外部 AAA サーバでのセキュリティ機能の設定

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。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認証やローカル データベースによる認可、またはリモート認証や AAA サーバによる認可を実行します。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（4-2 ページ）
- スイッチの AAA 機能（4-3 ページ）
- AAA サーバのモニタリング パラメータをグローバルに設定（4-12 ページ）
- LDAP の設定（4-13 ページ）
- RADIUS サーバ モニタリング パラメータの設定（4-22 ページ）
- ワンタイム パスワード サポート（4-32 ページ）
- TACACS+ サーバ モニタリング パラメータの設定（4-33 ページ）
- サーバ グループの設定（4-44 ページ）
- AAA サーバへの配信（4-47 ページ）
- CHAP 認証（4-51 ページ）
- MSCHAP による認証（4-52 ページ）
- ローカル AAA サービス（4-53 ページ）
- アカウンティング サービスの設定（4-55 ページ）
- Cisco Access Control Servers の設定（4-57 ページ）
- デフォルト設定（4-60 ページ）

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。

- CLI セキュリティ オプション（4-2 ページ）
- SNMP セキュリティ オプション（4-2 ページ）

CLI セキュリティ オプション

CLI 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）を使用してアクセスできます。

- 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」セクション（4-22 ページ）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」セクション（4-33 ページ）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」セクション（4-53 ページ）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。

- Small Computer Systems Interface over IP（iSCSI）認証

  『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』、『*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。

Fabric Manager と Device Manager の詳細については、『*Cisco Fabric Manager Fundamentals Configuration Guide*』を参照してください。

スイッチの AAA 機能

CLI または Fabric Manager あるいは SNMP アプリケーションを使用して、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（4-3 ページ）
- 認可（4-3 ページ）
- アカウンティング（4-4 ページ）
- リモート AAA サービス（4-4 ページ）
- リモート認証に関する注意事項（4-4 ページ）
- サーバ グループ（4-5 ページ）
- 認証と許可のプロセス（4-7 ページ）

認証

認証は、スイッチにアクセスするユーザまたはデバイスの識別情報を検証するプロセスです。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」）。

認可

すべての Cisco MDS スイッチに次の認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、ロールベースの認可を設定します。
- 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。
- オーバーレイ Ethernet 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です（『*Cisco Fabric Manager IP Services Configuration Guide*』および『*Cisco MDS 9000 Family NX-OS Configuration Guide*』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 サービス設定オプション

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*』および『*Cisco MDS 9000 Family NX-OS 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。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、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、認証用に設定されたすべての AAA サーバに到達不能であるかどうかがデフォルトで試行されます。ユーザは、このフォールバックを柔軟にディセーブルにすることができます。

RADIUS がタイムアウトする際は、フォールバック設定に応じてローカル 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。

表 4-1 に、AAA サービス設定オプションごとに CLI（コマンドライン インターフェイス）の関連コマンドを示します。

表 4-1　AAA サービス コンフィギュレーション コマンド

AAA サービス コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン（Cisco Fabric Manager および Device Manager ログイン）	**aaa authentication login default**
コンソール ログイン	**aaa authentication login console**
Small Computer Systems Interface over IP（iSCSI）認証	**aaa authentication iscsi default**
FC-SP 認証	**aaa authentication dhchap default**
アカウンティング	**aaa accounting default**

エラー対応ステータス

ログイン時にリモート AAA サーバが応答しない場合、そのログインは、ローカル ユーザ データベースにロール オーバーして処理されます。この場合は、error-enabled 機能をイネーブルにした場合、次のメッセージが画面に表示されます。

```
Remote AAA servers unreachable; local authentication done.
```

このメッセージの表示をイネーブルにするには、**aaa authentication login error-enable** コマンドを使用します。

このメッセージの表示をディセーブルにするには、**no aaa authentication login error-enable** コマンドを使用します。

現在の表示ステータスを確認するには、**show aaa authentication login error-enable** コマンドを使用します（例 4-1 を参照）。

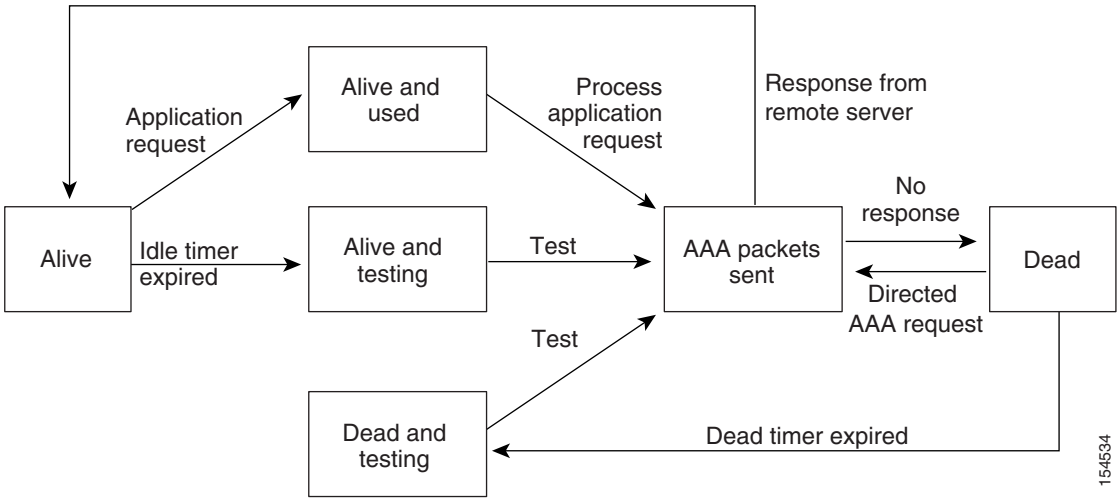
例 4-1　AAA 認証ログイン情報の表示

```
switch# show aaa authentication login error-enable
enabled
```

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 4-1 を参照してください。

図 4-1　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」セクション（4-22 ページ）、「RADIUS サーバ モニタリング パラメータの設定」セクション（4-26 ページ）および「RADIUS サーバの詳細の表示」セクション（4-31 ページ）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。

許可は、アクセス コントロールを提供します。これは、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。ユーザは、ユーザ ID とパスワードの組み合わせに基づいて認証および認可され、割り当てられているロールに従ってネットワークにアクセスします。スイッチで TACACS+ プロトコルを使用していれば、ユーザによる不正なアクセスを防ぐことができるパラメータを設定できます。

AAA の許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。Cisco NX-OS ソフトウェアでは、AAA サーバからダウンロードされる属性を使用して権限付与が行われます。RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。

認証と認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、デフォルトでローカル データベースが認証に使用されます。次の項で、このフォールバックをディセーブルにする方法について説明します。

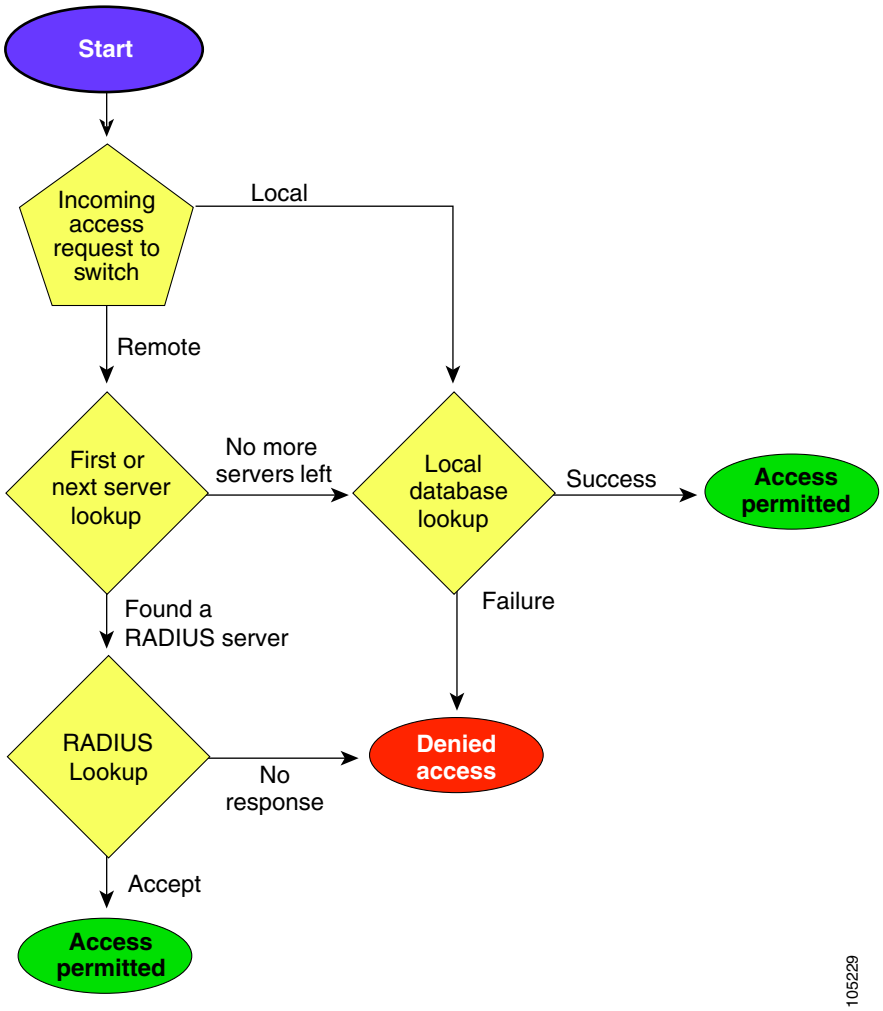
ステップ 3　リモートの AAA サーバにより認証に成功すると、場合に応じて次の処理が実行されます。

- 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 4-2 に、認可と認証のプロセスのフローチャートを示します。

図 4-2　スイッチの認可と認証のフロー



(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。

TACACS+ サーバでロールベースの認証を設定するには、次の手順に従います。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa authorization`	認証方式の設定を有効にします。
ステップ 3	`switch(config)# aaa authorization config-commands`	config モード Layer2 および Layer3 のすべてのコマンドの認証を有効にします。
ステップ 4	`switch(config)# aaa authorization config-commands default group tac1`	指定した TACACS+ サーバ グループの認証を有効にします。

