V7 AC RBAC功能控制用户操作AP权限典型配置

AP管理 设备管理 孙兆强 2017-07-31 发表

现场有两个AP，分别命名为AP1和AP2，有两个用户分别命名为user1和user2。要求user1仅能操作AP1，user2仅能操作AP2。两个用户能在对应AP上做所有操作。

关键配置
AC配置地址，配置路由，保证能和AC通信。此处配置省略
创建本地管理用户
#
local-user user1 class manage
 password hash user1
 service-type telnet
 authorization-attribute user-role user1
#
#
local-user user2 class manage
 password hash user2
 service-type telnet
 authorization-attribute user-role user2
#
开启telnet功能
telnet server enable
#
配置telnet用户的验证方式
#
line vty 0 31
 authentication-mode scheme
 user-role network-operator
#
创建用户角色
#
role name user1
 rule 1 permit command system-view;wlan ap AP1 *;*
#
#
role name user2
 rule 1 permit command system-view;wlan ap AP2 *;*
#
如果是console用户
本地用户增加如下命令
service-type terminal
#全局增加下面命令
line con 0
authentication-mode scheme
 user-role network-operator

效果验证
user1的用户登陆后无法进入AP2，user2的用户无法进入AP1。相应用户可以进入自己对应的AP并可以进行AP试图下的所有命令。
login: user1
Password:
<AC2V7>sys
[AC2V7]wlan ap AP2
Permission denied.

local user中的用户角色优先级高于vty视图下的用户角色
本地用户中的authorization-attribute user-role可以配置多条，支持的命取并集，注意将其他不需要的授权角色去掉
rule 1 permit command system-view;wlan ap AP2 *;*这条命令中AP名称和后面的*之间要有空格，分号和*之间不要有空格