# Cisco IOS ルータ： HTTP 接続のローカル、TACACS+ および RADIUS 認証の設定例

## 目次



## 概要

このドキュメントでは、HTTP 接続に対してローカル認証、TACACS+ 認証、および RADIUS 認証を適用するための設定方法を説明します。 また、関連するデバッグ コマンドについても説明します。

## はじめに

### 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

### 前提条件

このドキュメントに関する固有の要件はありません。

### 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。

- Cisco IOS ® ソフトウェア リリース 11.2 または それ 以降

- これらのソフトウェア リビジョンをサポートするハードウェア

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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

## 背景理論

Cisco IOSヨ ソフトウェア リリース 11.2 には、http を介してルータを管理する機能が追加されました。 『Cisco IOS 設定の基本情報、コマンド リファレンス』の「Cisco IOS Web ブラウザ コマンド」のセクションでは、この機能を次のように説明しています。

「ip http authentication コマンドを使用すると、HTTP サーバ ユーザ用の認証方式を指定できます。 HTTPサーバはイネーブルパスワード 方式を特権レベル 15 でユーザを認証するのに使用します。 **ip http authentication コマンドは**今イネーブル、ローカル、TACACS、または認証、許可、アカウンティング（AAA）HTTPサーバユーザ 認証を規定 することを可能にします」。

# 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

このドキュメントでは次に示す設定を使用しています。

- HTTPサーバユーザ向けのローカル認証の設定
- HTTPサーバユーザのための TACACS+ 認証設定
- HTTPサーバユーザ向けのRADIUS認証の設定

**注:** このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

## HTTPサーバユーザ向けのローカル認証の設定

- ルータの設定
- ユーザの結果

### ルータの設定

| Cisco IOS ソフトウェア リリース 11.2 を使用したローカル認証 |
| --- |
| `!--- This is the part of the configuration related to local authentication.` ! aaa new-model aaa authentication login default local aaa authorization exec local username one privilege 15 password one username three password three username four privilege 7 password four ip http server ip http authentication aaa ! `!--- Example of command moved from level 15 (enable) to level 7` ! privilege exec level 7 clear line |
| **Cisco IOS ソフトウェア リリース 11.3.3.T 以降を使用したローカル認証** |
| |

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

### ユーザの結果

これらの結果は前のルータコンフィギュレーションのユーザに適用します。

- **ユーザ One**ユーザは URL が http://# として入る場合ウェブの承認を渡します。#.#.#.ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ユーザは、ログインの後イネーブル モードになります（show privilege の出力結果は 15 になります）。ルータにコマンド認可が追加されても、ユーザはすべてのコマンドを実行できます。
- **ユーザ Three**権限レベルがないため、このユーザは Web 認可を通過できません。ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ユーザは、ログインの後に非イネーブル モードになります（show privilege の出力結果は 1 になります）。ルータにコマンド認可が追加されても、ユーザはすべてのコマンドを実行できます。
- **ユーザ Four**URL に http://#.#.#.#/level/7/exec と入力すると、ユーザは Web 認可を通過します。レベル 1 のコマンドとレベル 7 の clear line コマンドが表示されます。ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ログイン後、ユーザは権限レベル 7（show privilege の結果は 7）になります。ルータにコマンド認可が追加されても、ユーザはすべてのコマンドを実行できます。

