S5130S-EI ssh结合ldap登录后配置权限不够

SSH AAA 甄锡坤 2022-05-31 发表

组网及说明

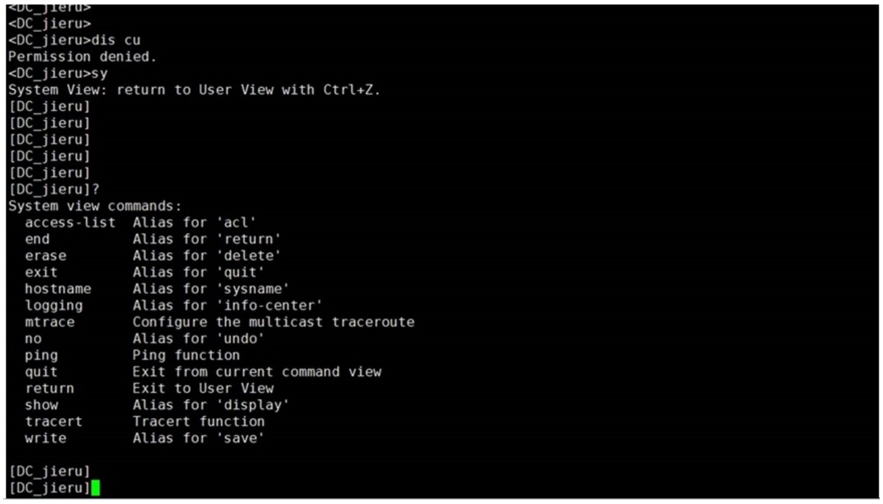
不涉及

问题描述

参考官网1.18.4 SSH用户的LDAP认证配置

https://www.h3c.com/cn/d_202205/1615010_30005_0.htm#_Toc104452543

配置后登录权限不够



```
<DC_jieru>
<DC_jieru>
<DC_jieru>dis cu
Permission denied.
<DC_jieru>sy
System View: return to User View with Ctrl+Z.
[DC_jieru]
[DC_jieru]
[DC_jieru]
[DC_jieru]
[DC_jieru]
[DC_jieru]?
System view commands:
  access-list  Alias for 'acl'
  end          Alias for 'return'
  erase        Alias for 'delete'
  exit         Alias for 'quit'
  hostname     Alias for 'sysname'
  logging      Alias for 'info-center'
  mtrace       Configure the multicast traceroute
  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'

[DC_jieru]
[DC_jieru]
```

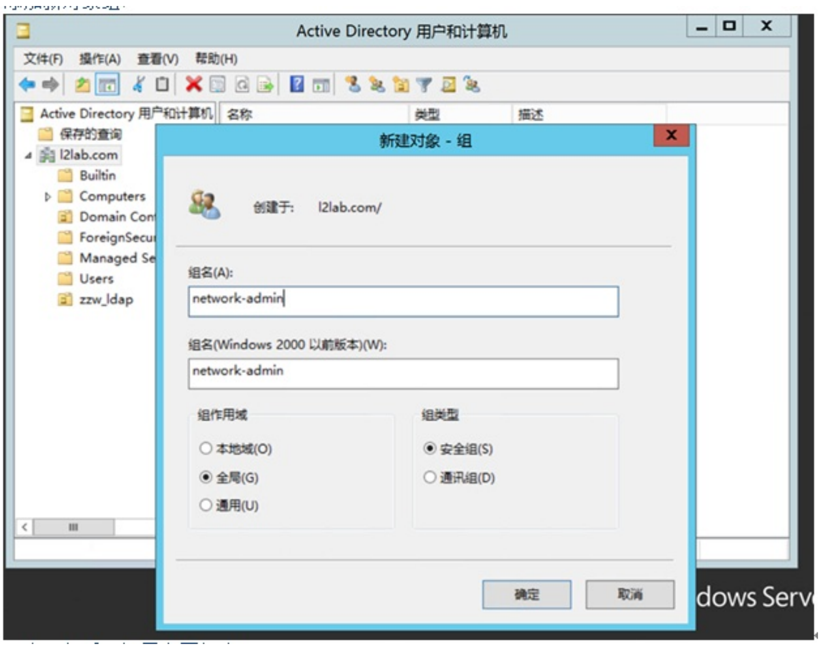
过程分析

修改为network-admin后还是不可以

```
line vty 0 63
authentication-mode scheme
user-role network-operator
```

