CHAPTER 4

Cisco DCNM-SAN での認証の設定

この章では、スイッチとの通信を行う Cisco DCNM-SAN の相互依存ソフトウェア コンポーネント、認証手順、および、ファブリックとコンポーネントで認証を設定するためのベスト 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。

Cisco DCNM-SAN 認証の概要

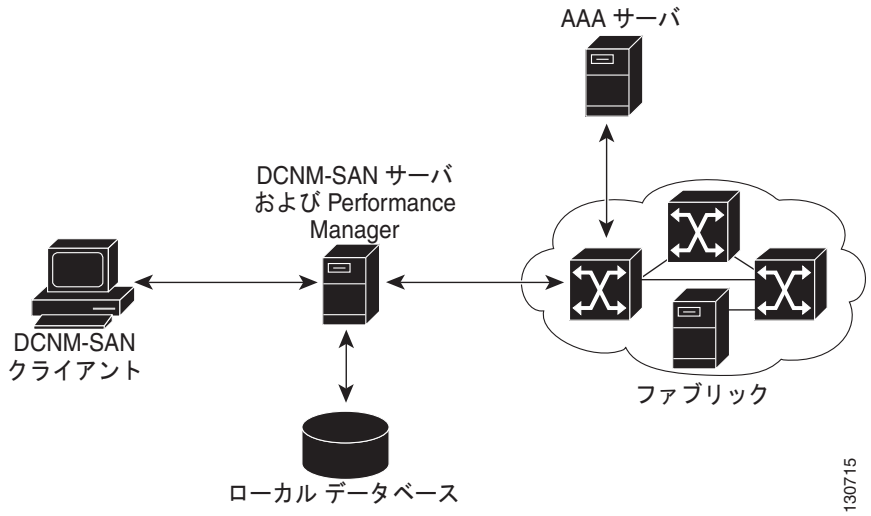
Cisco DCNM-SAN には複数のコンポーネントが含まれており、これらが相互に対話してファブリックを管理します。

次のコンポーネントが含まれます。

- Cisco DCNM-SAN クライアント
- Cisco DCNM-SAN サーバ
- 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（任意）

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　Cisco DCNM-SAN の認証例



管理者は Cisco DCNM-SAN クライアントを起動して、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 Cisco DCNM-SAN サーバに渡され、シード スイッチの認証に使用されます。このユーザ名とパスワードが、認識されている SNMP ユーザ名およびパスワードと異なる場合、Cisco DCNM-SAN クライアントまたは Cisco DCNM-SAN サーバがスイッチに対する CLI セッションを開き（SSH または Telnet）、ユーザ名とパスワードのペアを再試行します。スイッチは、ローカル スイッチ認証データベースまたはリモート AAA サーバでユーザ名とパスワードを認識すると、Cisco DCNM-SAN クライアントおよびサーバ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 サーバを使用して Cisco DCNM-SAN 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） Cisco DCNM-SAN クライアントと Cisco DCNM-SAN サーバ間にあるファイアウォールを CLI セッションが通過できるよう許可する必要があります。

（注） SNMPv3 ユーザ名認証のパスワードとプライバシー 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。

ファブリック検出のベスト プラクティス

Cisco DCNM-SAN サーバは、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 Cisco DCNM-SAN サーバでは、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ので、Cisco DCNM-SAN クライアントを起動すると、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　Cisco DCNM-SAN サーバの CPU 使用率が 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。

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、Cisco DCNM-SAN サーバでファブリックを詳細に表示できるようになります。以降の Cisco DCNM-SAN クライアント セッションでは、ログインしているクライアントの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 があり、これらの VSAN のサブセットに制限されたユーザを作成するとします。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 Cisco DCNM-SAN サーバでファブリックの検出を開始すると、ファブリック内のすべての VSAN を表示できます。VSAN 制限のあるユーザが Cisco DCNM-SAN クライアントを起動すると、管理が許可されている VSAN だけが表示されます。

（注）　Cisco DCNM-SAN サーバは、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。

ファブリック検出の設定

Cisco DCNM-SAN サーバがファブリック全体を検出できるようにするには、次の手順を実行します。

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、ファブリック内のスイッチごとに専用の Cisco DCNM-SAN 管理ユーザ名を作成します。または AAA サーバ内に専用の Cisco DCNM-SAN 管理ユーザ名を作成し、この AAA サーバを認証に使用するように、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 Cisco DCNM-SAN 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、および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　Cisco DCNM-SAN 管理ユーザを使用して Cisco DCNM-SAN クライアントを起動します。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、Cisco DCNM-SAN サーバを設定します。

ステップ 5　Cisco DCNM-SAN サーバで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、Cisco DCNM-SAN サーバ 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、Cisco DCNM-SAN サーバ 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。Cisco DCNM-SAN サーバ データベースを更新するには、Cisco DCNM-SAN サーバからファブリックを削除し、その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、次の手順を実行します。

ステップ 1　Cisco DCNM-SAN で [Server] > [Admin] の順にクリックします。

[Control Panel] ダイアログボックスが表示され、[Fabrics] タブが開きます。

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、[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。Cisco DCNM-SAN サーバでユーザ名とパスワードが更新されます。

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] の順に選択して 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。

Cisco DCNM-SAN Web クライアントの認証

Cisco DCNM-SAN Web サーバは、ファブリック内のスイッチと直接通信しません。Cisco DCNM-SAN Web サーバは、ローカルに格納される、あるいは AAA サーバでリモートに格納される、独自のユーザ名とパスワードの組み合わせを使用します。

Cisco DCNM-SAN Web サーバ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 Cisco DCNM-SAN Web 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　Cisco DCNM-SAN Web クライアントを起動します。

ステップ 2　[Admin] > [Management Users] > [Remote AAA] の順に選択して、Cisco DCNM-SAN Web クライアントで使用される認証を更新します。

ステップ 3　認証モード属性を [radius] に設定します。

ステップ 4　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 5　[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 Cisco DCNM-SAN Web 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　Cisco DCNM-SAN Web クライアントを起動します。

ステップ 2　[Admin] > [Management Users] > [Remote AAA] の順に選択して、Cisco DCNM-SAN Web クライアントで使用される認証を更新します。

ステップ 3　認証モード属性を [tacacs] に設定します。

ステップ 4　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 5　[Modify] をクリックして、この情報を保存します。

（注）　Cisco DCNM-SAN は SNMP 認証と互換性がないため、SecureID をサポートしません。Cisco DCNM-SAN では、ファブリック内のすべてのスイッチに対応する同一のログイン クレデンシャルが使用されます。認証に SecureID を 2 回以上使用することはできないので、Cisco DCNM-SAN が SecureID を使用して 2 つ目のスイッチとの接続を確立することはできません。