	コマンド	目的
ステップ 5	`switch(config)# aaa authorization commands`	すべての EXEC モード コマンドへの AAA 許可を有効にします。
ステップ 6	`switch(config)# aaa authorization commands default group tac1`	指定した TACACS+ サーバ グループの認証を有効にします。
ステップ 7	`switch(config)# aaa authorization commands default group local`	デフォルトの TACACS+ サーバ グループの認証を有効にします。認証は、ローカル ユーザ データベースに基づいています。
ステップ 8	`switch(config)# no aaa authorization command default group tac1`	認証されたユーザに対し指定した機能の認証を削除します。

（注）　承認の設定は、TACACS+ サーバを使用して実施する認証にのみ提供されます。

（注）　AAA 許可方式の [none] オプションは廃止されました。4.x イメージからアップグレードし、[none] を許可方式の 1 つとして設定した場合、ローカルに置き換えられます。機能は変わりません。

AAA 認証に関する情報と、リモート認証に割り当てられたデフォルト ユーザ ロールを表示するには、**show** コマンドを使用できます。（例 4-2 から例 4-3 を参照してください）。

例 4-2　AAA 許可情報の詳細の表示

```
switch# show aaa authorization all
AAA command authorization:
         default authorization for config-commands: local
         default authorization for commands: local
         cts: group rad1
```

例 4-3　リモート認証のデフォルト ユーザ ロールの表示

```
switch# show aaa user default-role
enabled
```

認証のフォールバック メカニズムの設定

リモート認証が設定され、すべての AAA サーバに到達不能（認証エラー）である場合は、ローカル データベースへのフォールバックをイネーブルまたはディセーブルにできます。認証エラーの場合、フォールバックはデフォルトでローカルに設定されています。コンソール ログインと ssh/telnet ログインの両方に対して、このフォールバックをディセーブルにすることもできます。このフォールバックを無効にすると、認証のセキュリティが強化されます。

CLI 構文と動作は次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。

ステップ 2	`switch(config)# show run aaa all`
	`aaa authentication login default fallback error local`
	`aaa authentication login console fallback error local`
		デフォルトのフォールバックの動作が表示されます。

ステップ 3	`switch(config)# no aaa authentication login default fallback error local` `WARNING!!! Disabling fallback can lock your switch.`	認証用のローカル データベースへのフォールバックをディセーブルにします。 (注)　コンソールへフォールバックをディセーブルにするには、このコマンドの **default** を **console** で置き換えます。

注意　デフォルトとコンソールの両方に対してフォールバックがディセーブルである場合は、リモート認証がイネーブルになり、サーバに到達不能であるため、スイッチはロックされます。

認可プロファイルの確認

各種コマンドの認可プロファイルを確認できます。イネーブルの場合、すべてのコマンドは、検証用に Access Control Server（ACS）に転送されます。検証が完了すると、検証の詳細が表示されます。

```
switch# terminal verify-only username sikander
switch# config terminal
Enter configuration commands, one per line.End with CNTL/Z.
switch(config)# feature telnet
% Success
switch(config)# feature ssh
% Success
switch(config)# end
% Success
switch# exit
```

(注)　このコマンドは、コマンドを確認するだけで設定をイネーブルにしません。

認証のテスト

コマンドの認証設定をテストできます。

コマンドの認証をテストするには、**test aaa authorization command-type** コマンドを使用します。

```
switch(config)# test aaa authorization command-type commands user u1 command "feature dhcp"
% Success
```

AAA サーバのモニタリング パラメータをグローバルに設定

AAA サーバ モニタリング パラメータは、すべてのサーバにグローバルに設定、または特定のサーバに対して個別に設定できます。この項では、グローバル コンフィギュレーションの設定方法について説明します。グローバル コンフィギュレーションは、個別のモニタリング パラメータが定義されていないすべてのサーバに適用されます。各サーバで、特定のサーバに対して定義された個々のテスト パラメータは、グローバル設定よりも常に優先されます。

RADIUS サーバのグローバル モニタリング パラメータを設定するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server deadtime 10`	RADIUS サーバのグローバル デッド タイムを 10 分間に設定します。 許容範囲は 0 ～ 1440 分です。
ステップ 3	`switch(config)# radius-server timeout 20f`	RADIUS サーバのグローバル タイムアウトを 20 分間に設定します。 許容範囲は 1 ～ 60 分です。
ステップ 4	`switch(config)# radius-server retransmit 2`	RADIUS サーバのグローバル再送信回数を 2 に設定します。 許容範囲は 0 ～ 5 です。
ステップ 5	`switch(config)# radius-server test username username password password idle-time time`	RADIUS サーバのテスト パラメータをグローバルに設定します。
	`switch(config)# radius-server test username username password password no`	RADIUS サーバのグローバルなテスト パラメータを無効にします。

(注)　TACACS サーバのグローバル テスト パラメータの設定の場合に相当するコマンドを取得するには、上記の手順の radius を tacacs と置き換えます。

グローバル AAA サーバ モニタリング パラメータは次の動作を確認します。

- 新しい AAA サーバを設定すると、その AAA サーバは、グローバル テスト パラメータを使用して監視されます(定義されている場合)。
- グローバル テスト パラメータが追加または変更されると、テスト パラメータが設定されていないすべての AAA サーバは、新しいグローバル テスト パラメータを使用して監視されるようになります。
- サーバのサーバ テスト パラメータを削除した場合、またはアイドル時間を 0(デフォルト値)に設定した場合、そのサーバは、グローバル テスト パラメータを使用して監視されるようになります(定義されている場合)。
- グローバル テスト パラメータを削除したり、グローバル アイドル時間を 0 に設定したりしても、サーバ テスト パラメータが存在するサーバは影響を受けません。ただし、これまではグローバル パラメータを使用して監視されていた他のすべてのサーバのモニタリングが停止します。
- ユーザ指定のサーバ テスト パラメータによってサーバのモニタリングが失敗した場合は、グローバル テスト パラメータにフォールバックしません。

LDAP の設定

Lightweight Directory Access Protocol（LDAP）は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行います。LDAP サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する LDAP デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した LDAP 機能を使用可能にするには、LDAP サーバにアクセスして設定しておく必要があります。

LDAP では、認証と認可のファシリティが別々に提供されます。LDAP では、1 つのアクセス コントロール サーバ（LDAP デーモン）が認証と許可の各サービスを個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

LDAP クライアント/サーバ プロトコルでは、トランスポート要件を満たすために、TCP（TCP ポート 389）を使用します。Cisco NX-OS デバイスは、LDAP プロトコルを使用して集中型の認証を行います。

（注）　Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

この項では、次のトピックについて取り上げます。

- LDAP 認証および許可（4-14 ページ）
- LDAP の注意事項と制約事項（4-14 ページ）
- LDAP の前提条件（4-14 ページ）
- デフォルト設定（4-15 ページ）
- LDAP のイネーブル化（4-15 ページ）
- LDAP サーバ ホストの設定（4-15 ページ）
- LDAP サーバの RootDN の設定（4-16 ページ）
- LDAP サーバ グループの設定（4-17 ページ）
- グローバルな LDAP タイムアウト間隔の設定（4-18 ページ）
- LDAP サーバのタイムアウト間隔の設定（4-18 ページ）
- グローバル LDAP サーバ ポートの設定（4-19 ページ）
- TCP ポートの設定（4-19 ページ）
- LDAP 検索マップの設定（4-20 ページ）
- LDAP デッド タイム間隔の設定（4-20 ページ）
- LDAP サーバでの AAA 許可の設定（4-21 ページ）
- LDAP のディセーブル化（4-21 ページ）
- LDAP の設定例（4-22 ページ）

LDAP 認証および許可

クライアントは、簡易バインド（ユーザ名とパスワード）を使用して LDAP サーバとの TCP 接続および認証セッションを確立します。許可プロセスの一環として、LDAP サーバはそのデータベースを検索し、ユーザ プロファイルやその他の情報を取得します。

バインドしてから検索する（認証を行ってから許可する）か、または検索してからバインドするように、バインド操作を設定できます。デフォルトでは、検索してからバインドする方式が使用されます。

検索してからバインドする方式の利点は、baseDN の前にユーザ名（cn 属性）を追加することで認定者名（DN）を形成するのではなく、検索結果で受け取った DN をバインディング時にユーザ DN として使用できることです。この方式は、ユーザ DN がユーザ名と baseDN の組み合わせとは異なる場合に特に役立ちます。ユーザ バインドのために、bindDN が baseDN + append-with-baseDN として構成されます。ここで、append-with-baseDN は cn=$userid のデフォルト値です。

（注）　バインド方式の代わりに、比較方式を使用して LDAP 認証を確立することもできます。比較方式では、サーバでユーザ入力の属性値を比較します。たとえば、ユーザ パスワード属性を比較して認証を行うことができます。デフォルトのパスワード属性タイプは userPassword です。

LDAP の注意事項と制約事項

LDAP に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の LDAP サーバを設定できます。
- Cisco NX-OS は LDAP バージョン 3 だけをサポートします。
- Cisco NX-OS は次の LDAP サーバだけをサポートします。
  - OpenLDAP
  - Microsoft Active Directory
- Secure Sockets Layer（SSL）上の LDAP は、SSL バージョン 3 および Transport Layer Security（TLS）バージョン 1 だけをサポートします。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。

LDAP の前提条件

LDAP の前提条件は次のとおりです。

- LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること
- Cisco NX-OS デバイスが AAA サーバの LDAP クライアントとして設定されていること

デフォルト設定

表 4-2 は、LDAP パラメータのデフォルト設定の一覧です。

表 4-2　LDAP パラメータのデフォルト設定

パラメータ	デフォルト
LDAP	ディセーブル
LDAP 認証方式	検索してからバインド
LDAP 認証メカニズム	プレーン
デッド間隔時間	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	60 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	シスコ

LDAP のイネーブル化

デフォルトでは、Cisco NX-OS デバイスの LDAP 機能はディセーブルになっています。認証に関するコンフィギュレーション コマンドと検証コマンドを使用するには、LDAP 機能を明示的にイネーブルにする必要があります。

