Cisco IOS の管理アクセスで使用される FreeRADIUS の設定例

内容

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® 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いています。

- 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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、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。

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、スイッチのRADIUSサーバに設定されている共有秘密と一致する必要があります。

4. RADIUS サーバのアベイラビリティをテストするには、**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。

```
client 192.168.1.1 {
```

```
secret = secretkey
nastype = cisco
shortname = switch
}
```

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。

```
cisco Cleartext-Password := "password"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=15"
```

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。

```
DEFAULT Group == cisco-rw, Auth-Type = System
Service-Type = NAS-Prompt-User,
cisco-avpair :="shell:priv-lvl=15"
```

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 nano/etc/freeradius/users

life Cleartext-Password := "testing"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=3"

Restart the FreeRADIUS service:
sudo /etc/init.d/freeradius restart
```

注：このドキュメントの設定は、Ubuntu 12.04 LTEおよび13.04で稼働する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)
```

トラブルシュート

現在、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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。