AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウンティング（AAA）を設定する手順について説明します。

この章は、次の項で構成されています。

AAA について

ここでは、Cisco NX-OS デバイスの AAA について説明します。

AAA セキュリティ サービス

AAA 機能を使用すると、Cisco NX-OS デバイスを管理するユーザの ID を確認し、ユーザにアクセスを許可し、ユーザの実行するアクションを追跡できます。Cisco NX-OS デバイスは、Remote

Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。

Cisco NX-OS は入力されたユーザ ID およびパスワードの組み合わせに基づいて、ローカル データベースによるローカル認証または許可、あるいは 1 つまたは複数の AAA サーバによるリモート認証または許可を実行します。Cisco NX-OS デバイスと AAA サーバの間の通信は、事前共有秘密キーによって保護されます。すべての AAA サーバ用または特定の AAA サーバ専用に共通秘密キーを設定できます。

AAA セキュリティは、次のサービスを実行します。

認証

ログインとパスワードのダイアログ、チャレンジとレスポンス、メッセージング サポート、および選択したセキュリティ プロトコルに応じた暗号化などを使用してユーザを識別します。
認証は、デバイスにアクセスする人物またはデバイスの ID を確認するプロセスです。この ID の確認は、Cisco NX-OS デバイスにアクセスするエンティティから提供されるユーザ ID とパスワードの組み合わせに基づいて行われます。Cisco NX-OS デバイスでは、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。

許可

アクセス コントロールを提供します。AAA 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。

アカウンティング

情報を収集する、情報をローカルのログに記録する、情報を AAA サーバに送信して課金、監査、レポート作成などを行う方法を提供します。
アカウンティング機能では、Cisco NX-OS デバイスへのアクセスに使用されるすべての管理セッションを追跡し、ログに記録して管理します。この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

（注） Cisco NX-OS ソフトウェアでは、認証、許可、およびアカウンティングを個別にサポートしています。たとえば、アカウンティングは設定せずに、認証と許可を設定したりできます。

AAA を使用する利点

AAA は、次のような利点を提供します。

- アクセス設定の柔軟性と制御性の向上
- 拡張性
- 標準化された認証方式（RADIUS、TACACS+ など）
- 複数のバックアップ デバイス

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 Cisco NX-OS デバイスのユーザ パスワード リストの管理が容易になります。
- AAA サーバはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべての Cisco NX-OS デバイスのアカウンティング ログを中央で管理できます。
- ファブリック内の各 Cisco NX-OS デバイスについてユーザ属性を管理する方が、Cisco NX-OS デバイスのローカル データベースを使用するより簡単です。

AAA 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 グループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバです。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 NX-OS デバイスは、最初のグループ内のサーバからエラーを受け取った場合、次のサーバ グループ内のサーバで試行します。

AAA サービス設定オプション

Cisco NX-OS デバイスの AAA 設定は、サービス ベースです。次のサービスごとに異なった AAA 設定を作成できます。

- User Telnet または Secure Shell（SSH）ログイン認証
- コンソール ログイン認証
- ユーザ管理セッション アカウンティング

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。

表 *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	**aaa authentication login default**
コンソール ログイン	**aaa authentication login console**
ユーザ セッション アカウンティング	**aaa accounting default**

AAA サービスには、次の認証方式を指定できます。

すべての RADIUS サーバ

RADIUS サーバのグローバル プールを使用して認証を行います。

指定サーバ グループ

設定した特定の RADIUS、TACACS+、または LDAP サーバ グループを使用して認証を行います。

ローカル

ローカルのユーザ名またはパスワード データベースを使用して認証を行います。

なし

AAA 認証が使用されないように指定します。

（注） 「指定サーバ グループ」方式でなく、「すべての RADIUS サーバ」方式を指定した場合、Cisco NX-OS デバイスは、設定された RADIUS サーバのグローバル プールから設定の順に RADIUS サーバを選択します。このグローバル プールからのサーバは、Cisco NX-OS デバイス上の RADIUS サーバ グループ内で選択的に設定できるサーバです。

