CHAPTER 41

RADIUS および TACACS+ の設定

認証、許可、アカウンティング（AAA）機能は、スイッチを管理するユーザの ID 確認、ユーザへのアクセス権付与、およびユーザ アクションの追跡を実行します。リモート AAA サーバを利用するソリューションを提供するため、すべての Cisco MDS 9000 ファミリ スイッチで RADIUS および TACACS+ の各プロトコルを利用します。

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認証やローカル データベースによる許可、またはリモート認証や AAA サーバによる許可を実行します。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。

この章は、次の項で構成されています。

スイッチ管理のセキュリティ

Cisco MDS 9000 ファミリ スイッチの管理セキュリティは、コマンドライン インターフェイス（CLI）や簡易ネットワーク管理プロトコル（SNMP）を含む、すべての管理アクセス方式にセキュリティを提供します。

この項では、次のトピックについて取り上げます。

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、コンソール（シリアル接続）、Telnet、または セキュア シェル（SSH）のいずれかを使用できます。管理方法（コンソール、Telnet、および SSH）ごとに、セキュリティ制御オプションを 1 つまたは複数設定できます。設定できるオプションは、ローカル、リモート（RADIUS か TACACS+）、または none です。

- 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.41-8）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.41-14）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.41-26）を参照してください。

これらのセキュリティ機能は、次のシナリオにも設定できます。

- iSCSI 認証（「iSCSI 認証設定時の注意事項およびシナリオ」（P.50-58）を参照）
- FC-SP 認証（第 45 章「FC-SP および DHCHAP の設定」を参照）

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。

第 40 章「SNMP の設定」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。

この項では、次のトピックについて取り上げます。

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 プロトコル データ ユニット（PDU）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 の操作を実行できません。

（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 スイッチに次の許可ロールがあります。

- 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を変更できません。
- 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 を利用する権限があります（Fabric Manager および Device Manager）。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の 1 つだけに属している場合、このロールが削除されると、ユーザにはただちにデフォルトの network-operator ロールが設定されます。

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 プロトコルおよび TACACS+ プロトコルを介して提供されるリモート AAA サービスには、ローカル AAA サービスと比べて次のような利点があります。

- 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 サーバはすでに企業全体に配置済みであり、簡単に導入できます。
- 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 で到達可能になっている必要があります。
- 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てください。
- スイッチにオーバーレイ イーサネット LAN が接続されている場合は、AAA サーバに簡単に到達できます（第 52 章「IP ストレージの設定」を参照）。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、アカウンティングのためのリモート AAA サーバは、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、リモート AAA サーバが応答できなくなったときにフェールオーバー サーバを提供することです。グループ内の最初のリモート サーバが応答しなかった場合、いずれかのサーバが応答を送信するまで、グループ内の次のリモート サーバで試行が行われます。サーバ グループ内のすべての AAA サーバが応答しなかった場合、そのサーバ グループ オプションは障害が発生しているものと見なされます。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（第 50 章「iSCSI の設定」を参照）
- FC-SP 認証（第 45 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　TACACS+、RADIUS、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 SAN-OS はすべてが数字のユーザ名はサポートしません。すべてが数字のローカル ユーザ名は作成できません。すべてが数字のユーザ名が 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されません。

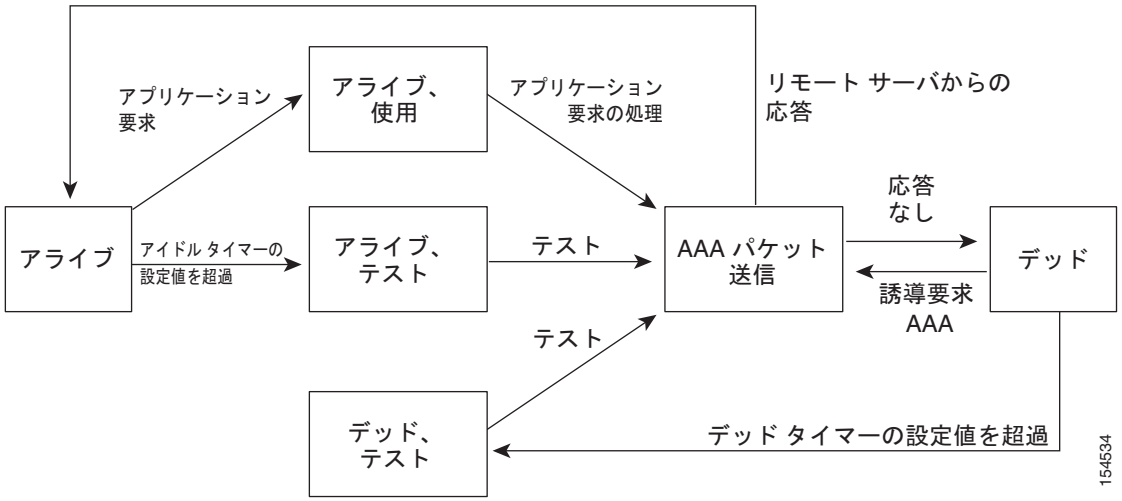
（注）　オプションの 1 つとしてローカルが指定されていない場合でも、その他のすべての設定オプションに失敗したときは、ローカル方式が試行されます。

