

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[認証と認可用にスイッチを設定](#)

[FreeRADIUS の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、サードパーティの RADIUS サーバ ( FreeRADIUS ) を使用して Cisco IOS<sup>®</sup> スイッチ上で RADIUS 認証を設定する方法について説明します。この例では、認証時における特権 15 モードへのユーザの直接配置を説明します。

## 前提条件

### 要件

IP アドレスによって Cisco スイッチを FreeRADIUS にクライアントとして定義したことおよび同じ共有秘密キーを FreeRADIUS とスイッチに定義したことを確認します。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- FreeRADIUS
- Cisco IOS バージョン 12.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 設定

## 認証と認可用にスイッチを設定

1. フォールバック アクセスの完全な権限を持つローカル ユーザをスイッチに作成するには、次のように入力します。

```
Switch(config)#username admin privilege 15 password 0 cisco123!
```

2. AAA をイネーブルにするには、次のように入力します。

```
switch(config)# aaa new-model
```

3. RADIUS サーバのIP アドレスおよびキーを指定するには、次のように入力します。

```
switch# configure terminal
```

```
switch(config)#radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
```

```
switch(config)#radius-server key hello123
```

注 キーは、スイッチ用に RADIUS サーバに設定された共有秘密キーと一致する必要があります。

4. RADIUS サーバの可用性をテストするには、`test aaa` コマンドを入力します。

```
switch# test aaa server Radius 172.16.71.146 user1 Ur2Gd2BH
```

まだ設定されていないためテスト認証はサーバからの Rejection によって失敗しますが、サーバ自体が到達可能であることは確認されます。

5. RADIUS が到達不能の場合に、ローカル ユーザにフォールバックするようにログイン認証を設定するには、次のように入力します。

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

6. ユーザが認証される場合のために、特権レベル 15 用の認可を設定するには、次のように入力します。

```
switch(config)#aaa authorization exec default group radius if-authenticated
```

## FreeRADIUS の設定

### FreeRADIUS サーバでクライアントを定義

1. 設定ディレクトリに移動するには、次のように入力します。

```
# cd /etc/freeradius
```

2. `clients.conf` ファイルを編集するには、次のように入力します。

```
# sudo nano clients.conf
```

3. ホスト名で特定された各デバイス ( ルータとスイッチ ) を追加し、正しい共有秘密を含めるために、次のように入力します。

```
# sudo nano clients.conf
```

4. `users` ファイルを編集するには、次のように次のように入力します。

```
# sudo nano users
```

5. デバイスへのアクセスを許可された各ユーザを追加します。次の例は、ユーザ「cisco」に Cisco IOS 特権レベル 15 を設定する方法を示します。

```
# sudo nano users
```

6. FreeRADIUS を再起動するには、次のように入力します。

```
# sudo /etc/init.d/freeradius restart
```

7. `cisco-rw` のメンバであるすべてのユーザに特権レベル 15 を付与するために、ユーザのファイルの DEFAULT ユーザグループを変更するには、次のように入力します。

```
# sudo /etc/init.d/freeradius restart
```

8. FreeRADIUS の `users` ファイルに、必要に応じて、異なる特権レベルで他のユーザを追加できます。たとえば、このユーザ ( `life` ) にはレベル 3 ( システム メンテナンス ) が付与されます。

```
# sudo /etc/init.d/freeradius restart
```

注 このドキュメントの設定は、Ubuntu 12.04 LTS および 13.04 で動作する FreeRADIUS に基づいています。

## 確認

スイッチの設定を確認するには、次のコマンドを使用します。

```
switch# show run | in radius      (Show the radius configuration)
switch# show run | in aaa         (Show the running AAA configuration)
switch# show startup-config Radius (Show the startup AAA configuration in
start-up configuration)
```

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [FreeRADIUS](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)