次の表に、AAA サービスに対応して設定できる AAA 認証方式を示します。

表 *2*：*AAA* サービスの *AAA* 認証方式

AAA サービス	AAA の方式
コンソール ログイン認証	サーバ グループ、ローカル、なし
ユーザ ログイン認証	サーバ グループ、ローカル、なし

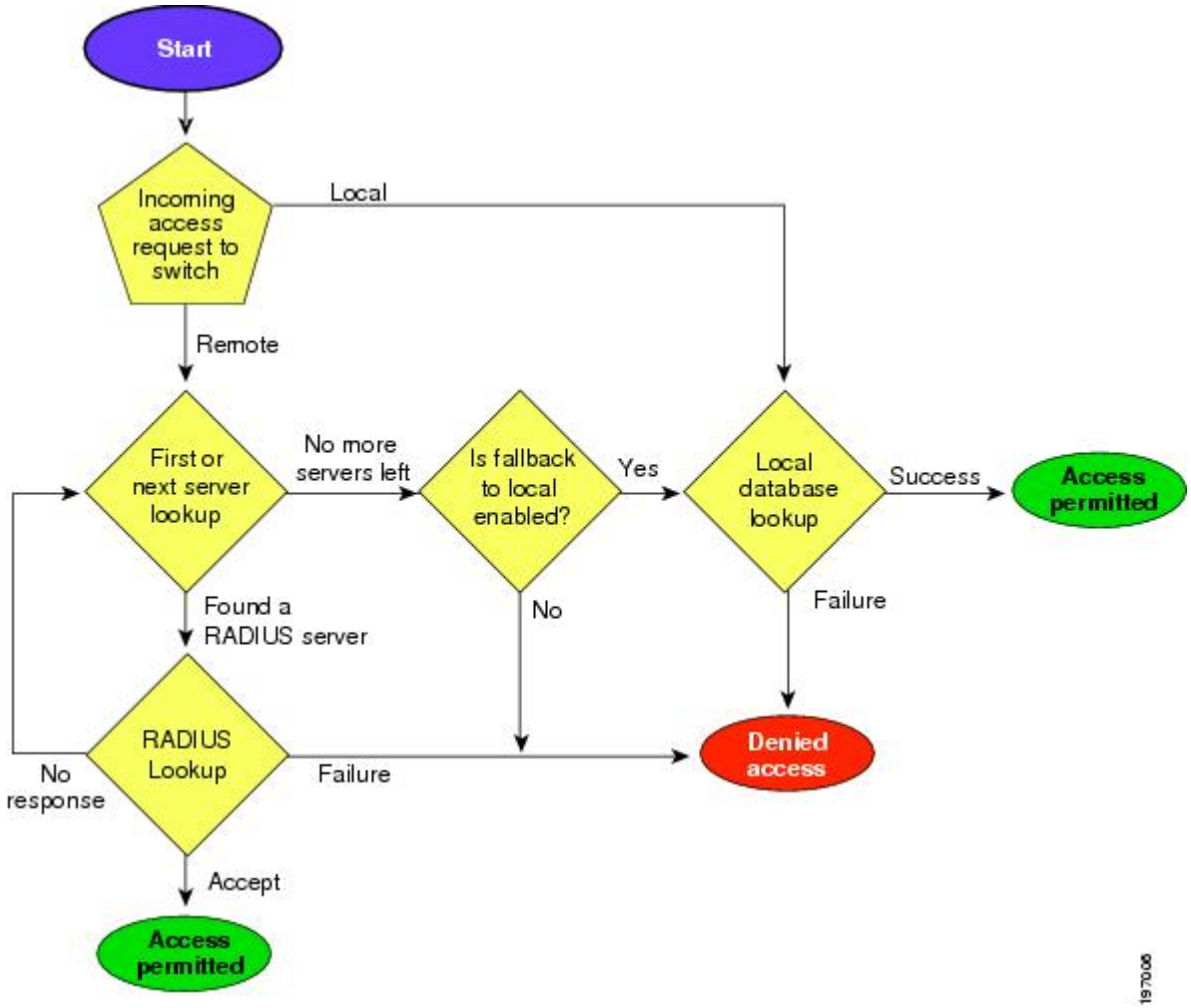
AAA サービス	AAA の方式
ユーザ管理セッション アカウンティング	サーバ グループ、ローカル

（注） コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッション アカウンティングについて、Cisco NX-OS デバイスは各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカル オプションがデフォルト方式です。**no aaa authentication login** {**console** | **default**} **fallback error local** コマンドを使用すると、コンソール ログインまたはデフォルト ログインの local オプションをディセーブルにできます。

ユーザ ログインの認証および許可プロセス

次の図に、ユーザ ログインの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 *1*：ユーザ ログインの認証および許可フロー



次に、このプロセスについて順番に説明します。

- Cisco NX-OS デバイスへのログイン時に、Telnet、SSH、またはコンソール ログインのオプションを使用できます。
- サーバ グループ認証方式を使用して AAA サーバ グループを設定している場合は、Cisco NX-OS デバイスが次のように、グループ内の最初の AAA サーバに認証要求を送信します。
  - 特定の AAA サーバが応答しなかった場合は、その次の AAA サーバ、さらにその次へと、各サーバが順に試行されます。この処理は、リモート サーバが認証要求に応答するまで続けられます。

- サーバ グループのすべての AAA サーバが応答しなかった場合、その次のサーバ グループのサーバが試行されます。
- コンソール ログインでローカルへのフォールバックがディセーブルでないかぎり、設定されている認証方式がすべて失敗した場合、ローカル データベースを使用して認証が実行されます。