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 ログインに成功するには、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 サーバが応答している（または稼働している）かどうかを確認できます。MDS スイッチは、応答のない AAA サーバを停止中としてマーク付けします。また、停止中のいずれの 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停止中の AAA サーバを監視し、応答するようになったら稼働中と認識します。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 サーバが稼働中であることを確認します。AAA サーバのステートが停止中または稼働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 サーバのステートについては、図 41-1 を参照してください。

図 41-1　AAA サーバのステート



（注）　稼働中のサーバと停止中のサーバのモニタリング間隔はそれぞれ別で、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.41-8）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　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て、Cisco MDS 9000 ファミリの目的のスイッチにログインできます。

ステップ 2　サーバ グループ認証方式を使用するサーバ 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方式で応答が得られなかった場合、ローカル データベースが認証に使用されます。

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、場合に応じて次の処理が実行されます。

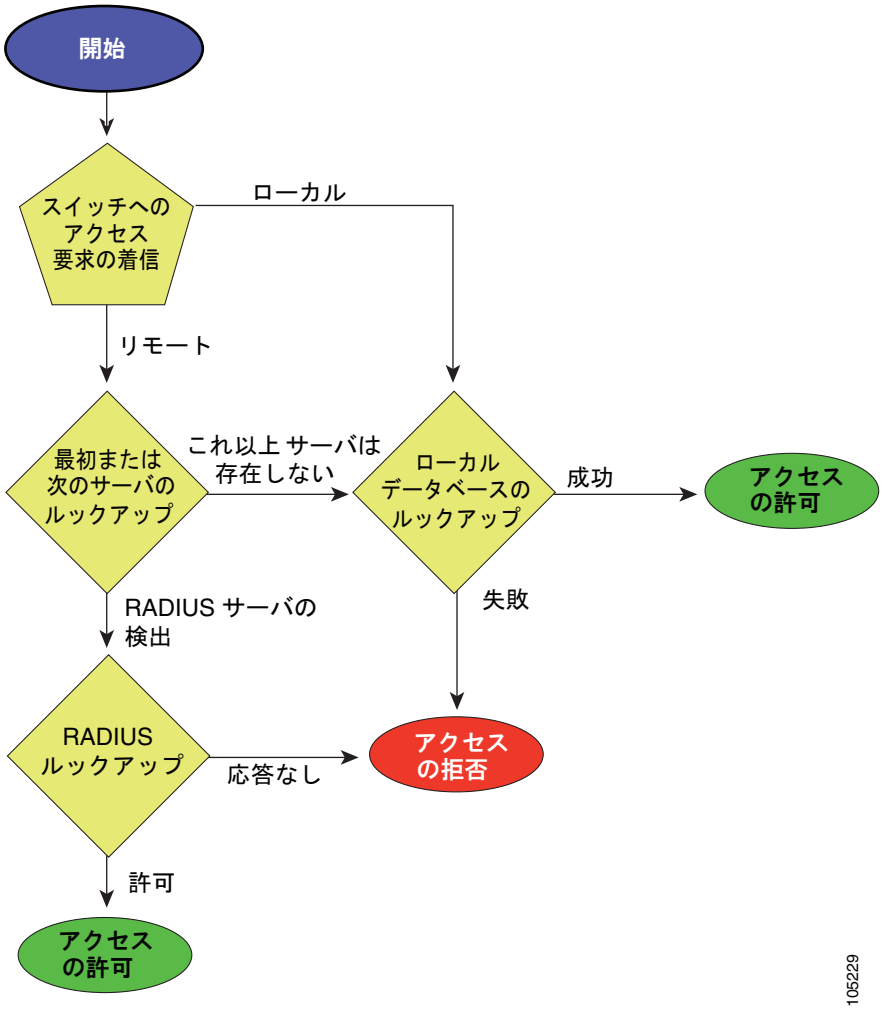
- AAA サーバのプロトコルが RADIUS の場合は、認証応答に伴って **cisco-av-pair** 属性で指定されたユーザ ロールがダウンロードされます。

