CHAPTER 4

RADIUS および TACACS+ の設定

Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）機能は、スイッチを管理するユーザの ID 確認、アクセス権付与、およびアクション追跡を実行します。Cisco MDS 9000 ファミリのすべてのスイッチで、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルを使用することで、リモート AAA サーバを使用するソリューションが実現されます。

指定されたユーザ ID およびパスワードの組み合わせに基づいて、スイッチはローカル データベースを使用したローカル認証または許可、あるいは AAA サーバを使用したリモート認証または許可を実行します。スイッチと AAA サーバ間の通信は、事前共有秘密キーによって保護されます。この秘密キーはすべての AAA サーバ、または特定の AAA サーバに設定できます。このセキュリティ機能により、AAA サーバを中央で管理できます。

この章の内容は、次のとおりです。

スイッチ管理のセキュリティ

Cisco MDS 9000 ファミリのスイッチ製品における管理セキュリティでは、Command Line Interface（CLI; コマンドライン インターフェイス）や Simple Network Management Protocol（SNMP）などのすべての管理アクセス手段にセキュリティを提供します。

ここで説明する内容は、次のとおりです。

Fabric Manager のセキュリティ オプション

Fabric Manager にアクセスするには、Transmission Control Protocol（TCP; 伝送制御プロトコル）/User Datagram Protocol（UDP; ユーザ データグラム プロトコル）SNMP または Hypertext Transfer Protocol（HTTP）トラフィックを使用します。管理パス（コンソール、Telnet、および Secure Shell（SSH; セキュア シェル））ごとに、ローカル、リモート（RADIUS または TACACS+）、または none のいずれか、あるいは複数のセキュリティ制御オプションを設定できます。

- リモート セキュリティ制御
  - RADIUS を利用

    「RADIUS サーバ モニタリング パラメータの設定」（P.4-8）を参照してください。
  - TACACS+ を利用

    「TACACS+ サーバ モニタリング パラメータの設定」（P.4-14）を参照してください。
- ローカル セキュリティ制御

  「ローカル AAA サービス」（P.4-27）を参照してください。

これらのセキュリティ機能は、次の場合にも設定できます。

- Small Computer Systems Interface over IP（iSCSI）認証

  『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください。
- Fibre Channel Security Protocol（FC-SP）認証

  第 8 章「FC-SP および DHCHAP の設定」を参照してください。

SNMP セキュリティ オプション

SNMP エージェントは、SNMPv1、SNMPv2c、および SNMPv3 のセキュリティ機能をサポートしています。SNMP を使用するすべてのアプリケーション（Cisco MDS 9000 Fabric Manager など）に、標準 SNMP セキュリティ機能が適用されます。

SNMP セキュリティ オプションは Fabric Manager と Device Manager にも適用できます。

SNMP セキュリティ オプションの詳細については、『*Cisco MDS 9000 NX-OS Family System Management Configuration Guide* 』を参照してください。

スイッチの AAA

CLI または Fabric Manager を使用して、すべての Cisco MDS 9000 ファミリ スイッチに AAA スイッチ機能を設定できます。

ここで説明する内容は、次のとおりです。

認証

認証は、スイッチを管理する人物またはそのスイッチにアクセスするデバイスの ID を確認するプロセスです。この ID 確認は、スイッチにアクセスしようとするエンティティが提出するユーザ ID およびパスワードの組み合わせに基づいて行われます。Cisco MDS 9000 ファミリ スイッチでは、ローカル認証（ローカル ルックアップ データベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。

（注）　Telnet または SSH により Fabric Manager または Device Manager を利用して Cisco MDS スイッチに正常にログインした場合、スイッチに AAA サーバベースの認証が設定されていると、1 日の有効期限で一時的な SNMP ユーザ エントリが自動的に作成されます。スイッチは、使用している Telnet または SSH ログイン名を SNMPv3 ユーザ名として、SNMPv3 Protocol Data Unit（PDU; プロトコル データ ユニット）を認証します。管理ステーションは、Telnet または SSH ログイン名を SNMPv3 の **auth** および **priv** パスフレーズとして、一時的に使用できます。この一時的な SNMP ログインが許可されるのは、1 つ以上のアクティブな MDS シェル セッションが存在する場合だけです。指定時刻にアクティブなセッションが存在しない場合は、ログインが削除され、SNMPv3 の運用を実行できません。

（注）　Fabric Manager は末尾が空白スペースの AAA パスワードをサポートしません（例「passwordA」）。

許可

すべての Cisco MDS スイッチ製品に次の許可ロールが存在します。

- ネットワーク オペレータ（network-operator）：設定を表示する権限だけがあります。オペレータは設定内容の変更はできません。
- ネットワーク管理者（network-admin）：すべてのコマンドを実行し、設定内容を変更する権限があります。管理者は最大 64 の追加ロールを作成し、カスタマイズできます。
- デフォルトロール：GUI（Fabric Manager および Device Manager）を使用する権限があります。このアクセス権は、GUI にアクセスすることを目的として、すべてのユーザに自動的に与えられます。

これらのロールは変更または削除ができません。追加のロールを作成することで、次のオプションを設定できます。

- ユーザ ロールをローカルに割り当てるか、またはリモート AAA サーバを使用して、ロール ベースの許可を設定します。
- ロール情報を格納するように、リモート AAA サーバのユーザ プロファイルを設定します。このロール情報は、リモート AAA サーバを通じてユーザを認証したときに、自動的にダウンロードされ、使用されます。

（注）　ユーザが新しく作成されたロールのうち 1 つだけに属している場合、このロールが削除されると、ユーザにはデフォルトで network-operator ロールがただちに設定されます。

アカウンティング

アカウンティング機能はスイッチへのアクセスに使用されるすべての管理設定のログを追跡し、管理します。この情報を利用して、トラブルシューティングや監査に使用するレポートを生成できます。アカウンティング ログはローカルで保存したり、リモート AAA サーバに送信したりできます。

リモート AAA サービス

RADIUS および TACACS+ により提供されるリモート AAA サービスは、ローカルの AAA サービスに比べて次の利点があります。

- ファブリック内の各スイッチに対するユーザ パスワード リストをより簡単に管理できます。
- AAA サーバは通常、企業全体に配備済みであり、簡単に採用できます。
- ファブリック内のすべてのスイッチのアカウンティング ログを集中管理できます。
- ファブリック内の各スイッチに対するユーザ ロール設定をより簡単に管理できます。

リモート認証に関する注意事項

リモート AAA サーバを使用する場合は、次の注意事項に従ってください。

- 最低 1 つの AAA サーバが IP で到達可能でなければなりません。
- すべての AAA サーバが到達不能である場合のポリシーとして、適切なローカル AAA ポリシーを必ず設定します。
- オーバーレイ イーサネット LAN がスイッチに接続している場合、AAA サーバは容易に到達可能になります（『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください）。この方法を推奨します。
- スイッチに接続された SAN ネットワーク内のゲートウェイ スイッチを 1 つまたは複数、AAA サーバに到達するイーサネット LAN に接続する必要があります。

サーバ グループ

認証、許可、アカウンティングを行うためのリモート AAA サーバを、サーバ グループを使用して指定できます。サーバ グループは、同じ AAA プロトコルを実装するリモート AAA サーバ セットです。サーバ グループの目的は、1 台のリモート AAA サーバが応答に失敗した場合に、フェールオーバー サーバを提供することにあります。グループ内の最初のリモート サーバが応答に失敗すると、グループ内の次のリモート サーバが応答を試行します。いずれかのサーバが応答を送信するまで、この処理は続きます。サーバ グループ内のすべての AAA サーバが応答に失敗した場合、このサーバ グループ オプションは失敗と見なされます。必要に応じて、複数のサーバ グループを指定できます。Cisco MDS スイッチが最初のグループ内のサーバからエラーを受信すると、次のサーバ グループのサーバが試行されます。

AAA 設定オプション

Cisco MDS 9000 ファミリ スイッチ製品内の AAA 設定は、サービス ベースです。次のサービスごとに、異なる AAA 設定を作成できます。

- Telnet または SSH ログイン（Fabric Manager および Device Manager ログイン）

- コンソール ログイン
- iSCSI 認証（『*Cisco Fabric Manager IP Services Configuration Guide*』を参照）
- FC-SP 認証（第 8 章「FC-SP および DHCHAP の設定」を参照）
- アカウンティング

一般に、AAA 設定の任意のサービスに対して指定できるオプションは、サーバ グループ、ローカル、および none の 3 つです。各オプションは指定した順序で試行されます。すべてのオプションが失敗した場合、ローカルが試行されます。

注意　Cisco MDS NX-OS では、ユーザ名がアルファベットで始まる限り、リモートで作成するか（TACACS+ または RADIUS を使用）ローカルで作成するかに関係なく、英数字または特定の特殊文字（+ [プラス]、= [等号]、_ [下線]、- [ハイフン]、\ [バックスラッシュ]、および . [ピリオド]）を使って作成したユーザ名がサポートされます。ローカル ユーザ名をすべて数字で作成したり、特殊文字（上記の特殊文字を除く）を使用して作成したりすることはできません。数字だけのユーザ名やサポートされていない特殊文字によるユーザ名が AAA サーバに存在し、ログイン時に入力されると、そのユーザはアクセスを拒否されます。

