



# 認証、許可、アカウンティングの設定

この章は、次の項で構成されています。

- [AAA の概要 \(1 ページ\)](#)
- [リモート AAA の前提条件, on page 5](#)
- [AAA の注意事項と制約事項 \(6 ページ\)](#)
- [AAA の設定 \(6 ページ\)](#)
- [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 , on page 17](#)
- [AAA 設定の確認, on page 17](#)
- [AAA の設定例, on page 18](#)
- [デフォルトの AAA 設定, on page 18](#)

## AAA の概要

### AAA セキュリティ サービス

認証、許可、アカウンティング (AAA) 機能では、Cisco Nexus デバイスを管理するユーザーの ID 確認、アクセス権付与、およびアクション追跡を実行できます。Cisco Nexus 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 device Plus (TACACS+) プロトコルをサポートします。

ユーザーが入力したユーザー ID とパスワードに基づいて、スイッチは、ローカルデータベースを使用してローカル認証/ローカル許可を実行するか、1 つまたは複数の AAA サーバーを使用してリモート認証/リモート許可を実行します。スイッチと AAA サーバー間の通信は、事前共有秘密キーによって保護されます。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** : ユーザーを識別します。選択したセキュリティプロトコルに応じて、ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージング サポート、暗号化などが行われます。
- **許可** : アクセス コントロールを実行します。

Cisco Nexus デバイスにアクセスする許可は、AAA サーバーからダウンロードされる属性によって提供されます。RADIUS や TACACS+ などのリモートセキュリティサーバーは、適切なユーザー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、ユーザーに特定の権限を付与します。

- アカウンティング：課金、監査、レポートのための情報収集、ローカルでの情報のログイン、および AAA サーバーへの情報の送信の方式を提供します。



**Note** Cisco NX-OS ソフトウェアは、認証、許可、アカウントングをそれぞれ個別にサポートします。たとえば、アカウントングは設定せずに、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スイッチに関するユーザーパスワードリストを簡単に管理できます。
- AAA サーバー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スイッチのアカウントング ログを集中管理できます。
- スイッチ上のローカルデータベースを使用する方法に比べて、ファブリック内の各スイッチのユーザー属性は管理が簡単です。

## AAA サーバグループ

認証、許可、アカウント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 サーバーです。リモート AAA サーバーが応答しなかった場合、サーバグループは、フェールオーバー サーバーを提供します。グループ内の最初のリモート サーバーが応答しなかった場合、いずれかのサーバー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ーで試行

が行われます。サーバー グループ内のすべての AAA サーバーが応答しなかった場合、そのサーバー グループ オプションに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、複数のサーバー グループを指定できます。スイッチが最初のグループ内のサーバーからエラーを受信すると、次のサーバー グループのサーバーが試行されます。

## AAA サービス設定オプション

Cisco Nexus デバイスでは、次のサービスに個別の AAA 設定を使用できます。

- 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
- ユーザー管理セッション アカウンティング

次の表に、AAA サービス設定オプションの CLI 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	<b>aaa authentication login default</b>
コンソール ログイン	<b>aaa authentication login console</b>
ユーザー 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。

- RADIUS サーバー グループ：RADIUS サーバーのグローバルプールを認証に使用します。
- 特定のサーバー グループ：指定した RADIUS または TACACS+ サーバー グループを認証に使用します。
- ローカル：ユーザー名またはパスワードのローカル データベースを認証に使用します。
- なし：ユーザー名だけを使用します。



**Note** 方式がすべて RADIUS サーバーになっており、特定のサーバー グループが指定されていない場合、Cisco Nexus デバイスは、設定されている RADIUS サーバーのグローバルプールから、設定された順序で RADIUS サーバーを選択します。このグローバルプールからのサーバーは、Cisco Nexus デバイス上の RADIUS サーバー グループ内で選択的に設定できるサーバーです。

次の表に、AAA サービスに対して設定できる 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
ユーザー ログイン認証	サーバグループ、ローカル、なし
ユーザー管理セッション 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、ユーザーログイン認証、およびユーザー管理セッションアカウンティングでは、Cisco Nexus 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。

## ユーザー ログインの認証および許可プロセス

ユーザー ログインの認証および許可プロセスは、次のように実行されます。

- 目的のCisco Nexus デバイスにログインする際、Telnet、SSH、Fabric Manager または Device Manager、コンソール ログインのいずれかのオプションを使用できます。
- サーバー グループ認証方式を使用して AAA サーバー グループが設定してある場合は、Cisco Nexus デバイスが、グループ内の最初の AAA サーバーに認証要求を送信し、次のように処理されます。

