



# 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 7](#)
- [AAA のデフォルト設定, on page 8](#)
- [AAA の設定, on page 8](#)
- [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 31](#)
- [AAA 設定の確認, on page 32](#)
- [AAA の設定例, on page 33](#)
- [ログインパラメータの設定例 \(34 ページ\)](#)
- [パスワードプロンプト機能の設定例 \(34 ページ\)](#)
- [AAA に関する追加情報, on page 35](#)

## 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	<b>aaa authentication login console</b>
ユーザ セッション アカウンティング	<b>aaa accounting default</b>

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

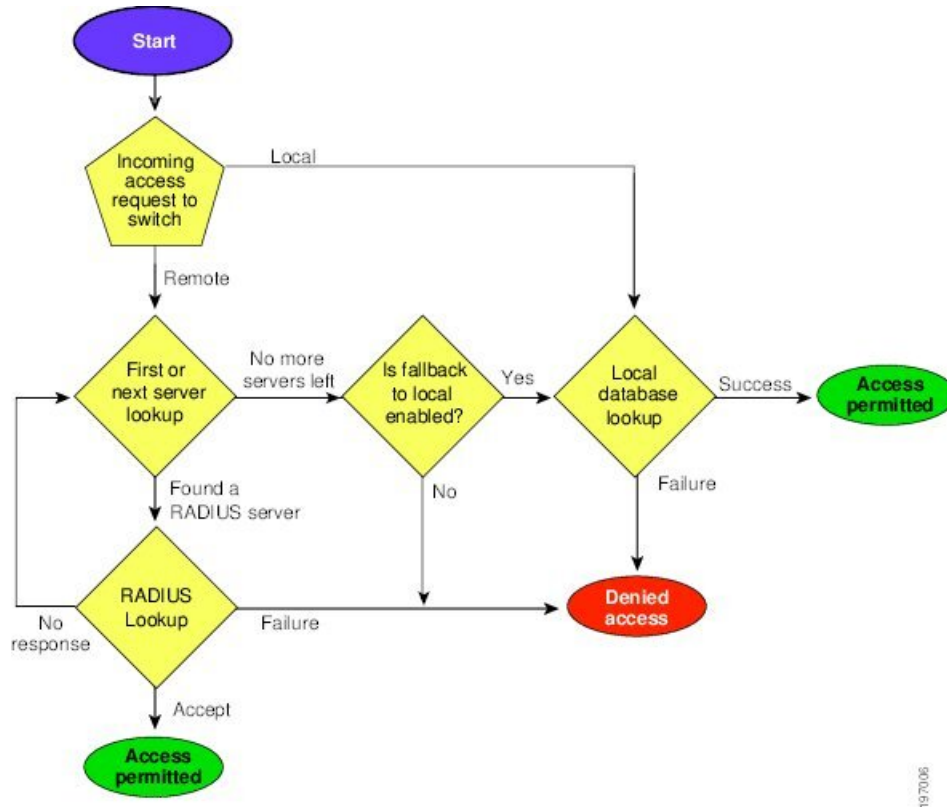


**Note** コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッションアカウンティングについて、Cisco NX-OS デバイスは各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカルオプションがデフォルト方式です。コンソールまたはデフォルトログインのローカルオプションを無効にするには、**no aaa authentication login {console | default} fallback error local** コマンドを使用します。

## ユーザ ログインの認証および許可プロセス

Figure 1: ユーザ ログインの認証および許可フロー

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。



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。



**Note** 「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) を有効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無効にしない限り、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。

- Cisco NX-OS リリース 10.2 (1) F 以降では、`cisco-av-pair` の `shell : roles` 属性の前に `SNMPV3` 属性を指定できます。
- LDAP は「`snmpv3`」属性をサポートしていません。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ 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。
- Cisco NX-OS Release 10.2(2)F 以降、新しい非同期化 CLI が導入され、SNMP とセキュリティ コンポーネントの間のユーザー同期を無効にするオプションを提供します。詳細については、『*System Management Configuration Guide*』の「SNMP の構成」の章を参照してください。  
リリース 7.0(3)I7(1) から現在のリリースまでのさまざまな機能をサポートする Cisco Nexus 9000 スイッチの詳細については、[Nexus スイッチプラットフォーム サポート マトリックス](#) を参照してください。
- 非同期化 CLI が有効なときに、リモート ユーザーは SNMP データベースに同期されません。
- DCNM (リリース 12.0.1.a 以降 Nexus Dashboard Fabric Controller と呼ばれる) を使用したセキュリティ ユーザーには、非同期 CLI が有効でないときに、対応する SNMPv3 がありません。同期化が無効なときに、セキュリティ コンポーネント上で作成されたユーザーはスイッチにログインできますが、コントローラがセキュリティ ユーザーに対してスイッチを検出するために SNMP 構成を使用するため、スイッチはコントローラにより検出され