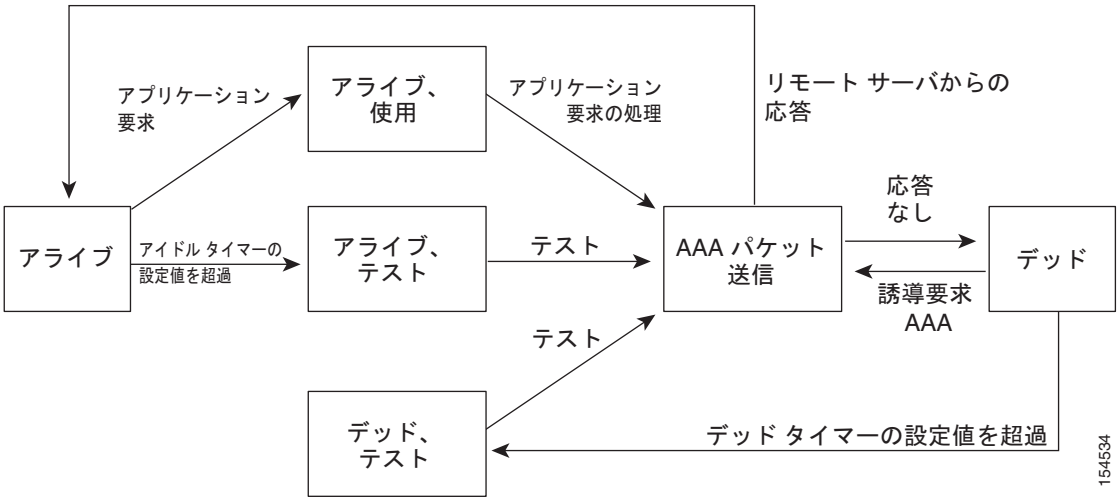
（注）　オプションの 1 つとしてローカルが指定されていない場合でも、その他のすべての設定オプションに失敗したときは、ローカル方式が試行されます。

RADIUS がタイムアウトする際は、常にローカル ログインが試行されます。このローカル ログインを成功させるには、同一のパスワードを持つそのユーザのローカル アカウントが存在し、かつ RADIUS のタイムアウトと再試行は 40 秒未満でなければなりません。そのユーザが認証されるのは、ローカルの認証設定にそのユーザ名とパスワードが存在する場合です。

AAA サーバのモニタリング

応答の途絶えた AAA サーバは AAA 要求の処理に遅延をもたらします。AAA 要求の処理時間を節約するため、MDS スイッチは定期的に AAA サーバをモニタして AAA サーバが応答する（または機能している）かどうかを確認することができます。MDS スイッチは、応答のない AAA サーバを機能停止と記録します。また、機能停止のいずれの AAA サーバにも AAA 要求を送りません。MDS スイッチは定期的に機能停止の AAA サーバをモニタし、応答するようになったら機能中と認識します。このモニタリング プロセスでは、実際の AAA 要求を送出する前にその AAA サーバが稼動中であることを確認します。AAA サーバが機能停止または機能中に変化すると常に SNMP トラップが生成され、MDS スイッチはパフォーマンスに影響が出る前に、管理者に対して障害が発生していることを警告します。AAA サーバの状態遷移は図 4-1 を参照してください。

図 4-1　AAA サーバの状態遷移



（注）　稼動中のサーバと停止中のサーバのモニタリング間隔は別々で、ユーザが設定できます。AAA サーバのモニタリングはテスト用認証要求を AAA サーバに送信することで行われます。

テスト パケットで使用されるユーザ名とパスワードは設定が可能です。

「RADIUS サーバ モニタリング パラメータの設定」（P.4-8）を参照してください。

認証と許可のプロセス

認証は、スイッチを管理する人物の ID を確認するプロセスです。この ID 確認は、スイッチを管理しようとする人物が入力したユーザ ID およびパスワードの組み合わせに基づいて行われます。Cisco MDS 9000 ファミリ スイッチでは、ローカル認証（ルックアップ データベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。

認証と許可の手順は、次のとおりです。

ステップ 1　Cisco MDS 9000 ファミリ内の必要なスイッチへのログインには、Telnet、SSH、Fabric Manager/Device Manager、またはコンソールのログイン オプションを使用します。

ステップ 2　サーバ グループ認証手順を使用するサーバ グループを設定した場合は、グループ内の最初の AAA サーバに認証要求が送信されます。

- その AAA サーバが応答に失敗すると次の AAA サーバに送信され、リモート サーバが認証要求に応答するまで繰り返されます。
- サーバ グループ内のすべての AAA サーバが応答に失敗した場合は、次のサーバ グループのサーバに送信が行われます。
- 設定されているすべての手順が失敗に終わった場合は、ローカル データベースを利用して認証が行われます。

ステップ 3　リモートの AAA サーバにより認証に成功すると、場合に応じて次のアクションが実行されます。

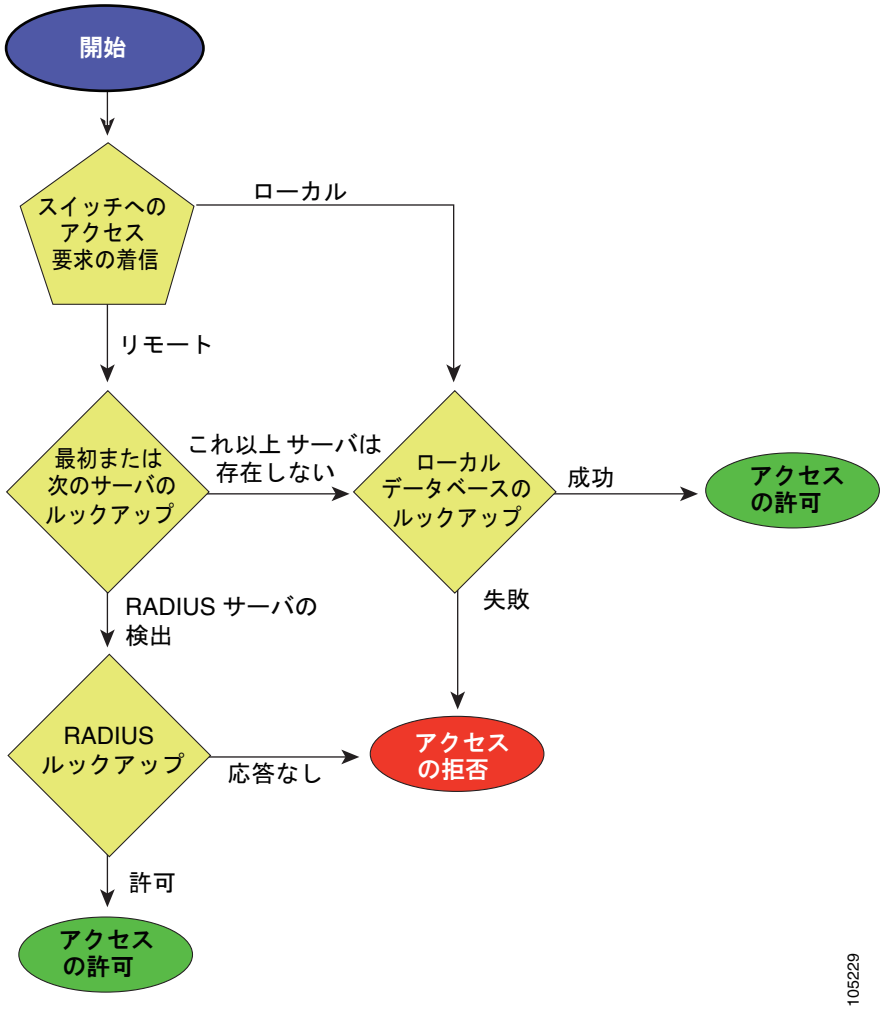
- AAA サーバのプロトコルが RADIUS の場合は、認証応答に伴って **cisco-av-pair** 属性で指定されたユーザ ロールがダウンロードされます。

- AAA サーバのプロトコルが TACACS+ の場合は、同じサーバに別の要求を送信して、シェルのカスタム属性として指定されているユーザ ロールを入手します。
- リモート AAA サーバからのユーザ ロールの入手に失敗した場合、**show aaa user default-role** コマンドがイネーブルであれば、ユーザには network-operator ロールが割り当てられます。このコマンドがディセーブルの場合には、アクセスが拒否されます。

ステップ 4　ユーザ名とパスワードがローカルで認証に成功した場合は、ログインが許され、ローカル データベースに設定されているロールが割り当てられます。

図 4-2 に許可と認証プロセスのフローチャートを示します。

図 4-2　スイッチの許可と認証のフロー



（注）　残りのサーバ グループがない = どのサーバ グループからも応答がない。
残りのサーバがない = このサーバ グループのどのサーバからも応答がない。

RADIUS サーバ モニタリング パラメータの設定

Cisco MDS 9000 ファミリ スイッチは、RADIUS プロトコルを使用してリモート AAA サーバと通信できます。複数の RADIUS サーバおよびサーバ グループを設定し、タイムアウトおよび再試行回数を設定できます。