その AAA サーバーが応答しなかった場合、リモートのいずれかの AAA サーバーが認証要求に応答するまで、試行が継続されます。

サーバーグループのすべての AAA サーバーが応答しなかった場合、その次のサーバーグループのサーバーが試行されます。

設定されているすべての認証方式が失敗した場合、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 Nexus デバイスがリモート AAA サーバーで正常に認証できた場合は、次の条件が適用されます。

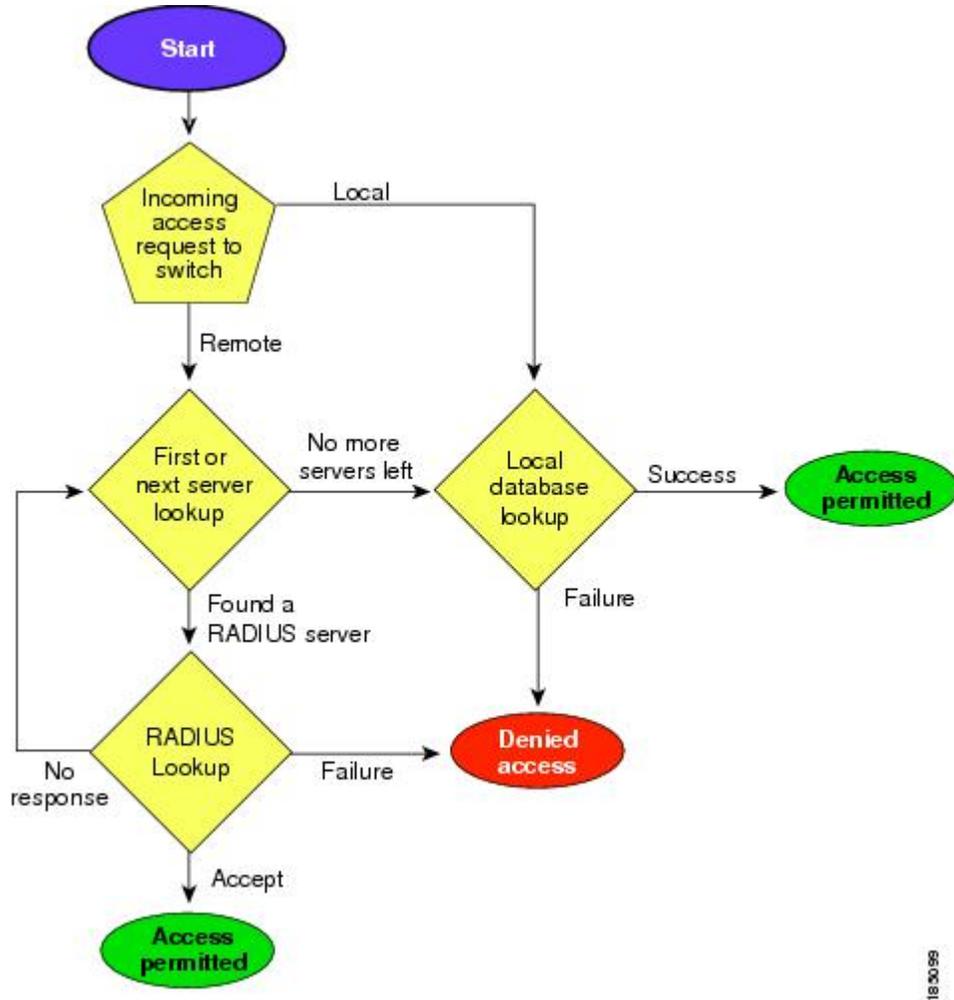
AAA サーバープロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザーロールが認証応答とともにダウンロードされます。

AAA サーバープロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザーロールを取得するために、もう 1 つの要求が同じサーバーに送信されます。

- ユーザー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 Nexus 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。

次の図に、認証および許可プロセスのフローチャートを示します。

Figure 1: ユーザー ログインの認証および許可のフロー



この図に示されている「残りのサーバーなし」とは、現在のサーバーグループ内のいずれのサーバーからも応答がないということです。

## リモート 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 サーバーまたは TACACS+ サーバーが、IP で到達可能であること。
- Cisco Nexus デバイスが AAA サーバーのクライアントとして設定されている。
- 事前に共有された秘密キーが Cisco Nexus デバイス上およびリモート AAA サーバー上で設定されている。