- Cisco NX-OS デバイスがリモート AAA サーバ経由で正常に認証を実行した場合は、次の可能性があります。
  - AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともに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。
- ユーザ名とパスワードがローカルで正常に認証された場合は、Cisco NX-OS デバイスにログインでき、ローカル データベース内で設定されているロールが割り当てられます。

（注） 「残りのサーバ グループなし」とは、すべてのサーバ グループのいずれのサーバからも応答がないということです。「残りのサーバなし」とは、現在のサーバ グループ内のいずれのサーバからも応答がないということです。

AES パスワード暗号化およびマスター暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）をイネーブルにすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能をイネーブルにし、パスワード暗号化および復号化に使用されるマスター暗号キーを設定する必要があります。

AES パスワード暗号化をイネーブルにしてマスター キーを設定すると、タイプ 6 パスワード暗号化をディセーブルにしない限り、サポートされているアプリケーション（現在は RADIUS と TACACS+）の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を設定することもできます。

AAA のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	AAA にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 少なくとも 1 台の RADIUS サーバ、TACACS+ サーバ、または LDAP サーバが IP を使用して到達可能であることを確認します。
- Cisco NX-OS デバイスが、AAA サーバのクライアントとして設定されていること。
- 秘密キーが、Cisco NX-OS デバイスおよびリモート AAA サーバに設定されていることを確認します。
- リモート サーバが Cisco NX-OS デバイスからの AAA 要求に応答することを確認します。

AAA の注意事項と制約事項

AAA に関する注意事項と制約事項は次のとおりです。

- 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。

AAA のデフォルト設定

次の表に、AAA パラメータのデフォルト設定を示します。

表 *3*：*AAA* パラメータのデフォルト設定

パラメータ	デフォルト
コンソール認証方式	local
デフォルト認証方式	local

パラメータ	デフォルト
ログイン認証失敗メッセージ	ディセーブル
CHAP 認証	ディセーブル
MSCHAP 認証	ディセーブル
デフォルト アカウンティング方式	local
アカウンティング ログの表示サイズ	250 KB

AAA の設定

ここでは、Cisco NX-OS デバイスで AAA 機能を設定する手順について説明します。

（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。

AAA の設定プロセス

AAA 認証およびアカウンティングを設定するには、次の作業を行います。

1. 認証にリモート RADIUS、TACACS+、または LDAP サーバを使用する場合は、Cisco NX-OS デバイス上でホストを設定します。
2. コンソール ログイン認証方式を設定します。
3. ユーザ ログインのためのデフォルトのログイン認証方式を設定します。
4. デフォルト AAA アカウンティングのデフォルト方式を設定します。

コンソール ログイン認証方式の設定

ここでは、コンソール ログインの認証方式を設定する方法を説明します。

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース

- ユーザ名だけ（none）

デフォルトの方式はローカルですが、ディセーブルにするオプションがあります。

（注） **aaa authentication** コマンドの **group radius** および **group***server-name* 形式は、以前に定義された RADIUS サーバのセットを参照します。**radius-server host** コマンドを使用してホスト サーバを設定します。サーバの名前付きグループを作成するには、**aaa group server radius** コマンドを使用します。

（注） リモート認証がイネーブルになっているときにパスワード回復を実行すると、パスワード回復の実行後すぐにコンソール ログインのローカル認証がイネーブルになります。そのため、新しいパスワードを使用して、コンソール ポート経由で Cisco NX-OS デバイスにログインできます。ログイン後は、引き続きローカル認証を使用するか、または AAA サーバで設定された管理者パスワードのリセット後にリモート認証をイネーブルにすることができます。パスワード回復プロセスに関する詳細情報については、『*Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*』を参照してください。

はじめる前に

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa authentication login console** {**group***group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 authentication login console** {**group***group-list* [**none**]	**local**	**none**} 例： `switch(config)# aaa authentication login console group radius`	コンソールのログイン認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。

	コマンドまたはアクション	目的
		radius RADIUS サーバのグローバル プールを使用して認証を行います。 ***named-group*** RADIUS、TACACS+、または LDAP サーバの指定サブセットを使用して認証を行います。 **local** 方式では、ローカル データベースを認証に使用します。**none** 方式では、AAA 認証が使用されないように指定します。 デフォルトのコンソール ログイン方式は **local** です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対してローカルへのフォールバックがディセーブルでない限り、使用されます。

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

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） コンソール ログイン認証方式の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

デフォルトのログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名だけ

デフォルトの方式はローカルですが、ディセーブルにするオプションがあります。

はじめる前に

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa authentication login default** {**group***group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 authentication login default** {**group***group-list* [**none**]	**local**	**none**} 例： `switch(config)# aaa authentication login default group radius`	デフォルト認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：認証に RADIUS、TACACS+ または LDAP サーバの名前付きサブセットを使用します。 **local** 方式では、ローカル データベースを認証に使用します。**none** 方式では、AAA 認証が使用されないように指定します。デフォルトのログイン方式は **local** です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対してローカルへのフォール バックがディセーブルでない限り、使用されます。 次のいずれかを設定できます。 • AAA 認証グループ • 認証なしの AAA 認証グループ • ローカル認証 • 認証なし

	コマンドまたはアクション	目的
		（注） **local** キーワードは、AAA 認証グループを設定するときはサポートされません（必須ではありません）。これは、ローカル認証は、リモートサーバが到達不能の場合のデフォルトであるためです。たとえば、**aaa authentication login default group g1** を設定した場合、AAA グループ g1 を使用して認証を行うことができなければ、ローカル認証が試行されます。これに対し、**aaa authentication login default group g1 none** を設定した場合、AAA グループ g1 を使用して認証を行うことができなければ、認証は実行されません。

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

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） デフォルトのログイン認証方式の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

ローカル認証へのフォールバックのディセーブル化

デフォルトでは、コンソールログインまたはデフォルトログインのリモート認証が設定されている場合、どのAAAサーバにも到達不能なときに（認証エラーになります）、ユーザがCisco NX-OSデバイスからロックアウトされないように、ローカル認証にフォールバックされます。ただし、セキュリティを向上させるために、ローカル認証へのフォールバックをディセーブルにできます。

注意 ローカル認証へのフォールバックをディセーブルにすると、Cisco NX-OSデバイスがロックされ、パスワード回復を実行しないとアクセスできなくなることがあります。デバイスからロックアウトされないようにするために、ローカル認証へのフォールバックをディセーブルにする対象は、デフォルト ログインとコンソール ログインの両方ではなく、いずれかだけにすることを推奨します。

はじめる前に

コンソール ログインまたはデフォルト ログインのリモート認証を設定します。

手順の概要

1. **configure terminal**
2. **no aaa authentication login {console | default} fallback error local**
3. （任意） **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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	**no aaa authentication login {console | default} fallback error local** 例： `switch(config)# no aaa authentication login console fallback error local`	コンソール ログインまたはデフォルト ログインについて、リモート認証が設定されている場合にどの AAA サーバにも到達不能なときに実行されるローカル認証へのフォールバックをディセーブルにします。 ローカル認証へのフォールバックをディセーブルにすると、次のメッセージが表示されます。 "WARNING!!! Disabling fallback can lock your switch."

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

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） コンソール ログインおよびデフォルト ログイン認証方式の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

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、RADIUS または TACACS+ 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、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。

手順の概要

1. **configure terminal**
2. **aaa user default-role**
3. **exit**
4. （任意） **show aaa user default-role**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** 例： `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** の形式を使用します。

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

ステップ 4	**show aaa user default-role** 例： `switch# show aaa user default-role`	（任意） AAA デフォルト ユーザ ロールの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

ログイン認証失敗メッセージのイネーブル化

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。このような場合に、ログイン失敗メッセージがイネーブルになっていると、次のメッセージがユーザの端末に表示されます。

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

手順の概要

1. **configure terminal**
2. **aaa authentication login error-enable**
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 authentication login error-enable** 例： `switch(config)# aaa authentication login error-enable`	ログイン認証失敗メッセージをイネーブルにします。デフォルトではディセーブルになっています。

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

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） ログイン失敗メッセージの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

成功および失敗したログイン試行のロギング

成功および失敗したすべてのログイン試行のログを、設定済みの syslog サーバへ記録するようにスイッチを設定できます。

手順の概要

1. **configure terminal**
2. **[no] login on-failure log**
3. **[no] login on-success log**
4. （任意） **show login on-failure log**
5. （任意） **show login on-successful log**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	**[no] login on-failure log** 例： `switch(config)# login on-failure log`	失敗した認証に関するすべてのメッセージを、設定済みの syslog サーバに記録します。この設定では、次の syslog メッセージが失敗したログインの後に表示されます。 「AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user admin from 172.22.00.00」 （注） ログ レベルで authpriv を 6 とした場合、前述のメッセージと併せて追加の Linux カーネル認証メッセージも表示されます。これらの追加メッセージを無視させたい場合は、authpriv 値を 3 に設定する必要があります。
ステップ 3	**[no] login on-success log** 例： `switch(config)# login on-success log`	成功した認証に関するすべてのメッセージを、設定済みの syslog サーバに記録します。この設定では、次の syslog メッセージが成功したログインの後に表示されます。 「AUTHPRIV-6-SYSTEM_MSG: pam_aaa:Authentication success for user admin from 172.22.00.00」 （注） ログ レベルで authpriv を 6 とした場合、前述のメッセージと併せて追加の Linux カーネル認証メッセージも表示されます。