RADIUS は、不正アクセスからネットワークを保護する分散型クライアント/サーバ プロトコルです。シスコの実装では、RADIUS クライアントは Cisco MDS 9000 ファミリ スイッチで稼動し、認証要求を、すべての認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに送信します。

ここでは、RADIUS の動作を定義し、ネットワーク環境を識別し、設定できる内容について説明します。

ここで説明する内容は、次のとおりです。

RADIUS サーバのデフォルト設定の概要

Fabric Manager を利用すると、スイッチとの通信を設定するどの RADIUS サーバにも利用できるデフォルト設定をセットアップできます。デフォルト設定には次の内容が含まれます。

- 暗号の種類
- タイムアウトの値
- 送信試行回数
- ログインの際に RADIUS サーバの指定を可能にする

RADIUS サーバにおける暗号の種類と事前共有キーのデフォルト値の概要

スイッチを RADIUS サーバに対して認証するには、RADIUS 事前共有キーを設定する必要があります。キーの長さは 64 文字に制限され、出力可能な任意の ASCII 文字を使用できます（スペースは使用できません）。スイッチのすべての RADIUS サーバ設定で使用されるグローバル キーを設定できます。

グローバル キーの割り当てを上書きするには、個々の RADIUS サーバの設定時に **key** オプションを使用する必要があります。

RADIUS サーバ における暗号の種類と事前共有キーのデフォルト値の設定

Fabric Manager を使用して RADIUS サーバの暗号の種類と事前共有キーのデフォルト値を設定する手順は、次のとおりです。

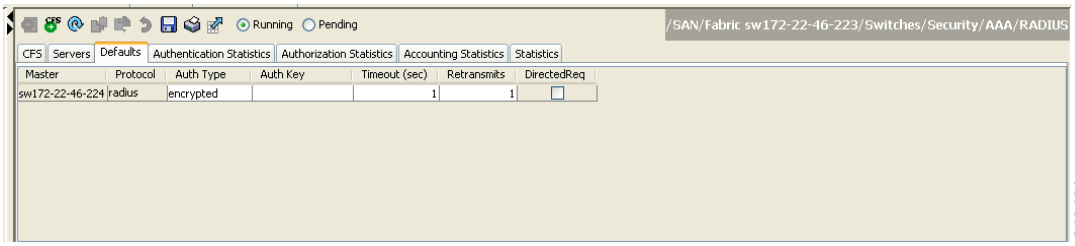
ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします。

RADIUS のデフォルト設定が表示されます（図 4-3 を参照）。

図 4-3　RADIUS のデフォルト設定



ステップ 3　[AuthType] ドロップダウン メニューで [plain] または [encrypted] を選択します。

ステップ 4　[Auth Key] フィールドにキーを設定します。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

RADIUS サーバのタイムアウト間隔および再送信のデフォルト値の設定

デフォルトでは、スイッチはローカル認証に戻る前に、RADIUS サーバへの送信の再試行を 1 回だけ行います。再試行の回数はサーバごとに最大 5 回まで増やせます。RADIUS サーバに対してタイムアウトの値を設定することもできます。

Fabric Manager を使用して再試行回数と RADIUS サーバへの再送信の間隔を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Defaults] タブを選択します。

RADIUS のデフォルト設定が表示されます。

ステップ 3　認証再試行の [Timeout] および [Retransmits] の各フィールドを入力します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

RADIUS サーバの概要

最大 64 台の RADIUS サーバを追加できます。RADIUS キーは永続的なストレージに暗号化形式で常に格納されています。実行コンフィギュレーションにも、暗号化されたキーが表示されます。新しい RADIUS サーバを設定する際は、デフォルト設定を利用することも、パラメータのいずれかを修正してデフォルトの RADIUS サーバ設定を上書きすることもできます。

RADIUS サーバの設定

Fabric Manager を使用して RADIUS サーバとオプションのすべてを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

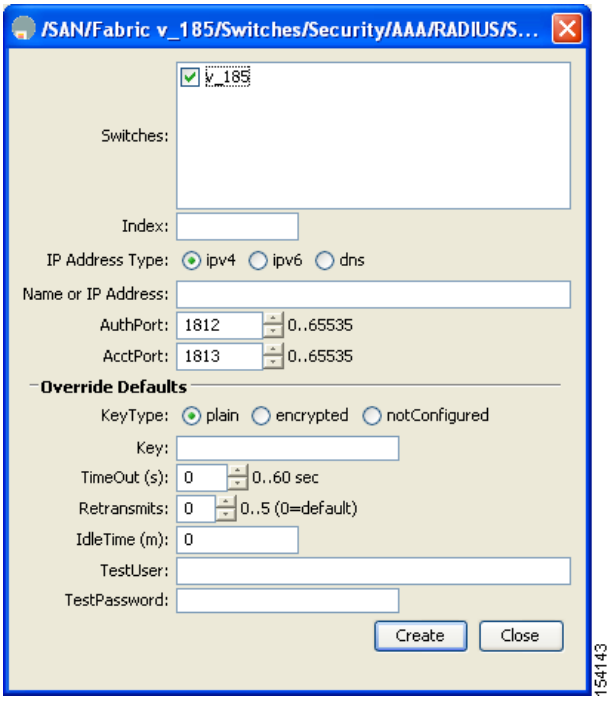
ステップ 2　[Servers] タブをクリックします。

既存の RADIUS サーバが表示されます。

ステップ 3　新しい RADIUS サーバを追加するには、[Create Row] アイコンをクリックします。

[Create RADIUS Server] ダイアログボックスが表示されます（図 4-4 を参照）。

図 4-4　[Create RADIUS Server]



ステップ 4　RADIUS サーバとして割り当てるスイッチを選択します。

ステップ 5　RADIUS サーバを識別するためのインデックス番号を割り当てます。

ステップ 6　RADIUS サーバに与える IP アドレスの種類を選択します。

ステップ 7　RADIUS サーバの IP アドレスまたは名前を入力します。

ステップ 8　（任意）RADIUS サーバが使用する認証用ポートおよびアカウンティング用ポートを修正します。

ステップ 9　RADIUS サーバに与える適切なキーの種類を選択します。

ステップ 10　タイムアウトの値を秒で選択します。有効な範囲は 0 ～ 60 秒です。

ステップ 11　ローカル認証に戻る前に、スイッチが RADIUS サーバへの接続を試行する回数を選択します。

ステップ 12　テスト用のアイドル間隔の値を分で入力します。有効な範囲は 1 ～ 1440 分です。

ステップ 13　テスト ユーザをデフォルト パスワードとともに入力します。デフォルトのユーザ名は test です。

ステップ 14　[Create] ボタンをクリックして変更内容を保存します。

テスト アイドル タイマーの設定

テスト アイドル タイマーには、MDS スイッチがテスト パケットを送るまで RADIUS サーバが要求を待つ時間間隔を指定します。

（注）　アイドル タイマーのデフォルト値は 0 分です。アイドル タイマーの時間間隔が 0 分の場合は、RADIUS サーバによる定期的なモニタリングが行われません。

テスト アイドル タイマーを設定するには、「RADIUS サーバの設定」（P.4-10）を参照してください。

テスト ユーザ名の設定

RADIUS サーバによる定期的なサーバ ステータスのテスト実施に使用するユーザ名とパスワードを設定できます。RADIUS サーバをモニタするためのテスト メッセージを発行するためにテスト ユーザ名とパスワードを設定する必要はありません。デフォルトのテスト ユーザ名（test）とデフォルトのパスワード（test）を利用できます。

（注）　セキュリティ上の理由から、テスト ユーザ名を RADIUS データベースに存在する既存のユーザ名と同一にしないことを推奨します。

RADIUS サーバによる定期的なサーバ ステータスのテスト実施に使用するオプションのユーザ名とパスワードの設定については、「RADIUS サーバの設定」（P.4-10）を参照してください。

RADIUS サーバの検証の概要

Cisco SAN-OS リリース 3.0(1) では、RADIUS サーバを定期的に検証できます。スイッチは、設定されたユーザ名とパスワードを使用してテスト用認証をサーバに送信します。このテスト認証にサーバが応答しない場合、サーバは応答能力がないものと見なされます。

（注）　セキュリティ上の理由から、RADIUS サーバでテスト ユーザ名として設定されたユーザ名を使用しないことを推奨します。

サーバを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

RADIUS サーバの定期的な検証

Fabric Manager を使用して RADIUS サーバを定期的にテストするようにスイッチを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Servers] タブをクリックします。

既存の RADIUS サーバが表示されます。

ステップ 3　新しい RADIUS サーバを追加するには、[Create Row] アイコンをクリックします。

[Create RADIUS Server] ダイアログボックスが表示されます（図 4-4 を参照）。

ステップ 4　IP アドレスを入力します。

ステップ 5　RADIUS サーバが使用する認証用ポートおよびアカウンティング用ポートを修正します。

ステップ 6　[TestUser] フィールドに入力し、必要に応じて [TestPassword] フィールドを入力します。テスト用のデフォルト パスワードは **Cisco** です。

