外部 AAA サーバー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ーの ID 確認、アクセス権付与、およびアクション追跡を実行します。Cisco MDS 9000 ファミリのすべてのスイッチで、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルを使用することで、リモート AAA サーバーを使用するソリューションが実現されます。

指定されたユーザー 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 サーバーによる認可を実行します。スイッチと AAA サーバー間の通信は、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 サーバー、または特定の AAA サーバーに設定できます。このセキュリティ機能により、AAA サーバー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。

• デフォルト設定, on page 80

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。

このセクションは、次のトピックで構成されています。

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 サーバー モニタリング パラメータの設定, on page 32を参照してください。
  - TACACS+ を利用

    TACACS+ サーバー モニタリング パラメータの設定, on page 48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, on page 73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*』および『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください。
- Fibre Channel Security Protocol（FC-SP）認証

  「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。

このセクションは、次のトピックで構成されています。

認証

認証は、スイッチにアクセスするユーザー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ー 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 サーバーまたは TACACS+ サーバーを使用）を実行できます。

Note 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」）。

認証

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、すべてのユーザー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。

- ユーザー ロールをローカルに割り当てるか、またはリモート AAA サーバーを使用して、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 サーバーのユーザー 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 サーバーを通じてユーザーを認証したときに、自動的にダウンロードされ、使用されます。

Note ユーザー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、ユーザー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 サーバー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ー パスワード リストをより簡単に管理できます。
- AAA サーバー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ー 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 サーバーを使用する場合は、次の注意事項に従ってください。

- 最低 1 つの AAA サーバーが IP で到達可能になっている必要があります。
- すべての AAA サーバー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 サーバー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 サーバーに到達するイーサネット LAN に接続する必要があります。

サーバー 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 サーバーは、サーバー グループを使用して指定できます。サーバー グループは、同じ AAA プロトコルを実装するリモート AAA サーバーセットです。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ーからエラーを受信すると、次のサーバー グループのサーバーが試行されます。

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（「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、サーバー 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。

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

Note 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 サーバー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。ユーザーは、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ーのローカル 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。そのユーザーが認証されるのは、ローカルの認証設定にそのユーザー名とパスワードが存在する場合です。

次の表に、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。

***Table 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**

Note コンソールで認証方法を何も設定しない場合は、コンソールと Telnet または SSH の両方にデフォルトの認証方法が適用されます。

エラー対応ステータス

ログイン時にリモート AAA サーバーが応答しない場合、そのログインは、ローカル ユーザー 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表示するには、**show aaa authentication login error-enable** コマンドを使用します（次の例を参照）。

AAA 認証ログイン情報の表示

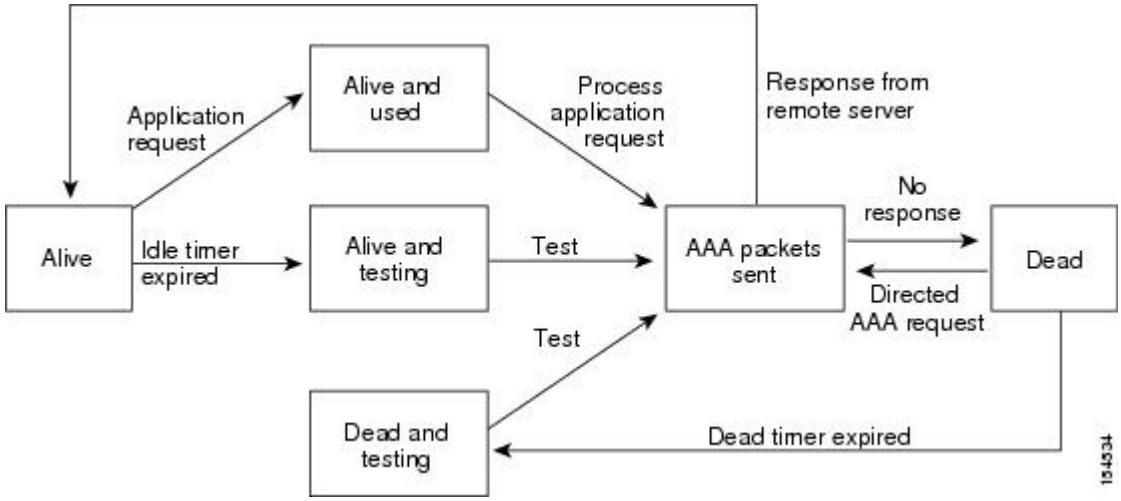
```
switch# show aaa authentication login error-enable enabled
```

AAA サーバーのモニタリング

応答の途絶えた AAA サーバーは 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 サーバーをモニターして AAA サーバーが

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 サーバー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 サーバーにも AAA 要求を送りません。MDS スイッチは定期的に停止中の AAA サーバーを監視し、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 サーバーが稼働中であることを確認します。AAA サーバー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 サーバーのステートについては、Figure 1: AAA サーバーのステート, on page 7 を参照してください。

***Figure 1: AAA* サーバーのステート**



Note 稼働中のサーバーと停止中のサーバーのモニタリング間隔はそれぞれ別で、ユーザーが設定できます。AAA サーバーのモニタリングはテスト用認証要求を AAA サーバー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ー名とパスワードは設定が可能です。

RADIUS サーバー モニタリング パラメータの設定, on page 32とRADIUS サーバーの詳細の表示, on page 44の項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ー 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 サーバーまたは TACACS+ サーバーを使用）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、ユーザー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。ユーザーは、ユーザー 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、ユーザー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、ユーザー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。

Procedure

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 サーバー グループ認証方式を使用するサーバー グループを設定した場合は、グループ内の最初の AAA サーバーに認証要求が送信されます。

- そのAAAサーバーが応答に失敗すると次のAAAサーバーに送信され、リモートサーバーが認証要求に応答するまで繰り返されます。
- サーバー グループ内のすべてのAAAサーバーが応答に失敗した場合は、次のサーバー グループのサーバー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 サーバー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 サーバーのプロトコルが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ー ロールがダウンロードされます。
- AAA サーバー 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ー ロールを取得するために、もう1つの要求が同じサーバーに送信されます。
- リモート AAA サーバーからのユーザー 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、ユーザーには 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 ユーザー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。

AAA 認証のデフォルト ユーザ ロールのイネーブル化

ユーザ ロールを持たないリモート ユーザに、デフォルトのユーザ ロールを使用して、リモート認証による Cisco NX-OS デバイスへのログインを許可できます。AAA のデフォルトのユーザ ロール機能をディセーブルにすると、（デバイスの中でローカルに一致したユーザ ロールを持たない）リモート ユーザはデバイスにログインできなくなります。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`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	**aaa user default-role** **Example:** `switch(config)# aaa user default-role`	AAA 認証のためのデフォルト ユーザ ロールをイネーブルにします。デフォルトではイネーブルになっています。 デフォルト ユーザ ロールの機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

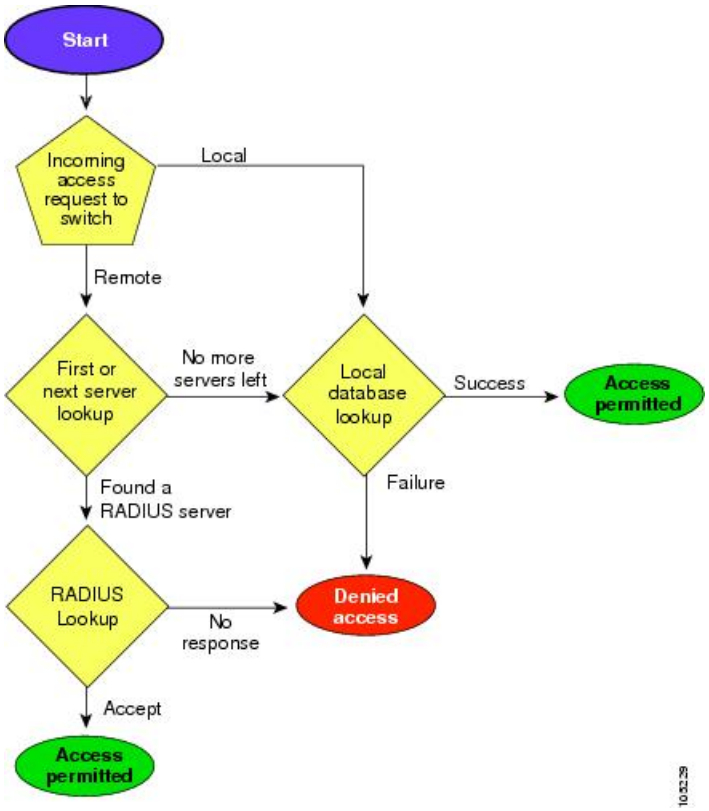
ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **show aaa user default-role** **Example:** `switch# show aaa user default-role`	AAA デフォルト ユーザ ロールの設定を表示します。