	コマンドまたはアクション	目的
ステップ 4	**show login on-failure log** 例： `switch(config)# show login on-failure log`	（任意） ログイン認証失敗メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
ステップ 5	**show login on-successful log** 例： `switch(config)# show login on-successful log`	（任意） ログイン認証成功メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

CHAP 認証のイネーブル化

Cisco NX-OS ソフトウェアは、チャレンジ ハンドシェーク認証プロトコル（CHAP）をサポートしています。このプロトコルは、業界標準の Message Digest（MD5）ハッシュ方式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方式のプロトコルです。リモート認証サーバ（RADIUS または TACACS+）を通じて、Cisco NX-OS デバイスへのユーザ ログインに CHAP を使用できます。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート 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。CHAP がイネーブルの場合は、CHAP ベンダー固有属性（VSA）を認識するように RADIUS サーバまたは TACACS+ サーバを設定する必要があります。

次の表に、CHAP に必要な RADIUS および TACACS+ VSA を示します。

表 *4*：*CHAP RADIUS* および *TACACS+ VSA*

ベンダー ID 番号	ベンダー タイプ番号	VSA	説明
311	11	CHAP-Challenge	AAA サーバから CHAP 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。

ベンダー ID 番号	ベンダー タイプ番号	VSA	説明
211	11	CHAP-Response	チャレンジに対する応答として CHAP ユーザが入力した値を保持します。Access-Request パケットだけで使用します。

はじめる前に

ログイン用の AAA ASCII 認証をディセーブルにします。

手順の概要

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login chap enable**
4. （任意） **exit**
5. （任意） **show aaa authentication login chap**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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	**no aaa authentication login ascii-authentication** 例： `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証をディセーブルにします。
ステップ 3	**aaa authentication login chap enable** 例： `switch(config)# aaa authentication login chap enable`	CHAP 認証をイネーブルにします。デフォルトではディセーブルになっています。 （注） Cisco NX-OS デバイスで、CHAP と MSCHAP（または MSCHAP V2）の両方をイネーブルにすることはできません。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		（任意）
		設定モードを終了します。

ステップ 5	**show aaa authentication login chap** 例： `switch# show aaa authentication login chap`	（任意） CHAP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

MSCHAP または MSCHAP V2 認証のイネーブル化

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 NX-OS ソフトウェアは、MSCHAP Version 2（MSCHAP V2）にも対応しています。リモート認証サーバ（RADIUS または TACACS+）を通じて、Cisco NX-OS スイッチへのユーザ ログインに MSCHAP を使用できます。MSCHAP V2 では、リモート認証 RADIUS サーバを介した Cisco NX-OS デバイスへのユーザ ログインだけがサポートされます。MSCHAP V2 の場合に TACACS+ グループを設定すると、デフォルトの AAA ログイン認証では、次に設定されている方式が使用されます。他のサーバ グループが設定されていない場合は、ローカル方式が使用されます。

（注） Cisco NX-OS ソフトウェアは、次のメッセージを表示する場合があります。

「Warning: MSCHAP V2 is supported only with Radius.」

この警告メッセージは単なる情報メッセージであり、RADIUS での MSCHAP V2 の動作には影響しません。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート 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 または MSCHAP V2 をイネーブルにする場合は、MSCHAP および MSCHAP V2 ベンダー固有属性（VSA）を認識するように RADIUS サーバを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

表 *5* : *MSCHAP* および *MSCHAP V2 RADIUS VSA*

ベンダー ID 番号	ベンダー タイプ番号	VSA	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP または MSCHAP V2 ユーザに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	MSCHAP-Response	チャレンジに対する応答として MSCHAP または MSCHAP V2 ユーザが入力した値を保持します。Access-Request パケットでしか使用されません。

はじめる前に

ログイン用の AAA ASCII 認証をディセーブルにします。

手順の概要

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login** {**mschap** | **mschapv2**} **enable**
4. **exit**
5. （任意） **show aaa authentication login** {**mschap** | **mschapv2**}
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	**no aaa authentication login ascii-authentication** 例： `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証をディセーブルにします。
ステップ 3	**aaa authentication login** {**mschap** | **mschapv2**} **enable** 例： `switch(config)# aaa authentication login mschap enable`	MSCHAP または MSCHAP V2 認証をイネーブルにします。デフォルトではディセーブルになっています。 （注） Cisco NX-OS デバイスで、MSCHAP と MSCHAP V2 の両方をイネーブルにすることはできません。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show aaa authentication login** {**mschap** | **mschapv2**} 例： `switch# show aaa authentication login mschap`	（任意） MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

デフォルトの AAA アカウンティング方式の設定

Cisco NX-OS ソフトウェアは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。Cisco NX-OS デバイスは、ユーザ アクティビティをアカウンティング レコードの形で TACACS+ セキュリティ サーバまたは RADIUS セキュリティ サーバに報告します。各アカウンティング レコードに、アカウンティング属性値（AV）のペアが入っており、それが AAA サーバに格納されます。