- AAA サーバ プロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザ ロールを取得するために、もう 1 つの要求が同じサーバに送信されます。
- リモート AAA サーバからのユーザ ロールの取得に失敗した場合、ユーザには network-operator ロールが割り当てられます。

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、ログインが許可され、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 41-2 に、許可と認証のプロセスのフローチャートを示します。

図 41-2　スイッチの許可と認証のフロー



（注）　残りのサーバ グループがないということは、どのサーバ グループのどのサーバからも応答がないということを意味します。
残りのサーバがないということは、このサーバ グループのどのサーバからも応答がないということを意味します。

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 はネットワークへの不正なアクセスを防ぐ分散型クライアント/サーバ プロトコルです。Cisco の実装では、RADIUS クライアントは Cisco MDS 9000 ファミリ スイッチで実行され、ユーザ認証およびネットワーク サービス アクセス情報がすべて含まれる RADIUS 中央サーバに認証要求が送信されます。

ここでは、RADIUS の動作の定義、ネットワーク環境の特定、および設定可能な内容について説明します。

この項では、次のトピックについて取り上げます。

RADIUS サーバのデフォルト設定

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
- ユーザによるログイン時の RADIUS サーバ指定の許可

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 文字を含めることができます（スペースは使用できません）。グローバル キーは、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。

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。

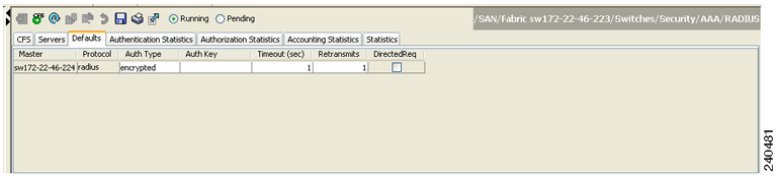
ステップ 1　[Switches] > [Security] > [AAA] を開いてから、[RADIUS] を選択します。

[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 41-3 を参照）。

図 41-3　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す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。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] を開いてから、[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] の各フィールドに入力します。

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 のキーは永続性ストレージに必ず暗号化して保存されます。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] を開いてから、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

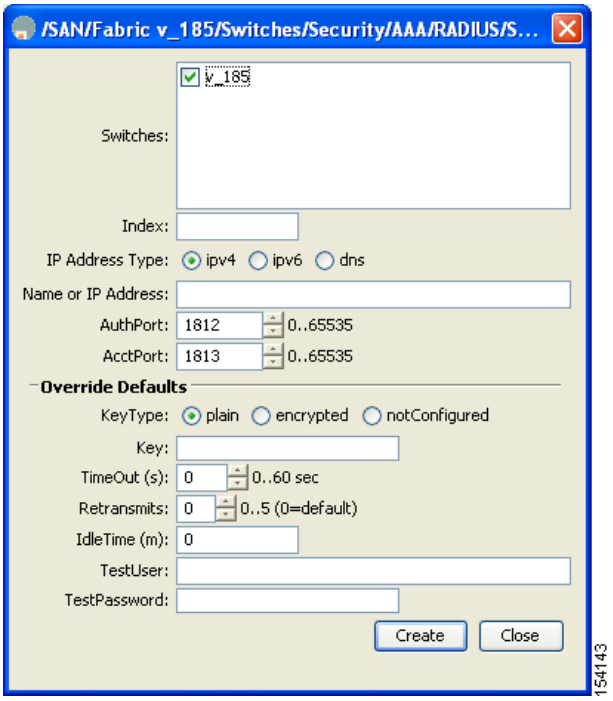
ステップ 2　[Servers] タブをクリックします。

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] 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 41-4 を参照）。

