# AAA の設定

この章の内容は、次のとおりです。



# AAA について

## AAA セキュリティ サービス

AAA は、ユーザ ID とパスワードの組み合わせに基づいて、ユーザを認証および許可するために使用されます。 キーは、AAA サーバとの通信を保護します。

多くの場合、AAA は RADIUS または TACACS+ などのプロトコルを使用してセキュリティ機能を管理します。 ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA が使用されます。

AAA は主要な（推奨される）アクセス コントロール方式ですが、さらに、ローカル ユーザ名認証、回線パスワード認証、イネーブル パスワード認証など、AAA の範囲外で簡単なアクセス コントロールを行う機能も用意されています。 ただし、これらの機能では、AAA を使用した場合と同レベルのアクセス コントロールは実現できません。

次のサービスごとに別個の AAA 設定が作成されます。

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

| AAAサービス コンフィギュレーションオプション | 関連コマンド |
|---|---|
| Telnet または SSH ログイン | aaa authentication login default |
| コンソール ログイン | aaa authentication login console |

## 認証

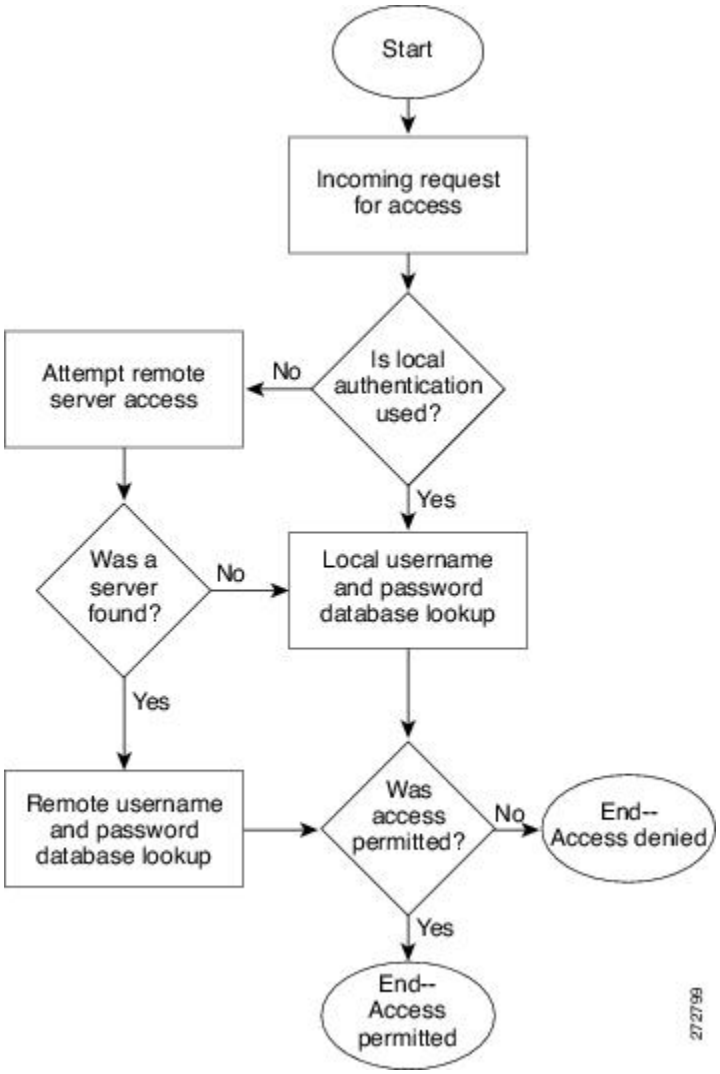
認証は、ログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および選択したセキュリティ プロトコルによっては暗号化など、ユーザを識別する手段を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。AAA認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

認証は次のように実行されます。

| 認証方式 | 説明 |
|---|---|
| ローカル データベース | ユーザ名またはパスワードのローカル ルックアップデータベースによって次の認証を行います。<br>• コンソール ログイン認証<br>• ユーザ ログイン認証<br>• ユーザ管理セッション アカウンティング |
| リモート RADIUS または TACACS+ サーバ | ユーザ名またはパスワードのローカル ルックアップデータベースによって次の認証を行います。<br>• コンソール ログイン認証<br>• ユーザ ログイン認証<br>• ユーザ管理セッション アカウンティング |

| 認証方式 | 説明 |
|---|---|
| なし | ユーザ名だけで次の認証を行います。<br>• コンソール ログイン認証<br>• ユーザ ログイン認証<br>• ユーザ管理セッション アカウンティング |

**図 *1*：ユーザ ログインの認証**



### 許可

許可では、ユーザが実行を許可される操作を制限します。 ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモート アクセスの制御方法を提供します。