## HTTPサーバユーザのための TACACS+ 認証設定



### ルータの設定

**Cisco IOS ソフトウェア リリース 11.2 を使用した認証**

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

**Cisco IOS ソフトウェアの 11.3.3.T 以降で 12.0.5.T よりも前のリリースを使用した認証**

```
aaa new-model
aaa authentication login default tacacs+
```

```
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

**Cisco IOS ソフトウェア リリース 12.0.5.T 以降を使用した認証**

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

## ユーザの結果

上記のサーバ設定でのユーザの結果は、次のようになります。

- **ユーザ One**ユーザは URL が http://# として入る場合ウェブの承認を渡します。#.#.#.ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ユーザは、ログインの後イネーブル モードになります（show privilege の出力結果は 15 になります）。ルータにコマンド認可が追加されても、ユーザはすべてのコマンドを実行できます。
- **ユーザ Two**ユーザは URL が http://# として入る場合ウェブの承認を渡します。#.#.#.ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ユーザは、ログインの後イネーブル モードになります（show privilege の出力結果は 15 になります）。ルータにコマンド認可が追加されると、ユーザはすべてのコマンドを実行に失敗します。これは、これらのコマンドがサーバ設定で認可されていないためです。
- **ユーザ Three**権限レベルがないため、このユーザは Web 認可を通過できません。ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ユーザは、ログインの後に非イネーブル モードになります（show privilege の出力結果は 1 になります）。ルータにコマンド認可が追加されても、ユーザはすべてのコマンドを実行できます。
- **ユーザ Four**URL に http://#.#.#.#/level/7/exec と入力すると、ユーザは Web 認可を通過します。レベル 1 のコマンドとレベル 7 の clear line コマンドが表示されます。ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ログイン後、ユーザは権限レベル 7（show privilege の結果は 7）になります。ルータにコマンド認可が追加されても、ユーザはすべてのコマンドを実行できます。

## フリーウェア デーモン サーバの設定

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
```

```
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

## Cisco Secure ACS for UNIX サーバの設定

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

## Cisco Secure ACS for Windows サーバの設定

**グループ One のユーザ One**

- グループ設定shell (exec) をチェックします。privilege level=15 をチェックします。Default (Undefined) Services をチェックします。**注:** このオプションが表示されない場合は、Interface Configuration に移動して TACACS+ を選択し、続いて Advanced Configuration Options を選択します。 Display enable default (undefined) service 設定を選択します。
- ユーザ設定どのデータベースからのパスワード; パスワードを入力し、top area で確認して下さい。

**グループ Two のユーザ Two**

- グループ設定shell (exec) をチェックします。privilege level=15 をチェックします。Default (Undefined) Services はチェックしません。
- ユーザ設定どのデータベースからのパスワード; パスワードを入力し、top area で確認して下さい。

**グループ Three のユーザ Three**

- グループ設定shell (exec) をチェックします。privilege levelをブランクのままにします。Default (Undefined) Services をチェックします。**注:** このオプションが表示されない場合は、Interface Configuration に移動して TACACS+ を選択し、続いて Advanced Configuration Options を選択します。 Display enable default (undefined) service 設定を選択します。
- ユーザ設定どのデータベースからのパスワード; パスワードを入力し、top area で確認して下さい。

**グループ Four のユーザ Four**

- グループ設定shell (exec) をチェックします。privilege level=7 をチェックします。Default (Undefined) Services をチェックします。**注:** このオプションが表示されない場合は、Interface Configuration に移動して TACACS+ を選択し、続いて Advanced Configuration Options を選択します。 Display enable default (undefined) service 設定を選択します。
- ユーザ設定どのデータベースからのパスワード; パスワードを入力し、top area で確認して下さい。

## HTTPサーバユーザ向けのRADIUS認証の設定



### ルータの設定

| Cisco IOS ソフトウェア リリース 11.2 を使用した認証 |
| --- |

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
```

```
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

**Cisco IOS ソフトウェアの 11.3.3.T 以降で 12.0.5.T よりも前のリリースを使用した認証**

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

**Cisco IOS ソフトウェア リリース 12.0.5.T 以降を使用した認証**

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

## ユーザの結果

上記のサーバ設定でのユーザの結果は、次のようになります。

- **ユーザ One**ユーザは URL が http://# として入る場合ウェブの承認を渡します。#.#.#.ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ユーザは、ログインの後イネーブル モードになります（show privilege の出力結果は 15 になります）。
- **ユーザ Three**権限レベルがないため、このユーザは Web 認可を通過できません。ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ユーザは、ログインの後に非イネーブル モードになります（show privilege の出力結果は 1 になります）。
- **ユーザ Four**URL に http://#.#.#.#/level/7/exec と入力すると、ユーザは Web 認可を通過します。レベル 1 のコマンドとレベル 7 の clear line コマンドが表示されます。ルータに Telnet 接続し、ログイン認証した後、ユーザはすべてのコマンドを実行できます。ログイン後、ユーザは権限レベル 7（show privilege の結果は 7）になります。

## Cisco AV ペアをサポートするサーバでの RADIUS 設定

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

### Cisco Secure ACS for UNIX サーバの設定

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

### Cisco Secure ACS for Windows サーバの設定

- User = one、service type (attribute 6) = administrative
- User = three、service type (attribute 6) = login
- User = four、service type (attribute 6) = login、Cisco AV-pairs のボックスをチェックし、shell:priv-lvl=7 を入力

## 確認

現在、この設定に使用できる確認手順はありません。

# トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

## トラブルシューティングのためのコマンド

HTTP 認証のデバッグを行う場合は、次のコマンドが便利です。 次のコマンドをルータで発行します。

**注: debug** コマンドを使用する前に、『debug コマンドに関する重要な情報』を参照してください。

- terminal monitor - 現在の端末およびセッションの debug コマンドの出力とシステム エラー メッセージを表示します。
- debug aaa authentication - AAA/TACACS+ の認証に関する情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。
- **debug radius** - RADIUS に関連する詳細なデバッグ情報を表示します。
- debug tacacs - TACACS に関連する情報を表示します。
- debug ip http authentication：HTTP 認証の問題をトラブルシューティングするためのコマンドです。 ルータが使用した認証方式と認証特有の状況メッセージを表示します。

# 関連情報

- Cisco TACACS+ アクセス ソフトウェア サポートページ
- RADIUS に関するサポート ページ
- Cisco Secure ACS for Windows に関するサポート ページ
- Cisco Secure ACS for UNIX に関するサポート ページ
- Requests for Comments ( RFC )
- テクニカルサポートとドキュメント - Cisco Systems