



AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウントिंग（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, on page 1](#)
- [AAA の前提条件, on page 6](#)
- [AAA の注意事項と制約事項, on page 6](#)
- [AAA のデフォルト設定, on page 7](#)
- [AAA の設定, on page 7](#)
- [ローカル AAA アカウントング ログのモニタリングとクリア , on page 29](#)
- [AAA 設定の確認, on page 30](#)
- [AAA の設定例, on page 31](#)
- [ログインパラメータの設定例 \(31 ページ\)](#)
- [パスワードプロンプト機能の設定例 \(32 ページ\)](#)
- [AAA に関する追加情報, on page 33](#)

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。

アカウントティング

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。

アカウントティング機能では、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。アカウントティングログは、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。



Note Cisco NX-OS ソフトウェアでは、認証、許可、およびアカウントティングを個別にサポートしています。たとえば、アカウント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トिंग 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、アカウントिंग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 アカウントिंग

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	<code>aaa authentication login default</code>

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
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。



Note 「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。

Table 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
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

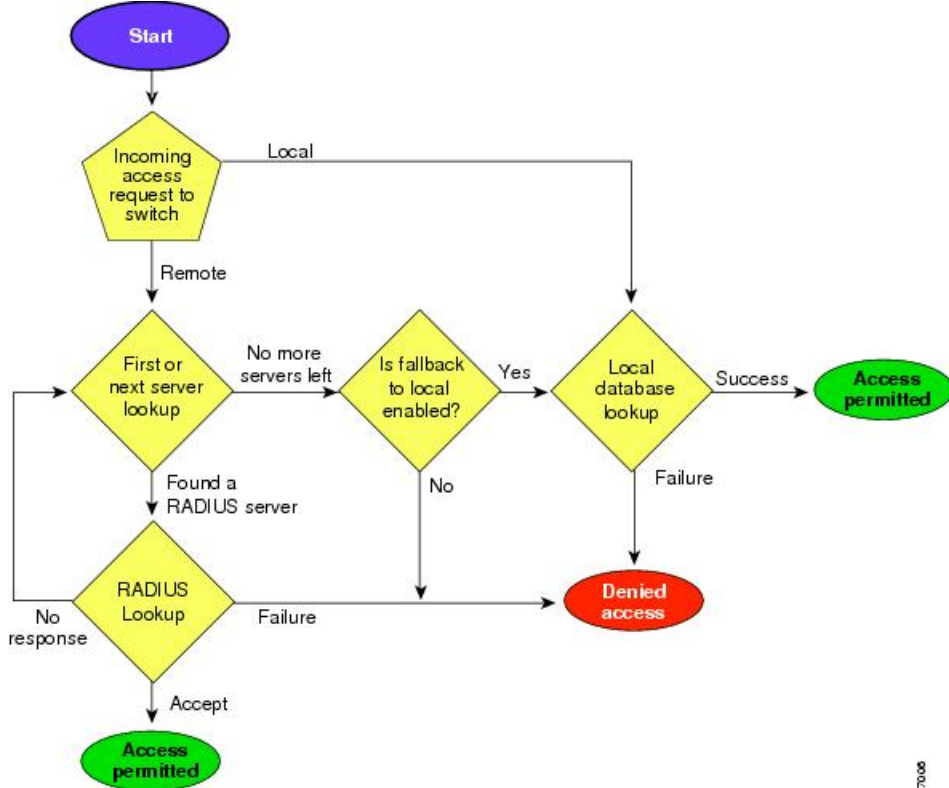


Note コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッションアカウンティングについて、Cisco NX-OS デバイスは各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカルオプションがデフォルト方式です。コンソールまたはデフォルトログインのローカルオプションを無効にするには、**no aaa authentication login {console | default} fallback error local** コマンドを使用します。

???

Figure 1: ???

??????



157006

??????

- Cisco NX-OS Telnet/SSH
- Cisco NX-OS AAA
 - AAA RADIUS cisco-av-pair
 - AAA TACACS+
- Cisco NX-OS AAA

**Note**

?????? ?????????????????? ??
 ???

AES パスワード暗号化およびプライマリ暗号キー

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有効にし、パスワード暗号化および復号化に使用されるプライマリ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プライマリ 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。
- Cisco Nexus 9000 シリーズスイッチは、TACACS + でのみ **aaa authentication login ascii-authentication** コマンドをサポートします (RADIUS ではサポートしません)。
- デフォルトのログイン認証方式を (**local** キーワードを使用せずに) 変更すると、コンソールログイン認証方式が設定によって上書きされます。コンソール認証方式を明示的に設定

するには、`aaa authentication login console {group group-list [none] | local | none}` コマンドを使用します。

- **login block-for** および **login quiet-mode** コンフィギュレーション モード コマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。
- **system login quiet-mode access-class QUIET_LIST** コマンドを使用する場合は、指定したトラフィックのみをブロックするようにアクセスリストが正しく定義されていることを確認する必要があります。たとえば、信頼できないホストからのユーザログインのみをブロックする必要がある場合、アクセスリストは、それらのホストからのSSH、Telnet、およびHTTP ベースのアクセスに対応するポート22、23、80、および443を指定する必要があります。

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。

Table 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	ローカル
デフォルト認証方式	ローカル
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	ローカル
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。



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りますので注意してください。



Note Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、`syslog` エラーが表示されます。

AAA の設定プロセス

AAA 認証およびアカウントिंग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 アカウントिंग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。



Note `aaa authentication` コマンドの `group radius` および `groupserver-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。ホストサーバを設定するには、`radius server-host` コマンドを使用します。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。

**Note**

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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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} Example: <pre>switch(config)# aaa authentication login console group radius</pre>	コンソールのログイン認証方式を設定します。 <i>group-list</i> 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 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