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。 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ことで機能します。 これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。

### アカウンティング

アカウンティングで、ユーザ識別、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数などといったセキュリティ サーバ情報の収集と送信を行い、課金、監査、およびレポートに使用する手段を提供します。 アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

アカウンティングでは、すべての SVS 管理セッションを追跡し、ログに記録して管理します。 この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。 アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

## AAA サーバ グループ

リモート AAA サーバ グループは、1 台のリモート AAA サーバが応答しない場合にフェールオーバーを提供できます。すなわち、グループの最初のサーバが応答しない場合に、サーバが応答するまでグループ内の次のサーバで試行します。 複数のサーバ グループがある場合、同じ方法で、相互にフェールオーバーを提供できます。

すべてのリモート サーバ グループが応答しない場合は、ローカル データベースが認証に使用されます。

# AAA の前提条件

- 少なくとも 1 台の TACACS+ サーバまたは RADIUS サーバが IP で到達可能になっていること。
- VSM が AAA サーバのクライアントとして設定されていること。
- 共有秘密キーが VSM およびリモート AAA サーバに設定されていること。

# 注意事項と制限事項

Cisco Nexus 1000V では、すべてが数字のユーザ名はサポートされず、すべてが数字のローカル ユーザ名は作成されません。 すべてが数字のユーザ名が AAA サーバにすでに存在し、ログインの際に入力された場合、Cisco Nexus 1000V はそのユーザを認証します。

# AAA のデフォルト設定

| パラメータ | デフォルト |
|---|---|
| コンソール認証方式 | local |
| デフォルト認証方式 | local |
| ログイン認証失敗メッセージ | Disabled |

# AAA の設定

## ログイン認証方式の設定

TACACS+ サーバ グループを使用して認証が行われる場合は、グループが追加済みです。

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログイン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** | 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** | switch(config)# **aaa authentication login** {**console** \| **default**} {**group** *group-list* [**none**] \| **local** \| **none**} | コンソールまたはデフォルト ログイン認証方式を設定します。 次のキーワードと引数があります。<br>• group：サーバ グループによって認証が行われます。<br>• group-list：スペースで区切ったサーバ グループ名のリストです。認証なしの場合は none です。<br>• group-list none：認証なし。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • local：ローカル データベースが認証に使用されます。<br>（注） デフォルトは local で、方式が設定されていない場合、または設定されたすべての認証方式で応答が得られなかった場合に使用されます。<br>• none：ユーザ名によって認証が行われます |
| ステップ 3 | switch(config)# **exit** | グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。 |
| ステップ 4 | switch# **show aaa authentication** | （任意）<br>設定されたログイン認証方式を表示します。 |
| ステップ 5 | switch# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# aaa authentication login console group tacgroup
switch(config)# exit
switch# show aaa authentication
         default: group tacgroup
         console: group tacgroup
switch# copy running-config startup-config
switch#
switch# configure terminal
switch(config)# aaa authentication login default group tacacs
switch(config)# aaa authentication login console group tacacs
```

# ログイン認証失敗メッセージのイネーブル化

リモート AAA サーバが応答しない場合のログイン認証失敗メッセージの表示をイネーブルにするには、次の手順を実行します。

次に、ログイン認証エラー メッセージを示します。

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

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログイン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 | 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 | 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 | switch(config)# **exit** | グローバル コンフィギュレーション モードを終了して、EXEC モードに戻ります。 |
| ステップ 4 | switch# **show aaa authentication login error-enable** | （任意）<br>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 | switch# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# aaa authentication login error-enable
switch(config)# exit
switch# show aaa authentication login error-enable
enabled
```

# AAA 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

| コマンド | 目的 |
|---|---|
| **show aaa authentication** [**login** {**error-enable** \| **mschap**}] | AAA 認証情報を表示します。 |
| **show aaa groups** | AAA サーバ グループの設定を表示します。 |
| **show 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 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。 |

**例：show aaa authentication**

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

**例：show running config aaa**

```
switch# show running-config aaa all
version 4.0(1)
aaa authentication login default local
aaa accounting default local
no aaa authentication login error-enable
no aaa authentication login mschap enable
no radius-server directed-request
no snmp-server enable traps aaa server-state-change
no tacacs-server directed-request
switch#
```

**例：show startup-config aaa**

```
switch# show startup-config aaa
version 4.0(1)
```

# AAA の設定例

次に、AAA の設定例を示します。

```
aaa authentication login default group tacacs
aaa authentication login console group tacacs
```

# AAA 機能の履歴

この表には、機能への追加または変更が行われたリリースの更新のみが含まれています。

| 機能名 | リリース | 機能情報 |
|---|---|---|
| AAA | 4.0(4)SV1(1) | この機能が導入されました。 |