某局点SSLVPN结合LDAP配置后用户组限制不生效

AAA SSL VPN 孔凡安 2023-11-10 发表

组网及说明

不涉及

告警信息

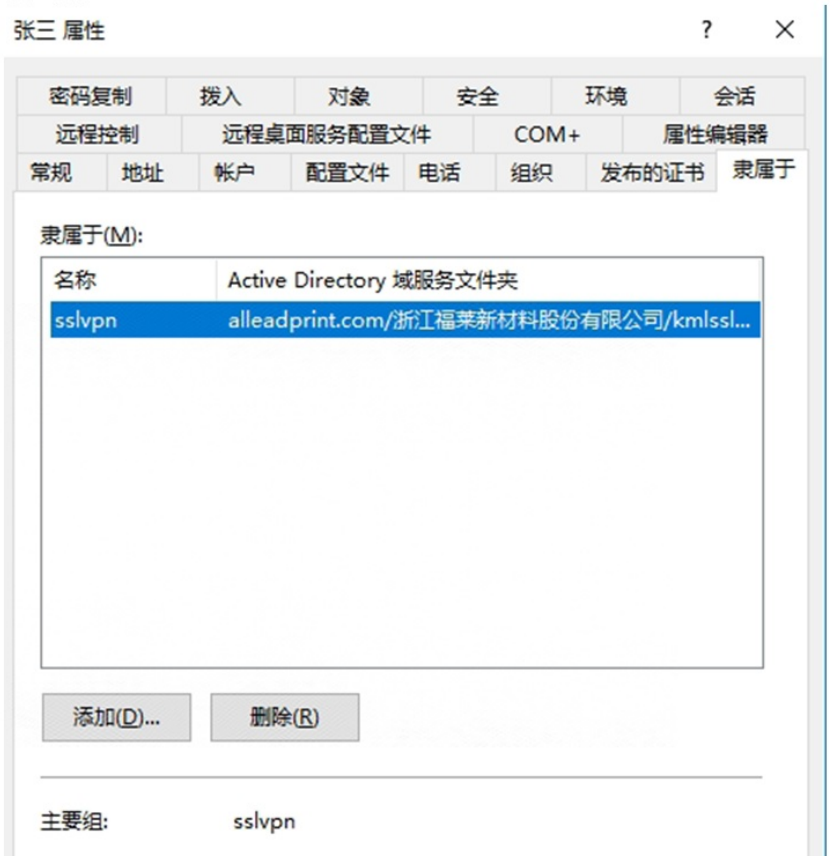
不涉及

问题描述

现场配置SSLVPN结合LDAP认证，需求为不在用户组内的成员无法拨号成功，只有用户组内成员才可以拨号成功。

实际测试发现所有用户均可以成功登录。

如测试用户张三：



过程分析

首先检查设备配置发现现场在开始的时候在sslvpn context视图下配置default-policy-group，配置该命令之后当AAA服务器授权失败时将由缺省策略组下发授权。命令解释如下：

> default-policy-group命令用来指定缺省策略组。
> undo default-policy-group命令用来恢复缺省情况。
> 【命令】
> default-policy-group group-name
> undo default-policy-group
> 【缺省情况】
> 未指定缺省策略组。
> 【视图】
> SSL VPN访问实例视图
> 【缺省用户角色】
> network-admin
> mdc-admin
> vsys-admin
> 【参数】
> group-name：策略组名称，为1～31个字符的字符串，不区分大小写，支持输入中文字符。指定的策略组必须在设备上已经存在。
> 【使用指导】
> 一个SSL VPN访问实例下可以配置多个策略组。远端接入用户访问SSL VPN访问实例时，AAA服务器将授权给该用户的策略组信息下发给SSL VPN网关。该用户可以访问的资源由授权的策略组决定。如果AAA服务器没有为该用户进行授权，则用户可以访问的资源由决定。
> 【举例】
> # 指定名为pg1的策略组为缺省策略组。
> <Sysname> system-view
> [Sysname] sslvpn context ctx1
> [Sysname-sslvpn-context-ctx1] policy-group pg1
> [Sysname-sslvpn-context-ctx1-policy-group-pg1] quit
> [Sysname-sslvpn-context-ctx1] default-policy-group pg1
> 【相关命令】
> · display sslvpn context
> · policy-group

现场后续取消了该配置，但是发现不在下发授权的用户组内用户依然可以登陆。

> %Nov 8 15:46:51:643 2023 Firewall SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=60.176.205.241-User=admin; Command is undo default-policy-group

解决方法

重新使能sslvpn context和sslvpn gateway可以生效。相关授权下发原理见链接：https://zhiliao.h3c.com/Theme/details/193493

示例：

```
ldap attribute-map test
 map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
```

正常携带memberOf属性的报文如下，属性值cn=开头，以","结尾的值，即zgzt就会作为用户组。设备上需要配置user-group zgzt，就能完成授权

```
user-group zgzt
 authorization-attribute sslvpn-policy-group 1
```