IOS 权限级别看不到完整的运行配置

目录

简介

本文档阐述权限级别如何影响用户能否在路由器上执行某些命令。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

查看路由器配置

当通过权限级别配置对路由器的访问时，常见的问题是在用户权限级别或更低权限级别配置 **show running 或 write terminal 命令。**当用户执行命令时，配置看起来是空白的。实际上这是有意而为，原因如下：

- **write terminal / show running-config 命令显示空白配置。**此命令显示当前用户可修改的所有命令（即用户当前权限级别或之下权限级别的所有命令）。 为安全起见，该命令不得显示用户当前权限级别以上的命令。否则，即可使用 **snmp-server community 等命令修改路由器的当前配置，从而获得对路由器的完全访问。**
- **show config / show start-up config 命令显示完整配置，但并非真正显示实际的配置。**该命令只

是打印出 NVRAM 的内容，刚好就是用户执行 **write memory** 时路由器的配置。

权限级别

要使特权用户可以查看内存中的完整配置，用户需要修改路由器上所配置的所有命令的权限。例如：

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local

username john privilege 9 password 0 doe
username six privilege 6 password 0 six
username poweruser privilege 15 password poweruser
username inout password inout
username inout privilege 15 autocommand show running

privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

要了解此示例，必须了解权限级别。默认情况下，路由器上有三个命令级别：

- 权限级别 0 - 包括 **disable**、enable、exit、help 和 logout 命令。
- 权限级别 1 - Telnet 上的普通级别；包括 `router>`
- 权限级别 15 - 包括 `router#`

在 router 提示符下键入 **？可找到特定路由器中某个特定级别提供的命令。**使用 **privilege 命令可在权限级别之间移动命令，如示例所示。**虽然本例展示的是本地身份验证和授权，但这些命令对于 TACACS+ 或 RADIUS 身份验证和 exec 授权的作用类似（通过用服务器实施 TACACS+ 命令授权，可以实现对路由器更精细的控制）。

示例中还介绍了有关用户和权限级别的其他详细信息：

- 用户 *six 可以远程登录和执行* **show run 命令，但得到的配置实际上是空白的，因为此用户不能配置任何内容（configure terminal 在第 8 级，而非第 6 级）。** 不允许该用户查看其他用户的用户名和口令，或查看简单网络管理协议 (SNMP) 信息。
- 用户 *john 可以远程登录和执行* **show run 命令，但只能看到他可以配置的命令（路由器配置的 snmp-server community 部分，因为此用户是我们的网络管理员）。** 他可以配置 **snmp-server community，因为 configure terminal 在第 8 级（在第 9 级或之下），而 snmp-server community 是第 8 级命令。**不允许该用户查看其他用户的用户名和口令，但委托他管理 SNMP 配置。
- 用户 *inout 可以远程登录，并且由于该用户是为* **autocommand show running** 配置的，因此还可以查看所显示的配置，但随后即断开连接。
- 用户 *poweruser 可以远程登录和执行* **show run 命令。**此用户位于第 15 级，因此可以查看所有命令。所有命令都在第 15 级或之下；此级别的用户还可以查看和控制用户名和口令。

相关信息

- 命令查找工具（仅限注册用户）
- TACACS+ 和 RADIUS 的 IOS 文档

- TACACS/TACACS+支持页面
- RADIUS 支持页
- 请求注解 (RFC)
- 技术支持 - Cisco Systems