図 41-4　[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　任意で、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] をクリックして、変更を保存します。

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 サーバが要求を受信しないでいる時間間隔を指定します。

（注）　デフォルトのアイドル タイマー値は 0 分です。アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

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.41-10）を参照してください。

テスト ユーザ名の設定

定期的な RADIUS サーバのステータス テストに使用するユーザ名とパスワードを設定できます。RADIUS サーバを監視するテスト 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。

定期的な RADIUS サーバのステータス テスト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.41-10）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 サーバで設定されたユーザ名をテスト ユーザ名として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 を利用して 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] を開いてから、[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] 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 41-4 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、任意に [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　[IdleTime] フィールドに、テスト認証を送信するまでサーバがアイドル状態になっている時間を設定します。

ステップ 8　[Create] をクリックして、変更を保存します。

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] を開いてから、[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 サーバの統計情報が表示されます。

ユーザによるログイン時の RADIUS サーバ指定の概要

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。誘導要求オプションをイネーブルにすると、どの RADIUS サーバに認証要求を送信するかをユーザが指定できるようにスイッチを設定できます。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。

ログイン時にユーザによる RADIUS サーバの指定を許可

Fabric Manager を利用して、MDS スイッチにログインしているユーザが認証用の RADIUS サーバを選択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] を開いてから、[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、変更を保存します。

ベンダー固有属性の概要

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 ベンダー固有属性（VSA）の通信方式が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には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、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションを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 seperator 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、認証結果とともに許可情報などのユーザ属性を戻すように RADIUS サーバに指示します。この許可情報は、VSA で指定されます。

VSA の形式

Cisco SAN-OS ソフトウェアでは次の VSA プロトコル オプションをサポートしています。

- **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：Accounting-Request 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。

次の属性が Cisco SAN-OS ソフトウェアでサポートされています。

- **roles**：この属性は、ユーザが属する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文字列です。たとえば、ユーザが **vsan-admin** および **storage-admin** のロールに属している場合、値フィールドは「**vsan-admin storage-admin**」になります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性は shell プロトコル値とだけ併用できます。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 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 PDU 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。

また、VSA フォーマットには、オプションで SNMPv3 認証と機密保全プロトコルの属性を次のように指定できます。

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

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と 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 Terminal Access Controller Access Control System Plus（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。

この項では、次のトピックについて取り上げます。

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ているため、コネクション型プロトコルによる確実な転送を実行します。
- 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、高度なデータ機密性を実現します。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

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
- ユーザによるログイン時の TACACS+ サーバ指定の許可

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 文字を含めることができます（スペースは使用できません）。グローバル キーは、スイッチにあるすべての TACACS+ サーバ コンフィギュレーションで使用するよう設定できます。

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] を開いてから、[TACACS+] を選択します。

[Information] ペインに TACACS+ 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] を開いてから、[TACACS+] を選択します。

[Information] ペインに TACACS+ 設定が表示されます。

ステップ 2　[Defaults] タブを選択します （[Defaults] タブが無効化されている場合は、[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。TACACS+ サーバの設定を行うと、Fabric Manager または Device Manager によって自動的に TACACS+ の機能がイネーブルになります。

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、キーでドル記号（$）を使用できますが、二重引用符で囲む必要があります（例、"k$"）。パーセント記号（%）は使用できません。Cisco MDS SAN-OS リリース 2.1(2) 以降では、二重引用符なしでドル記号（$）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。