AAA アカウンティングをアクティブにすると、Cisco NX-OS デバイスは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

特定のアカウンティング方式を定義するデフォルト方式リストを作成できます。次の方式を含めることができます。

RADIUS サーバ グループ

RADIUS サーバのグローバル プールを使用してアカウンティングを行います。

指定されたサーバ グループ

指定された RADIUS または TACACS+ サーバ グループを使用してアカウンティングを行います。

ローカル

ローカルのユーザ名またはパスワード データベースを使用してアカウンティングを行います。

（注） サーバ グループが設定されていて、そのサーバ グループが応答しない場合、デフォルトではローカル データベースが認証に使用されます。

はじめる前に

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa accounting default** {**group***group-list* | **local**}
3. **exit**
4. （任意） **show aaa accounting**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 accounting default** {**group***group-list* | **local**} 例： `switch(config)# aaa accounting default group radius`	デフォルトのアカウンティング方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** を指定すると、RADIUS サーバのグローバル プールがアカウンティングに使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウンティングに使用されます。

	コマンドまたはアクション	目的
		local 方式では、アカウンティングにローカルデータベースが使用されます。 デフォルトの方式は、**local** です。これはサーバ グループが何も設定されていない場合、または設定されたすべてのサーバ グループから応答が得られなかった場合に使用されます。

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

ステップ 4	**show aaa accounting** 例： `switch# show aaa accounting`	（任意） デフォルトの AAA アカウンティング方式の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

Cisco NX-OS デバイスによる AAA サーバの VSA の使用

ベンダー固有属性（VSA）を使用して、AAA サーバ上での Cisco NX-OS ユーザ ロールおよび SNMPv3 パラメータを指定できます。

VSA 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 サーバと RADIUS サーバの間での 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、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

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

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

Cisco NX-OS デバイスでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

VSA の形式

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

Shell

ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Accounting

accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲んでください。

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

ユーザに割り当てられたすべてのロールの一覧です。値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。たとえば、ユーザが network-operator および network-admin のロールに属している場合、値フィールドは network-operator network-admin となります。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例を示します。

```
shell:roles=network-operator network-admin
```

```
shell:roles*network-operator network-admin
```

次に、FreeRADIUS でサポートされるロール属性の例を示します。

```
Cisco-AVPair = shell:roles=\network-operator network-admin\
```

```
Cisco-AVPair = shell:roles*\network-operator network-admin\
```

（注） VSA を、shell:roles*"network-operator network-admin" または "shell:roles*\"network-operator network-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo

標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性が送信されるのは、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分内だけです。この属性は、アカウンティング プロトコル関連の PDU でしか使用できません。

AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバで VSA cisco-av-pair を使用して、次の形式で、Cisco NX-OS デバイスのユーザ ロール マッピングを指定できます。

```
shell:roles="roleA roleB …"
```

cisco-av-pair 属性にロール オプションを指定しなかった場合のデフォルトのユーザ ロールは、network-operator です。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
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。cisco-av-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

セキュア ログイン機能の設定

ログイン パラメータの設定

ログイン パラメータの設定では、サービス妨害（DoS）攻撃の可能性が検出された場合に、以降のログイン試行を自動的にブロックさせる、あるいは接続試行の失敗が複数検出された場合に、辞書攻撃の進行をスロー ダウンさせるため強制的に待機モードに入らせることができます。

（注） システムのスイッチオーバーが発生するか、または AAA プロセスが再起動した場合、この機能は再起動します。

手順の概要

1. **configure terminal**
2. [**no**] **login block-for***seconds***attempts***tries***within***seconds*
3. （任意） [**no**] **login quiet-mode access-class***acl-name*
4. （任意） **show login** [**failures**]
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	[**no**] **login block-for***seconds***attempts***tries***within***seconds* 例： `switch(config)# login block-for 100 attempts 2 within 60`	待機モードの期間を設定します。すべての引数の範囲は 1 ～ 65535 です。 ここの例では、60 秒以内に 2 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しています。 このコマンドを入力すると、Telnet または SSH を経由したログイン試行は、待機モード中にすべて拒否されます。アクセス コントロール リスト（ACL）は、**login quiet-mode access-class** コマンドが入力されない限り、待機時間から除外されません。 （注） このコマンドは、その他のログイン コマンドを使用する前に入力する必要があります。
ステップ 3	[**no**] **login quiet-mode access-class***acl-name* 例： `switch(config)# login quiet-mode access-class myacl`	（任意） 待機モードに切り替わるときに、スイッチに適用される ACL を指定します。スイッチが待機モードにある場合、すべてのログイン要求が拒否され、使用可能な接続はコンソールを経由したものだけになります。
ステップ 4	**show login** [**failures**] 例： `switch(config)# show login`	（任意） ログイン パラメータを表示します。**failures** オプションは、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。
ステップ 5	**copy running-config startup-config** 例： `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。