TACACS+ サーバーでのロールベース認証の設定

次の図に、認証および許可プロセスのフロー チャートを示します。

図 *2:* スイッチの認可と認証のフロー



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

TACACS+ サーバー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。

手順

ステップ 1 switch# **configure terminal**

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+ サーバー グループの認証を有効にします。

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+ サーバー 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+ サーバー グループの認証を有効にします。認証は、ローカル ユーザー 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**

認証されたユーザー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+サーバーを使用して実施する認証にのみ提供されます。
- 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。
- コマンド許可では、デフォルト ロールを含むユーザーのロールベース許可コントロール（RBAC）がディセーブルになります。

AAA 許可情報の詳細の表示

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 ユーザー ロールを表示するには、show コマンドを使用できます。（次の例を参照）

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

リモート認証のデフォルト ユーザー 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 サーバーに到達不能（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。

Procedure

ステップ 1 switch# **configure terminal**

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。

Note 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。

Caution 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、サーバー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
```

Note 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
```

ログイン パラメータの設定

Cisco MDS 9000 デバイスへの DoS 攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログイン パラメータを設定するには、ここに示す手順を実行します。

すべてのログイン パラメータは、デフォルトではディセーブルです。他のログイン コマンドを使用する前に、デフォルトのログイン機能をイネーブルにする login block-for コマンドを入力する必要があります。login block-for コマンドをイネーブルにすると、次のデフォルトが強制されます。

- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、login quiet-mode access-class コマンドが入力されるまで、ACL はログイン時間から除外されません。

ログイン パラメータを設定するには、次の手順を実行します。

Procedure

ステップ 1 コンフィギュレーション モードを開始します。

switch# **configure terminal**

ステップ 2 Cisco MDS 9000 デバイスで DoS の検出に役立つログイン パラメータを設定します。

switch(config)# **login block-for 100 attempts 2 within 100**

Note このコマンドは、その他のログイン コマンドの前に発行する必要があります。

ステップ 3 （任意）このコマンドはオプションですが、デバイスが静音モードに切り替わるときにデバイスに適用される ACL を指定するように設定することを推奨します。デバイスが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。

switch(config)# **login quiet-mode access-class myacl**

ステップ 4 特権 EXEC モードに戻ります。

switch(config)# **exit**

ステップ 5 ログイン パラメータを表示します。

switch# **show login**

ステップ 6 失敗したログイン試行に関連する情報のみを表示します。

switch# **show login failures**

ログイン パラメータの設定

ログイン パラメータなしの確認

ログイン パラメータの確認

失敗したログイン試行に関する情報の表示

次に、100 秒以内に 15 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。待機時間中、ACL 「myacl」からのホスト以外、すべてのログイン要求が拒否されます。

```
switch(config)# login block-for 100 attempts 15 within 100
switch(config)# login quiet-mode access-class myacl
```

show login コマンドからの次のサンプル出力は、ログイン パラメータが指定されていないことを確認します。

```
switch# show login

No Quiet-Mode access list has been configured, default ACL will be applied.
Switch is enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.
Switch presently in Normal-Mode.
Current Watch Window remaining time 49 seconds.
Present login failure count 0.
```

show login コマンドからの次のサンプル出力は、ログイン パラメータが指定されていることを確認します。

```
switch# show login

Quiet-Mode access list myacl is applied.
Switch is enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 49 seconds.
Present login failure count 0.
```

show login failures コマンドからの次のサンプル出力は、スイッチ上で失敗したすべてのログイン試行を表示します。

```
switch# show login failures

Information about last 20 login failures with the device.
---------------------------------------------------------
Username   TimeStamp        Line    Source                Appname
admin    Wed Jun 10 04:56:16 2015     pts/0        10.10.10.1           login
admin    Wed Jun 10 04:56:19 2015        pts/0       10.10.10.2        login
```

show login failures コマンドからの次のサンプル出力は、現在記録されている情報がないことを確認します。

```
switch# show login failures

*** No logged failed login attempts with the device.***
```

AAAサーバーのモニタリングパラメータをグローバルに設定

AAA サーバー モニタリング パラメータは、すべてのサーバーにグローバルに設定、または特定のサーバー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ーに適用されます。各サーバーで、特定のサーバー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 サーバーのグローバル 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。

Procedure

ステップ 1 switch# **configure terminal**

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 サーバーのグローバル 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 サーバーのグローバル 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 サーバー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 サーバーのテスト パラメータをグローバルに設定します。

ステップ 6 switch(config)# **radius-server test username username password password no**

RADIUS サーバーのグローバルなテスト パラメータを無効にします。

Example

Note TACACS サーバーのグローバル 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 サーバー 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 サーバーを設定すると、その AAA サーバーは、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 サーバーは、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。
- サーバーのサーバー 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、そのサーバーは、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、サーバーテストパラメータが存在するサーバー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ーのモニタリングが停止します。
- ユーザー指定のサーバーテストパラメータによってサーバー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ー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 サーバー（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ー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/サーバープロトコルでは、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。

Note 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。

このセクションは、次のトピックで構成されています。

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。

Note 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
- Cisco MDS NX-OS リリース 8.1（1）以降から、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 1.0と 1.2 をサポートします。

- DNSSEC による安全な DNS 探索はサポートされていません。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザー アカウントが、AAA サーバー上のリモート ユーザー アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバー上に設定されているユーザー ロールではなく、ローカル ユーザー アカウントのユーザー ロールをリモート ユーザーに適用します。
- Cisco MDS スイッチは、次のすべての条件を満たし、LDAP がリモート認証プロトコルを使用している場合、ローカル ロールをリモート ユーザーに割り当てます。
  - LDAP サーバーのリモート ユーザー名は、Cisco MDS スイッチのローカル ユーザーと同じ名前です。（たとえば、「test」が AD サーバーでのユーザー名の場合は、Cisco MDS スイッチでも同じユーザー名が作成されます）
  - LDAP サーバーは、Cisco MDS スイッチで AAA 認証として設定されます。
  - ローカル ユーザーとリモート ユーザーに割り当てられるロールは異なります。

次の例では、LDAP サーバーのユーザー名が "test" で、AD グループ "testgroup" のメンバーである場合について検討します。Cisco MDS スイッチは、名前が "testgroup" に設定されたロールを使用し、このロールには特定の許可ロールが割り当てられています。このロールは Cisco MDS スイッチで作成され、LDAP を使用してスイッチにログインするリモート ユーザー用です。また、Cisco MDS スイッチにはローカル ユーザー名 "test" も使用し、ロールとして "network-admin" が割り当てられています。Cisco MDS スイッチは AAA 認証用に設定され、認証プロトコルとして LDAP を使用します。この場合、ユーザーがユーザー名 "test" を使用して Cisco MDS スイッチにログインすると、スイッチは LDAP 認証を使用するユーザーを認証します（AD サーバーで作成された "test" ユーザーのパスワードを使用します）。ただし、ロールは、リモートで認証されたユーザーに割り当てられる「testgroup」ロールではなく、ローカルユーザー「test」に割り当てられる「network-admin」が割り当てられます。

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

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。

Procedure

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。

リモート LDAP サーバ プロファイルを構成

リモートの LDAP サーバにアクセスするには、Cisco NX-OS デバイス上で最初にプロファイルをサーバ IP アドレスまたはホスト名と一緒に作成します。サーバのプロファイル内の同じパラメーターによって上書きされない限り、グローバル LDAP サーバ パラメーターが使用されます。