- リモート サーバーが Cisco Nexus デバイスからの AAA 要求に応答する。

## AAA の注意事項と制約事項

そのユーザー名が TACACS+ または RADIUS で作成されたのか、ローカルで作成されたのかに関係なく、Cisco Nexus デバイスでは、すべて数値のユーザー名はサポートされません。AAA サーバーに数字だけのユーザー名が存在し、ログイン時にその名前を入力した場合でも、ユーザーは Cisco Nexus デバイスにログインを許可されます。



**注意** すべて数値のユーザー名でユーザー アカウントを作成しないでください。

## AAA の設定

### コンソール 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 サーバーまたは TACACS+ サーバーの名前付きサブセット
- Cisco Nexus デバイス上のローカル データベース
- ユーザー名だけ **none**

デフォルトの方式は、ローカルです。



**Note** 事前に設定されている一連の RADIUS サーバーに関しては、**aaa authentication** コマンドの **group radius** 形式および **group server-name** 形式を使用します。ホスト サーバーを設定するには、**radius server-host** コマンドを使用します。サーバー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。

必要に応じて、コンソール ログイン認証方式を設定する前に RADIUS または TACACS+ サーバー グループを設定します。

#### Procedure

	Command or Action	Purpose
ステップ 1	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。

	Command or Action	Purpose
ステップ 2	switch(config)# <b>aaa authentication login console { group group-list [none]   local   none}</b>	<p>コンソールのログイン認証方式を設定します。</p> <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>radius RADIUS</b> サーバー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> を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットが認証に使用されます。</li> </ul> <p><b>local</b> 方式では、ローカルデータベースが認証に使用されます。 <b>none</b> 方式では、ユーザー名だけが使用されます。</p> <p>デフォルトのコンソール ログイン方式は、<b>local</b> です。これは認証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かった場合に使用されます。</p>
ステップ 3	switch(config)# <b>exit</b>	グローバル 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) 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) 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。

### Example

次に、コンソール ログインの認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
switch(config)# exit
switch# show aaa authentication
switch# copy running-config startup-config
```

## デフォルトのログイン認証方式の設定

デフォルトの方式は、ローカルです。

必要に応じて、デフォルトのログイン認証方式を設定する前に RADIUS または TACACS+ サーバー グループを設定します。

### Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# <b>aaa authentication login default { group group-list [none]   local   none}</b>	<p>デフォルト認証方式を設定します。</p> <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>radius</b> RADIUS サーバーのグローバル プールを使用して認証を行います。</li> <li>• <b>named-group</b> を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットが認証に使用されます。</li> </ul> <p><b>local</b> 方式では、ローカル データベースが認証に使用されます。 <b>none</b> 方式では、ユーザー名だけが使用されます。</p> <p>デフォルトのログイン方式は <b>local</b> です。この方式は、方式が一切設定されていない場合、または設定済みのどの方式でも応答が得られなかった場合に使用されます。</p>
ステップ 3	switch(config)# <b>exit</b>	設定モードを終了します。
ステップ 4	(Optional) switch# <b>show aaa authentication</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	実行設定を、スタートアップ設定にコピーします。

## ログイン認証失敗メッセージの有効化

ユーザーがログインして、リモート AAA サーバーが応答しなかった場合は、ローカルユーザーデータベースによってログインが処理されます。ログイン失敗メッセージの表示をイネーブルにしていた場合は、次のようなメッセージが表示されます。

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

### Procedure

	Command or Action	Purpose
ステップ 1	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	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。デフォルトでは無効になっています。
ステップ 3	switch(config)# <b>exit</b>	設定モードを終了します。
ステップ 4	(Optional) 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) switch# <b>copy running-config startup-config</b>	実行設定を、スタートアップ設定にコピーします。

## AAA コマンド許可の設定

TACACS+ サーバーの許可方式が設定されている場合は、ユーザーが TACACS+ サーバーで実行するすべてのコマンド（すべての EXEC モード コマンドおよびすべてのコンフィギュレーションモード コマンドを含む）を許可できます。

許可方式には、次のものがあります。

- Group : TACACS+ サーバー グループ
- Local : ローカル ロールベース許可
- None : 許可は実行されません

デフォルトの方式は、Local です。



(注) コンソールセッションでの許可は、Cisco Nexus 5000 プラットフォームではサポートされていません。Cisco Nexus 5500 プラットフォーム、リリース 6.x 以降ではサポートされています。

## 始める前に

AAA コマンドの許可を設定する前に、TACACS+ をイネーブルに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： switch# configure terminal switch(config)#	グローバル コンフィギュレーションモードを開始します。
ステップ 2	<b>aaa authorization {commands   config-commands} {default} {[ group group-name]   [ local]}   {[ group group-name]   [ none]}</b> 例： switch(config)# aaa authorization config-commands default group tac1  例： switch# aaa authorization commands default group tac1	許可パラメータを設定します。 EXEC モードコマンドを許可するには、 <b>commands</b> キーワードを使用します。 コンフィギュレーションモードコマンドの許可には、 <b>config-commands</b> キーワードを使用します。 許可方式を指定するには、 <b>group</b> 、 <b>local</b> 、または <b>none</b> キーワードを使用します。

## 例

次に、TACACS+ サーバー グループ *tac1* で EXEC モードコマンドを許可する例を示します。

