【完整版+解释】SSL VPN结合LDAP认证配置

SSL VPN AAA 孔梦龙 2021-07-18 发表

组网及说明

要求：

终端的11.11.11.99终端要拨到SSL VPN网关（FW），防火墙上没有用户，用户要到LDAP服务器上认证，LDAP认真通过后给用户kkk授权可以访问内网的10.10.20.10的服务器。

注意：

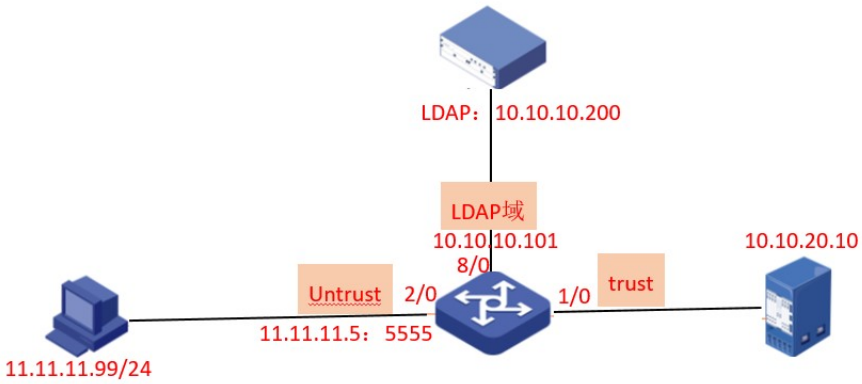
（1）本组网的前提，不管是否存在同网段，两设备之间需要路由可达；

（2）外网口属于Untrust，内网口是trust，连接LDAP是LDAP域，AC口在AC域；SSLVPN拨号需要放通Untrust到Local，认证需要放通local到LDAP，访问内网资源需要放通AC域到trust。【按现场的实际情况，开局建议先使用全通策略，避免策略阻断】

（3）本案例的LDAP安装在WIN 2016上，使用华三最新的INODE软件。

（4）本案例访问的资源以下发路由的形式，现场也可以使用访问URL的形式，资源的访问和LDAP认证没有关系。

（5）本案例假设您具有LDAP的基础知识。



配置步骤

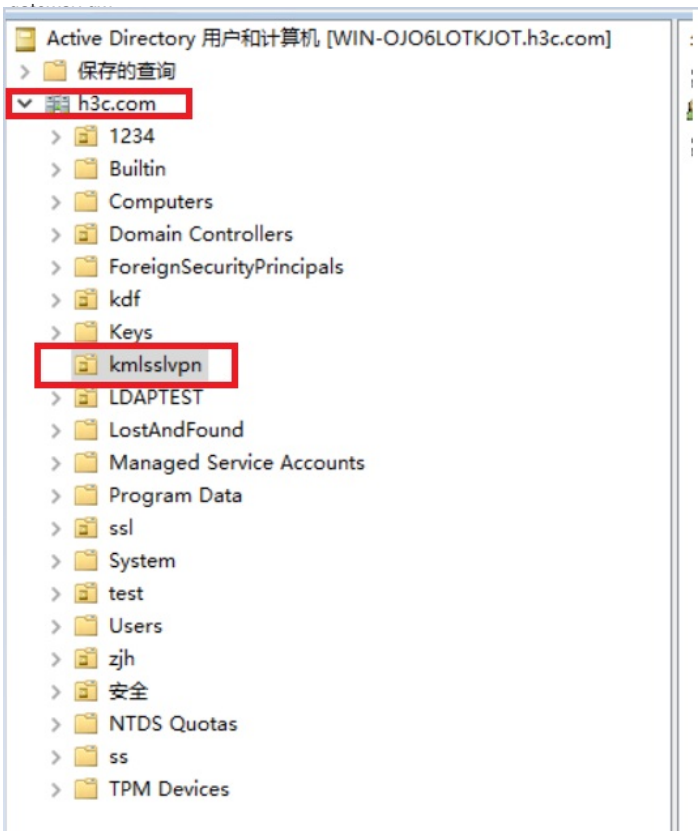
```
# interface GigabitEthernet2/0
 port link-mode route
 ip address 11.11.11.5 255.255.255.0
#
 interface GigabitEthernet8/0
 port link-mode route
 ip address 10.10.10.101 255.255.255.0
#
interface SSLVPN-AC1
 ip address 12.12.12.1 255.255.255.0
#
security-zone name Local
#
 security-zone name Trust
 import interface GigabitEthernet1/0
#
security-zone name DMZ
#
security-zone name Untrust
 import interface GigabitEthernet2/0
#
 security-zone name Management
#
 security-zone name LDAP
 import interface GigabitEthernet8/0
#
 security-zone name AC
 import interface SSLVPN-AC1
 #
 ip route-static 10.10.20.0 24 XXXXX //去往内网服务器的路由
#
 acl advanced 3000 rule 0 permit ip //自己需要过滤的IP，这里没有过滤
 #
 ldap server ldap
 login-dn cn=administrator,cn=users,dc=h3c,dc=com //这个administrator是LDAP的超管的账户
 search-base-dn ou=kmlsslvpn,dc=h3c,dc=com
 ip 10.10.10.200 //LDAP的地址
 login-password simple 123456 // 这个是LDAP的administrator对应的密码
#
 ldap scheme shml
 authentication-server ldap
 authorization-server ldap
 attribute-map test
#
 ldap attribute-map test
 map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
#
 domain h3c.com
 authentication sslvpn ldap-scheme shml
 authorization sslvpn ldap-scheme shml
 accounting sslvpn none
#
 domain system
 #
 domain default enable system
#
 user-group kml1
 authorization-attribute sslvpn-policy-group pg1
```

```
#
 sslvpn ip address-pool kml 12.12.12.2 12.12.12.253
 #
 sslvpn gateway gw
 ip address 11.11.11.5 port 5555
 service enable
#
sslvpn context sslvpn
```