TACACS+ サーバの設定

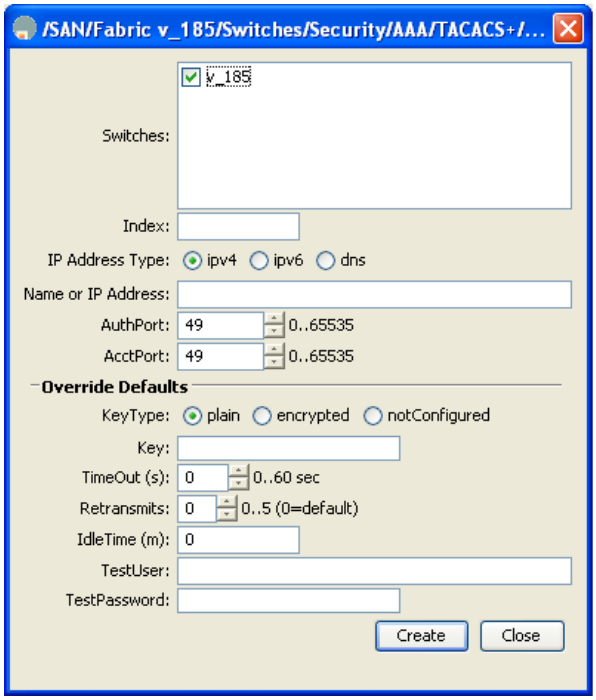
Fabric Manager を使用して TACACS+ サーバとオプションのすべてを設定する手順は次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を開いてから、[TACACS+] を選択します。
[Information] ペインに TACACS+ 設定が表示されます。

ステップ 2　[Servers] タブを選択します。
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] 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 41-5 を参照）。

図 41-5　[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] をクリックして、変更を保存します。

TACACS+ サーバの検証の概要

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 を利用して 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は「TACACS+ サーバ モニタリング パラメータの設定」（P.41-14）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] を開いてから、[TACACS+] を選択します。

[Information] ペインに TACACS+ 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。

ユーザによるログイン時の TACACS+ サーバ指定の概要

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。どの TACACS+ サーバに認証要求を送信するかをユーザが指定できるようにスイッチを設定できます。この機能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 TACACS+ サーバの名前です。

ユーザによるログイン時の TACACS+ サーバ指定の許可

Fabric Manager を利用して、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] を開いてから、[TACACS+] を選択します。

[Information] ペインに TACACS+ 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、変更を保存します。

ロールのカスタム属性の概要

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** 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）　TACACS+ カスタム属性は、Access Control Server（ACS）でさまざまなサービス（シェルなど）用に定義できます。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 SAN-OS ソフトウェアでは現在、下記の 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 グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて同じプロトコル（RADIUS または TACACS+）に属している必要があります。設定した順序に従ってサーバが試行されます。

AAA サーバ モニタリング機能は AAA サーバを停止中としてマーク付けできます。スイッチが停止中の 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.41-5）を参照）。

この項では、次のトピックについて取り上げます。

サーバ グループの設定の概要

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、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 ユーザや Device Manager ユーザに設定できます。

サーバ グループの設定

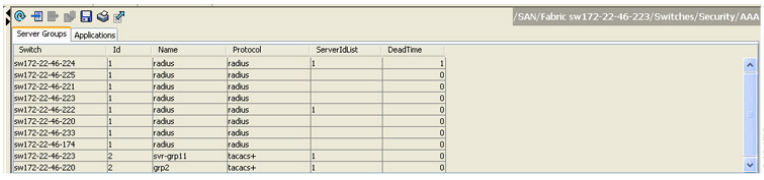
Fabric Manager を使用して RADIUS または TACACS+ サーバ グループを設定する手順は次のとおりです。

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

[Information] ペインに AAA 設定が表示されます（図 41-6 を参照）。図 41-6 に示す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 41-6　AAA Server Groups



ステップ 2　サーバ グループを作成するには [Create Row] 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 ボタンを選択します。TACACS+ サーバ グループを追加するには、[tacacs+] を選択します。

ステップ 4　[ServerIdList] フィールドにサーバ名を入力します。

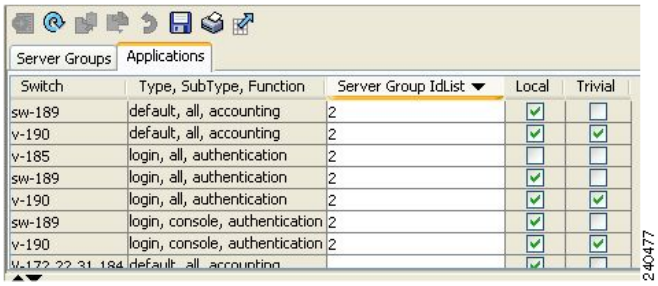
ステップ 5　バイパス（回避）とマーク付けされるまでのサーバ無応答の分数を [DeadTime] フィールドに設定します。「無応答サーバのバイパス（回避）の概要」（P.41-21）を参照してください。

