

第四章 TACAS+

4.1. 用户登录集中鉴权

提问 使用集中的鉴权方式对用户登录设备进行控制

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login default group tacacs+
```

```
Router1(config)#aaa authentication enable default group tacacs+
```

```
Router1(config)#tacacs-server host 172.25.1.1
```

```
Router1(config)#tacacs-server key COOKBOOK
```

```
Router1(config)#end
```

```
Router1#
```

注释 部署集中化鉴权就不需要在每台设备上配置用户名密码了，改密码也变得简单了

4.2. 限制特定命令的执行权限

提问 对设备可执行命令权限进行基于用户的授权

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authorization exec default group tacacs+
```

```
Router1(config)#aaa authorization commands 15 default group tacacs+
```

```
Router1(config)#tacacs-server host 172.25.1.1
```

```
Router1(config)#tacacs-server key neoshi
```

```
Router1(config)#end
```

```
Router1#
```

注释 无

4.3. TACACS+服务器无法访问

提问 防止出现 TACACS+服务器故障导致所有用户都不能登录

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login default group tacacs+ enable
```

```
Router1(config)#aaa authentication enable default group tacacs+ enable
```

```
Router1(config)#aaa authorization commands 15 default group tacacs+ if-authenticated
```

```
Router1(config)#tacacs-server host 172.25.1.1
```

```
Router1(config)#tacacs-server key COOKBOOK
```

```
Router1(config)#end
```

```
Router1#
```

注释 在认证服务器出现故障的情况下使用 enable 密码作为备份，同时建议使用 if-authenticated 参数在你配置授权的时候

4.4. 在特定端口禁用 TACACS+鉴权

提问 为了方便禁止在控制口使用 TACACS+鉴权

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login default group tacacs+ local
```

```
Router1(config)#aaa authentication login NEOSHI line
```

```
Router1(config)#line con 0
```

```
Router1(config-line)#login authentication NEOSHI
```

```
Router1(config-line)#end
```

```
Router1#
```

注释

4.5. 记录用户行为

提问 记录用户输入的配置命令和时间

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa accounting commands 1 default stop-only group tacacs+
```

```
Router1(config)#aaa accounting commands 15 default stop-only group tacacs+
```

```
Router1(config)#end
```

```
Router1#
```

注释 下面是一条日志记录，很详尽吧

```
Fri Jan 3 11:08:47 2006      toronto ijbrown tty66 172.25.1.1 stop task_id=512
start_time=1041610127  timezone=EST service=shell priv-lvl=15 cmd=configure
terminal <cr>
```

4.6. 记录系统事件

提问 记录系统事件

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa accounting exec default start-stop group tacacs+
```

```
Router1(config)#aaa accounting connection default start-stop group tacacs+
```

```
Router1(config)#aaa accounting system default stop-only group tacacs+
```

```
Router1(config)#end
```

```
Router1#
```

注释 除了可以记录用户输入命令以外还提供了 exec (用户开始和中止 exec 会话的时间记录), connection (用户发起外部连接的时间, 地址, 数据包 多少等信息记录比如 telnet ssh 等) 和 system (系统重启, 禁用 AAA 等系统信息) 等三种系统事件的记录

4.7. 设置 TACACS+消息的源地址

提问 发送 TACACS+消息时只使用特定的源地址

回答

```
Router1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router1(config)#ip tacacs source-interface Loopback0
```

```
Router1(config)#end
```

```
Router1#
```

注释 所有本设备的记录都来自于同一地址方便对日志进行汇总和统计

```
<!--[if !supportLists]-->4.8.      <!--[endif]-->TACACS+服务器配置文件样本
```

注释 可以使用思科免费的 TACACS+服务器也可以使用商业的服务器，配置方式略