

知 某局点S12508F-AF 用户权限问题

SSH 陈阳 2023-07-30 发表

组网及说明

不涉及

## 问题描述

设备创建了本地用户test，指定权限为level-1，然后用该用户登录设备，发现用户在用户视图和系统视图下的权限相差很大，用户视图下只有十几条命令可以输入，而系统视图则所有命令都可以输入

<H3C>?

System view commands:

```
access-list  Alias for 'acl'  
display      Display current system information  
end          Alias for 'return'  
erase       Alias for 'delete'  
exit        Alias for 'quit'  
hostname    Alias for 'sysname'  
logging     Alias for 'info-center'  
no          Alias for 'undo'  
ping        Ping function  
quit        Exit from current command view  
return      Exit to User View  
show        Alias for 'display'  
tracert     Tracert function  
write       Alias for 'save'
```

[H3C]?

System view commands:

```
aaa AAA configuration  
access-list Alias for 'acl'  
acl Specify ACL configuration information  
acl-outbound-enhance Outbound ACL performance enhancement  
XXX...
```

## 过程分析

检查配置，本地用户test的配置正常

```
local-user test class manage
```

```
password hash
```

```
$h$6$eaGCiZr7XNlrnUfa$EiJuHk4XRZIYIc7E9pUqGBS6pTJegx1ZEshgvwhFYIeGAuP3LpldLkx4hds  
4LzukaQYTUvOVBX04rbM0hweaXnQ==
```

```
service-type ssh terminal
```

```
authorization-attribute user-role level-1
```

查看level-1的配置，在角色level-1中添加了system-view命令的权限

```
role name level-1
```

```
description Predefined level-1 role
```

```
rule 1 permit command system-view
```

将rule 1删除测试，发现用户登录后在两个视图的权限一致，说明rule 1的含义不是给用户能输入这条命令的权限，而是给用户能在系统视图下输入所有命令的权限。

## 解决方法

删除下发给用户的system-view权限。

