用于在Cisco IOS上进行管理访问的FreeRADIUS配置示例

目录

简介

本文档介绍如何使用第三方RADIUS服务器(FreeRADIUS)在Cisco IOS®交换机上配置RADIUS身份验证。本示例介绍身份验证时用户直接进入特权15模式的情况。

先决条件

要求

确保在FreeRADIUS中将您的Cisco交换机定义为客户端，并且在FreeRADIUS和交换机上定义了IP地址和相同的共享密钥。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FreeRADIUS
- 思科IOS版本12.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

配置交换机进行身份验证和授权

1. 要在交换机上创建具有完全回退访问权限的本地用户，请输入：

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

2. 要启用AAA，请输入：

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

3. 要提供RADIUS服务器的IP地址和密钥，请输入：

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

   注：密钥必须与交换机的RADIUS服务器上配置的共享密钥匹配。

4. 要测试RADIUS服务器可用性，请输入**test aaa**命令：

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

   测试身份验证失败，服务器拒绝，因为它尚未配置，但它将确认服务器本身可以访问。

5. 要将登录身份验证配置为在无法访问RADIUS时回退到本地用户，请输入：

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

6. 要配置权限级别为15的授权，只要对用户进行身份验证，请输入：

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

FreeRADIUS配置

在FreeRADIUS服务器上定义客户端

1. 要导航到配置目录，请输入：

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

2. 要编辑**clients.conf**文件，请输入：

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

3. 要添加由主机名标识的每个设备（路由器/交换机）并包括正确的共享密钥，请输入：

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

4. 要编辑用户文件，请输入：

```
# sudo nano users
```

5. 添加允许访问设备的每个用户。此示例演示如何为用户“cisco”设置15的Cisco IOS权限级别。

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

6. 要重新启动FreeRADIUS，请输入：

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

7. 要更改用户文件中的DEFAULT用户组，以便为cisco-rw成员的所有用户授予15的权限级别，请输入：

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

8. 您可以根据需要在FreeRADIUS用户文件中添加处于不同权限级别的其他用户。例如，此用户（寿命）的级别为3（系统维护）：

```
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：本文档中的配置基于在Ubuntu 12.04 LTE和13.04上运行的FreeRADIUS。

验证

要验证交换机上的配置，请使用以下命令：

```
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)
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- FreeRADIUS
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。