ステップ 7　テスト認証を送信するまでサービスをアイドル状態に置く [IdleTime] フィールドを設定します。

ステップ 8　[Create] ボタンをクリックして変更内容を保存します。

RADIUS サーバ統計情報の表示

Fabric Manager を使用して RADIUS サーバ統計情報を表示する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Statistics] タブをクリックします。

RADIUS の統計情報が表示されます。

ログイン時に RADIUS サーバを指定するユーザの概要

デフォルトでは、MDS スイッチは認証要求を RADIUS サーバ グループの最初のサーバに転送します。スイッチに対して要求送信の誘導オプションをイネーブルにする設定を行うと、どの RADIUS サーバに認証要求を送信させるかをユーザが指定できるようになります。このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。*hostname* は設定した RADIUS サーバの名前です。

ユーザがログイン時に RADIUS サーバを指定可能にする

Fabric Manager を使用して、ユーザが認証用の RADIUS サーバを選択するために MDS スイッチにログインできるようにする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします。

RADIUS のデフォルト設定が表示されます。

ステップ 3　RADIUS サーバの [DirectedReq] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

VSA（ベンダー固有属性）について

Internet Engineering Task Force（IETF）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバ間での Vendor-Specific Attribute（VSA; ベンダー固有属性）の通信方法が規定されています。IETF では属性 26 が使用されます。ベンダーは VSA を使用することにより、一般的な用途に適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、仕様で推奨されたフォーマットを使用するベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は **cisco-avpair** です。値は、次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。**separator** は、必須の属性の場合は = （等号記号）、省略可能な属性の場合は * （アスタリスク）です。

Cisco MDS 9000 ファミリ スイッチに対するユーザ認証に RADIUS サーバを使用した場合、RADIUS プロトコルは、認証情報などのユーザ属性およびユーザ結果を戻すように RADIUS サーバに指示します。この許可情報は、VSA を使用して指定されます。

VSA のフォーマット

Cisco NX-OS ソフトウェアでは、次の VSA プロトコル オプションがサポートされています。

- [Shell] プロトコル：ユーザ プロファイル情報を提供するために Access-Accept パケットで使用されます。
- [Accounting] プロトコル：アカウンティング要求パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Cisco NX-OS ソフトウェアでは、次の属性がサポートされています。

- **roles**：この属性は、ユーザが属すすべてのロールをリストします。値フィールドは、グループ名のスペース区切りリストを含むストリングです。たとえば、ユーザが **vsan-admin** および **storage-admin** の各ロールに属している場合、値フィールドは「**vsan-adminstorage-admin**」になります。このサブ属性は Access-Accept フレームの VSA 部分に保管され、RADIUS サーバから送信されます。この属性と併用できるのは、シェル プロトコル値だけです。次に、ロール属性を使用する 2 つの例を示します。

  ```
  shell:roles="network-admin vsan-admin"
  ```

```
shell:roles*"network-admin vsan-admin"
```

VSA が **shell:roles*"network-admin vsan-admin"** として指定されている場合は、この VSA がオプション属性としてフラグ設定されます。その他のシスコ製デバイスはこの属性を無視します。

- **accountinginfo**：この属性は、標準の RADIUS アカウンティング プロトコルに含まれる属性を補足する追加的なアカウンティング情報を表します。この属性が送信されるのは、Account-Request フレームの VSA 部分に保管され、スイッチ上の RADIUS クライアントから送信される場合だけです。この属性を併用できるのは、アカウンティング プロトコル関連の Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

AAA サーバでの SNMPv3 の指定

ベンダー / カスタム属性 **cisco-av-pair** は、次のフォーマットを使用してユーザのロール マッピングを指定する場合に使用できます。

```
shell:roles="roleA roleB …"
```

cisco-av-pair 属性でロール オプションが設定されていない場合、デフォルトのユーザ ロールは network-operator になります。

VSA フォーマットはオプションとして、SNMPv3 認証と機密保持プロトコルの属性を次のようにも指定できます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコル オプションは SHA および MD5 です。プライバシー プロトコル オプションは AES-128 および DES です。これらのオプションが ACS サーバの **cisco-av-pair** 属性で指定されていない場合は、MD5 および DES がデフォルトで使用されます。

TACACS+ サーバ モニタリング パラメータの設定

Cisco MDS スイッチは TACACS+ プロトコルを使用して、リモート AAA サーバと通信します。複数の TACACS+ サーバを設定し、タイムアウト値を指定できます。

ここで説明する内容は、次のとおりです。

TACACS+ の概要

TACACS+ は、TCP（TCP ポート 49）を使用してトランスポート要件を満たすクライアント/サーバ プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチは、TACACS+ プロトコルを使用して中央から認証できます。TACACS+ には、RADIUS 認証と比較して次のような利点があります。

- 独立したモジュラ式 AAA ファシリティを提供します。認証を行わずに、許可を実行できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用し、コネクション型プロトコルによる確実な転送を行います。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、さらに優れたデータ保護を実現できます。RADIUS プロトコルはパスワードだけを暗号化します。

TACACS+ サーバのデフォルト設定の概要

Fabric Manager を利用すると、スイッチとの通信を設定するどの TACACS+ サーバにも利用できるデフォルト設定をセットアップできます。デフォルト設定には次の内容が含まれます。

- 暗号の種類
- 事前共有キー
- タイムアウトの値
- 送信試行回数
- ログインの際に TACACS+ サーバの指定を可能にする

TACACS+ サーバ における暗号の種類と事前共有キーのデフォルト値の概要

スイッチを TACACS+ サーバに対して認証するには、TACACS+ 事前共有キーを設定する必要があります。キーの長さは 64 文字に制限され、出力可能な任意の ASCII 文字を使用できます（スペースは使用できません）。スイッチのすべての TACACS+ サーバ設定で使用されるグローバル キーを設定できます。

グローバル キーの割り当てを上書きするには、個々の TACACS+ サーバの設定時に **key** オプションを使用する必要があります。

TACACS+ サーバにおける暗号の種類と事前共有キーのデフォルト値の設定

Fabric Manager を使用して TACACS+ サーバの暗号種類と事前共有キーのデフォルト値を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Defaults] タブが無効になっている場合は、[CFS] タブをクリックします。

ステップ 3　[Defaults] タブをクリックします。

TACACS+ のデフォルト設定が表示されます。

ステップ 4　[AuthType] ドロップダウン メニューで [plain] または [encrypted] を選択し、[Auth Key] フィールドにキーを設定します。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

TACACS+ サーバのタイムアウト間隔および再送信のデフォルト値の設定

デフォルトでは、スイッチは TACACS+ サーバを 1 回だけ試行します。この回数は設定可能です。最大試行回数は、各サーバで 5 回です。TACACS+ サーバに対してタイムアウトの値を設定することもできます。

Fabric Manager を使用して再試行回数と TACACS+ サーバへの再送信の間隔を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします （[Defaults] タブがディセーブルの場合は、[CFS] タブを最初にクリックします）。

TACACS+ のデフォルト設定が表示されます。

ステップ 3　認証再試行の [Timeout] および [Retransmits] の各フィールドに値を入力します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

TACACS+ サーバの概要

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで TACACS+ 機能がディセーブルに設定されています。Fabric Manager または Device Manager は TACACS+ サーバの設定を行うと、自動的に TACACS+ の機能をイネーブルにします。

設定されたサーバに秘密キーが設定されていない場合、グローバル キーが設定されていないと、警告メッセージが発行されます。サーバ キーが設定されていない場合は、グローバル キー（設定されている場合）が該当サーバで使用されます。

（注）　Cisco MDS SAN-OS Release 2.1(2) よりも前のバージョンでは、キーの中にドル記号（$）を使用できますが、「"」で囲む必要があります（例、"k$"）。パーセント記号（%）は使えません。Cisco MDS SAN-OS リリース 2.1(2) 以降では、引用符号なしにドル記号（$）を使用でき、パーセント記号（%）はグローバル秘密キーで使用できます。

すべての TACACS+ サーバで秘密キーに対するグローバル値を設定できます。

（注）　秘密キーが個々のサーバに設定されている場合は、グローバル設定されたキーよりもそれらのキーが優先されます。

ACACS+ サーバの設定

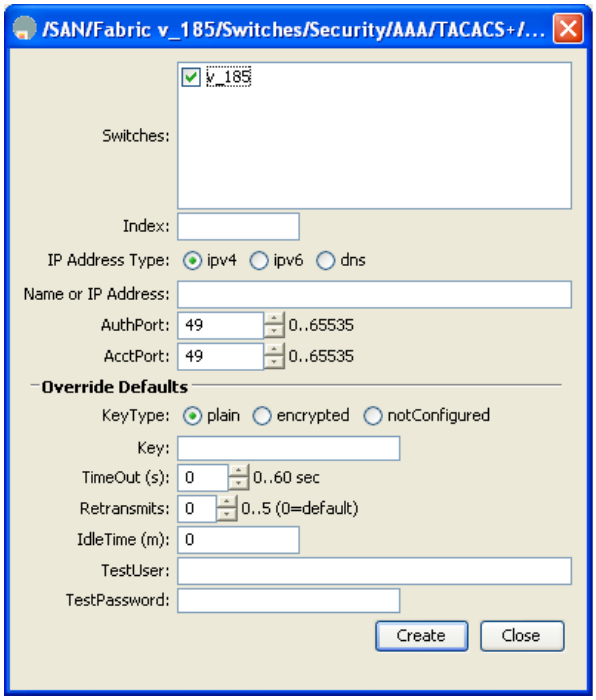
Fabric Manager を使用して TACACS+ サーバとオプションのすべてを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。
[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Servers] タブをクリックします。
既存の TACACS+ サーバが表示されます。