ません。さらに、SNMP は userDB の非同期化状態のため、作成されたセキュリティ ユーザーを認識しないため、その結果としてスイッチの検出に失敗します。したがって、スイッチをコントローラにより検出させるために、SNMP ユーザーは明示的に作成される必要があります。DCNM 機能と共に非同期化 CLI を使用することはお勧めしません。詳細については、『Cisco Nexus 9000 NX-OS Security Configuration Guide』を参照してください。

- Cisco NX-OS リリース 10.3(1)F 以降、AAA は Cisco Nexus 9800 プラットフォーム スイッチでサポートされます。

## 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
- ユーザ名のみ (none)

デフォルトの方式はローカルですが、無効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 `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。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 シリーズ NX-OS トラブルシューティング ガイド』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	<b>configure terminal</b> <b>Example:</b> <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	<b>aaa authentication login console {group group-list [none]   local   none}</b> <b>Example:</b> <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。  <b>radius</b> 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。  <b>named-group</b> 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。  <b>local</b> 方式は、ローカル データベースを認証に使用します。 <b>none</b> 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 <b>local</b> 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	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) <b>show aaa authentication</b> <b>Example:</b> switch# <b>show aaa authentication</b>	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) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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、無効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	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa authentication login default {group group-list [none]   local   none}</b>	デフォルト認証方式を設定します。

Command or Action	Purpose
<p><b>Example:</b></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"> <li>• <b>radiusRADIUS</b> サーバのグローバルプールを使用して認証を行います。</li> <li>• <b>named-group</b> : 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。</li> </ul> <p><b>local</b> 方式は、ローカルデータベースを認証に使用します。<b>none</b> 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 <b>local</b> 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"> <li>• AAA 認証グループ</li> <li>• 認証なしの AAA 認証グループ</li> <li>• ローカル認証</li> <li>• 認証なし</li> </ul>

	Command or Action	Purpose
		<p><b>Note</b> <b>local</b> 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、<b>aaa authentication login default group g1</b> を設定した場合、AAA グループ <b>g1</b> 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、<b>aaa authentication login default group g1 none</b> を設定した場合、AAA グループ <b>g1</b> 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><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	<p>コンフィギュレーション モードを終了します。</p>
ステップ 4	<p>(Optional) <b>show aaa authentication</b></p> <p><b>Example:</b></p> <pre>switch# show aaa authentication</pre>	<p>デフォルトのログイン認証方式の設定を表示します。</p>
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	<p>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。</p>

## ローカル認証へのフォールバックの無効化

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無効にできます。



**Caution** ローカル認証へのフォールバックを無効にすると、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無効にする対象は、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	<b>configure terminal</b> <b>Example:</b> <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	<b>no aaa authentication login {console   default} fallback error local</b> <b>Example:</b> <pre>switch(config)# no aaa authentication login console fallback error local</pre>	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無効にします。  ローカル認証へのフォールバックを無効にすると、次のメッセージが表示されます。 <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">             "WARNING!!! Disabling fallback can lock your switch."           </div>
ステップ 3	(Optional) <b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	コンフィギュレーションモードを終了します。
ステップ 4	(Optional) <b>show aaa authentication</b> <b>Example:</b> <pre>switch# show aaa authentication</pre>	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <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。

## 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	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa user default-role</b> <b>Example:</b> switch(config)# <b>aaa user default-role</b>	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 <b>no</b> 形式を使用します。
ステップ 3	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa user default-role</b> <b>Example:</b> switch# <b>show aaa user default-role</b>	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) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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有効化

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有効になっていると、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	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa authentication login error-enable</b> <b>Example:</b> switch(config)# <b>aaa authentication login error-enable</b>	ログイン認証失敗メッセージを有効にします。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	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa authentication</b> <b>Example:</b> switch# <b>show aaa authentication</b>	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) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

## 成功したログイン試行と失敗したログイン試行

成功したログイン試行と失敗したログイン試行をすべて、設定されたsyslogサーバに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	<b>configure terminal</b> <b>例:</b> switch# <b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	必須: <b>[no] login on-failure log</b> <b>例:</b> switch(config)# <b>login on-failure log</b>	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、ログイン



