用於Cisco IOS上的管理訪問的FreeRADIUS配置示例

目錄

簡介

本檔案介紹如何在使用第三方RADIUS伺服器(FreeRADIUS)的Cisco IOS®交換器上設定RADIUS驗證。本示例介紹身份驗證時使用者直接進入特權15模式的情況。

必要條件

需求

確保將您的Cisco交換機定義為FreeRADIUS中的客戶端，並且在FreeRADIUS和交換機上定義了IP地址和同一共用金鑰。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FreeRADIUS
- Cisco IOS版本12.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

設定交換器以進行驗證和授權

1. 若要在交換器上建立具有完全回退存取許可權的本地使用者，請輸入：

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

2. 要啟用AAA，請輸入：

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

3. 若要提供RADIUS伺服器的IP位址和金鑰，請輸入：

```
switch# configure terminal
switch(config)#radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
switch(config)#radius-server key hello123
```

註：金鑰必須與在RADIUS伺服器上為交換機配置的共用金鑰匹配。

4. 若要測試RADIUS伺服器可用性，請輸入test aaa指令：

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

測試身份驗證失敗，伺服器拒絕，因為它尚未配置，但將確認伺服器本身可以訪問。

5. 若要將登入驗證設定為在RADIUS無法連線時回退到本機使用者，請輸入：

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

6. 要配置許可權級別15的授權，只要使用者經過身份驗證，請輸入：

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

FreeRADIUS組態

定義FreeRADIUS伺服器上的客戶端

1. 若要導航至組態目錄，請輸入：

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

2. 若要編輯clients.conf檔案，請輸入：

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

3. 要新增由主機名標識的每個裝置（路由器/交換機）並包括正確的共用金鑰，請輸入：

```
client 192.168.1.1 {
secret = secretkey
nastype = cisco
shortname = switch
}
```

4. 要編輯使用者檔案，請輸入：

```
# sudo nano users
```

5. 新增允許訪問裝置的每個使用者。此示例演示如何為使用者「cisco」設定Cisco IOS許可權級

別15。

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

6. 若要重新啟動FreeRADIUS，請輸入：

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

7. 若要變更使用者檔案中的DEFAULT使用者群組，以便將cisco-rw的所有成員的許可權層級指定為15，請輸入：

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

8. 您可以根據需要在FreeRADIUS使用者檔案中新增處於不同許可權級別的其他使用者。例如，此使用者（壽命）的級別為3（系統維護）：

```
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
```

註：本文檔中的配置基於在Ubuntu 12.04 LTE和13.04上運行的FreeRADIUS。

驗證

若要驗證交換器上的組態，請使用以下命令：

```
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)
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- FreeRADIUS
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。