ステップ 3　新しい TACACS+ サーバを追加するには、[Create Row] アイコンをクリックします。
[Create TACACS+ Server] ダイアログボックスが表示されます（図 4-5 を参照）。

図 4-5　[Create TACACS+ Server] ダイアログボックス



ステップ 4　TACACS サーバとして割り当てるスイッチを選択します。

ステップ 5　TACACS サーバを識別するためのインデックス番号を割り当てます。

ステップ 6　TACACS サーバに与える IP アドレスの種類を選択します。

ステップ 7　TACACS サーバの IP アドレスまたは名前を入力します。

ステップ 8　TACACS サーバが使用する認証用ポートおよびアカウンティング用ポートを修正します。

ステップ 9　TACACS サーバに与える適切なキーの種類を選択します。

ステップ 10　タイムアウトの値を秒で選択します。有効な範囲は 0 ～ 60 秒です。

ステップ 11　ローカル認証に戻る前に、スイッチが TACACS サーバへの接続を試行する回数を選択します。

ステップ 12　テスト用のアイドル間隔の値を分で入力します。有効な範囲は 1 ～ 1440 分です。

ステップ 13　テスト ユーザをデフォルト パスワードとともに入力します。デフォルトのユーザ名は test です。

ステップ 14　[Create] ボタンをクリックして変更内容を保存します。

TACACS+ サーバ検証の概要

Cisco SAN-OS リリース 3.0(1) では、TACACS+ サーバを定期的に検証できます。スイッチは、設定されたテスト用ユーザ名とテスト用パスワードを使用してテスト用認証をサーバに送信します。このテスト認証にサーバが応答しない場合、サーバは応答能力がないものと見なされます。

（注）　セキュリティ上の理由から、TACACS+ サーバにはテスト用ユーザを設定しないことを推奨します。

サーバを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

TACACS+ サーバの定期的な検証

Fabric Manager を使用して TACACS+ サーバを定期的にテストするようにスイッチを設定する手順については、「TACACS+ サーバ モニタリング パラメータの設定」（P.4-14）を参照してください。

TACACS+ サーバ統計情報の表示

Fabric Manager を使用して TACACS+ サーバ統計情報を表示する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Statistics] タブを選択します。

TACACS+ サーバの統計情報が表示されます。

ログイン時に TACACS+ サーバを指定するユーザの概要

デフォルトでは、MDS スイッチは認証要求を TACACS+ サーバ グループの最初のサーバに転送します。スイッチを設定すると、どの TACACS+ サーバに認証要求を送信させるかをユーザが指定できるようになります。この機能を有効化すると、ユーザは *username@hostname* としてログインできます。*hostname* は設定した TACACS+ サーバの名前です。

ログイン時における TACACS+ サーバの指定許可

Fabric Manager を使用して、ユーザがログイン時に TACACS+ サーバを指定できるようにスイッチを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします。

TACACS+ のデフォルト設定が表示されます。

ステップ 3　[DirectedReq] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ロールのカスタム属性について

Cisco MDS 9000 ファミリ スイッチでは、ユーザが所属するロールの設定には、サービス シェルの TACACS+ カスタム属性を使用します。TACACS+ 属性は **name=value** の形式で指定します。このカスタム属性の属性名は **cisco-av-pair** です。この属性を使用してロールを指定する例を次に示します。

```
cisco-av-pair=shell:roles=”network-admin vsan-admin”
```

オプションのカスタム属性を設定して、同じ AAA サーバを使用する MDS 以外のシスコ製スイッチとの競合を回避することもできます。

```
cisco-av-pair*shell:roles="network-admin vsan-admin"
```

追加カスタム属性 shell:roles もサポートされています。

```
shell:roles="network-admin vsan-admin"
```

または

```
shell:roles*"network-admin vsan-admin”
```

（注）　Access Control Server（ACS）には、さまざまなサービス（シェルなど）用に TACACS+ カスタム属性を定義できます。Cisco MDS 9000 ファミリ スイッチでは、サービス シェルの TACACS+ カスタム属性を使用して、ロールを定義する必要があります。

サポート対象の TACACS+ サーバ

Cisco NX-OS ソフトウェアは現在、指定した TACACS+ サーバに対して次のパラメータをサポートしています。

- TACACS+

  ```
  cisco-av-pair=shell:roles="network-admin"
  ```

- Cisco ACS TACACS+

  ```
  shell:roles="network-admin"
  shell:roles*"network-admin"
  ```

```
cisco-av-pair*shell:roles="network-admin"
cisco-av-pair*shell:roles*"network-admin"
cisco-av-pair=shell:roles*"network-admin"
```

- Open TACACS+

```
cisco-av-pair*shell:roles="network-admin"
cisco-av-pair=shell:roles*"network-admin"
```

サーバ グループ

サーバ グループを使用すると、ユーザを認証するための 1 つまたは複数のリモート AAA サーバを指定できます。RADIUS と TACACS+ のいずれにおいても、グループのメンバーはすべて同じプロトコルに属す必要があります。設定した順序に従って一連のサーバが試行されます。

AAA サーバ モニタリング機能は AAA サーバを機能停止として記録できます。スイッチが機能停止の AAA サーバに要求を送信するまでの経過時間を分で設定できます （「AAA サーバのモニタリング」（P.4-5）を参照してください）。

ここで説明する内容は、次のとおりです。

サーバ グループ設定の概要

これらのサーバ グループはいつでも設定できますが、有効にするには、AAA サービスに適用する必要があります。AAA ポリシーは CLI ユーザ、または Fabric Manager または Device Manager のユーザに設定できます。

サーバ グループの設定

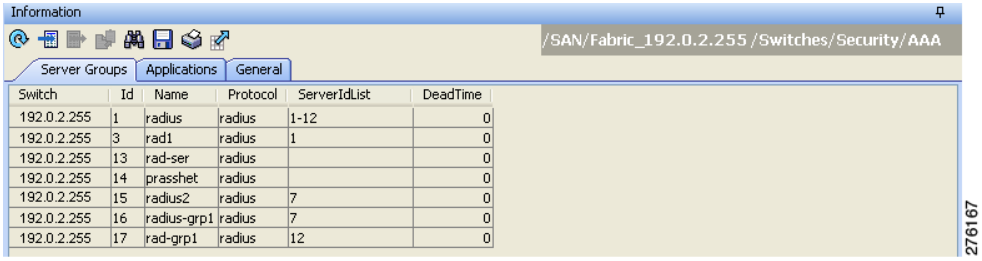
Fabric Manager を使用して RADIUS または TACACS+ サーバ グループを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[AAA] を選択します。

AAA 設定が [Information] ペインに表示されます（図 4-6 を参照）。図 4-6 のような画面が表示されない場合は、[Server Groups] タブをクリックします。

設定した RADIUS または TACACS+ サーバ グループが表示されます。

図 4-6　AAA サーバ グループ



Switch	Id	Name	Protocol	ServerIdList	DeadTime
192.0.2.255	1	radius	radius	1-12	0
192.0.2.255	3	rad1	radius	1	0
192.0.2.255	13	rad-ser	radius		0
192.0.2.255	14	prasshet	radius		0
192.0.2.255	15	radius2	radius	7	0
192.0.2.255	16	radius-grp1	radius	7	0
192.0.2.255	17	rad-grp1	radius	12	0

ステップ 2　サーバ グループを作成するには [Create Row] アイコンをクリックします。

[Create Server] ダイアログボックスが表示されます。

ステップ 3　RADIUS サーバ グループを追加するには、[radius] オプション ボタンをクリックします。TACACS+ サーバ グループを追加するには、[tacacs+] オプション ボタンをクリックします。

ステップ 4　ServerIdList フィールドにサーバ名を入力します。

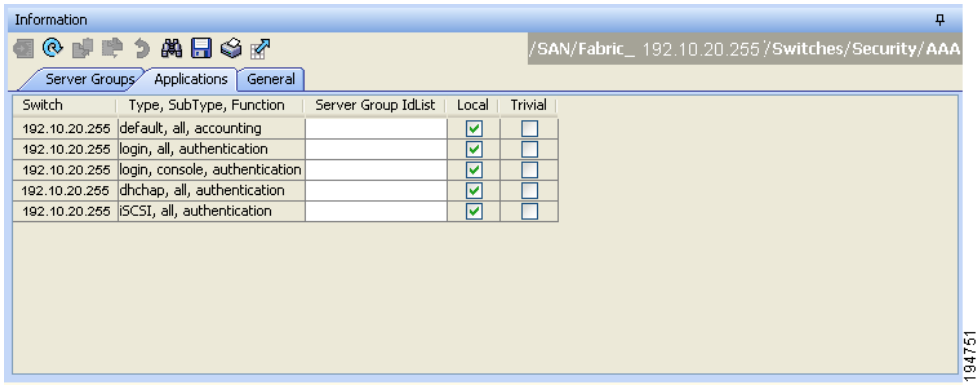
ステップ 5　バイパス（回避）と記録されるまでのサーバ無応答の分数を [DeadTime] フィールドに設定します。「無応答サーバのバイパス（回避）の概要」（P.4-22）を参照してください。