LDAP をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# configure terminal` `switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# feature ldap`	LDAP をイネーブルにします。
ステップ 3	`switch(config)# exit` `switch#`	設定モードを終了します。
ステップ 4	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP サーバ ホストの設定

リモートの LDAP サーバにアクセスするには、Cisco NX-OS デバイス上でその LDAP サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の LDAP サーバを設定できます。

（注）　デフォルトでは、LDAP サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスで設定すると、LDAP サーバがデフォルトの LDAP サーバ グループに追加されます。LDAP サーバを別の LDAP サーバ グループに追加することもできます。

LDAP サーバ ホストを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap-server host 10.10.2.2 enable-ssl**	LDAP サーバの IPv4 または IPv6 アドレス、あるいはホスト名を指定します。 **enable-ssl** キーワードは、LDAP クライアントに Secure Sockets Layer（SSL）セッションを確立させてからバインドまたは検索の要求を送信することにより、転送されたデータの整合性と機密保持を保証します。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 4	switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP サーバの RootDN の設定

LDAP サーバ データベースのルート指定名（DN）を設定できます。rootDN は、LDAP サーバにバインドしてそのサーバの状態を確認するために使用します。

LDAP サーバに RootDN を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60**	LDAP サーバ データベースの rootDN を指定し、ルートのパスワードをバインドします。 任意で、サーバに送る LDAP メッセージに使用する TCP ポートを指定します。有効な範囲は 1 ～ 65535 です。デフォルトの TCP ポートはグローバル値です（グローバル値が設定されていない場合は 389）。また、サーバのタイムアウト間隔も指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 4	switch# **show ldap-server**	（任意）LDAP サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP サーバ グループの設定

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。グループのメンバはすべて、LDAP を使用するように設定する必要があります。設定した順序に従ってサーバが試行されます。

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。

Cisco MDS NX-OS リリース 6.2(1) 以降では、Cisco MDS 9000 シリーズ スイッチがグループ ベースのユーザ ロールをサポートします。また、LDAP サーバにグループを作成し、Cisco MDS スイッチにまったく同じ名前のグループを作成してから、そのグループにユーザを追加できます。ユーザ ロール属性は設定されたグループのユーザに継承されます。これは Microsoft LDAP サーバの内蔵の memberOf 属性を使用して実行できます。memberOf 属性を使用するには、スイッチのロール名を作成していることを確認します。ロール名は LDAP サーバのグループ名と同じである必要があります。

(注)
- ユーザはスイッチで使用可能な 1 つのグループだけに属することができます。
- ユーザは複数のグループに属することができますが、スイッチ ロールに含めることができるのは 1 つのグループのみです。
- グループ名にスペースを含めることはできません。

LDAP サーバ グループを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa group server ldap LDAPServer1** switch(config-ldap)#	LDAP サーバ グループを作成し、そのグループの LDAP サーバ グループ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-ldap)# **server 10.10.2.2**	LDAP サーバを、LDAP サーバ グループのメンバとして設定します。 指定した LDAP サーバが見つからない場合は、ldap-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	switch(config-ldap)# **authentication compare password-attribute TyuL8r**	(任意)バインド方式または比較方式を使用して LDAP 認証を実行します。デフォルトの LDAP 認証方式は、検索してからバインドするバインド方式です。
ステップ 5	switch(config-ldap)# **enable user-server-group**	(任意)グループ検証をイネーブルにします。LDAP サーバでグループ名を設定する必要があります。ユーザは、ユーザ名が LDAP サーバで設定されたこのグループのメンバとして示されている場合にだけ、公開キー認証を通じてログインできます。
ステップ 6	switch(config-ldap)# **enable Cert-DN-matc**h	(任意)ユーザ プロファイルでユーザ証明書のサブジェクト DN がログイン可能と示されている場合にだけユーザがログインできるようにします。

	コマンド	目的
ステップ 7	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 8	switch# **show ldap-server groups**	(任意)LDAP サーバ グループの設定を表示します。
ステップ 9	switch# **show run ldap**	(任意)LDAP の設定を表示します。
ステップ 10	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グローバルな LDAP タイムアウト間隔の設定

Cisco NX-OS デバイスがすべての LDAP サーバからの応答を待つ時間を決定するグローバル タイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

グローバルな LDAP タイムアウト間隔を設定するには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap-server timeout 10**	LDAP サーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 4	switch# **show ldap-server**	(任意)LDAP サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが LDAP サーバからの応答を待つ時間を決定するタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

LDAP サーバにタイムアウト間隔を設定するには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap-server host server1 timeout 10**	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 (注)　特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。

ステップ 4	switch# **show ldap-server**	(任意)LDAP サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グローバル LDAP サーバ ポートの設定

クライアントが TCP 接続を開始するグローバル LDAP サーバ ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

グローバルな LDAP サーバ ポートを設定するには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap-server port 2**	サーバへの LDAP メッセージに使用するグローバル TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 4	switch# **show ldap-server**	(任意)LDAP サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、LDAP サーバ用に別の TCP ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

TCP ポートを設定するには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap-server host 10.10.1.1 port 200 timeout 5**	サーバに送る LDAP メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。任意でサーバのタイムアウト間隔を指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です(グローバル値が設定されていない場合は 5 秒)。 **(注)**　特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。

ステップ 4	switch# **show ldap-server**	(任意)LDAP サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP 検索マップの設定

検索クエリーを LDAP サーバに送信するように LDAP 検索マップを設定できます。サーバはそのデータベースで、検索マップで指定された基準を満たすデータを検索します。

LDAP 検索マップを設定するには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap search-map map1** switch(config-ldap-search-map)#	LDAP 検索マップを設定します。
ステップ 3	例 1: switch(config-ldap-search-map)# **userprofile attribute-name description search-filter "(&(objectClass=inetOrgPerson)(cn=$userid))" base-DN dc=acme,dc=com** 例 2: switch(config-ldap-search-map)# **userprofile attribute-name "memberOf" search-filter "(&(objectClass=inetOrgPerson)(cn=$userid))" base-DN dc=acme,dc=com**	(任意)ユーザ プロファイル、信頼できる証明書、CRL、証明書 DN 一致、公開キー一致、または user-switchgroup ルックアップ検索操作の属性名、検索フィルタ、およびベース DN を設定します。これらの値は、検索クエリーを LDAP サーバに送信するために使用されます。 ユーザがメンバーとして所属しているグループを指定します。
ステップ 4	switch(config-ldap-search-map)# **exit** switch(config)#	LDAP 検索マップ コンフィギュレーション モードを終了します。
ステップ 5	switch(config)# **show ldap-search-map**	(任意)設定された LDAP 検索マップを表示します。
ステップ 6	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP デッド タイム間隔の設定

すべての LDAP サーバのデッド タイム間隔を設定できます。デッド タイム間隔では、Cisco NX-OS デバイスが LDAP サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。

(注)　デッド タイム間隔に 0 分を設定すると、LDAP サーバは、応答を返さない場合でも、デッドとしてマークされません。デッド タイム間隔はグループ単位で設定できます。

LDAP のデッド タイム間隔を設定するには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ldap-server deadtime 5**	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。範囲は 1 ～ 60 分です。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 4	switch# **show ldap-server**	(任意)LDAP サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

LDAP サーバに AAA 許可を設定するには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2**	LDAP サーバのデフォルトの AAA 許可方式を設定します。 **ssh-certificate** キーワードは、証明書認証を使用した LDAP 許可またはローカル許可を設定し、ssh-publickey キーワードは、**SSH 公開キー**を使用した LDAP 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。 group-list 引数は、スペースで区切られた LDAP サーバ グループ名のリストです。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local** 方式では、許可にローカル データベースが使用されます。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 4	switch(config)# **show aaa authorization**	(任意)AAA 許可の設定を表示します。all キーワードは、デフォルト値を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

LDAP のディセーブル化

LDAP をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

LDAP をディセーブルにするには、次の手順を実行します。

ステップ 1	switch# **configure terminal** switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ldap**	LDAP をディセーブルにします。
ステップ 3	switch(config)# **exit** switch#	設定モードを終了します。
ステップ 4	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

このコマンドの出力フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference, Release 5.0(1a)*』を参照してください。

LDAP の設定例

次に、LDAP サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
    server 10.10.2.2
exit
show ldap-server
show ldap-server groups
```

次に、LDAP 検索マップを設定する例を示します。

