【MVS】Cisco设备在RADIUS服务器不可达的情况下需要让网络管理员在成功认证后能够执行所有命令的方式

设备管理 胡伟 2024-01-09 发表

问题描述

【MVS】Cisco设备在RADIUS服务器不可达的情况下需要让网络管理员在成功认证后能够执行所有命令的方式

解决方法

在RADIUS服务器不可达的情况下，如果需要让网络管理员在成功认证后能够执行所有命令，您需要确保配置了AAA（Authentication, Authorization, and Accounting）以便在远程服务器不可用时回退到本地认证和授权。以下是一个Cisco设备上的AAA配置示例，该配置允许在RADIUS服务器不可用时使用本地数据库进行用户认证和授权：

```cisco
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius local if-authenticated
aaa authorization commands 15 default group radius local if-authenticated

radius-server host <radius-server-ip> auth-port 1812 acct-port 1813 key <shared-secret>
```

在这个配置中：

- `aaa new-model` 启用AAA功能。
- `aaa authentication login default group radius local` 命令配置认证方法列表，首先尝试使用RADIUS组，如果RADIUS服务器不可用，则回退到本地数据库认证。
- `aaa authorization exec default group radius local if-authenticated` 和 `aaa authorization commands 15 default group radius local if-authenticated` 允许授权配置。如果用户已经通过RADIUS认证，那么即使RADIUS服务器对于授权请求无响应，配置也会允许用户执行所有命令。`if-authenticated` 关键字在这里很重要，因为它确保了只有在用户成功认证的情况下才会进行授权。
- `radius-server host` 命令定义了RADIUS服务器的IP地址、端口和共享密钥。

请注意，实际的RADIUS服务器IP地址、端口和共享密钥需要替换为您的网络中使用的真实值。同时，您需要确保设备的本地数据库中有适当的用户账户和密码，以便在RADIUS服务器不可用时能够进行本地认证。