構成可能なパラメーターは、SSL トランスポートの使用、サーバ上のターゲット ポート番号、要求のタイムアウト期間、ルート識別名（バインドユーザー）とパスワード、および検索参照です。

最大 64 の LDAP サーバ プロファイルがサポートされます。

Note 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 サーバを構成するには、次の手順を実行します。

Procedure

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**

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。

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 サーバーに RootDN を設定するには、次の手順を実行します。

Procedure

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 サーバー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ー ロールをサポートします。LDAP サーバで、LDAP ユーザーが、スイッチで作成されたロール名（カスタマイズされたロール）または組み込みのロール名（ネットワーク管理者または属性管理者）と同じグループに属していることを確認します。

Note

- ユーザー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。
- ユーザー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 サーバー グループを設定するには、次の手順を実行します。

Procedure

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 サーバー グループを作成し、そのグループの LDAP サーバー 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 サーバーを、LDAP サーバー グループのメンバとして設定します。

指定した LDAP サーバー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ーを設定し、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サーバー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ー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）ユーザープロファイルでユーザー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ーがログインできるようにします。

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 サーバー 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 LDAP クライアントが、タイムアウト エラーを宣言する前に LDAP サーバの応答を待機する最大時間を設定できます。LDAPサーバ グループに他のLDAPサーバーが存在する場合、タイムアウト後に次のサーバーが試行されます。他にLDAPサーバがない場合、リクエストは機能不全になります。デフォルトでは、Cisco NX-OS LDAP クライアントは、各 LDAP サーバが応答するために 5 秒のグローバル タイムアウト期間を使用します。グローバル タイムアウト値は、各 LDAP サーバ プロファイルで上書きできます。

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。

Procedure

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 サーバー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 サーバーの接続タイムアウトの構成

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。

LDAP サーバーに接続タイムアウト期間を設定するには、次の手順を実行します。

手順

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 timeout 3**

サーバのタイムアウト間隔を指定します。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 サーバー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 サーバー 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 サーバー宛て先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 サーバー ポートを設定するには、次の手順を実行します。

Procedure

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 789**

サーバーへの 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 サーバー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 サーバーの宛て先ポートを構成

特定のLDAPサーバに指定した宛て先ポートは、すべてのLDAPサーバで使用されるグローバルな宛て先ポートを上書きします。

接続先 TCP ポートを設定するには、次の手順を実行します。

Procedure

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 port 200**

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。

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 サーバー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 SSL トランスポートの構成

LDAP クライアントとサーバ間のトランスポートとして Secure Sockets Layer（SSL）を使用すると、ユーザー パスワードなどの転送データの完全性と機密性が保証されます。Cisco NX-OS LDAPクライアントは、バインドまたは検索要求を送信する前にSSL接続を交渉することをサポートしています。リモート LDAP サーバへのトランスポートとして SSL を使用するには、Cisco NX-OS デバイスの LDAP サーバ プロファイルで SSL オプションを有効にします。Cisco NX-OS デバイスでこの機能を有効にする前に、リモート LDAP サーバもこの機能をサポートしていることを確認してください。

TLS (SSL 経由) を介したリモートLDAPサーバーへの接続は、RFC4513 に準拠しています。これには、セキュア トランスポート交渉中にサーバによって提示される ID が、サーバー プロファイル名とスイッチ上の証明書の両方と正確に一致する必要があります。一致は、証明書の「情報カテゴリの別名」の IP アドレスまたはホスト名による可能性があります。この方式が

推奨されます。一致がない場合は、証明書「サブジェクト」の共通名 (CN) がチェックされますが、この方法はRFC4513によって非推奨になっています。サーバ証明書は、Cisco NX-OSデバイスに個別にインストールされます。詳しい情報を表示するために[認証局およびデジタル証明書の設定（Configuring Certificate Authorities and Digital Certificates）]章を参照します。

（注） Cisco MDS NX-OS リリース 8.2（1）以降、接続先 TCP ポートが636 として構成されている場合は、LDAP クライアントは自動的に SSL または TLS ネゴシエーションを開始されます。他の宛て先ポートを使用する場合は、**enable-ssl** オプションを使用して SSL トランスポートを手動で有効にする必要があります。

SSL トランスポートをリモート LDAP サーバに構成するには、次の手順を実行します。

手順

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**

リモートLDAPサーバーへのバインドおよび検索要求のSSLトランスポートを有効にします。

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 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。

Procedure

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）ユーザープロファイル、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サーバーに送信するために使用されます。

Note LDAP 検索フィルタ文字列は最大 128 文字に制限されています。

ユーザー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。

Note 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。

Procedure

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 サーバー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。

Before you begin

LDAP サーバで SSH 公開鍵と秘密鍵が構成されていることを確認してください。

Procedure

ステップ 1 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。

switch# **configure terminal**

ステップ 2 SSH 公開キーと SSH 証明書を構成します。

SSH 公開キー

a. LDAP サーバのデフォルトの AAA 許可方式を構成します。

switch(config)# **aaa authorization ssh-publickey default** {**group** *group-list* | **local**}

この **ssh-publickey** キーワードは、SSH 公開キーを使用して LDAP またはローカル承認を構成します。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 引数には、LDAP サーバ グループ名をスペースで区切ったリストを指定します。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** 方式はローカル データベースを使用して許可を行います。

b. 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：

switch(config)# **ldap-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **rootDN** *root-name* [**password** *password* [**port** *tcp-port* [**timeout** *seconds*] | **timeout** *seconds*]]

c. LDAP 検索マップを構成します：

switch(config)# **ldap search-map** *map-name*

d. 一致する公開キーを指定します：

switch(config-ldap-search-map)# **user-pubkey-match attribute-name** *attribute-name* **search-filter** *search-filter* **base-dn**

e. 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 を構成します。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。

switch(config-ldap-search-map)# **userprofile attribute-name “memberOf” search-filter “(&(objectClass=inetOrgPerson)(cn=$userid))” base-DN dc=acme,dc=com**

f. 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：

switch(config-ldap-search-map)# **aaa group server ldap** *group-name*

g. LDAP サーバを、LDAP サーバ グループのメンバとして構成します。

switch(config-ldap)# **server** {*ipv4-address* | *ipv6-address* | *host-name*}

[SSH 証明書（SSH Certificate）]

a. LDAP サーバのデフォルトの AAA 許可方式を構成します：

switch(config)# **aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2**

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 サーバー 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** 方式はローカル データベースを使用して許可を行います。

b. 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：

switch(config)# **ldap-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **rootDN** *root-name* [**password** *password* [**port** *tcp-port* [**timeout** *seconds*] | **timeout** *seconds*]]

c. LDAP 検索マップを構成します：

switch(config)# **ldap search-map** *map-name*

d. 証明書照合を指定します：

switch(config-ldap-search-map)# **user-certdn-match attribute-name** *attribute-name* **search-filter** *search-filter* **base-dn**

e. 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 を構成します。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。

switch(config-ldap-search-map)# **userprofile attribute-name "memberOf" search-filter "(&(objectClass=inetOrgPerson)(cn=$userid))" base-DN dc=acme,dc=com**

f. LDAP サーバ グループを作成し、そのグループの LDAP サーバ グループ構成モードを開始します：

switch(config-ldap-search-map)# **aaa group server ldap** *group-name*

g. LDAP サーバを、LDAP サーバ グループのメンバとして構成します。

switch(config-ldap)# **server** {*ipv4-address* | *ipv6-address* | *host-name*}

What to do next

SSH 証明書の場合、次の機能を構成します。

1. ホスト名または、IP ドメイン名の構成します。「ホスト名および IP ドメイン名の設定」を参照してください。
2. トラスト ポイント認証局関連付けを作成します。「トラスト ポイント認証局関連付けを作成」を参照してください。
3. トラスト ポイント認証局の認証します。「トラスト ポイントの認証局」を参照してください。