```
ldap search-map s0
userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
exit
show ldap-search-map
```

次に、LDAP サーバに対する証明書認証を使用して AAA 許可を設定する例を示します。

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

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。

- ログイン時にユーザによる RADIUS サーバの指定を許可(4-29 ページ)

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 サーバのアドレスの設定

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。

ホスト RADIUS サーバの IPv4 アドレスおよびその他のオプションを指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server host 10.10.0.0 key HostKey`	選択した RADIUS サーバの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは 10.10.0.0 で、キーは HostKey です。
ステップ 3	`switch(config)# radius-server host 10.10.0.0 auth-port 2003`	RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは 10.10.0.0 で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ～ 65366 です。
ステップ 4	`switch(config)# radius-server host 10.10.0.0 acct-port 2004`	RADIUS アカウンティング メッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティング ポートは 1813 で、有効な範囲は 0 ～ 65366 です。
ステップ 5	`switch(config)# radius-server host 10.10.0.0 accounting`	アカウンティングの目的のみに使用されるこのサーバを指定します。 （注）　**authentication** と **accounting** オプションのどちらも指定しないと、サーバは認証およびアカウンティングの両方の目的に使用されます。
ステップ 6	`switch(config)# radius-server host 10.10.0.0 key 0 abcd`	指定したサーバのクリア テキスト キーを指定します。キーの長さは 64 文字に制限されています。
	`switch(config)# radius-server host 10.10.0.0 key 4 da3Asda2ioyuoiuH`	指定したサーバの暗号化キーを指定します。キーの長さは 64 文字に制限されています。

ホスト RADIUS サーバの IPv6 アドレスおよびその他のオプションを指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server host 2001:0DB8:800:200C::417A Key HostKey`	選択した RADIUS サーバの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは 2001:0DB8:800:200C::417A で、キーは HostKey です。
ステップ 3	`switch(config)# radius-server host 2001:0DB8:800:200C::417A auth-port 2003`	RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは 2001:0DB8:800:200C::417A で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ～ 65366 です。
ステップ 4	`switch(config)# radius-server host 2001:0DB8:800:200C::417A acct-port 2004`	RADIUS アカウンティング メッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティング ポートは 1813 で、有効な範囲は 0 ～ 65366 です。
ステップ 5	`switch(config)# radius-server host 2001:0DB8:800:200C::417A accounting`	アカウンティングの目的のみに使用されるこのサーバを指定します。 (注)　**authentication** と **accounting** オプションのどちらも指定しないと、サーバは認証およびアカウンティングの両方の目的に使用されます。
ステップ 6	`switch(config)# radius-server host 2001:0DB8:800:200C::417A key 0 abcd`	指定したサーバのクリア テキスト キーを指定します。キーの長さは 64 文字に制限されています。
	`switch(config)# radius-server host 2001:0DB8:800:200C::417A key 4 da3Asda2ioyuoiuH`	指定したサーバの暗号化キーを指定します。キーの長さは 64 文字に制限されています。

ホスト RADIUS サーバの DNS 名およびその他のオプションを指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server host radius2 key HostKey`	選択した RADIUS サーバの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは radius2 で、キーは HostKey です。
ステップ 3	`switch(config)# radius-server host radius2 auth-port 2003`	RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは radius2 で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ～ 65366 です。

	コマンド	目的
ステップ 4	`switch(config)# radius-server host radius2 acct-port 2004`	RADIUS アカウンティング メッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティング ポートは 1813 で、有効な範囲は 0 ～ 65366 です。
ステップ 5	`switch(config)# radius-server host radius2 accounting`	アカウンティングの目的のみに使用されるこのサーバを指定します。 （注）　**authentication** と **accounting** オプションのどちらも指定しないと、サーバは認証およびアカウンティングの両方の目的に使用されます。
ステップ 6	`switch(config)# radius-server host radius2 key 0 abcd`	指定したサーバのクリア テキスト キーを指定します。キーの長さは 64 文字に制限されています。
	`switch(config)# radius-server host radius2 key 4 da3Asda2ioyuoiuH`	指定したサーバの暗号化キーを指定します。キーの長さは 64 文字に制限されています。

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）。グローバル鍵は、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、**radius-server host** コマンドで個々の RADIUS サーバの設定時に **key** オプションを明示的に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

RADIUS 事前共有キーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server key AnyWord`	RADIUS クライアントおよびサーバ間の通信を認証する事前共有キー（AnyWord）を設定します。デフォルトはクリア テキストです。
	`switch(config)# radius-server key 0 AnyWord`	RADIUS クライアントとサーバ間の通信を認証する、クリア テキスト（0 で指定）で記述された事前共有キー（AnyWord）を設定します。
	`switch(config)# radius-server key 7 abe4DFeeweo00o`	RADIUS クライアントとサーバ間の通信を認証する、暗号化テキスト（7 で指定）で指定された事前共有キー（暗号化テキストで指定）を設定します。

RADIUS サーバのタイムアウト間隔の設定

すべての RADIUS サーバに対して送信間のグローバル タイムアウト値を設定できます。

（注）　タイムアウト値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値よりもそれらの値が優先されます。

RADIUS サーバへの再送信間のタイムアウト値を指定するには、次の手順を実行してください。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server timeout 30`	スイッチがタイムアウト障害を宣言する前に、すべての RADIUS+ サーバからの応答を待機する、スイッチのグローバル タイムアウト期間（秒）を設定します。指定できる範囲は 1 ～ 1440 秒です。
	`switch(config)# no radius-server timeout 30`	送信時間をデフォルト値（1 秒）に戻します。

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。

RADIUS サーバがユーザを認証する試行回数を指定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server retransmit 3`	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（3）を設定します。
	`switch(config)# no radius-server retransmit`	デフォルトの試行回数（1）に戻します。

RADIUS サーバ モニタリング パラメータの設定

RADIUS サーバをモニタするためのパラメータを設定できます。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。

この項では、次のトピックについて取り上げます。

- テスト アイドル タイマーの設定（4-27 ページ）
- テスト ユーザ名の設定（4-27 ページ）
- デッド タイマーの設定（4-27 ページ）

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。

アイドル タイマーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server host 10.1.1.1 test idle-time 20`	テスト用のアイドル間隔の値を分で設定します。有効な範囲は 1 ～ 1440 分です。
ステップ 3	`switch(config)# no radius-server host 10.1.1.1 test idle-time 20`	デフォルト値(0 分)に戻します。

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を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server host 10.1.1.1 test username testuser`	テスト ユーザ(testuser)にデフォルトのパスワード(test)を設定します。デフォルトのユーザ名は test です。
	`switch(config)# no radius-server host 10.1.1.1 test username testuser`	テスト ユーザ名(testuser)を削除します。
	`switch(config)# radius-server host 10.1.1.1 test username testuser password Ur2Gd2BH`	テスト ユーザ(testuser)を設定し、強力なパスワードを割り当てます。

デッド タイマーの設定

デッド タイマーには、MDS スイッチが、RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを確認するためにテスト パケットを送信するまでの間隔を指定します。

(注)　デフォルトのデッド タイマー値は 0 分です。デッド タイマーの間隔が 0 分の場合、RADIUS サーバがサーバ グループの一部でグループのデッド タイム インターバルが 0 分を超えていないかぎり、RADIUS サーバ モニタリングは実行されません。(「サーバ グループ」セクション (4-5 ページ) を参照してください)。

(注)　デッド RADIUS サーバに RADIUS テスト メッセージが送信される前に、同サーバのデッド タイマーの期限が切れた場合、同サーバがまだ応答していないとしても再度アライブ状態としてマークされます。このシナリオを回避するには、デッド タイマーの時間よりも短いアイドル時間でテスト ユーザを設定します。

デッド タイマーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server deadtime 30`	デッド タイマー間隔値を分で設定します。有効な範囲は 1 ～ 1440 分です。
ステップ 3	`switch(config)# no radius-server deadtime 30`	デフォルト値 (0 分) に戻します。

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。

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 モニタリング パラメータの設定 (4-22 ページ) 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 モニタリング パラメータの設定（4-22 ページ）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。

モニタリング用 RADIUS テスト メッセージの送信

RADIUS サーバをモニタするテスト メッセージを手動で送信できます。

RADIUS サーバにテスト メッセージを送信するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# test aaa server radius 10.10.1.1 test test`	デフォルトのユーザ名（test）とパスワード（test）を使用して RADIUS サーバにテスト メッセージを送信します。
	`switch# test aaa server radius 10.10.1.1 testuser Ur2Gd2BH`	設定されたテスト ユーザ名（testuser）とパスワード（Ur2Gd2BH）を使用して RADIUS サーバにテスト メッセージを送信します。 (注)　設定済みのユーザ名およびパスワードはオプションです（「テスト ユーザ名の設定」セクション（4-27 ページ）を参照）。

ログイン時にユーザによる RADIUS サーバの指定を許可

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。

(注)　ユーザ指定のログインは Telnet セッションに限りサポートされます。

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。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server directed-request`	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。
	`switch(config)# no radius-server directed-request`	サーバ グループの最初のサーバに認証要求を送信するように戻します(デフォルト)。

RADIUS への誘導要求設定を表示するには、**show tacacs-server directed-request** コマンドを使用できます。

```
switch# show radius-server directed-request
disabled
```

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 separator value *
```

protocol は、特定の認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、認証結果とともに認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 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: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 NX-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** 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。

RADIUS サーバの詳細の表示

設定された RADIUS パラメータを例 4-4 に示されているように表示するには、**show radius-server** コマンドを使用します。

例 4-4　　設定された RADIUS 情報の表示

```
switch# show radius-server
Global RADIUS shared secret:*******
retransmission count:5
timeout value:10
following RADIUS servers are configured:
        myradius.cisco.users.com:
                available for authentication on port:1812
                available for accounting on port:1813
        172.22.91.37:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
```

例 4-5　設定済みの RADIUS サーバ グループ順序の表示

```
switch# show radius-server groups
total number of groups:4
following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
        group Group1:
                server: Server3 on auth-port 1812, acct-port 1813
                server: Server5 on auth-port 1812, acct-port 1813
        group Group5:
```

RADIUS サーバの統計情報の表示

show radius-server statistics コマンドを使用して、RADIUS サーバの統計情報を表示できます。

例 4-6　RADIUS サーバ統計情報の表示

```
switch# show radius-server statistics 10.1.3.2
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessful transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        successful transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors:
```

clear radius-server statistics 10.1.3.2 コマンドを使用して、RADIUS サーバの統計情報をクリアできます。

ワンタイム パスワード サポート

ワンタイム パスワード サポート（OTP）は、1 回のログイン セッションまたはトランザクションに有効なパスワードです。OTP は、通常の（スタティック）パスワードに関連する多数の欠点を回避します。OTP によって対処される最も重大な欠点は、リプレイ攻撃のリスクにさらされないことです。すでにサービスへのログインまたは操作の実行に使用された OTP を侵入者が記録しようとしても、OTP は有効ではなくなっているため、悪用されません。

ワンタイム パスワードは RADIUS や TACACS プロトコル デーモンに対してのみ適用できます。RADIUS プロトコル デーモンの場合、スイッチ側からの設定はありません。TACACS プロトコルの場合、次のコマンドで使用できる ascii 認証モードを有効にする必要があります。

```
aaa authentication login ascii-authentication
```