```
switch# aaa authorization commands default group tac1
```

次に、TACACS+ サーバー グループ *tac1* でコンフィギュレーションモードコマンドを許可する例を示します。

```
switch(config)# aaa authorization config-commands default group tac1
```

次に、TACACS+ サーバー グループ *tac1* でコンフィギュレーションモードコマンドを許可する例を示します。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバーに到達する際にエラーが生じた場合、コマンドはユーザーのローカルロールに基づいて許可されます。

```
switch(config)# aaa authorization config-commands default group tac1 local
```

次に、TACACS+ サーバー グループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバーに到達する際にエラーが生じた場合は、ローカル ロールにかかわらずコマンドを許可します。

```
switch# aaa authorization commands default group tac1 none
```

次に、ローカル ロールにかかわらず EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default none
```

次に、ローカル ロールを使用して EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default local
```

## MSCHAP 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。リモート 認証 サーバー (RADIUS または TACACS+) を通じて、Cisco Nexus デバイスへのユーザー ログインに MSCHAP を使用できます。

デフォルトでは、Cisco Nexus デバイスはスイッチとリモート サーバーの間でパスワード 認証 プロトコル (PAP) 認証を使用します。MSCHAP がイネーブルの場合は、MSCHAP VSA (Vendor-Specific Attribute; ベンダー固有属性) を認識するように RADIUS サーバーを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

**Table 3: MSCHAP 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 サーバーから MSCHAP ユーザーに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	MSCHAP-Response	チャレンジに対する応答として MSCHAP ユーザー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。

## Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# <b>aaa authentication login mschap enable</b>	MS-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。
ステップ 3	switch(config)# <b>exit</b>	設定モードを終了します。
ステップ 4	(Optional) switch# <b>show aaa authentication login mschap</b>	MS-CHAP 設定を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	実行設定を、スタートアップ設定にコピーします。

## デフォルトの AAA アカウンティング方式の設定

Cisco Nexus デバイスは、アカウントングに TACACS+ 方式と RADIUS 方式をサポートします。スイッチは、ユーザー アクティビティをアカウントング レコードの形で TACACS+ セキュリティ サーバーまたは RADIUS セキュリティ サーバーに報告します。各アカウントング レコードに、アカウントング属性値 (AV) のペアが入っており、それが AAA サーバーに格納されます。

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

特定のアカウントング方式を定義するデフォルト方式のリストを作成できます。それには次の方式があります。

- RADIUS サーバー グループ : RADIUS サーバーのグローバル プールをアカウントングに使用します。
- 特定のサーバー グループ : 指定した RADIUS または TACACS+ サーバー グループをアカウントングに使用します。
- ローカル : ユーザー名またはパスワードのローカルデータベースをアカウントングに使用します。



**Note** サーバー グループが設定されていて、そのサーバー 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、AAA アカウントングのデフォルト方式を設定する前に RADIUS または TACACS+ サーバー グループを設定します。

### Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# <b>aaa accounting default { group group-list   local}</b>	<p>デフォルトのアカウントング方式を設定します。スペースで区切ったリストで、1つまたは複数のサーバーグループ名を指定できます。</p> <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>radius</b> RADIUS サーバーのグローバル プールを使用してアカウントングを行います。</li> <li>• <b>named-group</b> を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットがアカウントングに使用されます。</li> </ul> <p><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トングを行います。</p> <p>デフォルトの方式は <b>local</b> です。サーバーグループが設定されていないとき、または設定済みのすべてのサーバーグループから応答がないときに、このデフォルトの方式が使用されます。</p>
ステップ 3	switch(config)# <b>exit</b>	設定モードを終了します。
ステップ 4	(Optional) switch# <b>show aaa accounting</b>	デフォルトの AAA アカウントング方式の設定を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	実行設定を、スタートアップ設定にコピーします。

## No Service Password-Recovery について

No Service Password-Recovery 機能により、コンソールへのアクセスを持つ誰もがルータおよびルータのネットワークにアクセスする機能を与えられることとなります。No Service Password-Recovery 機能を使用すると、『[Cisco Nexus 9000 Series NX-OS Troubleshooting Guide](#)』に記載されている標準的な手順でパスワードを回復できなくなります。

## No Service Password-Recovery のイネーブル化

No Service Password-Recovery 機能が有効になっている場合、ネットワーク権限を持つ管理者以外は管理者パスワードを変更できません。

### 始める前に

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