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。

Procedure

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。

Example

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
```

デフォルト設定

次の表に、LDAP パラメータのデフォルト設定を示します。

***Table 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	Cisco

RADIUS サーバー 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 サーバーと通信できます。複数の RADIUS サーバーおよびサーバー 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/サーバー 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、ユーザー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 中央サーバー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。

このセクションは、次のトピックで構成されています。

RADIUS サーバーのデフォルト設定

Fabric Manager を利用すると、スイッチとの通信を設定するどの RADIUS サーバー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

• ユーザーによるログイン時の RADIUS サーバー指定の許可

RADIUS サーバーの IPv4 アドレスの設定

最大 64 台の RADIUS サーバーを追加できます。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 サーバーの 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。

Procedure

ステップ 1 switch# **configure terminal**

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 サーバー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ーを指定します。

Note **authentication** と **accounting** オプションのどちらも指定しないと、サーバー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**

指定したサーバーのクリア 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。

ステップ 7 switch(config)# **radius-server host 10.10.0.0 key 4 da3Asda2ioyuoiuH**

指定したサーバー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 サーバーの IPv6 アドレスの設定

ホスト RADIUS サーバーの 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。

Procedure

ステップ 1 switch# **configure terminal**

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 サーバー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ーを指定します。

Note **authentication** と **accounting** オプションのどちらも指定しないと、サーバー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**

指定したサーバーのクリア 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。

ステップ 7 switch(config)# **radius-server host 2001:0DB8:800:200C::417A key 4 da3Asda2ioyuoiuH**

指定したサーバー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 サーバーの DNS 名の設定

ホスト RADIUS サーバーの 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。

手順

ステップ 1 switch# **configure terminal**

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 サーバー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。

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ーを指定します。

（注） **authentication** と **accounting** オプションのどちらも指定しないと、サーバー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**

指定したサーバーのクリア 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。

ステップ 7 switch(config)# **radius-server host radius2 key 4 da3Asda2ioyuoiuH**

指定したサーバー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 サーバー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 サーバー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 サーバー 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 サーバーの設定時に **key** オプションを明示的に使用する必要があります。

RADIUS サーバー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。

Procedure

ステップ 1 switch# **configure terminal**

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ー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。

ステップ 3 switch(config)# **radius-server key 0 AnyWord**

RADIUS クライアントとサーバー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。

ステップ 4 switch(config)# **radius-server key 7 abe4DFeeweo00o**

RADIUS クライアントとサーバー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 サーバーのタイムアウト間隔の設定

すべての RADIUS サーバー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。

Note タイムアウト値が個々のサーバー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 サーバー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。

Procedure

ステップ 1 switch# **configure terminal**

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+ サーバー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。

ステップ 3 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 サーバー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 サーバーへの送信を 1 回だけ再試行します。このリトライの回数は、サーバーごとに最大 5 回まで増やすことができます。RADIUS サーバー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 サーバーがユーザー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。

Procedure

ステップ 1 switch# **configure terminal**

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 サーバーへの接続を試行する回数（3）を設定します。

ステップ 3 switch(config)# **no radius-server retransmit**

デフォルトの試行回数（1）に戻します。

RADIUS サーバー モニタリング パラメータの設定

RADIUS サーバーをモニターするためのパラメータを設定できます。サーバー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。

このセクションは、次のトピックで構成されています。

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 サーバーが要求を受信しないでいる時間間隔を指定します。

Note 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。

Procedure

ステップ 1 switch# **configure terminal**

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 ユーザー名の設定

定期的な RADIUS サーバーのステータス テストに使用するユーザー名とパスワードを設定できます。RADIUS サーバーを監視するテスト メッセージを発行するために、テスト ユーザー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ー名（test）とデフォルトのパスワード（test）を利用できます。

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

定期的なRADIUSサーバーのステータステストに使用するオプションのユーザー名とパスワードを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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**

テストユーザー（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ー名は test です。

ステップ 3 switch(config)# **no radius-server host 10.1.1.1 test username testuser**

テスト ユーザー名（testuser）を削除します。

ステップ 4 switch(config)# **radius-server host 10.1.1.1 test username testuser password Ur2Gd2BH**

テスト ユーザー（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 サーバーをデッド状態であると宣言した後、そのサーバー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。

Note 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 サーバーがサーバー 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 サーバーモニタリングは実行されません。（サーバー グループ, on page 4を参照してください）。

Note デッド RADIUS サーバーに RADIUS テスト メッセージが送信される前に、同サーバーのデッド タイマーの期限が切れた場合、同サーバー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 ユーザーを設定します。

デッド タイマーを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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 サーバーの概要

最大 64 台の RADIUS サーバーを追加できます。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サーバーを設定する際は、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 サーバー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サーバーが要求を受信しないでいる時間間隔を指定します。

Note 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 サーバー モニタリング パラメータの設定, on page 32を参照してください。

テスト ユーザー名の設定

定期的な RADIUS サーバーのステータス テストに使用するユーザー名とパスワードを設定できます。RADIUS サーバーを監視するテスト メッセージを発行するために、テスト ユーザー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ー名（test）とデフォルトのパスワード（test）を利用できます。

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

定期的なRADIUSサーバーのステータステストに使用するオプションのユーザー名とパスワードの設定については、RADIUS サーバー モニタリング パラメータの設定, on page 32を参照してください。

RADIUS サーバーの検証の概要

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

Note セキュリティ上の理由から、RADIUSサーバーで設定されたユーザー名をテストユーザー名として使用しないことを推奨します。

サーバー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 サーバーをモニターするテスト メッセージを手動で送信できます。

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

Procedure

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ー名（test）とパスワード（test）を使用して RADIUS サーバーにテスト メッセージを送信します。

ステップ 2 switch# **test aaa server radius 10.10.1.1 testuser Ur2Gd2BH**

設定されたテストユーザー名（testuser）とパスワード（Ur2Gd2BH）を使用して RADIUS サーバーにテスト メッセージを送信します。

Note 設定済みのユーザー名およびパスワードはオプションです（テスト ユーザー名の設定, on page 55の項を参照）。

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 サーバー グループの最初のサーバーに転送します。誘導要求オプションをイネーブルにすると、どの RADIUS サーバーに認証要求を送信するかをユーザー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、ユーザーは *username@hostname* としてログインできます。*hostname* は設定した RADIUS サーバーの名前です。

Note ユーザー指定のログインは 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ーが認証用の RADIUS サーバーを選択できるようにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

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ーが認証要求の送信先となる RADIUS サーバーを指定できるようにします。

ステップ 3 switch(config)# **no radius-server directed-request**

サーバー グループの最初のサーバーに認証要求を送信するように戻します（デフォルト）。

Example

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

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバーと RADIUS サーバーの間でのベンダー固有属性（VSA）の通信のための方式を規定する標準を作成しています。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ー認証に RADIUS サーバーを使用した場合、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ー属性を戻すように RADIUS サーバーに指示します。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 オプションをサポートしています。

- **Shell** プロトコル：ユーザー 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、ユーザー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、 **vsan-admin** と **storage-admin** 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 サーバーから送信されます。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 サーバーでの 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ーのロール マッピングを指定する場合に使用できます。

```
shell:roles="roleA roleB ..."
```

Note 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 サーバー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 ユーザー 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 ユーザー名として 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。

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ー 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 サーバー

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。

Cisco MDS NX-OS リリース 8.5（1）から、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 サーバーの **cisco-av-pair** 属性で指定されていない場合は、MD5 および AES-128 がデフォルトで使用されます。

RADIUS サーバーの詳細の表示

設定された RADIUS パラメータを表示するには、 **show radius-server** コマンドを次の例のように使用します。

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:******
```

設定済みの RADIUS サーバー 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 サーバー統計情報の表示

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

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

RADIUS サーバー統計情報の表示

```
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 サーバー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
```

管理者パスワードの回復

次の 2 通りの方法のいずれかで管理者パスワードを回復できます。

- network-admin 権限を持つユーザー名による CLI の使用
- スイッチの電源再投入

ここでは、次の項目について説明します。

network-admin 権限での CLI の使用

network-admin 権限を持つユーザー名でスイッチにログインしているか、ログインできる場合に、管理者パスワードを回復するには、次の手順を実行します。

Procedure

ステップ 1 ユーザー名に network-admin 権限があることを確認するには、 **show user-accounts** コマンドを使用します。

Example:

```
switch# show user-account

user:admin
this user account has no expiry date
roles:network-admin
user:dbgusr
this user account has no expiry date
roles:network-admin network-operator
```