ステップ 6　このサーバ グループを作成するには [Create] ボタンをクリックします。

ステップ 7　[Applications] タブをクリックして、このサーバ グループをアプリケーションに割り当てます（図 4-7 を参照）。

サーバ グループをすべてのアプリケーションに関連付けることも、特定のアプリケーションを指定することもできます。

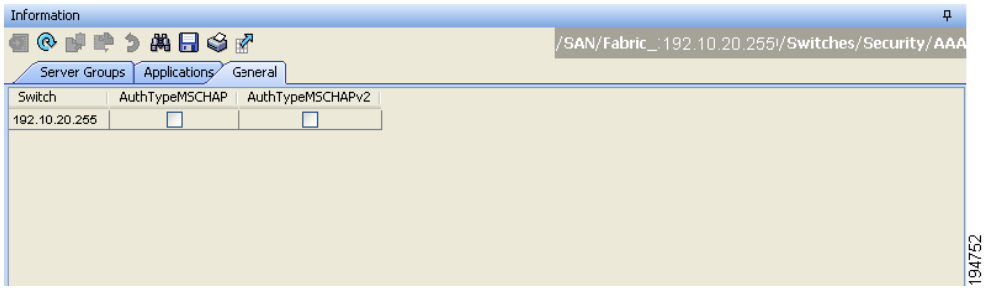
図 4-7　[Applications] タブ



ステップ 8　[General] タブをクリックして、このサーバ グループに認証の種類を割り当てます（図 3-8 を参照）。

サーバ グループの種類に基づいて、[MSCHAP] または [MSCHAPv2] のいずれかのチェックボックスをオンにします。

図 4-8　[General] タブ



ステップ 9　[Apply Changes] アイコンをクリックして、変更内容を保存します。

（注）　MSCHPv2 認証がイネーブルの場合は、TACACS+ グループを設定できません。

無応答サーバのバイパス（回避）の概要

Cisco SAN-OS リリース 3.0(1) では、サーバ グループ内の無応答 AAA サーバをバイパスできます。スイッチが無応答のサーバを検出すると、ユーザを認証する際にそのサーバをバイパスします。この機能を利用すると、障害を起こしたサーバが引き起こすログインの遅延を最小限にとどめることができます。無応答サーバに要求を送信し、認証要求がタイムアウトするまで待つかわりに、スイッチはサーバ グループ内の次のサーバに認証要求を送信します。サーバ グループに応答できる他のサーバが存在しない場合は、スイッチは無応答サーバに対して認証を試み続けます。

AAA サーバにおける配布

MDS スイッチの RADIUS および TACACS+ の AAA 設定は、Cisco Fabric Services（CFS）を使用して配布できます。デフォルトでは、配布はディセーブルです（『*Cisco Fabric Manager System Management Configuration Guide*』を参照）。

配布を有効にすると、最初のサーバまたはグローバル設定により、暗黙のセッションが開始します。それ以降に入力されたすべてのサーバ設定コマンドは、一時的なデータベースに保管され、データベースをコミットしたときに、ファブリック内のすべてのスイッチ（送信元スイッチを含む）に適用されます。サーバ キーおよびグローバル キーを除く、さまざまなサーバおよびグローバル パラメータが配布されます。サーバ キーおよびグローバル キーはスイッチに対する固有の秘密キーです。他のスイッチと共有しないでください。

（注）　サーバ グループ設定は配布されません。

ここで説明する内容は、次のとおりです。

- 「AAA サーバにおける配布のイネーブル化」（P.4-22）
- 「スイッチにおける配布セッションの開始」（P.4-23）
- 「セッション ステータスの表示」（P.4-23）
- 「配布する設定の表示」（P.4-24）
- 「配布のコミット」（P.4-24）
- 「配布セッションの廃棄」（P.4-24）
- 「セッションの消去」（P.4-25）
- 「RADIUS および TACACS+ 設定マージの注意事項」（P.4-25）

（注）　AAA サーバ設定配布を行う MDS スイッチは、Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS Release 4.1(1) を実行している必要があります。

AAA サーバにおける配布のイネーブル化

配布アクティビティに参加できるのは、配布がイネーブルであるスイッチだけです。

Fabric Manager を使用して RADIUS サーバでの配布を有効にする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[CFS] タブをクリックします。RADIUS CFS の設定が表示されます。

ステップ 3　RADIUS の CFS を有効にする全スイッチについて、[Admin] ドロップダウン リストで [enable] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更をファブリック全体に配布します。

Fabric Manager を使用して TACACS+ サーバでの配布を有効にする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[CFS] タブをクリックします。

TACACS+ CFS の設定が表示されます。

ステップ 3　TACACS+ の CFS を有効にする全スイッチについて、[Admin] ドロップダウン リストで [enable] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更をファブリック全体に配布します。

スイッチにおける配布セッションの開始

配布セッションは RADIUS/TACACS+ の設定またはグローバル設定を開始した瞬間に始まります。たとえば、次の作業を実行すると、暗黙のセッションが開始されます。

- RADIUS サーバのグローバル タイムアウトの指定
- TACACS+ サーバのグローバル タイムアウトの指定

（注）　AAA サーバに関連する最初の設定コマンドを発行すると、すべてのサーバおよびグローバル設定（配布セッションを開始する設定を含む）が一時バッファに格納されます。実行コンフィギュレーションには格納されません。

セッション ステータスの表示

暗黙の配布セッションが開始すると、Fabric Manager でセッションの状況を次の手順で確認できます。[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。

配布する設定の表示

一時バッファに保存された RADIUS または TACACS+ のグローバル設定またはサーバ設定を、Fabric Manager を使用して表示する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。

ステップ 2　[CFS] タブをクリックします。

[CFS] タブに配布状況が表示されます。

ステップ 3　[pending] または [running] オプション ボタンをクリックします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ステップ 5　[Servers] タブをクリックして保留中または実行中の設定を表示します。

配布のコミット

一時バッファに格納された RADIUS または TACACS+ グローバル設定またはサーバ設定は、ファブリック内のすべてのスイッチ（送信元スイッチを含む）の実行コンフィギュレーションに適用できます。

Fabric Manager を使用して RADIUS または TACACS+ の設定を配布する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。
[Information] ペインに RADIUS または TACACS+ の設定が表示されます。

ステップ 2　[CFS] タブをクリックします。RADIUS または TACACS+ の CFS 設定が表示されます。

ステップ 3　RADIUS または TACACS+ の CFS をイネーブルにする全スイッチについて、[Config Action] ドロップダウン リストで [commitChanges] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更をファブリック全体に配布します。

配布セッションの廃棄

進行中セッションの配布を廃棄すると、一時バッファ内の設定が廃棄されます。廃棄された配布は適用されません。

Fabric Manager を使用して RADIUS または TACACS+ の配布を廃棄する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。
[Information] ペインに RADIUS または TACACS+ いずれかの設定が表示されます。

ステップ 2　[CFS] タブをクリックします。RADIUS または TACACS+ いずれかの CFS 設定が表示されます。

ステップ 3　RADIUS または TACACS+ のペンディング配布を廃棄する各スイッチの [Config Action] ドロップダウン リストで [abort] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックします。

セッションの消去

Fabric Manager を使用して RADIUS または TACACS+ の配布を消去する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。

[Information] ペインに RADIUS または TACACS+ いずれかの設定が表示されます。

ステップ 2　[CFS] タブを選択します。RADIUS または TACACS+ いずれかの CFS 設定が表示されます。

ステップ 3　RADIUS または TACACS+ のペンディング配布を消去する各スイッチの [Config Action] ドロップダウン リストで [clear] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックします。

RADIUS および TACACS+ 設定マージの注意事項

RADIUS および TACACS+ のサーバ設定およびグローバル設定は 2 つのファブリックがマージするときにマージされます。マージされた設定は CFS 配布がイネーブルのスイッチに適用されます。

ファブリックのマージの際は次の条件に注意してください。

- サーバ グループはマージされません。
- サーバ キーとグローバル キーは、マージ中は変更されません。
- マージされた設定には、CFS がイネーブルのすべてのスイッチで扱われるすべてのサーバが含まれます。
- マージされた設定におけるタイムアウトと再送信のパラメータは、個々のサーバ設定とグローバル設定に存在する最大値になります。

注意　設定されたサーバ ポートの 2 台のスイッチ間に矛盾がある場合は、マージに失敗します。

MSCHAP による認証

Microsoft Challenge Handshake Authentication Protocol（MSCHAP）は Microsoft 版 の CHAP です。

Cisco MDS 9000 ファミリ スイッチのユーザ ログインでは、異なるバージョンの MSCHAP を使用してリモート認証を実行できます。MSCHAP は RADIUS サーバまたは TACACS+ サーバでの認証に使用され、MSCHAPv2 は RADIUS サーバでの認証に使用されます。

