TACACS+ および RADIUS による特権レベルの割り当て方法

目次

概要

この文書では、特定コマンドの特権レベルの変更方法について説明し、ルータと TACACS+ サーバおよび RADIUS サーバの設定例の一部による例を示します。

前提条件

要件

この ドキュメント を 読む人はルータの特権レベルのナレッジがあるはずです。

デフォルトで、ルータに 3 つの特権レベルがあります。

- 特権レベル 1 = 特権なし（プロンプトは router>）、ログインのデフォルト レベル
- 特権レベル 15 = 特権あり（プロンプトは router#）、イネーブル モードに入った後のレベル
- 特権レベル 0 = ほとんど使用されませんが、5 つのコマンド（ **disable**、**enable**、**exit**、**help**、および **logout**）が含まれています。

レベル 2 から 14 は、デフォルトの設定では使用されませんが、通常はレベル 15 のコマンドをこれらのレベルのいずれかに移動することができ、また、通常はレベル 1 のコマンドをこれらのレベルのいずれかに移動することもできます。 自明のとおり、このセキュリティ モデルはルータでの管理作業を含んでいます。

特権レベルをログインユーザとして判別するために、**show privilege コマンドを**タイプして下さい。 使用していることどんなコマンドが Cisco IOS® ソフトウェアのバージョンに特定の特権レベルで利用できるか判別するために、a を入力して下さい**か。** その特権レベルでログインしたときにコマンドラインから

注: 特権レベルを指定するかわりに、認証サーバが TACACS+ をサポートする場合コマンド許可

をすることができます。 RADIUS プロトコルではコマンドの許可はサポートされていません。

使用するコンポーネント

この文書に記載されている情報は基づいた on Cisco IOS ソフトウェア リリース 11.2 およびそれ以降です。

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。

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。

例

この例では、**snmp-server コマンドは**特権レベル 15（デフォルト）から特権レベル 7.に降ろされます。 **ping コマンドは**移動された特権レベル 1 から特権レベルから 7.です。 ユーザ 7 が認証されるとき、そのユーザはサーバによって特権レベル 7 を指定され、**show privilege コマンド** ディスプレイ「現在の特権レベルはユーザがコンフィギュレーションモードの snmp-server 設定を ping し、することができる 7." です。 その他の設定コマンドは使用できません。

設定 - ルータ

ルータ- 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

ルータ - 11.3.3.T 以降（12.0.5.T まで）

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
```

```
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

ルータ - 12.0.5.T 以降

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

設定 - サーバ

Cisco Secure NT TACACS+

次の手順に従って、サーバを設定してください。

1. ユーザ名とパスワードを入力します。
2. Group Settings で、シェルと exec がチェックされていることを確認し、特権レベルのボックスに 7 が入力されていることを確認します。

TACACS+ - フリーウェアサーバの Stanza

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Cisco Secure UNIX TACACS+

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
```

```
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Cisco Secure NT RADIUS

次の手順に従って、サーバを設定してください。

1. ユーザ名とパスワードを入力します。
2. IETF の Group Settings で、Service-type (attribute 6) = Nas-Prompt とします。
3. CiscoRADIUS のエリアで、AV-Pair をチェックし、その下の長方形のボックスに、shell:priv-lvl=7 と入力します。

Cisco Secure UNIX RADIUS

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

これは、ユーザ名「seven」用のユーザ ファイルです。

注: このサーバでは、シスコの AV ペアがサポートされている必要があります。

- seven Password = passwdxyz
- Service-Type = Shell-User
- Ciscoavpair =shell:priv-lvl=7

関連情報

- RADIUS に関するサポート ページ
- Requests for Comments (RFC)
- IOS での TACACS+ に関するドキュメント
- TACACS+ Support Page
- Cisco Secure UNIX 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
- テクニカルサポート - Cisco Systems