### 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 switch(config)#</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 service password-recovery</b> 例 : <pre>switch(config)# no service password-recovery WARNING: Executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch(config)# copy run start [#####] 100% Copy complete, now saving to disk (please wait)... Copy complete.</pre>	パスワード回復メカニズムを無効にします。
ステップ 3	(任意) <b>copy running-config startup-config</b> 例 : <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。
ステップ 4	<b>Reload</b>	

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>switch(config)# Reload This command will reboot the system. (y/n)? [n] y 2018 Jun 26 16:23:19 BAR %\$ VDC-1 %\$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface  CISCO SWITCH Ver 8.34  CISCO SWITCH Ver 8.34 Manual system restart from Command Line Interface writing reset reason 9, .. ..  switch(boot)# config t Enter configuration commands, one per line. End with CNTL/Z. switch(boot) (config)# admin-password Abcd!123\$ ERROR: service password-recovery disabled. Cannot change password! switch(boot) (config)#</pre>	
ステップ 5	<p><b>exit</b></p> <p>例 :</p> <pre>switch(config)# exit switch#</pre>	グローバル コンフィギュレーション モードを終了します。
ステップ 6	<p>(任意) <b>show user-account</b></p> <p>例 :</p> <pre>switch# show user-account</pre>	ロール設定を表示します。
ステップ 7	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

## AAA サーバーの VSA の使用

### VSA

ベンダー固有属性 (VSA) を使用して、AAA サーバー上での Cisco Nexus デバイスのユーザーロールおよび SNMPv3 パラメータを指定できます。

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 seperator value *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号 (=) で、アスタリスク (\*) は任意属性を示します。

Cisco Nexus デバイスでの認証に RADIUS サーバーを使用する場合は、認証結果とともに許可情報などのユーザー属性を返すよう、RADIUS プロトコルが RADIUS サーバーに指示します。この許可情報は、VSA で指定されます。

## VSA の形式

次の VSA プロトコル オプションが、Cisco Nexus デバイスでサポートされています。

- **Shell** : ユーザー プロファイル情報を提供する `access-accept` パケットで使用されます。
- **Accounting** : `accounting-request` パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲んでください。

次の属性が Cisco Nexus デバイスでサポートされています。

- **roles** : ユーザーに割り当てるすべてのロールをリストします。値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。
- **accountinginfo** : 標準の RADIUS アカウンティングプロトコルで処理される属性に加えて、追加のアカウントング情報が格納されます。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、アカウントングプロトコル関連の PDU でしか使用できません。

## AAA サーバー上でのスイッチのユーザー ロールと SNMPv3 パラメータの指定

AAA サーバーで VSA `cisco-av-pair` を使用して、次の形式で、Cisco Nexus デバイスのユーザー 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ー ロールは、`network-operator` です。



**Note** Cisco Unified Wireless Network TACACS+ 設定と、ユーザー ロールの変更については、『[Cisco Unified Wireless Network TACACS+ Configuration](#)』を参照してください。

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。

追加情報については、Cisco Nexus デバイスの『System Management Configuration Guide』の「Configuring User Accounts and RBAC」の章を参照してください。

## 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 Nexus 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。

### Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>show accounting log</b> [size] [start-time year month day hh : mm : ss]	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。サイズ引数を指定すれば、コマンドの出力を制限できます。指定できる範囲は 0 ~ 250000 バイトです。ログ出力の開始時刻を指定することもできます。
ステップ 2	(Optional) switch# <b>clear accounting log</b>	アカウンティング ログの内容をクリアします。

## 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 アカウンティングの設定を表示します。
<b>show aaa authentication</b> [login {error-enable [mschap]}	AAA 認証情報を表示します。
<b>show aaa authorization</b>	AAA 許可の情報を表示します。

コマンド	目的
<code>show aaa groups</code>	AAA サーバグループの設定を表示します。
<code>show running-config aaa [all]</code>	実行コンフィギュレーションのAAA設定を表示します。
<code>show startup-config aaa</code>	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。

## AAA の設定例

次に、AAA を設定する例を示します。

```
switch(config)# aaa authentication login default group radius
switch(config)# aaa authentication login console group radius
switch(config)# aaa accounting default group radius
```

## デフォルトの AAA 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 4: デフォルトの AAA パラメータ

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
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

## 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。