MSCHAP のイネーブル化の概要

デフォルトでは、スイッチはスイッチとリモート サーバの間で Password Authentication Protocol（PAP）認証を使用します。MSCHAP をイネーブルにする場合は、MSCHAP の VSA（vendor-specific attribute; ベンダー固有属性）を RADIUS サーバが認識するように設定する必要があります。「VSA（ベンダー固有属性）について」（P.4-13）を参照してください。表 4-1 に、MSCHAP に必要な RADIUS ベンダー固有属性を示します。

表 4-1　MSCHAP 用の RADIUS ベンダー固有属性

ベンダー ID 番号	ベンダー種別番号	ベンダー固有属性	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP ユーザへ送るチャレンジを格納。アクセス要求パケットとアクセス チャレンジ パケットの両方で使用可能
211	11	MSCHAP-Response	チャレンジへの応答として MS-CHAP ユーザにより提供される応答値を格納。アクセス要求パケットだけで使用

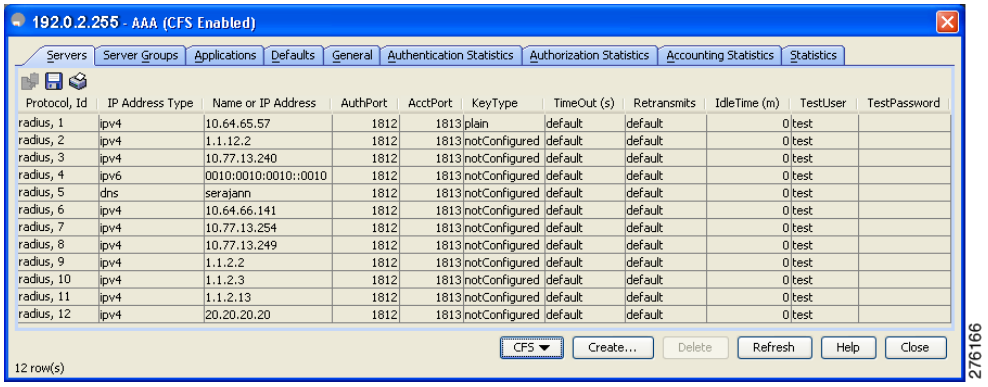
MSCHAP による認証のイネーブル化

Device Manager を使用して MSCHAP 認証をイネーブルにする手順は、次のとおりです。

ステップ 1　[Security] > [AAA] をクリックします。

AAA 設定が [Information] ペインに表示されます（図 4-9 を参照）。

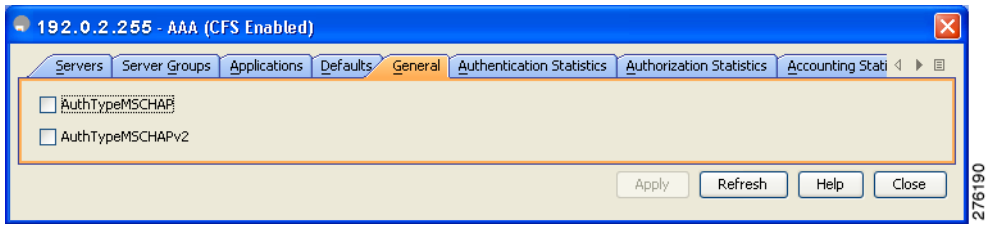
図 4-9　Device Manager での AAA 設定



ステップ 2　[General] タブをクリックします。

MSCHAP 設定が表示されます（図 4-10 を参照）。

図 4-10　MSCHAP の設定



ステップ 3　[AuthTypeMSCHAP] または [AuthTypeMSCHAPv2] チェックボックスをオンにして、スイッチでのユーザ認証に MSCHAP または MSCHAPv2 を利用します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ローカル AAA サービス

システムはユーザ名およびパスワードをローカルで維持し、パスワード情報は暗号化して保存します。ユーザの認証は、ローカルで保存されたユーザ情報に基づいて実行されます。

none オプションを使用して、パスワード確認をオフにできます。このオプションを設定すると、ユーザは有効なパスワードを提示しなくてもログインできます。ただし、ユーザは少なくとも Cisco MDS 9000 ファミリ スイッチ上のローカル ユーザでなければなりません。

注意　このオプションは注意して使用してください。このオプションを設定すると、あらゆるユーザがいつでもスイッチにアクセスできるようになります。

このオプションの設定手順については、『*Cisco MDS 9000 Family NX-OS Configuration Guide*』を参照してください。

Cisco Access Control Servers の設定

Cisco Access Control Server（ACS）は TACACS+ と RADIUS のプロトコルを利用して、セキュアな環境を作り出す AAA サービスを提供します。AAA サーバを使用する際のユーザ管理は、通常 Cisco ACS を使用して行われます。図 4-11、図 4-12、図 4-13 および図 4-14 に、RADIUS または TACACS+ を使用した ACS サーバの network-admin ロールおよび複数のロールのユーザ セットアップ設定のようすを示します。

注意　RADIUS または TACACS+ またはローカルのいずれで作成されたものであっても、Cisco MDS NX-OS は、すべて数字で構成されるユーザ名をサポートしません。名前がすべて数字のローカル ユーザは作成できません。すべて数字のユーザ名が AAA サーバに存在し、ログインの際に入力されても、そのユーザはログインできません。