ステップ 6　このサーバ グループを作成するには [Create] 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 41-7 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 41-7　[Applications] タブ



ステップ 8　[Apply Changes] アイコンをクリックして、変更を保存します。

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のではなく、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 サーバへの配信

MDS スイッチの RADIUS および TACACS+ の AAA 設定は、Cisco Fabric Services（CFS）を使用して配信できます。デフォルトでは、配信はディセーブルになっています（第 13 章「CFS インフラストラクチャの使用」を参照）。

配信をイネーブルにすると、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されます。それ以降に入力されたすべてのサーバ コンフィギュレーション 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 パラメータが配信されます。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 グループ設定は配信されません。

この項では、次のトピックについて取り上げます。

- 「AAA サーバへの配信のイネーブル化」（P.41-22）
- 「スイッチでの配信セッションの開始」（P.41-23）
- 「セッション ステータスの表示」（P.41-23）
- 「配信する設定の表示」（P.41-23）
- 「配信のコミット」（P.41-23）
- 「配信セッションの廃棄」（P.41-24）
- 「セッションのクリア」（P.41-24）
- 「RADIUS および TACACS+ 設定マージの注意事項」（P.41-24）

（注）　AAA サーバ設定配信を行う MDS スイッチでは、Cisco MDS SAN-OS Release 2.0(1b) 以降が稼働している必要があります。

AAA サーバへの配信のイネーブル化

アクティビティに参加できるのは、配信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 サーバでの配信をイネーブルにする手順は次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を開いてから、[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 をイネーブル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] をクリックして、変更をファブリック全体に配信します。

Fabric Manager を使用して TACACS+ サーバでの配信をイネーブルにする手順は次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を開いてから、[TACACS+] を選択します。

[Information] ペインに TACACS+ 設定が表示されます。

ステップ 2　[CFS] タブを選択します。

TACACS+ CFS の設定が表示されます。

ステップ 3　TACACS+ の CFS をイネーブル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] をクリックして、変更をファブリック全体に配信します。

スイッチでの配信セッションの開始

配信セッションは RADIUS/TACACS+ サーバ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コンフィギュレーション コマンドを発行すると、作成されたすべてのサーバおよびグローバル設定（配信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

暗黙の配信セッションが開始すると、Fabric Manager から [Switches] > [Security] > [AAA] を開いて [RADIUS] または [TACACS+] を選択することで、セッションの状況を確認できます。[CFS] タブに**配信状況**が表示されます。

配信する設定の表示

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] を開いてから、[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] タブに配信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] をクリックして、変更を保存します。

ステップ 5　[Servers] タブをクリックして保留中または実行コンフィギュレーションを表示します。

配信のコミット

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を、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+ の設定を配信する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を開いてから、[RADIUS] または [TACACS+] のいずれかを選択します。[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] タブを選択します。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] をクリックして、変更をファブリック全体に配信します。

配信セッションの廃棄

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

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

ステップ 1　[Switches] > [Security] > [AAA] を開いてから、[RADIUS] または [TACACS+] のいずれかを選択します。[Information] ペインに RADIUS または TACACS+ の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+ のいずれかの CFS 設定が表示されます。

ステップ 3　保留中の RADIUS または TACACS+ の配信を廃棄するスイッチごとに、[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] をクリックします。

セッションのクリア

Fabric Manager を使用して RADIUS または TACACS+ の配信をクリアする手順は次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を開いてから、[RADIUS] または [TACACS+] のいずれかを選択します。

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

ステップ 3　保留中の RADIUS または TACACS+ の配信をクリアするスイッチごとに、[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] 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 配信がイネーブルである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 キーおよびグローバル キーはマージ中に変更されません。
- マージされた設定には、CFS がイネーブルであるすべてのスイッチで見つかった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指定されている値の最大値になります。

注意　設定されたサーバ ポートの 2 つのスイッチの間で矛盾が存在する場合は、マージに失敗します。

MSCHAP による認証

Microsoft チャレンジ ハンドシェイク認証プロトコル（MSCHAP）は Microsoft 版の CHAP です。リモート認証サーバ（RADIUS または TACACS+）経由での MDS スイッチへのユーザ ログインに MSCHAP を使用できます。