ユーザ ログイン セッションの制限

ユーザあたりの同時ログイン セッションの最大数を制限できます。これは複数の不要なセッションをユーザに与えることを防止し、不正ユーザによる有効な SSH または Telnet セッションへのアクセスという潜在的なセキュリティ問題を解消します。

手順の概要

1. **configure terminal**
2. [**no**] **user max-logins***max-logins*
3. （任意） **show running-config all | i max-login**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	[**no**] **user max-logins***max-logins* 例： `switch(config)# user max-logins 1`	ユーザあたりの同時ログイン セッションの最大数を制限します。指定できる範囲は 1 ～ 7 です。最大ログイン制限を 1 に設定すると、ユーザあたりに割り当てられる Telnet または SSH セッションは 1 つだけになります。 （注） 設定されたログインの制限は、すべてのユーザに適用されます。個々のユーザごとに異なる制限を設定することはできません。
ステップ 3	**show running-config all | i max-login** 例： `switch(config)# show running-config all | i max-login`	（任意） ユーザごとに許可されたログイン セッションの最大数を表示します。
ステップ 4	**copy running-config startup-config** 例： `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。

パスワードの長さの制限

ユーザ パスワードの最小および最大の長さを制限できます。この機能を使用して、ユーザに強力なパスワードを入力するように強制することでシステムのセキュリティを高めることができます。

はじめる前に

password strength-check コマンドを使用して、パスワードの強度の確認をイネーブルにする必要があります。パスワードの長さは制限しているがパスワードの強度の確認はイネーブルにしていない場合、制限長を超えたパスワードをユーザが入力すると、エラーは表示されますが、ユーザ

アカウントは作成されます。パスワード長を強制的に適用させてこうしたユーザ アカウントの作成を防ぐには、パスワードの強度の確認をイネーブルにしてパスワードの長さを制限する必要があります。

手順の概要

1. **configure terminal**
2. [**no**] **userpassphrase** {**min-length***min-length* | **max-length***max-length*}
3. （任意） **show userpassphrase** {**length** | **max-length** | **min-length**}
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	[**no**] **userpassphrase** {**min-length***min-length*	**max-length***max-length*} 例： `switch(config)# userpassphrase min-length 8 max-length 80`	ユーザ パスワードの最小または最大の長さを制限します。パスワードの最小長は 4 ～ 127 文字であり、パスワードの最大長さは 80 ～ 127 文字です。
ステップ 3	**show userpassphrase** {**length**	**max-length**	**min-length**} 例： `switch(config)# show userpassphrase length`	（任意） ユーザ パスワードの最小および最大の長さが表示されます。
ステップ 4	**copy running-config startup-config** 例： `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。

ユーザ名のパスワード プロンプトのイネーブル化

ユーザによるユーザ名入力後にパスワード入力を要求するように、スイッチを設定できます。

手順の概要

1. **configure terminal**
2. **password prompt username**
3. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	**password prompt username**
	
	例：
	`switch(config)# password prompt username`
	`Password prompt username is enabled.`
	`After providing the required options in the username command, press enter.`
	`User will be prompted for the username password and password will be hidden.`
	`Note: Choosing password key in the same line while configuring user account, password will not be hidden.`
		password オプションを付けずに **username** コマンドまたは **snmp-server user** コマンドが入力された後に、ユーザに対してパスワード入力要求のプロンプトを表示するようスイッチを設定します。ユーザが入力したパスワードは非表示にされます。こ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	**copy running-config startup-config** 例： `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。

RADIUS または TACACS+ の共有秘密の設定

スイッチと RADIUS または TACACS+ サーバ間のアカウンティングおよびリモート認証用に設定する共有秘密は、機密情報であるため隠しておく必要があります。これらの暗号化された共有秘密の生成には、**radius-server** [**host**] **key** および **tacacs-server** [**host**] **key** コマンドをそれぞれ使用します。暗号化された共有秘密の保存には SHA256 ハッシュ メソッドが使用されます。

手順の概要

1. **configure terminal**
2. **generate type7_encrypted_secret**
3. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	**generate type7_encrypted_secret**
	
	例：
	`switch(config)# generate type7_encrypted_secret`
	`Type-7 (Vigenere) Encryption,`
	`Use this encrypted secret to configure radius and tacacs shared secret with key type 7.`
	`Copy complete secret with double quotes.`
	
	`Enter plain text secret:`
	`Confirm plain text secret:`
	`Type 7 Encrypted secret is : "fewhg"`
		RADIUS または TACACS+ 共有秘密をキー タイプ 7 で設定します。共有秘密をプレーン テキストで 2 回入力するよう求められます。秘密情報は、入力時に非表示にされます。その後、暗号化されたバージョンの秘密情報が表示されます。
		