	コマンドまたはアクション	目的
		<p>ン失敗後に次のsyslogメッセージが表示されます。</p> <p>AUTHPRIV-3-SYSTEM_MSG : pam_aaa : Authentication failed for user admin from 172.22.00.00</p> <p>(注) ログインレベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無視する必要がある場合、authpriv 値を 3 に設定する必要があります。</p>
ステップ 3	<p>必須: [no] login on-success log</p> <p>例 :</p> <pre>switch(config)# login on-success log switch(config)# logging level authpriv 6 switch(config)# logging level daemon 6</pre>	<p>ログインレベルが 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、ログインに成功すると次のsyslogメッセージが表示されます。</p> <p>AUTHPRIV-6-SYSTEM_MSG : pam_aaa : Authentication success for user admin from 172.22.00.00</p> <p>(注) ログインレベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無視する必要がある場合、authpriv 値を 3 に設定する必要があります。</p>
ステップ 4	<p>(任意) show login on-failure log</p> <p>例 :</p> <pre>switch(config)# show login on-failure log</pre>	<p>失敗した認証メッセージをsyslogサーバに記録するようにスイッチが設定されているかどうかを表示します。</p>

	コマンドまたはアクション	目的
ステップ 5	(任意) <b>show login on-successful log</b> 例： switch(config)# <b>show login on-successful log</b>	成功した認証メッセージをsyslogサーバに記録するようにスイッチが設定されているかどうかを表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	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。

## ユーザごとのログインブロックの設定

スイッチがグローバルコンフィギュレーションモードになっていることを確認します。

ユーザごとのログインブロック機能を使用すると、Denial of Service (DoS) 攻撃の疑いを検出して、辞書攻撃の影響を緩和することができます。この機能はローカルおよびリモートユーザに適用されます。ログインに失敗したユーザをブロックするように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。



(注) リリース 9.3(7) 以降では、リモートユーザのログインブロックを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	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	<b>aaa authentication rejected attemptsinsecondsbanseconds</b> 例： switch(config)# <b>aaa authentication rejected 3 in 20 ban 300</b>	ユーザをブロックするようにログインパラメータを設定します。  (注) デフォルトのログインパラメータに戻すには <b>no aaa authentication rejected</b> コマンドを使用します。
ステップ 3	<b>exit</b> 例： switch(config)# <b>exit</b>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	(任意) <b>show running config</b> 例： switch# <b>show running config</b>	ログイン パラメータを表示します。
ステップ 5	<b>show aaa local user blocked</b> 例： switch# <b>show aaa local user blocked</b>	ブロックされたローカル ユーザを表示します。
ステップ 6	<b>clear aaa local user blocked {username user  all}</b> 例： switch(config)# <b>switch# clear aaa local user blocked username testuser</b>	ブロックされたローカル ユーザをクリアします。 all : ブロックされたすべてのローカル ユーザをクリアします。
ステップ 7	<b>show aaa user blocked</b> 例： switch(config)# <b>show aaa user blocked</b>	ブロックされたすべてのローカル ユーザとリモート ユーザを表示します。
ステップ 8	(任意) <b>clear aaa user blocked {username user  all}</b> 例： switch# <b>clear aaa user blocked username testuser</b>	ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。 all : ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。

## 例



(注) network-admin および vdc-admin だけが show および clear コマンドを実行できます。

次に、20 秒の間に 3 回のログイン試行が失敗した場合に、300 秒間ユーザをブロックするログイン パラメータを設定する例を示します。

```
switch(config)# aaa authentication rejected 3 in 20 ban 300
switch# show run | i rejected
aaa authentication rejected 3 in 20 ban 300
switch# show aaa local user blocked
Local-user          State
testuser            Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa local user blocked username testuser
switch# show aaa user blocked
Local-user          State
testuser            Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa user blocked username testuser
```

## CHAP 認証の有効化

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 スイッチへのユーザ 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 が有効の場合は、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 認証を無効にします。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>no aaa authentication login ascii-authentication</b> <b>Example:</b> switch(config)# <b>no aaa authentication login ascii-authentication</b>	ASCII 認証を無効にします。
ステップ 3	<b>aaa authentication login chap enable</b> <b>Example:</b> switch(config)# <b>aaa authentication login chap enable</b>	CHAP 認証を有効にします。デフォルトでは無効になっています。 <b>Note</b> Cisco NX-OS デバイスで、CHAP と MSCHAP (または MSCHAP V2) の両方を有効にすることはできません。
ステップ 4	(Optional) <b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	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	(Optional) <b>show aaa authentication login chap</b> <b>Example:</b> switch# <b>show aaa authentication login chap</b>	CHAP の設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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 認証の有効化