ステップ 2 ユーザー名に network-admin 権限がある場合は、**username** コマンドを発行して新しい管理者パスワードを割り当てます。

Example:

```
switch# configure terminal
switch(config)# username admin password  <new password>
switch(config)# exit
switch#
```

ステップ 3 ソフトウェア設定を保存します。

Example:

```
switch# copy running-config startup-config
```

スイッチの電源の再投入

network-admin 特権を持つスイッチ上でセッションを開始できない場合は、スイッチの電源を再投入して管理者パスワードを回復する必要があります。

Caution この手順を実行すると、スイッチ上のすべてのトラフィックが中断されます。スイッチとの接続はすべて 2 ～ 3 分間切断されます。

Note 管理者パスワードは、Telnet または SSH セッションからは回復できません。ローカル コンソール接続を使用できる必要があります。コンソール接続のセットアップの詳細については、Cisco MDS 9000 Series Fundamentals Configuration Guideを参照してください。

スイッチの電源を再投入して、管理者パスワードを回復するには、次の手順を実行します。

Procedure

ステップ 1 スタンバイのスーパーバイザ モジュールをシャーシから取り外します。

ステップ 2 スイッチの電源を再投入します。

ステップ 3 スイッチが Cisco NX-OS ソフトウェアのブート シーケンスを開始したときに **Ctrl-]** キー シーケンスを押して、switch(boot)# プロンプト モードを開始します。

Ctrl-]

```
switch(boot)#
```

ステップ 4 コンフィギュレーション モードに切り替えます。

```
switch(boot)# configure terminal
```

ステップ 5 admin-password コマンドを発行して、管理者パスワードをリセットします。これは、コンソールを使用してログインのリモート認証を無効にします（有効な場合）。これはパスワードを回復した後、新しいパスワードで管理者がコンソールからログインできるようにするために行います。Telnet/SSH の認証は、これにより影響を受けません。

```
switch(boot-config)# admin-password <new password>
WARNING! Remote Authentication for login through console will be disabled#
```

強力なパスワードの詳細については、パスワード強度の確認の項を参照してください。

ステップ 6 EXEC モードに切り替えます。

```
switch(boot-config)# admin-password <new password>
```

ステップ 7 **load** コマンドを発行して、Cisco NX-OS ソフトウェアをロードします。

```
switch(boot)# load bootflash:m9700-sf4ek9-mz.8.4.1.bin
```

Caution コンフィギュレーションを保存するために使用するイメージより古いシステムイメージをブートし、**install all** コマンドを使用せずにシステムをブートする場合、スイッチはバイナリ コンフィギュレーションを消去し、ASCII コンフィギュレーションを使用します。この場合は、**init system** コマンドを使用してパスワードを回復する必要があります。

ステップ 8 新しい管理者パスワードを使用してスイッチにログインします。

```
switch login: admin
Password:<newpassword>
```

ステップ 9 Fabric Manager の SNMP パスワードとしても使用できるようにするために、新しいパスワードをリセットします。

```
switch# configure terminal
switch(config)# username admin password<new password>
switch(config)# exit
switch#
```

ステップ 10 ソフトウェア設定を保存します。

```
switch# copy running-config startup-config
```

ステップ 11 以前に取り外したスーパーバイザ モジュールをシャーシのスロット 6 に挿入します。

TACACS+ サーバー 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 サーバーと通信します。複数の TACACS+ サーバーを設定し、タイムアウト値を指定できます。

このセクションは、次のトピックで構成されています。

TACACS+ について

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/サーバー 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+ サーバーのデフォルト設定

Fabric Manager を利用すると、スイッチとの通信を設定するどの TACACS+ サーバー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
- ユーザーによるログイン時の TACACS+ サーバー指定の許可

TACACS+サーバー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+ サーバー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+ サーバー 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+ サーバーの設定時に **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。

Procedure

ステップ 1 switch# **configure terminal**

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。

ステップ 3 switch(config)# **no feature tacacs+**

（オプション）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+ サーバーの IPv4 アドレスの設定

設定されたサーバー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。サーバー 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）が該当サーバーで使用されます（TACACS+ サーバー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, on page 53の項を参照）。

Note 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+ サーバーの 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。

Procedure

ステップ 1 switch# **configure terminal**

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+ サーバーを設定します。

ステップ 3 switch(config)# **no tacacs-server host 171.71.58.91**

（オプション）IPv4 アドレスによって識別される特定の TACACS+ サーバーを削除します。デフォルトでは、サーバーは設定されません。

ステップ 4 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。

ステップ 5 switch(config)# **no tacacs-server host 171.71.58.91 port 2**

（オプション）サーバー 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 6 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+ サーバーを設定し、秘密キーを割り当てます。

ステップ 7 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、指定したサーバー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+ サーバーの IPv6 アドレスの設定

TACACS+ サーバーの 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。

Procedure

ステップ 1 switch# **configure terminal**

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+ サーバーを設定します。

ステップ 3 switch(config)# **no tacacs-server host 2001:0DB8:800:200C::417A**

（オプション）IPv6アドレスによって識別される特定のTACACS+サーバーを削除します。デフォルトでは、サーバーは設定されません。

ステップ 4 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。

ステップ 5 switch(config)# **no tacacs-server host 2001:0DB8:800:200C::417A port 2**

（オプション）サーバー 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 6 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+サーバーを設定し、秘密キーを割り当てます。

ステップ 7 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、指定したサーバー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+ サーバーの DNS 名の設定

TACACS+サーバーの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。

手順

ステップ 1 switch# **configure terminal**

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+ サーバーを設定します。

ステップ 3 switch(config)# **no tacacs-server host host1.cisco.com**

（オプション）指定の DNS 名によって識別される TACACS+ サーバーを削除します。デフォルトでは、サーバーは設定されません。

ステップ 4 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。

ステップ 5 switch(config)# **no tacacs-server host host1.cisco.com port 2**

（オプション）サーバー 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 6 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+ サーバーを設定し、秘密キーを割り当てます。

ステップ 7 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、指定したサーバー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+ サーバーで秘密キーに対するグローバル値を設定できます。

Note

- 秘密キーが個々のサーバー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。
- 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+ サーバーの秘密キーを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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+サーバー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 キーと各サーバー 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+ サーバーに送信されます。

ステップ 3 switch(config)# **no tacacs-server key oldPword**

（オプション）設定されたグローバル秘密キーを TACACS+ サーバー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ー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+サーバー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+ サーバーを 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、各サーバーで 5 回です。TACACS+ サーバー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+ サーバー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。

Note タイムアウト値が個々のサーバー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+ サーバーのグローバル タイムアウト値を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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+ サーバー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。

ステップ 3 switch(config)# **no tacacs-server timeout 30**

（オプション）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+ サーバーの概要

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+ サーバーの設定を行うと、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。

設定されたサーバー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。サーバー 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）が該当サーバーで使用されます。

Note 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+ サーバーで秘密キーに対するグローバル値を設定できます。

Note 秘密キーが個々のサーバー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+ サーバー モニタリング パラメータの設定

TACACS+ サーバーをモニターするためのパラメータを設定できます。

このセクションは、次のトピックで構成されています。

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+ サーバーが要求を受信しないでいる時間間隔を指定します。

Note 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。

Procedure

ステップ 1 switch# **configure terminal**

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**

（オプション）デフォルト値（0 分）に戻します。

テスト ユーザー名の設定

定期的なTACACS+サーバーのステータステストに使用するユーザー名とパスワードを設定できます。TACACS+ サーバーを監視するためのユーザー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 ユーザー名（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+ サーバーのステータス テストに使用するオプションのユーザー名とパスワードを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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**

テストユーザー（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ー名は test です。

ステップ 3 switch(config)# **no tacacs-server host 10.1.1.1 test username testuser**

（オプション）テスト ユーザー（testuser）を削除します。

ステップ 4 switch(config)# **tacacs-server host 10.1.1.1 test username testuser password Ur2Gd2BH**

テスト ユーザー（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+ サーバーをデッド状態であると宣言した後、そのサーバー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。