	Command or Action	Purpose
		ローカルへのフォールバックが無効でない限り、使用されます。
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 authentication Example: switch# show aaa authentication	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	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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。

Before you begin

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。

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 authentication login default { group group-list [none] local none }	デフォルト認証方式を設定します。

Command or Action	Purpose
<p>Example:</p> <pre>switch(config)# aaa authentication login default group radius</pre>	<p><i>group-list</i> 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。</p> <ul style="list-style-type: none"> • radiusRADIUS 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 : 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。 <p>local 方式は、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。</p> <p>次のいずれかを設定できます。</p> <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
		<p>Note 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。</p>
ステップ 3	<p>exit</p> <p>Example:</p> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	<p>(Optional) show aaa authentication</p> <p>Example:</p> <pre>switch# show aaa authentication</pre>	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	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch# copy running-config startup-config</pre>	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。

**Caution**

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。

Before you begin

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。

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	no aaa authentication login {console default} fallback error local Example: 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。 <div style="background-color: #f0f0f0; padding: 5px;">□ WARNING!!! Disabling fallback can lock your switch. □</div>
ステップ 3	(Optional) 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 authentication Example: switch# show aaa authentication	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。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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。

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。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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.
```

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 authentication login error-enable Example: 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 Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) show aaa authentication Example: switch# show aaa authentication	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	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	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	必須: [no] login on-failure log 例 : <pre>switch(config)# login on-failure log</pre>	<p>ロギング レベルが 6 に設定されている場合のみ、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。</p> <p>「AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user admin from 172.22.00.00」</p> <p>(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。</p>
ステップ 3	必須: [no] login on-success log 例 : <pre>switch(config)# login on-success log switch(config)# logging level authpriv 6 switch(config)# logging level daemon 6</pre>	<p>ロギング レベルが 6 に設定されている場合のみ、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。</p> <p>「AUTHPRIV-6-SYSTEM_MSG: pam_aaa:Authentication success for user admin from 172.22.00.00」</p> <p>(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。</p>

	コマンドまたはアクション	目的
ステップ 4	(任意) show login on-failure log 例： switch(config)# 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。
ステップ 5	(任意) show login on-successful log 例： switch(config)# 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。
ステップ 6	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	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イク認証プロトコル (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。



Note

Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。次に例を示します。

```
2017 Jun 14 16:14:15 N9K-1 %RADIUS-2-RADIUS_NO_AUTHEN_INFO: ASCII authentication not supported
2017 Jun 14 16:14:16 N9K-1 %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from 192.168.12.34 - dcos_sshd[16804]
```

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

Table 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。
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。

Before you begin

ログイン用の AAA ASCII 認証をディセーブルにします。

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	no aaa authentication login ascii-authentication Example: 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 Example: 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。 Note 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。
ステップ 4	(Optional) exit Example: switch(config)# exit switch#	設定モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) show aaa authentication login chap Example: switch# show aaa authentication login chap	CHAP の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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イク認証プロトコル (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。



Note 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。

Table 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。

Before you begin

ログイン用の AAA ASCII 認証をディセーブルにします。

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	no aaa authentication login ascii-authentication Example: 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 Example: 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。 Note 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 Example:	設定モードを終了します。

	Command or Action	Purpose
	switch(config)# exit switch#	
ステップ 5	(Optional) show aaa authentication login {mschap mschapv2} Example: switch# show aaa authentication login mschap	MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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 レコードの形式で 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。



Note

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。

Before you begin

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

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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} Example: <pre>switch(config)# aaa accounting default group radius</pre>	デフォルトのアカウント方式を設定します。 <i>group-list</i> 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。 <ul style="list-style-type: none"> • radiusRADIUS サーバのグローバルプールを使用してアカウントを行います。 • 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トに使用されます。 local 方式はローカルデータベースを使用してアカウントを行います。 デフォルトのアカウント方式は、 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 Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show aaa accounting Example: <pre>switch# show aaa accounting</pre>	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	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	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\
```



Note 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。



- (注) **login block-for** および **login quiet-mode** コンフィギュレーションモードコマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。

手順

	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] system login block-for seconds attempts tries within seconds 例： switch(config)# system 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) も、 system 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	(任意) [no] system login quiet-mode access-class acl-name 例： switch(config)# system login quiet-mode access-class myacl	待機モードに切り替わる時に、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	(任意) show system login [failures] 例： switch(config)# show system login	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	(任意) copy running-config startup-config 例：	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。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	

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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code>switch# configure terminal</code>	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： <code>switch(config)# user max-logins 1</code>	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	(任意) show running-config all i max-login 例： <code>switch(config)# show running-config all i max-login</code>	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	(任意) copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	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。

始める前に

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

	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	(任意) show userpassphrase {length max-length min-length} 例： switch(config)# show userpassphrase 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。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	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

	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	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	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トing 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

	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	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

	コマンドまたはアクション	目的
	quotes. Enter plain text secret: Confirm plain text secret: Type 7 Encrypted secret is : "fewhg"	(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ことができます。その際には、 radius-server [host] key および tacacs-server [host] key を使用します コマンドを使用します。
ステップ 3	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	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。

Procedure

	Command or Action	Purpose
ステップ 1	show accounting log [<i>size</i> last-index start-seqnum number start-time year month day hh:mm:ss] Example: 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、 <i>size</i> 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	(Optional) clear accounting log [logflash] Example:	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

	Command or Action	Purpose
	switch# clear aaa accounting log	ラッシュに保存されているアカウント 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。 Note clear login failures コ マンドは、現在の監 視期間内のログイン 失敗をクリアしま す。
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。

コマンド	目的
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 ライセンス ガイド

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