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 を有効にする場合は、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 認証を無効にします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>no aaa authentication login ascii-authentication</b>	ASCII 認証を無効にします。

	Command or Action	Purpose
	<b>Example:</b> <pre>switch(config)# no aaa authentication login ascii-authentication</pre>	
ステップ 3	<b>aaa authentication login {mschap   mschapv2} enable</b> <b>Example:</b> <pre>switch(config)# aaa authentication login mschap enable</pre>	MSCHAP または MSCHAP V2 認証を有効にします。デフォルトでは無効になっています。 <b>Note</b> Cisco NX-OS デバイスで、MSCHAP と MSCHAP V2 の両方を有効にすることはできません。
ステップ 4	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	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	(Optional) <b>show aaa authentication login {mschap   mschapv2}</b> <b>Example:</b> <pre>switch# show aaa authentication login mschap</pre>	MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <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。

## 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、ユーザーのアクティビティを、アカウンティングレコードの形式で TACACS+ または RADIUS セキュリティサーバーにレポートします。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	<b>configure terminal</b> <b>Example:</b> <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	<b>aaa accounting default {group group-list   local}</b> <b>Example:</b> <pre>switch(config)# aaa accounting default group radius</pre>	デフォルトのアカウンティング方式を設定します。 <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"> <li>• <b>radius</b>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。</li> <li>• <b>named-group</b> : 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。</li> </ul> <b>local</b> 方式はローカルデータベースを使用してアカウンティングを行います。 デフォルトのアカウンティング方式は、 <b>local</b> 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。



	Command or Action	Purpose
ステップ 3	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) <b>show aaa accounting</b>  <b>Example:</b> switch# <b>show aaa accounting</b>	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) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