		（注） プレーンテキストの秘密情報の暗号化バージョンを別途生成しておき、その後で暗号化された共有秘密を設定するには、**radius-server** [**host**] **key** および **tacacs-server** [**host**] **key** コマンドを使用します。

ステップ 3	**copy running-config startup-config** 例： `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。

ローカルAAAアカウンティングログのモニタリングとクリア

Cisco NX-OS デバイスは、AAA アカウンティング アクティビティのローカル ログを保持しています。このログはモニタリングしたりクリアしたりできます。

手順の概要

1. **show accounting log** [*size* | **last-index** | **start-seqnum***number* | **start-time***year month day hh*:*mm*:*ss*]
2. （任意） **clear accounting log**[**logflash**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show accounting log** [*size* | **last-index** | **start-seqnum***number* | **start-time***year month day hh*:*mm*:*ss*] 例： `switch# show accounting log`	アカウンティング ログを表示します。このコマンド出力には、デフォルトで最大 250,000 バイトのアカウンティング ログが表示されます。コマンドの出力を制限する場合は、*size* 引数を使用します。指定できる範囲は 0 ～ 250000 バイトです。また、ログ出力の開始シーケンス番号または開始時間を指定できます。開始インデックスの範囲は、1 ～ 1000000 です。アカウンティング ログ ファイルにある最後のインデックス番号の値を表示するには、**last-index** キーワードを使用します。
ステップ 2	**clear accounting log**[**logflash**] 例： `switch# clear aaa accounting log`	（任意） アカウンティング ログの内容をクリアします。**logflash** キーワードはログ フラッシュに保存されているアカウンティング ログをクリアします。

AAA 設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show aaa accounting	AAA アカウンティングの設定を表示します。
show aaa authentication [**login** {**ascii-authentication**| **chap**| **error-enable** | **mschap** | **mschapv2**}]	AAA 認証ログイン設定情報を表示します。
show aaa groups	AAA サーバ グループの設定を表示します。
show login [**failures**]	ログイン パラメータを表示します。**failures** オプションは、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。 （注） **clear login failures** コマンドは、現在の監視期間でのログインの失敗をクリアします。

コマンド	目的
show login on-failure log	ログイン認証失敗メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
show login on-successful log	ログイン認証成功メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
show running-config aaa [**all**]	実行コンフィギュレーションの AAA 設定を表示します。
show running-config all | i max-login	ユーザごとに許可されたログイン セッションの最大数を表示します。
show startup-config aaa	スタートアップ コンフィギュレーションの AAA 設定を表示します。
show userpassphrase {**length** | **max-length** | **min-length**}	ユーザ パスワードの最小および最大の長さが表示されます。

AAA の設定例

次に、AAA を設定する例を示します。

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

ログイン パラメータの設定例

次に、60 秒以内に 3 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。この例は、ログインの失敗を示しません。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# 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 3 login failures occur in 60 seconds or less,
 logins will be disabled for 100 seconds.

 Switch presently in Normal-Mode.
 Current Watch Window remaining time 45 seconds.
 Present login failure count 0.

switch(config)# show login failures
*** No logged failed login attempts with the device.***
```

以下に、待機モード ACL の設定例を示します。待機時間中、myacl の ACL 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。この例は、ログインの失敗も示します。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# login quiet-mode access-class myacl

switch(config)# show login

 Switch is enabled to watch for login Attacks.
 If more than 3 login failures occur in 60 seconds or less,
 logins will be disabled for 100 seconds.

 Switch presently in Quiet-Mode.
 Will remain in Quiet-Mode for 98 seconds.
 Denying logins from all sources.

switch(config)# show login failures
Information about last 20 login failure's with the device.
--------------------------------------------------------------------------------
Username      Line          SourceIPAddr    Appname    TimeStamp
--------------------------------------------------------------------------------
asd           /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:18:54 2015
qweq          /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:19:02 2015
qwe           /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:19:08 2015
--------------------------------------------------------------------------------
```

パスワード プロンプト機能の設定例

次の例では、**username** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、パスワードが入力されなかった場合にはエラー メッセージを表示するようスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password will
 not be hidden.


switch(config)# username user1
Enter password:
Confirm password:
warning: password for user:user1 not set. S/he may not be able to login
```

次の例では、**snmp-server user** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、その後、ユーザに提示するプロンプトを表示するようにスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
```

```
Note: Choosing password key in the same line while configuring user account, password will
 not be hidden.


N9K-1(config)# snmp-server user user1
Enter auth md5 password (Press Enter to Skip):
Enter auth sha password (Press Enter to Skip):
```

AAA に関する追加情報

ここでは、AAA の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
AAA に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html