某局点V7交换机RBAC不生效的处理经验案例

RBAC 孙铁宁 2020-10-31 发表

组网及说明

客户在V7交换机上使用RBAC自定义用户的权限

问题描述

客户的需求是XXXX角色的用户只允许display查看以及配置端口的port access vlan，配置如下：

role name XXXX
 rule 1 permit command system-view
 rule 2 permit command interface *
 rule 3 permit command display *
 rule 4 permit command port access vlan

实际测试发现不生效，登录后进入系统视图，能够使用系统视图下几乎所有的命令，比如配置ospf等：

sy
System View: return to User View with Ctrl+Z.
[access 2]ospf 1
[access 2-ospf-1]

过程分析

1、在用户视图下面使用？，发现没用reset、save等命令，但是系统视图下就发现一切正常

<access 2>?
User view commands:
 display Display current system information
 erase Alias for "delete"
 exit Alias for "quit"
 no Alias for "undo"
 quit Exit from current command view
 show Alias for "display"
 system-view Enter the System View
 write Alias for "save"

2、仔细阅读官网的命令手册，发现有如下说明：

若要描述多级视图下的命令，则需要使用分号（;）将命令特征字符串分成多个段，每一个段代表一个或一系列命令，后一个段中的命令是执行前一个段中命令所进入视图下的命令。一个段中可以包含多个星号（*），每个星号（*）代表了0个或多个任意字符。例如：命令特征字符串“system ; interface * ; ip * ;” 代表从系统视图进入到任意接口视图后，以ip开头的所有命令。

3、将role配置修改为下面的配置，满足客户需求

role name XXXX
 rule 1 permit command system-view ; interface * ; port access vlan *
 rule 2 permit command display *

解决方法

将role配置修改为下面的配置，满足客户需求

role name XXXX
 rule 1 permit command system-view ; interface * ; port access vlan *
 rule 2 permit command display *

输入命令特征字符串时，需要遵循以下规则：

(1) 段（segment）的划分

· 若要描述多级视图下的命令，则需要使用分号（;）将命令特征字符串分成多个段，每一个段代表一个或一系列命令，后一个段中的命令是执行前一个段中命令所进入视图下的命令。一个段中可以包含多个星号（*），每个星号（*）代表了0个或多个任意字符。例如：命令特征字符串“system ; interface * ; ip * ;” 代表从系统视图进入到任意接口视图后，以**ip**开头的所有命令。

· 除最后一个段外，其余段中的命令应为描述如何进入子视图的命令特征字符串。

· 一个段中必须至少出现一个可打印字符，不能全部为空格或Tab。

(2) 分号的使用

· 在输入命令特征字符串时必须指定该命令所在的视图，进入各视图的命令特征字符串由分号分隔。但是，对于能在任意视图下执行的命令（例如**display**命令）以及用户视图下的命令（例如**dir**命令），在配置包含此类命令的规则时，不需要在规则的命令匹配字符串中指定其所在的视图。

· 当最后一个段中的最后一个可见字符为分号时，表示所指的命令范围不再扩展，否则将向子视图中的命令扩展。例如：命令特征字符串“system ; radius scheme * ;”代表系统视图下以**radius sche**

me开头的所有命令；命令特征字符串“system ; radius scheme * ”代表系统视图下以**radius scheme**开头的所有命令，以及进入子视图（RADIUS方案视图）下的所有命令。

(3) 星号的使用

· 当星号（*）出现在一个段的首部时，其后面不能再出现其它可打印字符，且该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“system ; *”就代表了系统视图下的所有命令，以及所有子视图下的命令。

· 当星号（*）出现在一个段的中间时，该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“debugging * event”就代表了用户视图下所有模块的事件调试信息开关命令。

(4) 前缀匹配

· 命令关键字与命令特征字符串是采用前缀匹配算法进行匹配的，即只要命令行中关键字的首部若干连续字符或全部字符与规则中定义的关键字相匹配，就认为该命令行与此规则匹配。因此，命令特征字符串中可以包括完整的或部分的命令关键字。例如，若规则“rule 1 deny command dis mpls lsp protocol static”生效，则命令**display mpls lsp protocol static**和命令**display mpls lsp protocol static-cr**都会被禁止执行。

对于基于命令的规则，有以下使用注意事项：

· 基于命令的规则只对指定视图下的命令生效。若用户输入的命令在当前视图下不存在而在其父视图下被查找到时，用于控制当前视图下的命令的规则不会对其父视图下的命令执行权限进行控制。例如，定义一条规则“rule 1 deny command system ; interface * ; *”禁止用户执行接口视图下的任何命令。当用户在接口视图下输入命令**acl number** 3000时，该命令仍然可以成功执行，因为系统在接口视图下搜索不到指定的**acl**命令时，会回溯到系统视图（父视图）下执行，此时该规则对此命令不生效。

· **display**命令中的重定向符（“|”、“>”、“>>”）及其后面的关键字不被作为命令行关键字参与规则的匹配。例如，若规则“rule 1 permit command display debugging”生效，则命令**display debugging > log**是被允许执行的，其中的关键字**> log**将被忽略，RBAC只对重定向符前面的命令行**display debugging**进行匹配。但是，如果在规则中配置了重定向符，则RBAC会将其作为普通字符处理。例如，若规则“rule 1 permit command display debugging > log”生效，则命令**display debugging > log**将会匹配失败，因为其中的关键字**> log**被RBAC忽略了，最终是命令**display debugging**与规则进行匹配。因此，配置规则时不要使用重定向符。