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（4-33 ページ）
- TACACS+ サーバのデフォルト設定（4-34 ページ）
- 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（4-34 ページ）
- TACACS+ のイネーブル化（4-34 ページ）
- 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（4-26 ページ）
- TACACS+ サーバのアドレスの設定（4-34 ページ）
- グローバル秘密キーの設定（4-36 ページ）
- 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（4-37 ページ）
- タイムアウト値の設定（4-37 ページ）
- TACACS+ サーバの概要（4-37 ページ）
- TACACS+ サーバ モニタリング パラメータの設定（4-33 ページ）
- TACACS+ サーバの検証の概要（4-40 ページ）
- RADIUS サーバの統計情報の表示（4-32 ページ）
- モニタリング用 TACACS+ テスト メッセージの送信（4-39 ページ）
- TACACS+ サーバからのパスワード エージング通知（4-40 ページ）
- ユーザによるログイン時の TACACS+ サーバ指定の概要（4-41 ページ）
- ユーザによるログイン時の TACACS+ サーバ指定の許可（4-41 ページ）
- ロールのカスタム属性の定義（4-42 ページ）
- サポートされている TACACS+ サーバ パラメータ（4-42 ページ）
- TACACS+ サーバの詳細の表示（4-42 ページ）

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、認可を実行できます。
- 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）。グローバル鍵を設定して、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にできます。

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+ のイネーブル化

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。ファブリック認証に関するコンフィギュレーション コマンドと検証コマンドを使用するには、TACACS+ 機能を明示的にイネーブルにする必要があります。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

Cisco MDS スイッチの TACACS+ をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# feature tacacs+`	このスイッチの TACACS+ をイネーブルにします。
	`switch(config)# no feature tacacs+`	このスイッチの TACACS+ をディセーブル（デフォルト）にします。

TACACS+ サーバのアドレスの設定

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（「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」セクション（4-37 ページ）を参照）。

（注）　グローバル秘密キーにはドル記号（$）、パーセント記号（%）を使用できます。

TACACS+ サーバの IPv4 アドレスおよびその他のオプションを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server host 171.71.58.91`	指定の IPv4 アドレスによって識別される TACACS+ サーバを設定します。
	`switch(config)# no tacacs-server host 171.71.58.91`	IPv4 アドレスによって識別される特定の TACACS+ サーバを削除します。デフォルトでは、サーバは設定されません。
ステップ 3	`switch(config)# tacacs-server host 171.71.58.91 port 2`	すべての TACACS+ 要求に対し TCP ポートを設定します。
	`switch(config)# no tacacs-server host 171.71.58.91 port 2`	サーバ アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。
ステップ 4	`switch(config)# tacacs-server host 171.71.58.91 key MyKey`	指定されたドメイン名で指定された TACACS+ サーバを設定し、秘密キーを割り当てます。
ステップ 5	`switch(config)# tacacs-server host 171.71.58.91 timeout 25`	スイッチがタイムアウト障害を宣言する前に、指定したサーバからの応答を待機する、スイッチのタイムアウト期間を設定します。

TACACS+ サーバの IPv6 アドレスおよびその他のオプションを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A` `warning: no key is configured for the host`	指定の IPv6 アドレスによって識別される TACACS+ サーバを設定します。
	`switch(config)# no tacacs-server host 2001:0DB8:800:200C::417A`	IPv6 アドレスによって識別される特定の TACACS+ サーバを削除します。デフォルトでは、サーバは設定されません。
ステップ 3	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A port 2`	すべての TACACS+ 要求に対し TCP ポートを設定します。
	`switch(config)# no tacacs-server host 2001:0DB8:800:200C::417A port 2`	サーバ アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。
ステップ 4	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A key MyKey`	指定されたドメイン名で指定された TACACS+ サーバを設定し、秘密キーを割り当てます。
ステップ 5	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A timeout 25`	スイッチがタイムアウト障害を宣言する前に、指定したサーバからの応答を待機する、スイッチのタイムアウト期間を設定します。

TACACS+ サーバの DNS 名およびその他のオプションを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server host host1.cisco.com` `warning: no key is configured for the host`	指定の DNS 名によって識別される TACACS+ サーバを設定します。
	`switch(config)# no tacacs-server host host1.cisco.com`	指定の DNS 名によって識別される TACACS+ サーバを削除します。デフォルトでは、サーバは設定されません。
ステップ 3	`switch(config)# tacacs-server host host1.cisco.com port 2`	すべての TACACS+ 要求に対し TCP ポートを設定します。
	`switch(config)# no tacacs-server host host1.cisco.com port 2`	サーバ アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。
ステップ 4	`switch(config)# tacacs-server host host1.cisco.com key MyKey`	指定されたドメイン名で指定された TACACS+ サーバを設定し、秘密キーを割り当てます。
ステップ 5	`switch(config)# tacacs-server host host1.cisco.com timeout 25`	スイッチがタイムアウト障害を宣言する前に、指定したサーバからの応答を待機する、スイッチのタイムアウト期間を設定します。

グローバル秘密キーの設定

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。

(注)　グローバル秘密キーにはドル記号($)、パーセント記号(%)を使用できます。

TACACS+ サーバの秘密キーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server key 7 3sdaA3daKUngd`	TACACS+ サーバにアクセスするには、グローバル秘密キー(暗号化形式)を割り当てます。この例では、使用されている暗号化された形式を表示するのに **7** を指定します。このグローバル キーと各サーバ キーが設定されていない場合、クリア テキスト メッセージが TACACS+ サーバに送信されます。
	`switch(config)# no tacacs-server key oldPword`	設定されたグローバル秘密キーを TACACS+ サーバにアクセスするために削除し、すべての設定済みのサーバへのアクセスを許可する工場出荷時のデフォルトに戻します。

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。

タイムアウト値の設定

すべての TACACS+ サーバに対して送信間のグローバル タイムアウト値を設定できます。

(注)　タイムアウト値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値よりもそれらの値が優先されます。

TACACS+ サーバのグローバル タイムアウト値を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server timeout 30`	スイッチがタイムアウト障害を宣言する前に、すべての TACACS+ サーバからの応答を待機する、スイッチのグローバル タイムアウト期間（秒）を設定します。指定できる範囲は 1 ～ 1440 秒です。
	`switch(config)# no tacacs-server timeout 30`	設定済みのタイムアウト期間を削除し、工場出荷時のデフォルトである 5 秒に戻します。

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 リリース 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 モニタリング パラメータの設定

TACACS+ サーバをモニタするためのパラメータを設定できます。

この項では、次のトピックについて取り上げます。

- TACACS+ テスト アイドル タイマーの設定（4-38 ページ）
- テスト ユーザ名の設定（4-38 ページ）
- デッド タイマーの設定（4-39 ページ）

TACACS+ 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 TACACS+ 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 タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

アイドル タイマーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server host 10.1.1.1 test idle-time 20`	テスト用のアイドル間隔の値を分で設定します。有効な範囲は 1 ～ 1440 分です。
ステップ 3	`switch(config)# no tacacs-server host 10.1.1.1 test idle-time 20`	デフォルト値（0 分）に戻します。

テスト ユーザ名の設定

定期的な TACACS+ 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。TACACS+ サーバを監視するための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。

定期的な TACACS+ 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を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server host 10.1.1.1 test username testuser`	テスト ユーザ（testuser）にデフォルトのパスワード（test）を設定します。デフォルトのユーザ名は test です。
	`switch(config)# no tacacs-server host 10.1.1.1 test username testuser`	テスト ユーザ（testuser）を削除します。
	`switch(config)# tacacs-server host 10.1.1.1 test username testuser password Ur2Gd2BH`	テスト ユーザ（testuser）を設定し、強力なパスワードを割り当てます。

デッド タイマーの設定

デッド タイマーには、MDS スイッチが、TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを確認するためにテスト パケットを送信するまでの間隔を指定します。

(注)　デフォルトのデッド タイマー値は 0 分です。TACACS+ サーバ モニタリングは、TACACS+ サーバがデッド タイム インターバルが 0 分よりも長い、より大きなグループの一部でない限り、デッド タイマーの間隔が 0 分であれば実行されません。(「RADIUS サーバ モニタリング パラメータの設定」セクション(4-22 ページ) を参照)。

(注)　デッド TACACS+ サーバに TACACS+ テスト メッセージが送信される前に、同サーバのデッド タイマーの期限が切れた場合、同サーバがまだ応答していないとしても再度アライブ状態としてマークされます。このシナリオを回避するには、デッド タイマーの時間よりも短いアイドル時間でテスト ユーザを設定します。

デッド タイマーを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server deadtime 30`	デッド タイム インターバル値を分で設定します。有効な範囲は 1 ～ 1440 分です。
	`switch(config)# no tacacs-server deadtime 30`	デフォルト値(0 分)に戻します。 (注)　デッド タイム インターバルが 0 分の場合、TACACS+ サーバがサーバ グループの一部でグループのデッド タイム インターバルが 0 分を超えていないかぎり、TACACS+ サーバ モニタリングは実行されません。(「RADIUS サーバ モニタリング パラメータの設定」セクション(4-22 ページ)を参照してください)。

モニタリング用 TACACS+ テスト メッセージの送信

TACACS+ サーバをモニタするテスト メッセージを手動で送信できます。

TACACS+ サーバにテスト メッセージを送信するには、次の手順を実行します。

コマンド	目的
`switch# test aaa server tacacs+ 10.10.1.1 test`	デフォルトのユーザ名(test)とパスワード(test)を使用して TACACS+ サーバにテスト メッセージを送信します。
`switch# test aaa server tacacs+ 10.10.1.1 testuser Ur2Gd2BH`	設定されたテスト ユーザ名とパスワードを使用して TACACS+ サーバにテスト メッセージを送信します。 設定済みのユーザ名およびパスワードはオプションです(「テスト ユーザ名の設定」セクション(4-38 ページ)を参照)。

TACACS+ サーバからのパスワード エージング通知

パスワード エージング通知は、ユーザが TACACS+ アカウント経由で Cisco MDS 9000 スイッチに認証すると開始されます。パスワードの期限切れが近い、または期限が切れたときは、ユーザに通知されます。パスワードの期限が切れると、ユーザはパスワードを変更するように求められます。

（注）　Cisco MDS SAN-OS Release 3.2(1) では、TACACS+ だけがパスワード エージング通知をサポートしています。この機能をイネーブルにして RADIUS サーバを使用しようとすると、RADIUS は SYSLOG メッセージを生成し、認証はローカル データベースにフォールバックします。