Note

- デフォルトのデッド タイマー値は 0 分です。TACACS+ サーバー モニタリングは、TACACS+ サーバーがデッド 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 サーバー モニタリング パラメータの設定, on page 32 を参照）。
- デッドTACACS+サーバーにTACACS+テスト メッセージが送信される前に、同サーバーのデッド タイマーの期限が切れた場合、同サーバー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 ユーザーを設定します。

デッド タイマーを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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。

ステップ 3 switch(config)# **no tacacs-server deadtime 30**

（オプション）デフォルト値（0 分）に戻します。

Note デッド タイム インターバルが 0 分の場合、TACACS+ サーバーがサーバー 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+ サーバー モニタリングは実行されません。（RADIUS サーバー モニタリング パラメータの設定, on page 32の項を参照）。

モニタリング用 TACACS+ テスト メッセージの送信

TACACS+ サーバーをモニターするテスト メッセージを手動で送信できます。

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

手順

ステップ 1 switch# **test aaa server tacacs+ 10.10.1.1 test**

デフォルトのユーザー名（test）とパスワード（test）を使用して TACACS+ サーバーにテスト メッセージを送信します。

ステップ 2 switch# **test aaa server tacacs+ 10.10.1.1 testuser Ur2Gd2BH**

設定されたテスト ユーザー名とパスワードを使用して TACACS+ サーバーにテスト メッセージを送信します。設定済みのユーザー名およびパスワードはオプションです（テスト ユーザー名の設定 （55 ページ）の項を参照）。

TACACS+ サーバーからのパスワード エージング通知

パスワードエージング通知は、ユーザーが 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、ユーザーに通知されます。パスワードの期限が切れると、ユーザーはパスワードを変更するように求められます。

Note 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 サーバー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 サーバーが構成され、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 サーバーから開始します。

Note 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 サーバーのパスワード 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 サーバー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+ サーバーの検証の概要

Cisco SAN-OS リリース 3.0(1) では、TACACS+ サーバー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ー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ーに送信します。このテスト認証にサーバーが応答しない場合、サーバーは応答能力がないものと見なされます。

Note セキュリティ上の理由から、TACACS+ サーバーにはテスト用ユーザーを設定しないことを推奨します。

サーバー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+ サーバーの定期的な検証

Fabric Manager を利用して TACACS+ サーバー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+ サーバー モニタリング パラメータの設定, on page 48の項を参照してください。

ユーザーによるログイン時の TACACS+ サーバー指定の概要

デフォルトでは、MDS スイッチは認証要求を TACACS+ サーバー グループの最初のサーバーに転送します。どの TACACS+ サーバーに認証要求を送信するかをユーザー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、ユーザーは *username@hostname* としてログインできます。*hostname* は設定した TACACS+ サーバーの名前です。

Note ユーザー指定のログインは 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ーが認証用の TACACS+ サーバーを選択できるようにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

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、ユーザーが認証要求の送信先となる TACACS+ サーバーを指定できるようにします。

ステップ 3 switch(config)# **no tacacs-server directed-request**

サーバー グループの最初のサーバーに認証要求を送信するように戻します（デフォルト）。

Example

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。

Table 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、ユーザー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 サーバーを使用する 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"
OR
shell:roles*"network-admin vsan-admin”
```

Note 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+ サーバー パラメータ

Cisco NX-OS ソフトウェアでは現在、下記の TACACS+ サーバー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+ サーバーの詳細の表示

次の例で示すように、Cisco MDS 9000 ファミリ内のすべてのスイッチの TACACS+ サーバー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。

TACACS+ サーバー情報の表示

```
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:*****
```

AAA 認証情報の表示

```
switch# show aaa authentication

         default: group TacServer local none
         console: local
         iscsi: local
         dhchap: local
```

AAA 認証ログイン情報の表示

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

enabled
```

設定した TACACS+ サーバー 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:
```

すべての AAA サーバー グループの表示

```
switch# show aaa groups

radius
TacServer
```

TACACS+ サーバーの統計情報の表示

```
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+ サーバーの統計情報をクリアできます。

サーバー グループの設定

サーバー グループを使用して、1 台または複数台のリモート AAA サーバーによるユーザー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ーが試行されます。

AAA サーバーモニタリング機能は AAA サーバー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 サーバー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 サーバーのモニタリング, on page 6の項を参照）。

このセクションは、次のトピックで構成されています。

RADIUS サーバー グループの設定概要

これらのサーバー 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 ユーザー、または Fabric Manager ユーザーや Device Manager ユーザーに設定できます。

RADIUS サーバー グループを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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ー グループを作成し、そのグループの RADIUS サーバー 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 3 switch(config)# **no aaa group server radius RadServer**

（オプション）認証リストから RadServer という名前のサーバー グループを削除します。

ステップ 4 switch(config-radius)# **server 10.71.58.91**

IPv4 アドレス 10.71.58.91 の RADIUS サーバーをサーバー グループ RadServer 内で最初に実行されるように設定します。

Tip 指定した RADIUS サーバーが見つからなかった場合は、**radius-server host** コマンドを使用してサーバーを設定し、このコマンドをもう一度実行します。

ステップ 5 switch(config-radius)# **server 2001:0DB8:800:200C::417A**

IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバーをサーバー グループ RadServer 内で最初に実行されるように設定します。

ステップ 6 switch(config-radius)# **no server 2001:0DB8:800:200C::417A**

（オプション）IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバーをサーバー グループ RadServer から削除します。

ステップ 7 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 8 switch(config)# **aaa group server radius RadiusServer**

switch(config-radius)#

RadiusServer という名前のサーバー グループを作成し、そのグループの RADIUS サーバー 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 9 switch(config-radius)# **server ServerA**

ServerA を RadiusServer1 と呼ばれるサーバー グループ内で最初に試行されるように設定します。

Tip 指定した RADIUS サーバーが見つからなかった場合は、**radius-server host** コマンドを使用してサーバーを設定し、このコマンドをもう一度実行します。

ステップ 10 switch(config-radius)# **server ServerB**

ServerB をサーバー 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 11 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。

Note 個別の RADIUS サーバーのデッド タイム インターバルが 0 よりも大きい場合は、サーバー グループに設定された値よりもその値が優先されます。

ステップ 12 switch(config-radius)# **no deadtime 30**

（オプション）デフォルト値（0 分）に戻します。

Note RADIUS サーバー グループおよび RADIUS サーバーの個別の TACACS+ サーバー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 サーバー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 サーバーに対するデッド サーバー モニタリングを実行しません。（RADIUS サーバー モニタリング パラメータの設定, on page 37 の項を参照）。

Example

設定されたサーバー 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+ サーバー グループの設定概要

TACACS+ サーバー グループを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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ー 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。

ステップ 3 switch(config)# **no aaa group server tacacs+ TacacsServer1**

（オプション）認証リストから TacacsServer1 という名前のサーバー グループを削除します。

ステップ 4 switch(config-tacacs+)# **server ServerA**

ServerA を TacacsServer1 と呼ばれるサーバー グループ内で最初に試行されるように設定します。

Tip 指定した TACACS+ サーバーが見つからなかった場合は、**tacacs-server host** コマンドを使用してサーバーを設定し、このコマンドをもう一度実行します。

ステップ 5 switch(config-tacacs+)# **server ServerB**

ServerB をサーバー グループ TacacsServer1 内で 2 番目に試行されるように設定します。

ステップ 6 switch(config-tacacs+)# **no server ServerB**

（オプション）サーバーの TacacsServer1 リスト内の ServerB を削除します。

ステップ 7 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。

Note 個別の TACACS+ サーバーのデッド時間間隔が 0 よりも大きい場合は、サーバー グループに設定された値よりもその値が優先されます。

ステップ 8 switch(config-tacacs+)# **no deadtime 30**

（オプション）デフォルト値（0 分）に戻します。

Note TACACS+ サーバー グループおよび TACACS+ サーバーの個別の TACACS+ サーバー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+ サーバー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+ サーバーに対するデッド サーバー モニタリングを実行しません。（TACACS+ サーバー モニタリング パラメータの設定, on page 48の項を参照）。

