ファブリックのモニタリングに関する詳細は、「Fabric Manager Server ファブリックの管理」（P.3-7）を参照してください。

ファブリック検出の設定

Fabric Manager Server がファブリック全体を検出するように設定するには、次の手順に従います。

ステップ 1　ネットワーク管理者ロールまたはネットワーク オペレータ ロールを使用して、ファブリックのスイッチごとに専用の Fabric Manager 管理ユーザ名を作成します。または AAA サーバ内に専用の Fabric Manager 管理ユーザ名を作成し、この AAA サーバを使用して認証するように、ファブリック内のすべてのスイッチを設定します。

ステップ 2　この Fabric Manager 管理ユーザ名に使用されるロールがファブリック内のすべてのスイッチで同じであること、このロールにすべての VSAN へのアクセス権が含まれていることを確認します。

ステップ 3　Fabric Manager 管理ユーザを使用して、Fabric Manager Client を起動します。これにより、すべての VSAN がファブリック検出の対象になります。

ステップ 4　ファブリックを継続的に監視するように、Fabric Manager Server を設定します。

「Fabric Manager Server ファブリックの管理」（P.3-7）を参照してください。

ステップ 5　Fabric Manager Server を介して管理するファブリックごとに、ステップ 4 を繰り返します。

Performance Manager の認証

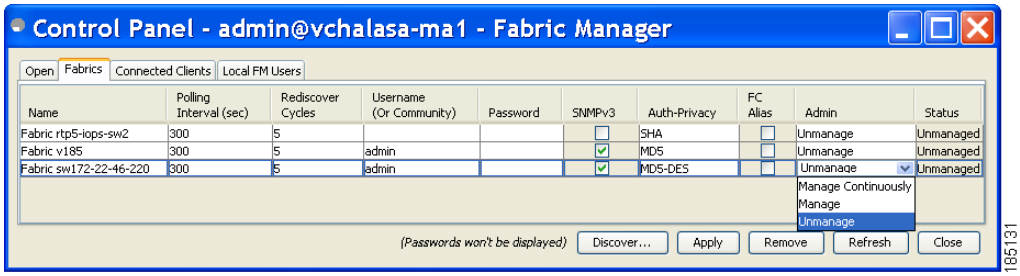
Performance Manager は Fabric Manager Server データベースに格納されたユーザ名およびパスワード情報を使用します。Performance Manager の動作中にファブリック内のスイッチでこの情報が変更された場合は、Fabric Manager Server データベースを更新して、Performance Manager を再起動する必要があります。Fabric Manager Server データベースを更新するには、Fabric Manager Server からファブリックを削除して、ファブリックを再検出する必要があります。

Performance Manager で使用されるユーザ名およびパスワード情報を更新するには、次の手順に従います。

ステップ 1　Fabric Manager で [Server] > [Admin] をクリックします。

[Control Panel] ダイアログボックスが表示され、[Fabrics] タブが開きます（図 4-2 を参照）。

図 4-2　[Control Panel] ダイアログボックスの [Fabrics] タブ



ステップ 2　ユーザ名およびパスワード情報を更新したファブリックをクリックします。

ステップ 3　[Admin] リストボックスから [Unmanage] を選択し、[Apply] をクリックします。

ステップ 4　正しいユーザ名とパスワードを入力して、[Apply] をクリックします。

ステップ 5　[Admin] リストボックスから [Manage] を選択し、[Apply] をクリックします。

ステップ 6　ファブリックを再検出するには、[Open] タブをクリックし、[Select] カラムから開くファブリックの横にあるチェックボックスをオンにします。

ステップ 7　[Open] をクリックして、ファブリックを再検出します。Fabric Manager Server がユーザ名およびパスワードの情報を更新します。

ステップ 8　再検出する必要があるファブリックそれぞれに対して、ステップ 3 ～ステップ 7 を繰り返します。

ステップ 9　[Performance] > [Collector] > [Restart] を選択して、Performance Manager を再起動し、新しいユーザ名およびパスワードを使用します。

Fabric Manager Web Server の認証

Fabric Manager Web Server は、ファブリック内のスイッチと直接通信しません。Fabric Manager Web Server は、ローカルに格納される、あるいは AAA サーバにリモートに格納される、独自のユーザ名およびパスワードの組み合わせを使用します。

Fabric Manager Web Server でのユーザ認証には、RADIUS または TACACS+ サーバを使用することを推奨します。

RADIUS 認証を使用するように Fabric Manager Web Server を設定するには、次の手順に従います。

ステップ 1　Fabric Manager Web Server を起動します。

「Fabric Manager Web Client の起動」（P.7-7）を参照してください。

ステップ 2　[Admin] タブ > [Configure] をクリックして、Fabric Manager Web Server で使用される認証を更新します。

ステップ 3　[AAA] をクリックします。

ステップ 4　認証モード属性を [radius] に設定します。

ステップ 5　最大 3 つの RADIUS サーバの RADIUS サーバ名、共有秘密、認証方法、使用ポートを設定します。

ステップ 6　[Modify] をクリックして、この情報を保存します。

TACACS+ 認証を使用するように Fabric Manager Web Server を設定するには、次の手順に従います。

ステップ 1　Fabric Manager Web Server を起動します。

「Fabric Manager Web Client の起動」（P.7-7）を参照してください。

ステップ 2　[Admin] > [Configure] をクリックして、Fabric Manager Web Server で使用される認証を更新します。

ステップ 3　[AAA] をクリックします。

ステップ 4　authenticationmode 属性を tacacs に設定します。

ステップ 5　最大 3 つの TACACS+ サーバの TACACS+ サーバ名、共有秘密、認証方法、使用ポートを設定します。

ステップ 6　[Modify] をクリックして、この情報を保存します。

（注）　Fabric Manager は SNMP と互換性がないため、SecureID はサポートされません。Fabric Manager では、ファブリックのスイッチすべてで使用されているログイン認証情報が使用されます。SecureID は認証に 1 回以上使用できないため、Fabric Manager SecureID を使用して 2 つ目のスイッチとの接続を確立できません。