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 サーバの間でパスワード認証プロトコル（PAP）認証を使用します。MSCHAP をイネーブルにする場合は、MSCHAP のベンダー固有属性を認識するように RADIUS サーバを設定する必要があります。「ベンダー固有属性の概要」（P.41-13）を参照してください。表 41-1 に MSCHAP に必要な RADIUS ベンダー固有属性を示します。

表 41-1　MSCHAP 用の RADIUS ベンダー固有属性

ベンダー ID 番号	ベンダー タイプ番号	ベンダー固有属性	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP ユーザに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
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が格納されます。Access-Request パケットでしか使用されません。

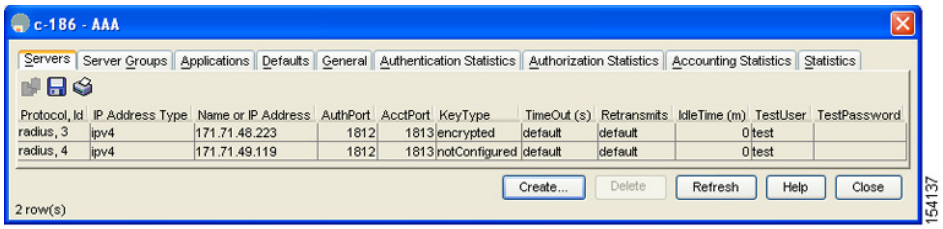
MSCHAP 認証のイネーブル化

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。

[Information] ペインに AAA 設定が表示されます（図 41-8 を参照）。

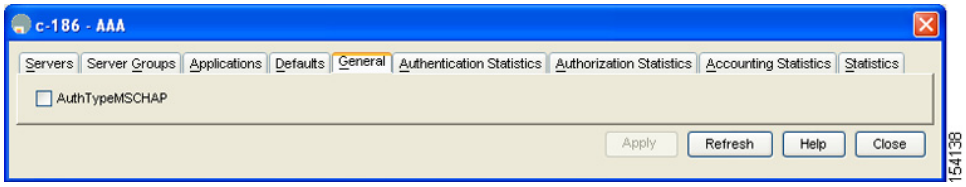
図 41-8　Device Manager での AAA 設定



ステップ 2　[General] タブをクリックします。

MSCHAP の設定が表示されます（図 41-9 を参照）。

図 41-9　MSCHAP の設定



ステップ 3　スイッチでのユーザ認証に MSCHAP を利用するには、[AuthTypeMSCHAP] チェックボックスをオンにします。

ステップ 4　[Apply Changes] をクリックして、変更を保存します。

ローカル AAA サービス

システムによりユーザ名およびパスワードはローカルで保持され、パスワード情報は暗号化形式で格納されます。ユーザの認証は、ローカルに保存されているユーザ情報に基づいて実行されます。「ロールとプロファイルの設定」（P.39-2）を参照してください。

none オプションを利用すると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 Family スイッチ上のローカル ユーザである必要があります。

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 CLI 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 41-10、図 41-11、図 41-12、および図 41-13 に、RADIUS または TACACS+ を利用した ACS サーバの network-admin ロールおよび複数ロールのユーザ セットアップ設定を示します。

注意　RADIUS、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 SAN-OS はすべてが数字のユーザ名はサポートしません。すべて数字の名前を持つローカル ユーザは作成できません。AAA サーバに数字だけのユーザ名が存在する場合、ログイン時に入力しても、そのユーザはログインできません。

図 41-10　RADIUS を使用する場合の network-admin ロールの設定

図 41-11　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

図 41-12　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

図 41-13　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

表 41-2 に、スイッチのすべてのスイッチ セキュリティ機能のデフォルト設定を示します。

表 41-2　スイッチ セキュリティのデフォルト設定

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
認証ポート	1821
アカウンティング ポート	1813
事前共有キーの送受信	クリア テキスト

表 41-2　スイッチ セキュリティのデフォルト設定 （続き）

パラメータ	デフォルト
RADIUS サーバのタイムアウト	1 秒
RADIUS サーバ再試行	1 回
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	未設定
TACACS+ サーバのタイムアウト	5 秒
TACACS+ サーバへの誘導要求	ディセーブル
AAA サーバへの配信	ディセーブル
アカウンティング ログ サイズ	250 KB