無応答サーバーのバイパス（回避）の概要

Cisco SAN-OS リリース 3.0(1) では、サーバー グループ内の無応答 AAA サーバーをバイパスできます。スイッチが無応答のサーバーを検出すると、ユーザーを認証する際にそのサーバーをバイパスします。この機能を利用すると、障害を起こしたサーバー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。無応答サーバーに要求を送信し、認証要求がタイムアウトするまで待つのではなく、スイッチはサーバー グループ内の次のサーバーに認証要求を送信します。サーバー グループに応答できる他のサーバーが存在しない場合は、スイッチは無応答サーバーに対して認証を試み続けます。

AAA サーバーへの配信

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、最初のサーバー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ー 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。サーバー キーおよびグローバル キーを除く、さまざまなサーバーおよびグローバル パラメータが配信されます。サーバー 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。

Note サーバー 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。

Note AAA サーバー設定配布を行う 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 RADIUS サーバー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 サーバーでの配信をイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

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。

ステップ 3 switch(config)# **no radius distribute**

（オプション）このスイッチのRADIUS設定の配信をディセーブル（デフォルト）にします。

AAA TACACS+ サーバーへの配信のイネーブル化

TACACS+ サーバーでの配信をイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

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。

ステップ 3 switch(config)# **no tacacs+ distribute**

（オプション）このスイッチの TACACS+ 設定の配信をディセーブル（デフォルト）にします。

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

Note AAA サーバー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ー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。

show radius コマンドを使用して CFS タブに**distribution status**を表示します。

```
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ー設定を、**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ー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
```

RADIUS 情報の配布のコミット

一時バッファに格納されたRADIUSまたはTACACS+グローバル設定またはサーバー設定を、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。

Procedure

ステップ 1 switch# **configure terminal**

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+ 情報の配信のコミット

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。

Procedure

ステップ 1 switch# **configure terminal**

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。

RADIUS の配布セッションの廃棄

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。

Procedure

ステップ 1 switch# **configure terminal**

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+ の配布セッションの廃棄

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。

Procedure

ステップ 1 switch# **configure terminal**

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+ のサーバー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。

- サーバー グループはマージされません。
- サーバー 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ーが含まれます。
- 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、個々のサーバー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。

Note 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。

Caution 設定されたサーバー 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、次の例のように RADIUS ファブリックのマージのステータスを参照できます。

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
```

TACACS+ ファブリックのマージのステータスの表示

show tacacs+ distribution status コマンドを使用して、次の例のように TACACS+ ファブリックのマージのステータスを参照できます。

```
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 サーバー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ーは、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 認証の有効化

CHAP 認証を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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。

ステップ 3 switch# **no aaa authentication login chap enable**

（オプション）CHAP ログイン認証をディセーブルにします。

Example

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

マイクロソフト チャレンジ ハンドシェーク認証プロトコル（MSCHAP）は、マイクロソフト版の CHAP です。

Cisco MDS 9000 ファミリ スイッチのユーザー 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 サーバーまたは TACACS+ サーバーでの認証に使用され、MSCHAPv2 は RADIUS サーバー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 サーバー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 サーバーを設定する必要があります。ベンダー固有属性の概要, on page 42を参照してください。次の表に MSCHAP に必要な RADIUS ベンダー固有属性を示します。

***Table 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 サーバーから MSCHAP ユーザー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 ユーザー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。

Procedure

ステップ 1 switch# **configure terminal**

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**

（オプション）MSCHAP ログイン認証をディセーブルにします。

MSCHAPv2 認証のイネーブル化

MSCHAPv2 認証をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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**

（オプション）MSCHAPv2 ログイン認証をディセーブルにします。

Example

Note

- 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。
- TACACS+ サーバーで 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 認証の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 認証の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ー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。ユーザーの認証は、ローカルに保存されているユーザー情報に基づいて実行されます。

ローカル ユーザー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、次の例のように **show accounting log** コマンドを使用します。

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、ユーザー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、ユーザーは少なくとも Cisco MDS 9000 Family スイッチ上のローカル ユーザーである必要があります。

Caution 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、あらゆるユーザーがいつでもスイッチにアクセスできるようになります。

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

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ーは、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次の例のように表示されます。

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。

Tip 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 サーバーに送信します。RADIUS サーバーは、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。一部のサーバーは、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。

Note 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。次の例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。

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
```

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:
...
```

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 サーバーを使用する際のユーザー管理は、通常 Cisco ACS を使用して行われます。Figure 3: RADIUS を使用する場合の network-admin ロールの設定, on page 77、Figure 4: RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定, on page 78、Figure 5: TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定, on page 79、Figure 6: TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定, on page 80 に、RADIUS または TACACS+ のいずれかを使用した際の network-admin ロールと複数のロールの ACS サーバーのユーザー セットアップ構成を示します。