パスワード エージング通知により、次の操作が容易になります。

- パスワードの変更: 空のパスワードを入力することによってパスワードを変更できます。
- パスワード エージング通知: パスワード エージングを通知します。通知は、AAA サーバが構成され、MSCHAP および MSCHAPv2 がディセーブルになっている場合にだけ発生します。
- 期限切れ後のパスワードの変更: 古いパスワードの期限が切れたら、パスワードの変更を開始します。AAA サーバから開始します。

（注）　MSCHAP および MSCHAPv2 認証をディセーブルにしていない場合、パスワード エージング通知は失敗します。

AAA サーバのパスワード エージング オプションをイネーブルにするには、次のコマンドを入力します。

```
aaa authentication login ascii-authentication
```

パスワード エージング通知を AAA サーバで有効または無効になっているかどうかを確認するには、次のコマンドを入力します。

```
show aaa authentication login ascii-authentication
```

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」セクション（4-33 ページ）を参照してください。

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。

（注）　ユーザ指定のログインは Telnet セッションに限りサポートされます

ユーザによるログイン時の TACACS+ サーバ指定の許可

MDS スイッチにログインしているユーザが認証用の TACACS+ サーバを選択できるようにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server directed-request`	ログイン時に、ユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。
	`switch(config)# no tacacs-server directed-request`	サーバ グループの最初のサーバに認証要求を送信するように戻します（デフォルト）。

TACACS+ への誘導要求設定を表示するには、**show tacacs-server directed-request** コマンドを使用できます。

```
switch# show tacacs-server directed-request
disabled
```

Cisco Secure ACS 5.x GUI でのロールの定義

ポリシー要素の GUI で次を入力します。

表 4-3　ロールの定義

属性	要件	値
shell:roles	任意	network-admin

ロールのカスタム属性の定義

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。

サポートされている TACACS+ サーバ パラメータ

Cisco NX-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"
  ```

TACACS+ サーバの詳細の表示

例 4-7 から 4-12 に示すように、Cisco MDS 9000 ファミリ内のすべてのスイッチの TACACS+ サーバの設定に関する情報を表示するには、**show aaa** および **show tacacs-server** コマンドを使用します。

例 4-7　TACACS+ サーバ情報の表示

```
switch# show tacacs-server
Global TACACS+ shared secret:***********
timeout value:30
total number of servers:3

following TACACS+ servers are configured:
        171.71.58.91:
                available on port:2
        cisco.com:
                available on port:49
        171.71.22.95:
                available on port:49
                TACACS+ shared secret:*****
```

例 4-8　AAA 認証情報の表示

```
switch# show aaa authentication
         default: group TacServer local none
         console: local
         iscsi: local
         dhchap: local
```

例 4-9　AAA 認証ログイン情報の表示

```
switch# show aaa authentication login error-enable
enabled
```

例 4-10　設定した TACACS+ サーバ グループの表示

```
switch# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group TacServer:
                server 171.71.58.91 on port 2
        group TacacsServer1:
                server ServerA on port 49
                server ServerB on port 49:
```

例 4-11　すべての AAA サーバ グループの表示

```
switch# show aaa groups
radius
TacServer
```

例 4-12　TACACS+ サーバの統計情報の表示

```
switch# show tacacs-server statistics 10.1.2.3
Server is not monitored

Authentication Statistics
        failed transactions: 0
        successful transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

```
Authorization Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        successful transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

TACACS+ サーバ統計情報のクリア

clear tacacs-server statistics 10.1.2.3 コマンドを使用してすべての TACACS+ サーバの統計情報をクリアできます。

サーバ グループの設定

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」セクション（4-6 ページ）を参照してください）。

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（4-44 ページ）
- サーバ グループの設定（4-44 ページ）

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。

RADIUS サーバ グループを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa group server radius RadServer` `switch(config-radius)#`	RadServer という名前のサーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。
	`switch(config)# no aaa group server radius RadServer`	認証リストから RadServer という名前のサーバ グループを削除します。

	コマンド	目的
ステップ 3	`switch(config-radius)# server 10.71.58.91`	IPv4 アドレス 10.71.58.91 の RADIUS サーバをサーバ グループ RadServer 内で最初に実行されるように設定します。 ヒント　指定した RADIUS サーバが見つからない場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	`switch(config-radius)# server 2001:0DB8:800:200C::417A`	IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバをサーバ グループ RadServer 内で最初に実行されるように設定します。
	`switch(config-radius)# no server 2001:0DB8:800:200C::417A`	IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバをサーバ グループ RadServer から削除します。
ステップ 5	`switch(config-radius)# exit`	コンフィギュレーション モードに戻ります。
ステップ 6	`switch(config)# aaa group server radius RadiusServer` `switch(config-radius)#`	RadiusServer という名前のサーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。
ステップ 7	`switch(config-radius)# server ServerA`	ServerA を RadiusServer1 と呼ばれるサーバ グループ内で最初に試行されるように設定します。 ヒント　指定した RADIUS サーバが見つからない場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 8	`switch(config-radius)# server ServerB`	ServerB をサーバ グループ RadiusServer1 内で 2 番目に試行されるように設定します。
ステップ 9	`switch(config-radius)# deadtime 30`	モニタリングのデッド タイムを 30 分に設定します。指定できる範囲は 0 ～ 1440 です。 (注)　個別の RADIUS サーバのデッド タイム インターバルが 0 よりも大きい場合は、サーバ グループに設定された値よりもその値が優先されます。
	`switch(config-radius)# no deadtime 30`	デフォルト値(0 分)に戻します。 (注)　RADIUS サーバ グループおよび RADIUS サーバの個別の TACACS+ サーバの両方のデッドタイム間隔が 0 に設定されている場合、スイッチは定期モニタリングによって応答がないと判明した場合に RADIUS サーバをデッドとしてマークしません。さらにスイッチは、その RADIUS サーバに対するデッド サーバ モニタリングを実行しません。(「RADIUS サーバ モニタリング パラメータの設定」セクション(4-26 ページ)を参照してください)。

設定されたサーバ グループ順序を確認するには、**show radius-server groups** コマンドを使用します。

```
switch# show radius-server groups
total number of groups:2

following RAIDUS server groups are configured:
        group RadServer:
                server 10.71.58.91 on port 2
        group RadiusServer1:
                server ServerA on port 49
                server ServerB on port 49:
```

TACACS+ サーバ グループを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa group server tacacs+ TacacsServer1` `switch(config-tacacs+)#`	TacacsServer1 という名前のサーバ グループを作成し、そのグループのサブモードを開始します。
	`switch(config)# no aaa group server tacacs+ TacacsServer1`	認証リストから TacacsServer1 という名前のサーバ グループを削除します。
ステップ 3	`switch(config-tacacs+)# server ServerA`	ServerA を TacacsServer1 と呼ばれるサーバ グループ内で最初に試行されるように設定します。 ヒント　指定した TACACS+ サーバが見つからない場合は **tacacs-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	`switch(config-tacacs+)# server ServerB`	ServerB をサーバ グループ TacacsServer1 内で 2 番目に試行されるように設定します。
	`switch(config-tacacs+)# no server ServerB`	サーバの TacacsServer1 リスト内の ServerB を削除します。
ステップ 5	`switch(config-tacacs+)# deadtime 30`	モニタリングのデッド タイムを 30 分に設定します。指定できる範囲は 0 ～ 1440 です。 (注)　個別の TACACS+ サーバのデッド時間間隔が 0 よりも大きい場合は、サーバ グループに設定された値よりもその値が優先されます。
	`switch(config-tacacs+)# no deadtime 30`	デフォルト値(0 分)に戻します。 (注)　TACACS+ サーバ グループおよび TACACS+ サーバの個別の TACACS+ サーバの両方のデッド タイム間隔が 0 に設定されている場合、スイッチは定期モニタリングによって応答がないと判明した場合に TACACS+ サーバをデッドとしてマークしません。さらにスイッチは、その TACACS+ サーバに対するデッド サーバ モニタリングを実行しません。(TACACS+ サーバ モニタリング パラメータの設定(4-33 ページ)を参照してください)。

(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。配信はデフォルトで無効になっています（『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』および『*Cisco Fabric Manager System Management Configuration Guide*』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（4-48 ページ）
- スイッチでの配信セッションの開始（4-48 ページ）
- セッション ステータスの表示（4-48 ページ）

(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。

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。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius distribute`	このスイッチの RADIUS 設定の配信をイネーブルにします。
	`switch(config)# no radius distribute`	このスイッチの RADIUS 設定の配信をディセーブルにします(デフォルト)。

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。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs+ distribute`	このスイッチの TACACS+ 設定の配信をイネーブルにします。
	`switch(config)# no tacacs+ distribute`	このスイッチの TACACS+ 設定の配信をディセーブルにします(デフォルト)。

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] タブに配信状況を表示するには、**show radius** コマンドを使用します。

```
switch# show radius distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

暗黙的な配信 セッションが開始されると、**show tacacs+ distribution status** コマンドを使用してセッション ステータスを確認できます。

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

配信する保留中の設定の表示

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、**show radius pending** コマンドを使用して表示する手順は次のとおりです。

```
switch(config)# show radius pending-diff
   +radius-server host testhost1 authentication accounting
   +radius-server host testhost2 authentication accounting
```

一時バッファに保存された TACACS+ のグローバル設定またはサーバ設定を表示するには、**show tacacs+ pending** コマンドを使用します。

```
switch(config)# show tacacs+ pending-diff
   +tacacs-server host testhost3
   +tacacs-server host testhost4
```

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。

RADIUS の設定変更をコミットするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius commit`	実行コンフィギュレーションへの RADIUS の設定変更をコミットします。

TACACS+ の設定変更をコミットするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs+ commit`	実行コンフィギュレーションへの TACACS+ の設定変更をコミットします。

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。

RADIUS セッションの進行中の配信を廃棄する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius abort`	実行コンフィギュレーションへの RADIUS の設定変更を破棄します。

TACACS+ セッションの進行中の配信を廃棄する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs+ abort`	実行コンフィギュレーションへの TACACS+ の設定変更を破棄します。