正常来说是需要配置LDAP属性映射来ying"suser-role的network-admin权限实现的

添加新对象组



新建对象 - 组

创建于: l2lab.com/

组名(A): network-admin

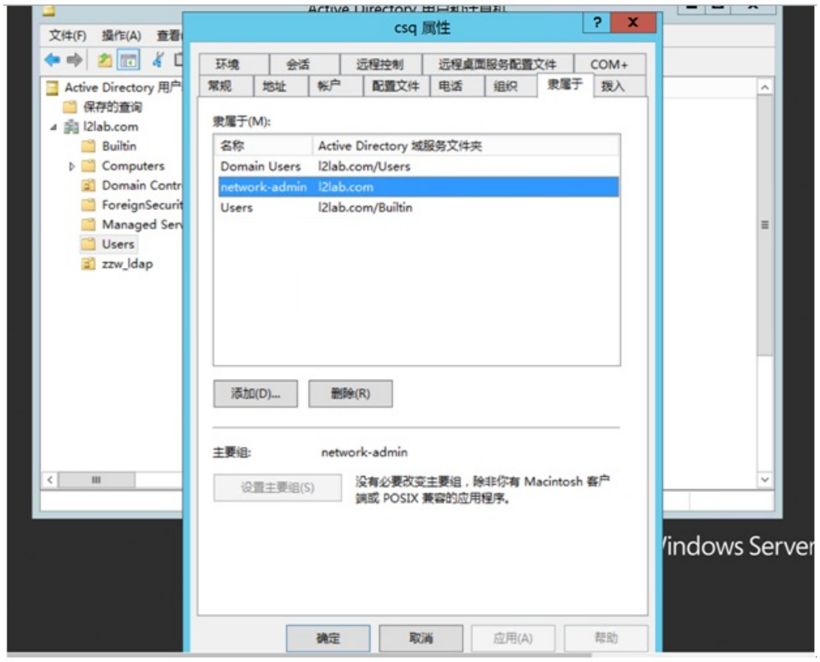
组名(Windows 2000 以前版本)(W): network-admin

组作用域: ○ 本地域(O) ● 全局(G) ○ 通用(U)

组类型: ● 安全组(S) ○ 通讯组(D)

确定 取消

用户添加后，设置主要组应用。



csq 属性

隶属于(M):

名称	Active Directory 域服务文件夹
Domain Users	l2lab.com/Users
network-admin	l2lab.com
Users	l2lab.com/Builtin

添加(D)... 删除(R)

主要组: network-admin

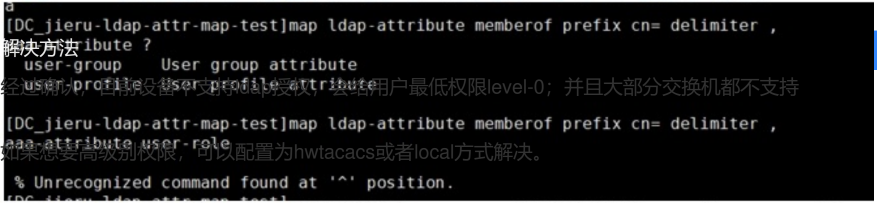
设置主要组(S) 没有必要改变主要组，除非你有 Macintosh 客户端或 POSIX 兼容的应用程序。

确定 取消 应用(A) 帮助

对应LDAP服务器的配置，设备需要配置

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

但是这个user-role实际是配置不上的，只能配置以下两个参数，并且测试创建user-group组后，也无法去调用user-role

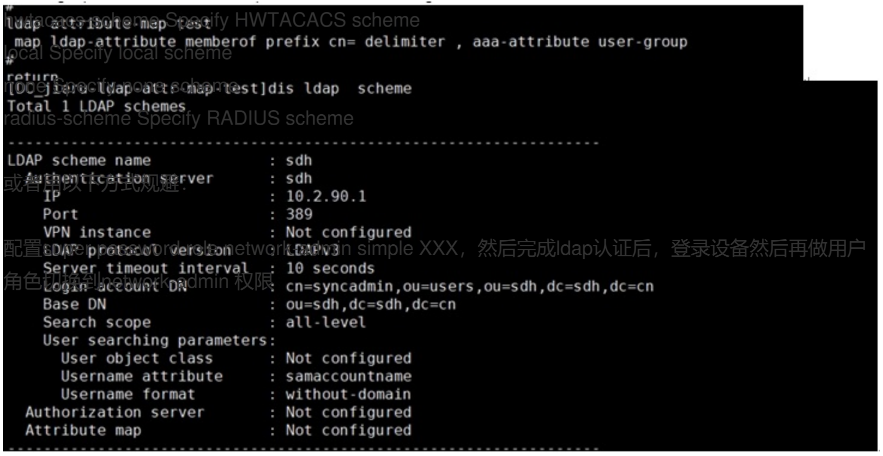


```
a
[DC_jieru-ldap-attr-map-test]map ldap-attribute memberof prefix cn= delimiter ,
aaa-attribute ?
  user-group    User group attribute
  user-profile  User profile attribute

[DC_jieru-ldap-attr-map-test]map ldap-attribute memberof prefix cn= delimiter ,
aaa-attribute user-role

 % Unrecognized command found at '^' position.
[DC_jieru-ldap-attr-map-test]
```

配置user-gourp是没有作用的，attribute map 这个参数后面还是 not configured。



```
#
ldap attribute-map test
 map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
#
return
[DC_jieru-ldap-attr-map-test]dis ldap  scheme
Total 1 LDAP schemes

------------------------------------------------------------------
LDAP scheme name              : sdh
  Authentication server       : sdh
    IP                        : 10.2.90.1
    Port                      : 389
    VPN instance              : Not configured
    LDAP protocol version     : LDAPv3
    Server timeout interval   : 10 seconds
    Login account DN          : cn=syncadmin,ou=users,ou=sdh,dc=sdh,dc=cn
    Base DN                   : ou=sdh,dc=sdh,dc=cn
    Search scope              : all-level
    User searching parameters:
      User object class       : Not configured
      Username attribute      : samaccountname
      Username format         : without-domain
  Authorization server        : Not configured
  Attribute map               : Not configured
------------------------------------------------------------------
```

解决方法

经过确认，目前设备不支持ldap授权，会给用户最低权限level-0；并且大部分交换机都不支持

如果想要高级别权限，可以配置为hwtacacs或者local方式解决。

```
[H3C-isp-aaa]authorization login ?
hwtacacs-scheme Specify HWTACACS scheme
local Specify local scheme
none Specify none scheme
radius-scheme Specify RADIUS scheme
```

或者用以下方式规避：

配置super password role network-admin simple XXX，然后完成ldap认证后，登录设备然后再做用户角色切换到network-admin 权限