***Figure 3: RADIUS** を使用する場合の **network-admin** ロールの設定*

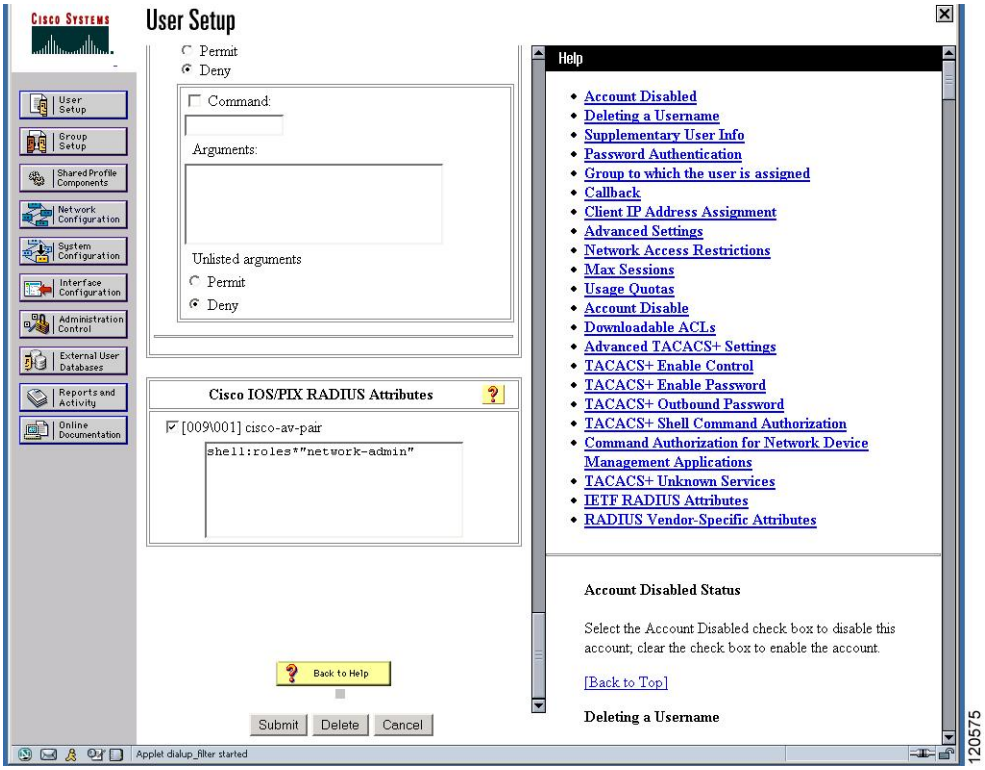


Figure 4: RADIUS を使用する場合の *SNMPv3* 属性を持つ複数ロールの設定

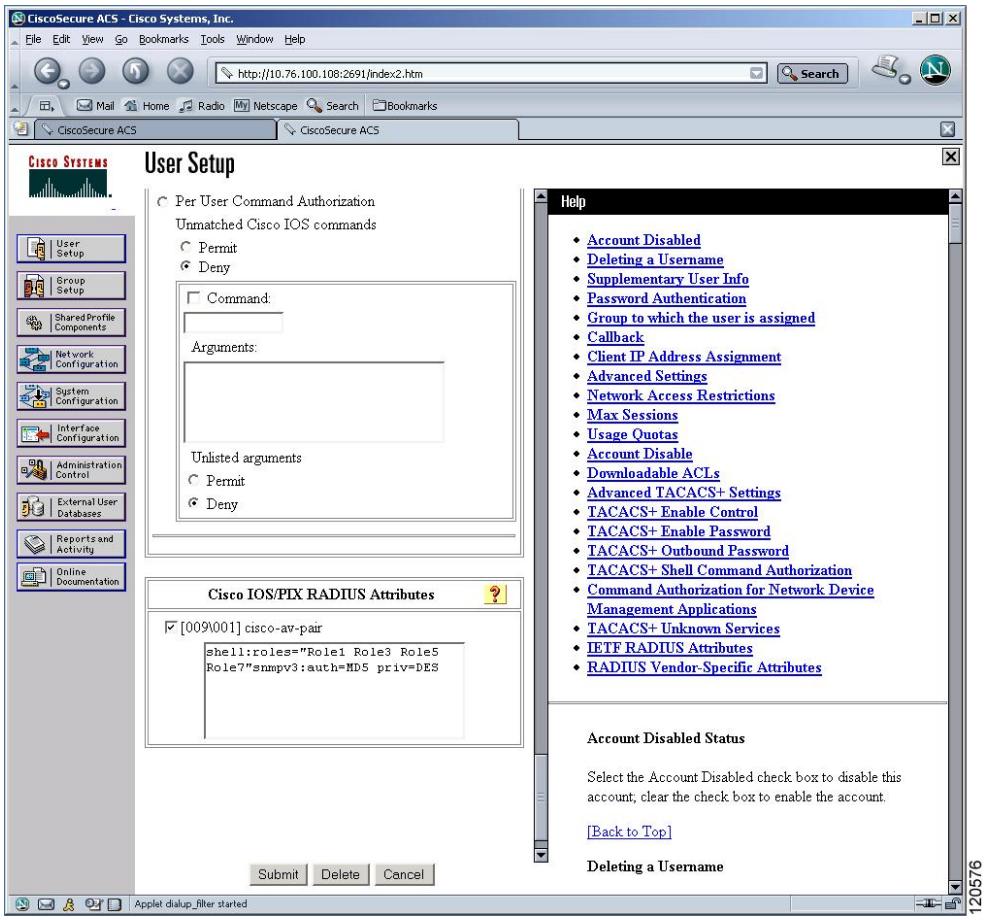


Figure 5: TACACS+ を使用する場合の *SNMPv3* 属性を持つ *network-admin* ロールの設定

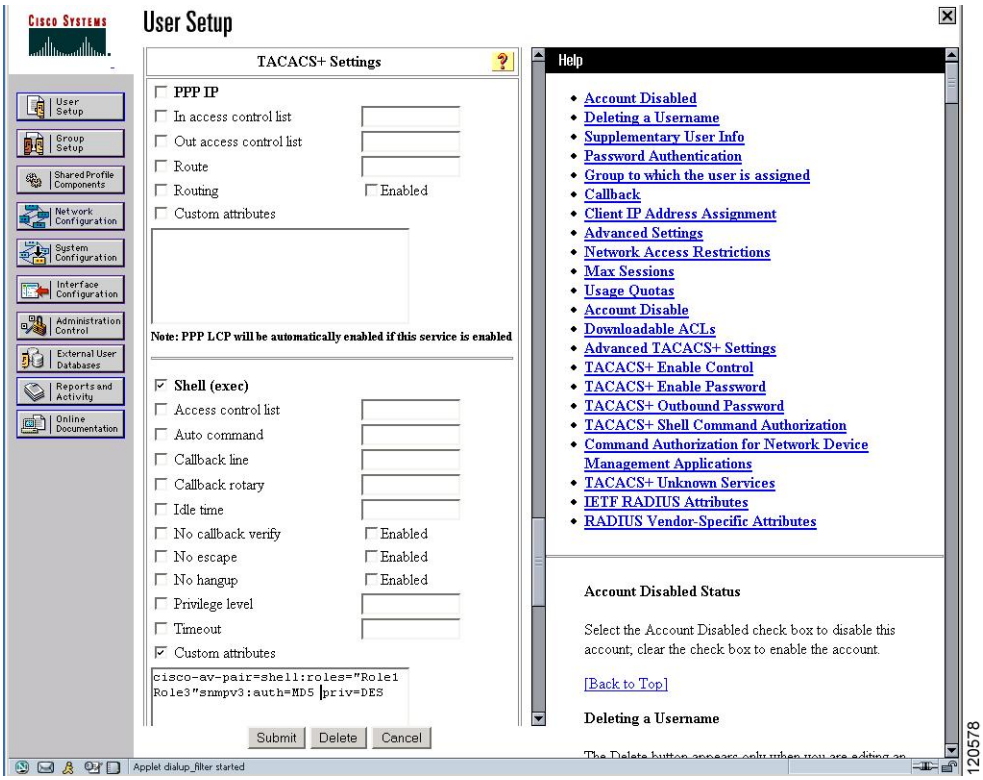
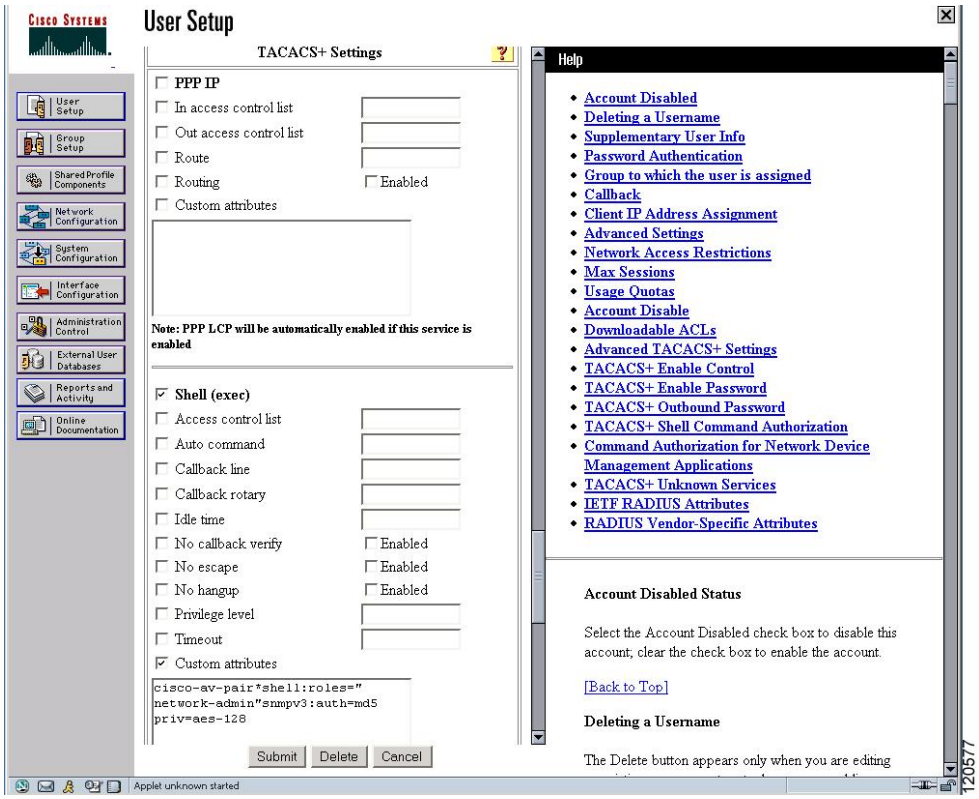


Figure 6: TACACS+ を使用する場合の ***SNMPv3*** 属性を持つ複数ロールの設定



デフォルト設定

次の表に、任意のスイッチにおける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。

Table 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
RADIUS サーバーのタイムアウト	1 秒
RADIUS サーバー再試行	1 回

パラメータ	デフォルト
許可	ディセーブル
デフォルトの AAA ユーザー ロール	enabled
RADIUS サーバーへの誘導要求	ディセーブル
TACACS+	ディセーブル
TACACS+ サーバー	未設定
TACACS+ サーバーのタイムアウト	5 秒
TACACS+ サーバーへの誘導要求	ディセーブル
AAA サーバーへの配信	ディセーブル
アカウンティング ログ サイズ	250 KB

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。