セッションのクリア

継続的な CFS 配信セッション（ある場合）をクリアし、RADIUS 機能のファブリックを最大限に引き出すには、ファブリック内のすべてのスイッチから **clear radius session** コマンドを入力します。

```
switch# clear radius session
```

継続的な CFS 配信セッション（ある場合）をクリアし、TACACS+ 機能のファブリックを最大限に引き出すには、ファブリック内のすべてのスイッチから **clear tacacs+ session** コマンドを入力します。

```
switch# clear tacacs+ session
```

RADIUS および TACACS+ 設定のマージに関する注意事項

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)　テスト パラメータは、CFS を通じて、TACACS+ デーモンのためだけに配信されます。ファブリックに NX-OS リリース 5.0 スイッチだけが含まれる場合、テスト パラメータは配信されます。5.0 バージョンを実行しているスイッチと NX-OS 4.x リリースを実行しているスイッチがファブリックに含まれる場合、テスト パラメータは配信されません。

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。

show radius distribution status コマンドを使用して、RADIUS ファブリックのマージのステータスを参照できます（例 4-13 を参照）。

例 4-13　RADIUS ファブリックのマージのステータスの表示

```
switch# show radius distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge response received
merge error: conflict: server dmtest2 has auth-port 1812 on this switch and 1999
on remote

last operation: enable
last operation status: success
```

show tacacs+ distribution status コマンドを使用して、TACACS+ ファブリックのマージのステータスを参照できます（例 4-14 を参照）。

例 4-14　TACACS+ ファブリックのマージのステータスの表示

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge activation done

last operation: enable
last operation status: success
```

CHAP 認証

CHAP（チャレンジ ハンドシェイク認証プロトコル）は、業界標準の Message Digest 5（MD5）ハッシング スキームを使用して応答を暗号化するチャレンジレスポンス認証プロトコルです。CHAP は、さまざまなネットワーク アクセス サーバおよびクライアントのベンダーによって使用されています。ルーティングおよびリモート アクセスを実行しているサーバは、CHAP を必要とするリモート アクセス クライアントが認証されるように、CHAP をサポートしています。このリリースでは、認証方式として CHAP がサポートされています。

CHAP 認証のイネーブル化

CHAP 認証を有効にするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa authentication login chap enable`	CHAP ログイン認証をイネーブルにします。
	`switch# no aaa authentication login chap enable`	CHAP ログイン認証をディセーブルにします。

CHAP 認証の設定を表示するには、**show aaa authentication login chap** コマンドを使用できます。

```
switch# show aaa authentication login chap
chap is disabled
```

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。

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」セクション（4-30 ページ）を参照してください。表 4-4 に MSCHAP に必要な RADIUS ベンダー固有属性を示します。

表 4-4　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	MS-CHAP ユーザがチャレンジへの応答として提供したレスポンス値が格納されます。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

MSCHAP 認証をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa authentication login mschap enable`	MSCHAP ログイン認証をイネーブルにします。
ステップ 3	`switch# no aaa authentication login mschap enable`	MSCHAP ログイン認証をディセーブルにします。

MSCHAPv2 認証をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa authentication login mschapv2 enable`	MSCHAPv2 ログイン認証をイネーブルにします。
ステップ 3	`switch# no aaa authentication login mschapv2 enable`	MSCHAPv2 ログイン認証をディセーブルにします。

(注)　パスワード エージング、MSCHAPv2、および MSCHAP 認証は、これらの認証のいずれかがディセーブルでないと失敗する可能性があります。

(注)　TACACS+ サーバで MSCHAPv2 認証をイネーブルにするコマンドを実行すると、警告メッセージが表示され、設定が失敗します。

MSCHAP 認証設定を表示するには、**show aaa authentication login mschap** コマンドを使用できます。

```
switch# show aaa authentication login mschap
mschap is disabled
```

MSCHAPv2 認証設定を表示するには、show aaa authentication login mschapv2 コマンドを使用できます。

```
switch# show aaa authentication login mschapv2
mschapv2 is enabled
```

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。

ローカル ユーザとそのロールを設定するには、**username** コマンドを使用します。

ローカル アカウンティング ログを表示するには、**show accounting log** コマンドを使用します（例 4-15 を参照）。

例 4-15　アカウンティング ログ情報の表示

```
switch# show accounting log

Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=enabled telnet
Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=configure terminal ;
feature telnet (SUCCESS)
Thu Dec 10 06:19:35 2009:type=start:id=171.69.16.56@pts/1:user=admin:cmd=
Thu Dec 10 06:20:16 2009:type=stop:id=171.69.16.56@pts/1:user=admin:cmd=shell te
rminated gracefully
Thu Dec 10 06:20:20 2009:type=stop:id=console0:user=root:cmd=shell terminated gr
acefully
Thu Dec 10 06:29:37 2009:type=start:id=72.163.177.168@pts/1:user=admin:cmd=
Thu Dec 10 06:29:42 2009:type=update:id=72.163.177.168@pts/1:user=admin:cmd=pwd
(SUCCESS)
Thu Dec 10 06:32:49 2009:type=start:id=72.163.190.8@pts/2:user=admin:cmd=
```

AAA 認証のディセーブル化

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。

パスワード確認をディセーブルにするには、**aaa authentication login** コマンドで **none** オプションを使用します。

username コマンドを入力して作成したユーザは、Cisco MDS 9000 ファミリ スイッチのローカルに存在します。

AAA 認証の表示

show aaa authentication コマンドでは、設定された認証方式が例 4-16 のように表示されます。

例 4-16　認証情報の表示

```
switch# show aaa authentication

    No AAA Authentication
    default: group TacServer local none
    console: local none
    iscsi: local
    dhchap: local
```

アカウンティング サービスの設定

アカウンティングは、スイッチの管理セッションごとに保管されるログ情報を意味しています。この情報はトラブルシューティングと監査を目的としたレポートの生成に利用できます。アカウンティングは、(RADIUS を使用して) ローカルまたはリモートで実装できます。アカウンティング ログのデフォルトの最大サイズは 250,000 バイトです。これは変更できません。

ヒント　Cisco MDS 9000 ファミリ スイッチは、interim-update RADIUS アカウンティング要求パケットを使用して、アカウンティング ログ情報を RADIUS サーバに送信します。RADIUS サーバは、これらのパケットで送信された情報を記録するように、適切に設定されている必要があります。一部のサーバは、通常、AAA クライアントの設定内に log update/watchdog packets フラグを持ちます。適切な RADIUS アカウンティングを確実に実行するには、このフラグをオンにします。

(注)　コンフィギュレーション モードで実行された設定操作は、自動的にアカウンティング ログに記録されます。重要なシステム イベント (設定保存やシステム スイッチオーバーなど) もアカウンティング ログに記録されます。

アカウンティング設定の表示

設定したアカウント情報を表示するには **show accounting** コマンドを使用します。例 4-17 ～ 4-19 を参照してください。表示されるローカル アカウンティング ログのサイズを指定するには、**show accounting log** コマンドを使用します。デフォルトでは、アカウンティング ログの約 250 KB が表示されます。

例 4-17　設定されたアカウンティング パラメータの 2 つの例の表示

```
switch# show accounting config
show aaa accounting
               default: local

switch# show aaa accounting
               default: group rad1
```

例 4-18　60,000 バイトのアカウンティング ログの表示

```
switch# show accounting log 60000
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
...
```

例 4-19　ログ ファイル全体の表示

```
switch# show accounting log
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:17 1981:stop:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:start:snmp_348530298_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:stop:snmp_348530298_171.71.150.105:admin:
...
Fri Jan 16 23:37:02 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 23:37:26 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Fri Jan 16 23:53:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server3
Fri Jan 16 23:54:00 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server5
Fri Jan 16 23:54:22 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerA
Fri Jan 16 23:54:25 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerB
Fri Jan 16 23:55:03 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Sat Jan 17 00:01:41 1981:start:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:41 1981:stop:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:start:snmp_348537702_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:stop:snmp_348537702_171.71.58.100:admin:
...
```

アカウンティング ログのクリア

現在のログの内容を消去するには、**clear accounting log** コマンドを使用します。