SNMPv3 属性は、シェル属性の前または後のいずれかにまとめます。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。

```
snmpv3:auth="SHA" priv="AES-128" shell:roles="network-admin" shell:priv-lvl=15
shell:roles="network-admin" shell:priv-lvl=15 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

可能性のあるサービス妨害 (DoS) 攻撃が検出された場合に、それ以降のログイン試行を自動的にブロックし、複数回の接続試行の失敗が検出された場合に待機期間を適用することでディクショナリ攻撃を遅らせるように、ログインパラメータを設定できます。



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



(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	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	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	<b>[no] system login block-for seconds attempts tries within seconds</b> 例： switch(config)# <b>system login block-for 100 attempts 2 within 60</b>	待機モード期間を設定します。すべての引数の範囲は 1 ~ 65535 です。 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する例を示します。 このコマンドを入力すると、TelnetまたはSSHを介したすべてのログイン試行は、待機期間中に拒否されます。アクセス コントロール リスト (ACL) も、 <b>system</b> コマンドが入力されます。 (注) 他のログインコマンドを使用する前に、このコマンドを入力する必要があります。

	コマンドまたはアクション	目的
ステップ 3	(任意) <b>[no] system login quiet-mode access-class acl-name</b> 例 : <pre>switch(config)# system login quiet-mode access-class myacl</pre>	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。
ステップ 4	(任意) <b>show system login [failures]</b> 例 : <pre>switch(config)# show system login</pre>	ログインパラメータを表示します。 <b>failures</b> 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) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# 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。

## ユーザ ログインセッションの制限

ユーザ 1 人あたりのあたりの同時ログインセッションの最大数を制限することができます。これにより、ユーザが複数の不要なセッションを持つことを防止し、有効な SSH または Telnet セッションにアクセスする不正ユーザの潜在的なセキュリティ問題を解決します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] user max-logins max-logins</b> 例 : <pre>switch(config)# user max-logins 1</pre>	ユーザ 1 人あたりの最大同ログイン時セッション数を制限します。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 1 人あたりの Telnet または SSH セッションが 1 に制限されます。 (注) 設定されたログイン制限は、すべてのユーザに適用されます。個々のユーザに異なる制限を設定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 3	(任意) <b>show running-config all   i max-login</b>  例 : <pre>switch(config)# show running-config all   i max-login</pre>	ユーザ 1 人あたりの最大同時セッション数を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b>  例 : <pre>switch(config)# 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。

## パスワードの長さの制限

ユーザパスワードの最小長と最大長を制限できます。この機能を使用すると、ユーザに強力なパスワードの入力を強制することで、システムのセキュリティを強化できます。

### 始める前に

パスワードの強度の確認を有効にするには、**password strength-check** コマンドを使用する必要があります。パスワードの長さを制限したが、パスワード強度チェックを有効にせず、ユーザが制限された長さの範囲内でないパスワードを入力すると、エラーが表示されますが、ユーザアカウントが作成されます。パスワードの長さを適用し、ユーザアカウントが作成されないようにするには、パスワード強度チェックを有効にし、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	<b>configure terminal</b>  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	<b>[no] userpassphrase {min-length min-length   max-length max-length}</b>  例 : <pre>switch(config)# userpassphrase min-length 8 max-length 80</pre>	ユーザパスワードの最小長または最大長を制限します。パスワードの最小長は 4 ~ 127 文字にすることができます。パスワードの最大長は 80 ~ 127 文字です。
ステップ 3	(任意) <b>show userpassphrase {length   max-length   min-length}</b>  例 : <pre>switch(config)# show userpassphrase length</pre>	ユーザパスワードの最小長と最大長を表示します。

	コマンドまたはアクション	目的
ステップ 4	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# 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。

## 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	<b>configure terminal</b> 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	<b>password prompt username</b> 例 : <pre>switch(config)# password prompt username</pre> 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.	<b>password</b> オプションを付けずに <b>username</b> コマンドまたは <b>snmp-server user</b> 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 <b>no</b> 形式を使用します。
ステップ 3	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# 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。

## RADIUS または TACACS+ の共有秘密の設定

スイッチとRADIUSまたはTACACS+サーバ間のリモート認証およびアカウントング用に設定する共有秘密は、機密情報であるため非表示にする必要があります。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。SHA256ハッシュ方式は、暗号化された共有秘密を保存するために使用されません。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : switch# <b>configure terminal</b>	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	<b>generate type7_encrypted_secret</b> 例 : switch(config)# <b>generate type7_encrypted_secret</b> 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"	キー タイプ 7 で RADIUS または TACACS+ の共有秘密を設定します。共有秘密の入力を 2 回平文で求められます。秘密は、入力すると非表示になります。次に、暗号化されたバージョンの秘密が表示されます。  (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ことができます。その際には、 <b>radius-server [host] key</b> および <b>tacacs-server [host] key</b> を使用します コマンドを発行します。
ステップ 3	(任意) <b>copy running-config startup-config</b> 例 : switch(config)# <b>copy running-config startup-config</b>	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	<b>show accounting log</b> [ <i>size</i>   <b>last-index</b>   <b>start-seqnum number</b>   <b>start-time year month day hh:mm:ss</b> ]	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

	Command or Action	Purpose
	<b>Example:</b> <pre>switch# show accounting log</pre>	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。アカウントング 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、 <b>last-index</b> キーワードを使用します。
ステップ 2	(Optional) <b>clear accounting log [logflash]</b> <b>Example:</b> <pre>switch# clear aaa accounting log</pre>	アカウントング ログの内容をクリアします。 <b>logflash</b> 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
<b>show aaa accounting</b>	AAA アカウントングの設定を表示します。
<b>show aaa authentication [login {ascii-authentication   chap   error-enable   mschap   mschapv2}]</b>	AAA 認証ログイン設定情報を表示します。
<b>show aaa groups</b>	AAA サーバグループの設定を表示します。
<b>show login [failures]</b>	ログインパラメータを表示します。 <b>failures</b> 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。 <b>Note</b> <b>clear login failures</b> 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。



コマンド	目的
<b>show login on-failure log</b>	syslog サーバに対して認証失敗メッセージをログ記録するようにスイッチが設定されているか表示します。
<b>show login on-successful log</b>	syslog サーバに対して認証成功メッセージをログ記録するようにスイッチが設定されているか表示します。
<b>show running-config aaa [all]</b>	実行コンフィギュレーションの AAA 設定を表示します。
<b>show running-config all   i max-login</b>	ユーザ 1 人あたりの最大同時セッション数を表示します。
<b>show startup-config aaa</b>	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。
<b>show userpassphrase {length   max-length   min-length}</b>	ユーザ パスワードの最小長と最大長を表示します。
<b>show userpassphrase sequence alphabet length</b>	ユーザー パスワードの英字シーケンスの最大長を表示します。
<b>show userpassphrase sequence keyboard length</b>	ユーザー パスワードのキーボードシーケンスの最大長を表示します。

## 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	<i>Cisco NX-OS</i> 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**

<b>MIB</b>	<b>MIB のリンク</b>
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。  <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>

## 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。