図 4-11　RADIUS を使用する場合の network-admin ロールの設定

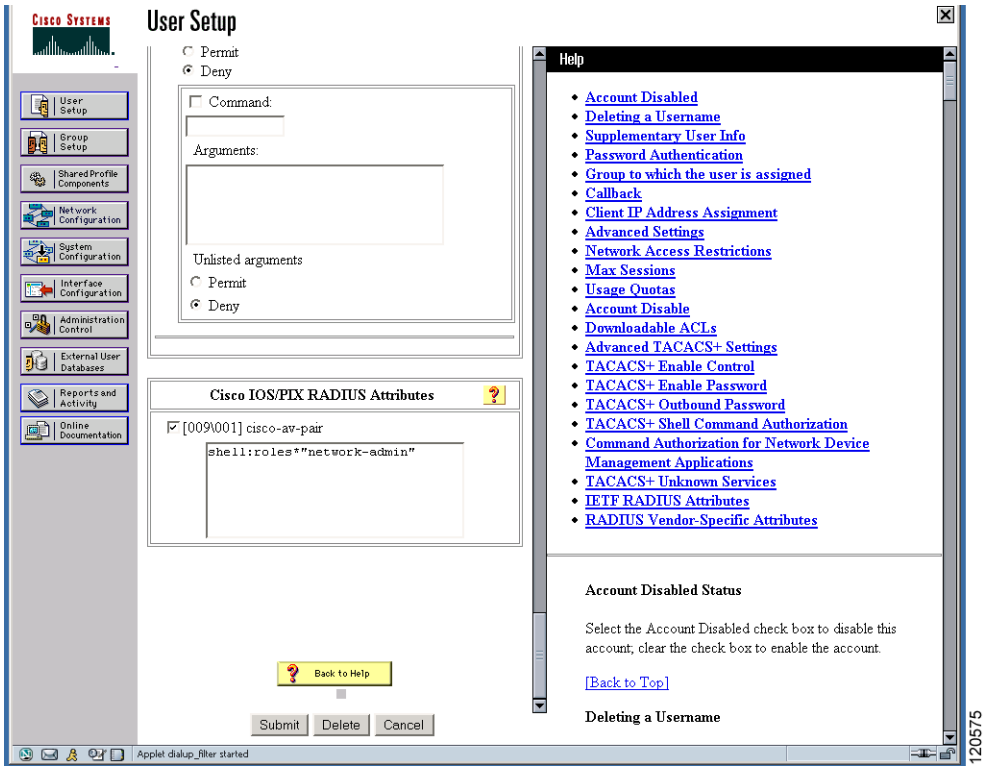


図 4-12　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

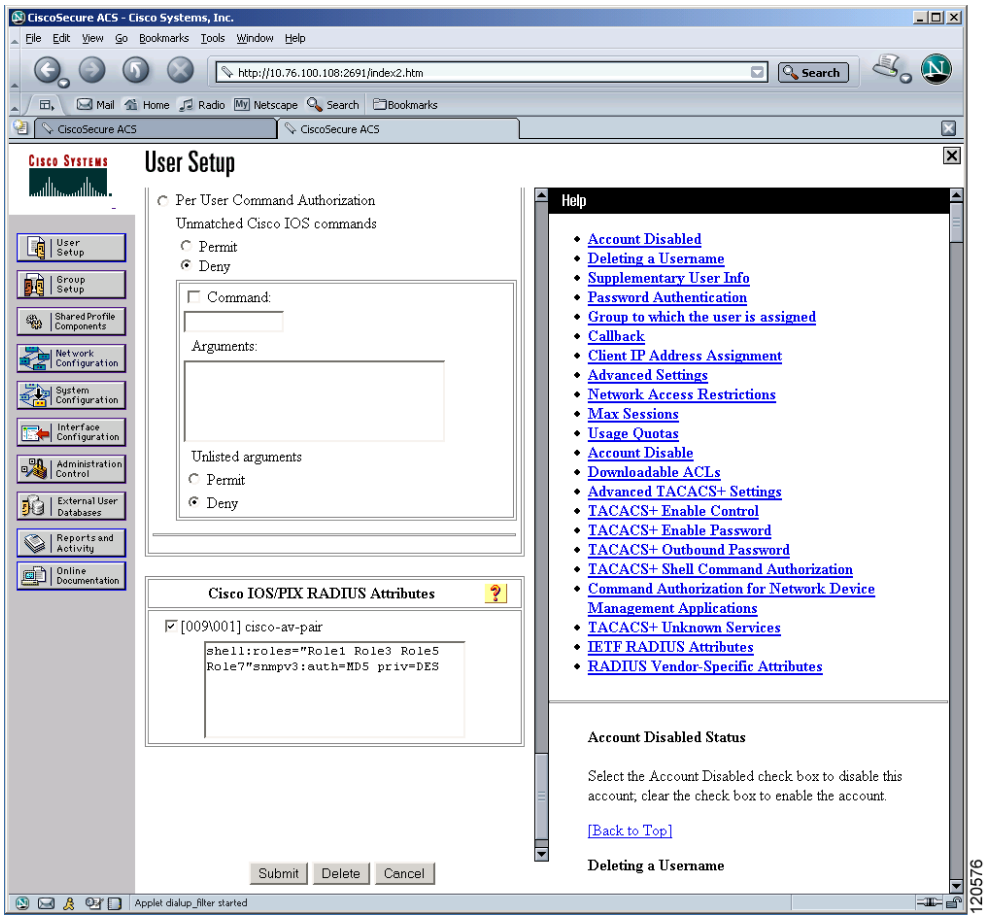


図 4-13　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

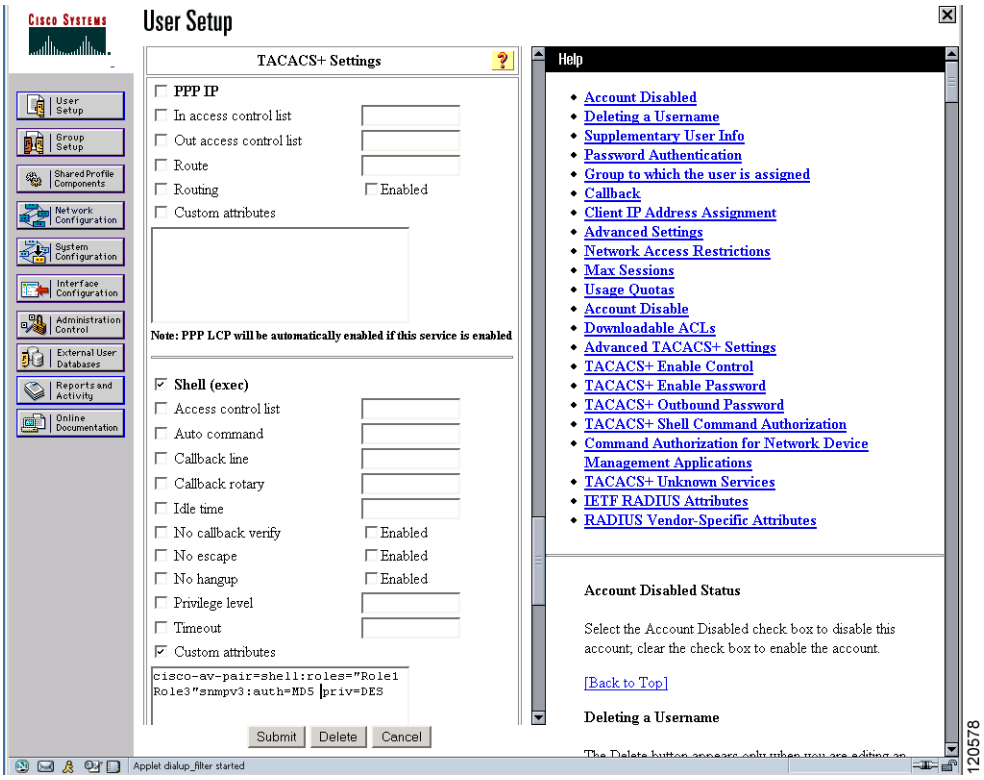
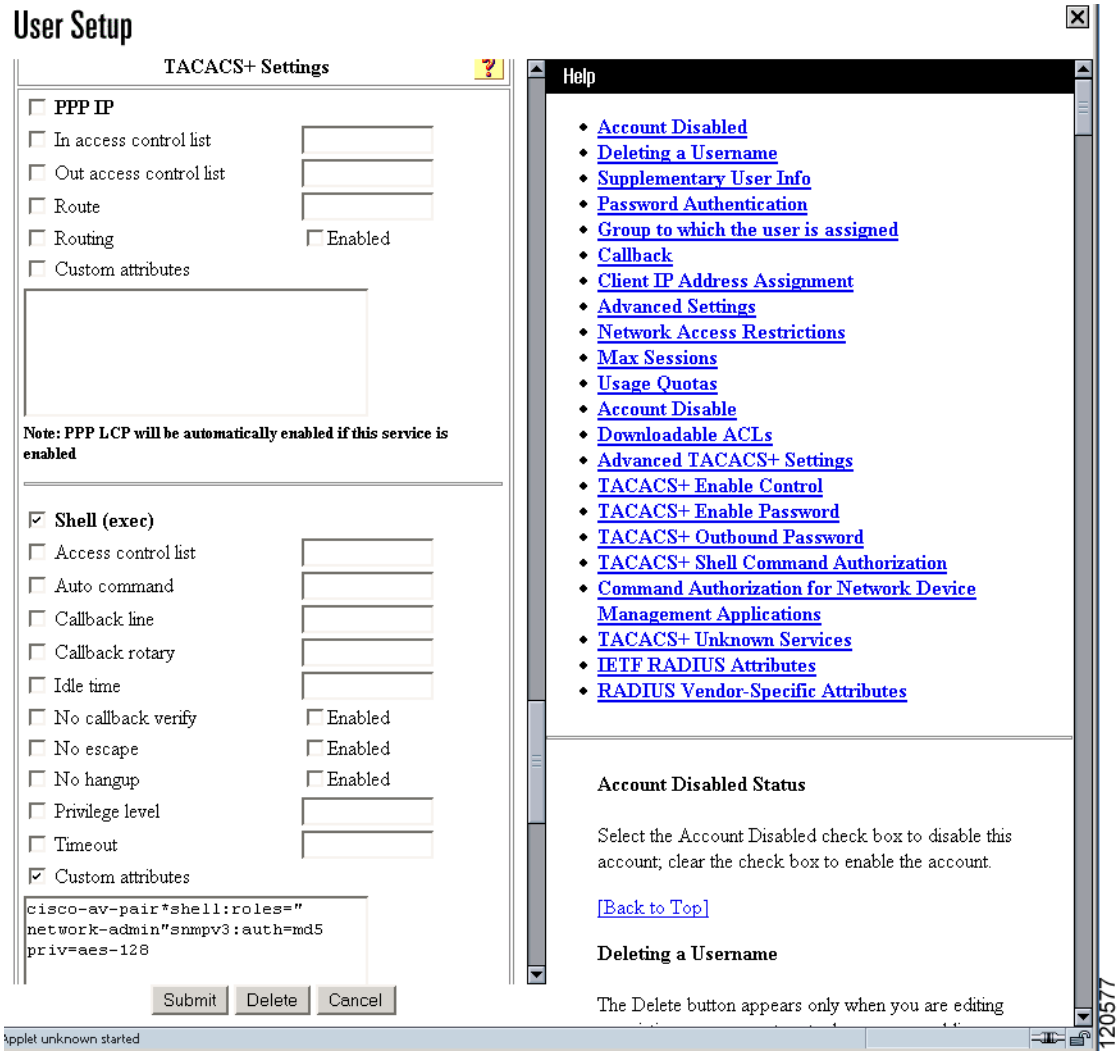


図 4-14　TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定



デフォルト設定値

表 4-2 はすべてのスイッチにおけるスイッチ セキュリティ機能のデフォルト設定です。

表 4-2　デフォルト スイッチ セキュリティ設定

パラメータ	デフォルト
Cisco MDS スイッチでのロール	ネットワーク オペレータ（network-operator）
AAA 設定サービス	ローカル
認証用ポート	1812
アカウンティング用ポート	1813
事前共有キーの送受信	クリア テキスト
RADIUS サーバ タイムアウト	1 秒

表 4-2　デフォルト スイッチ セキュリティ設定 （続き）

パラメータ	デフォルト
RADIUS サーバ再試行	1 回
許可	ディセーブル
デフォルトの AAA ユーザ ロール	イネーブル
RADIUS サーバへの誘導要求	ディセーブル
TACACS+	ディセーブル
TACACS+ サーバ	設定なし
TACACS+ サーバ タイムアウト	5 秒
TACACS+ サーバへの誘導要求	ディセーブル
AAA サーバへの配布	ディセーブル
アカウンティング ログ サイズ	250 KB