```
switch# clear accounting log
```

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 4-3、図 4-4、図 4-5、および図 4-6 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。

図 4-3　RADIUS を使用する場合の network-admin ロールの設定

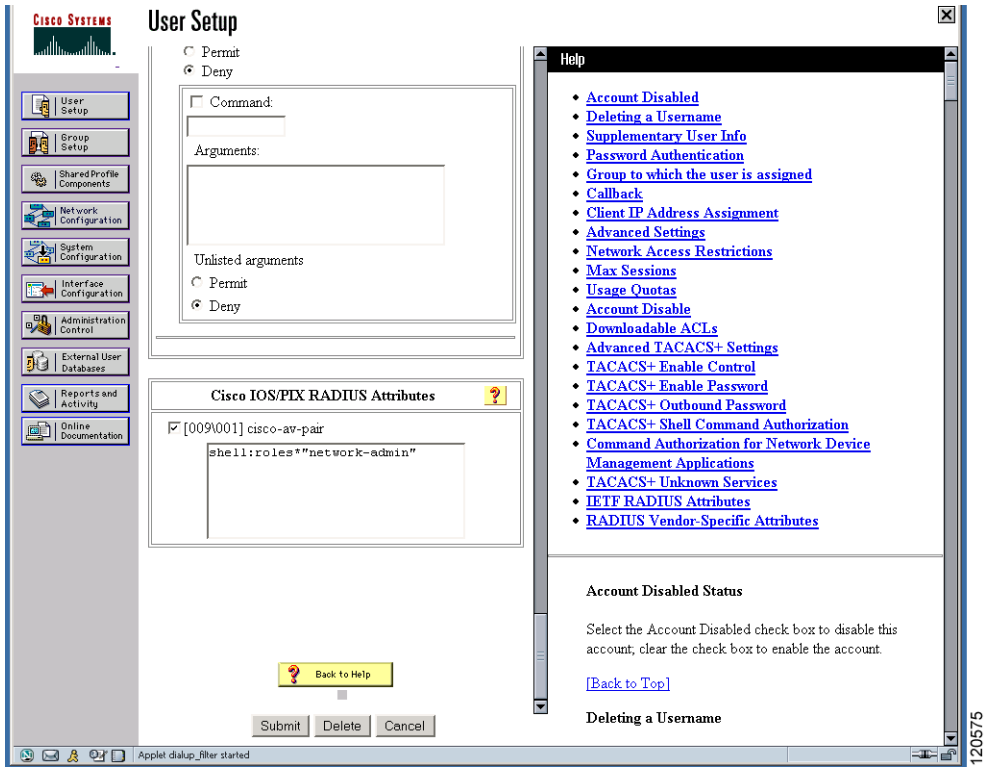


図 4-4　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

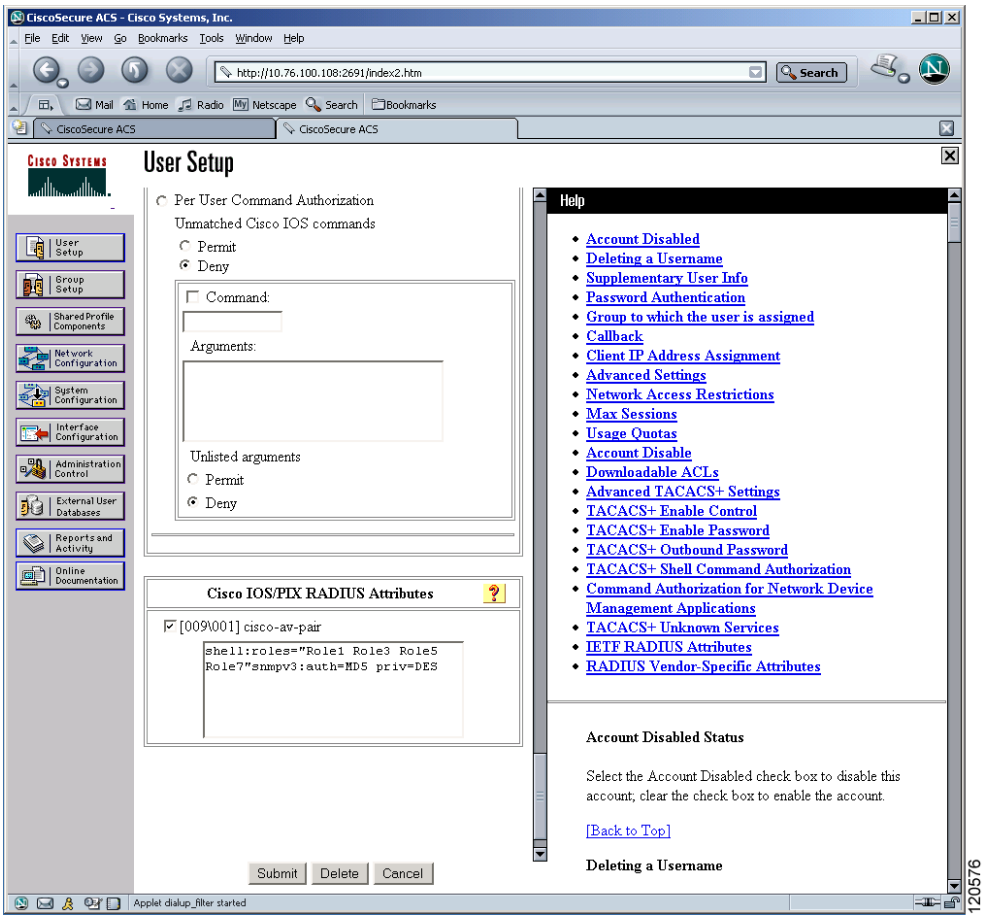


図 4-5　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

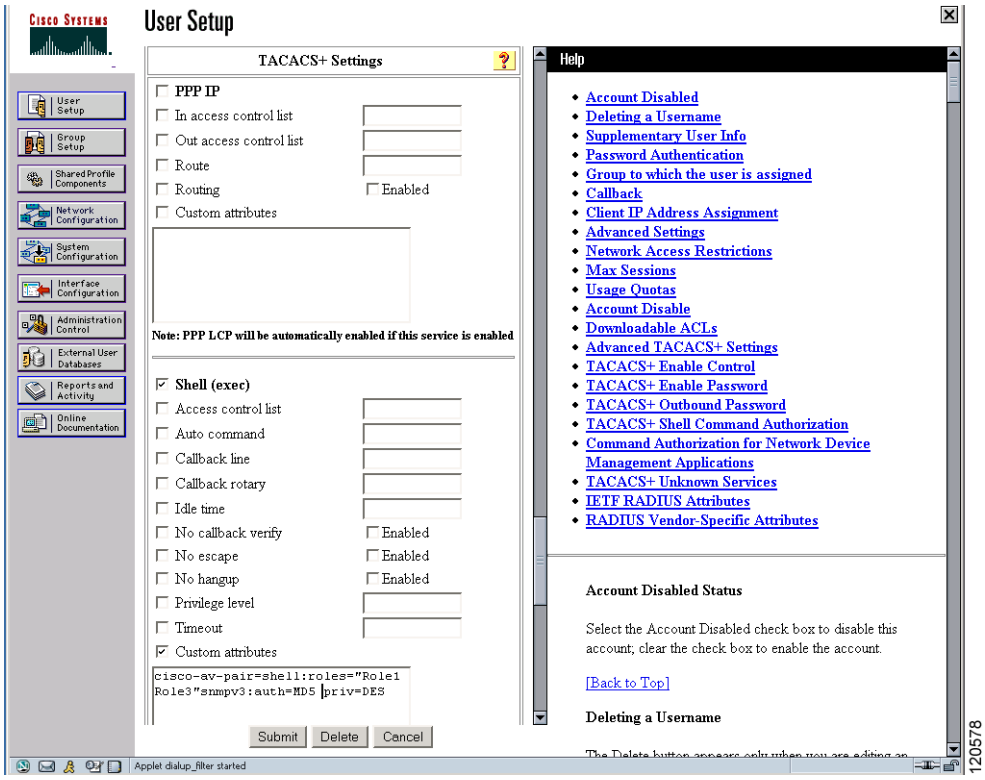
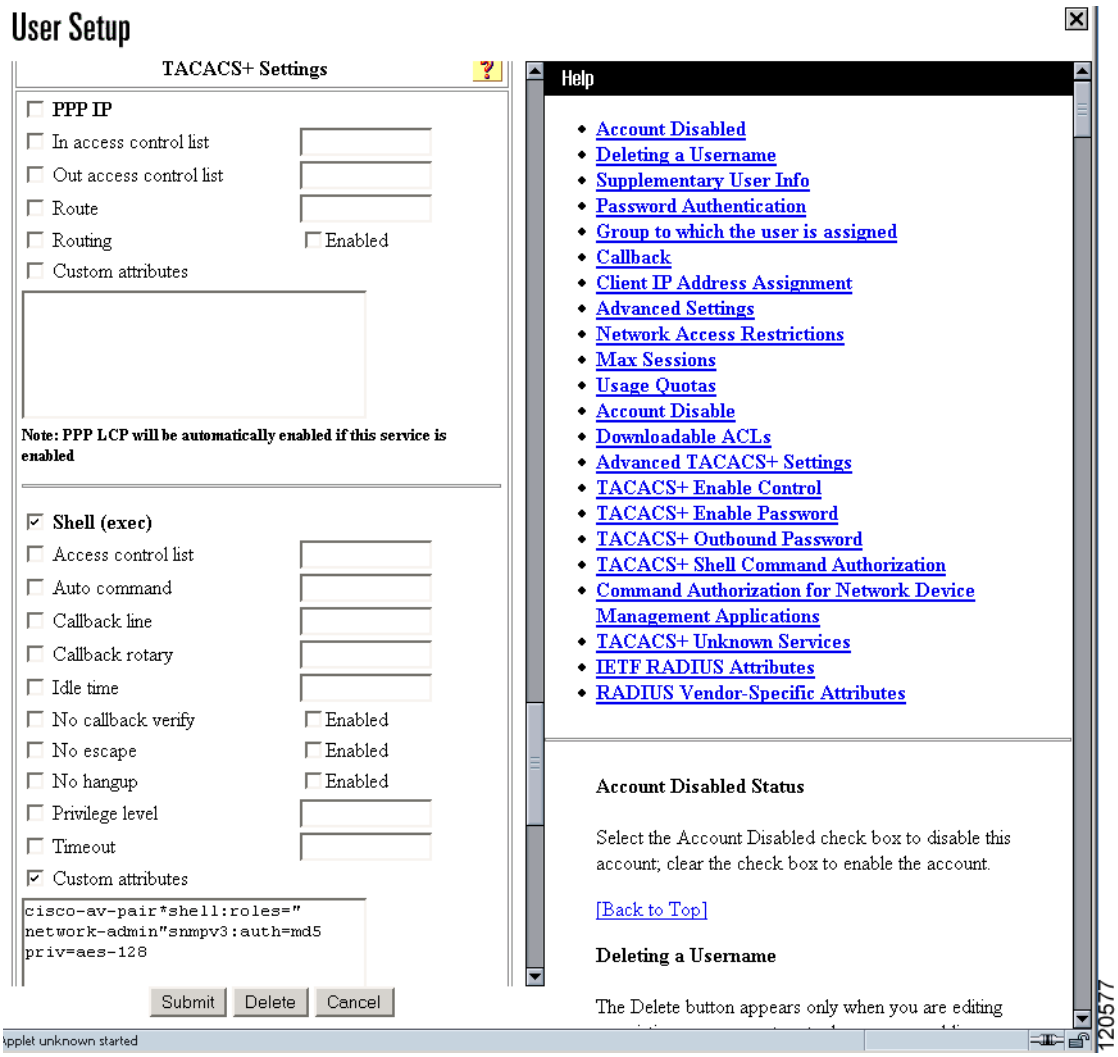


図 4-6　TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定



デフォルト設定

表 4-5 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 4-5　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	1812
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 4-5　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
許可	ディセーブル
デフォルトの AAA ユーザ ロール	enabled
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