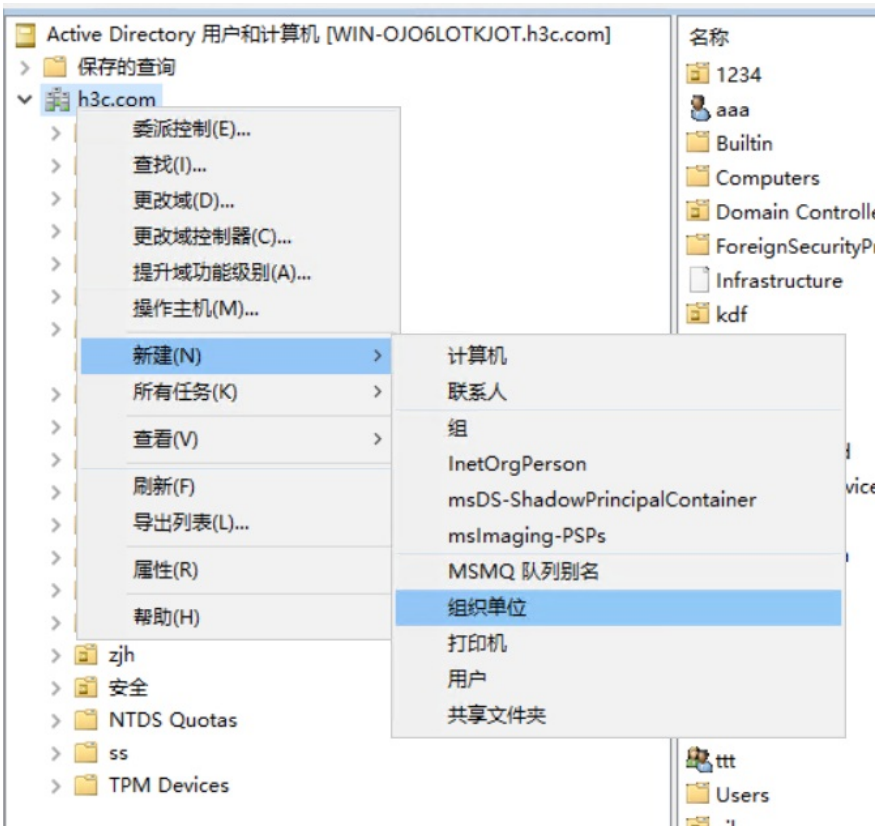
配置关键点

#DAP上的配置：

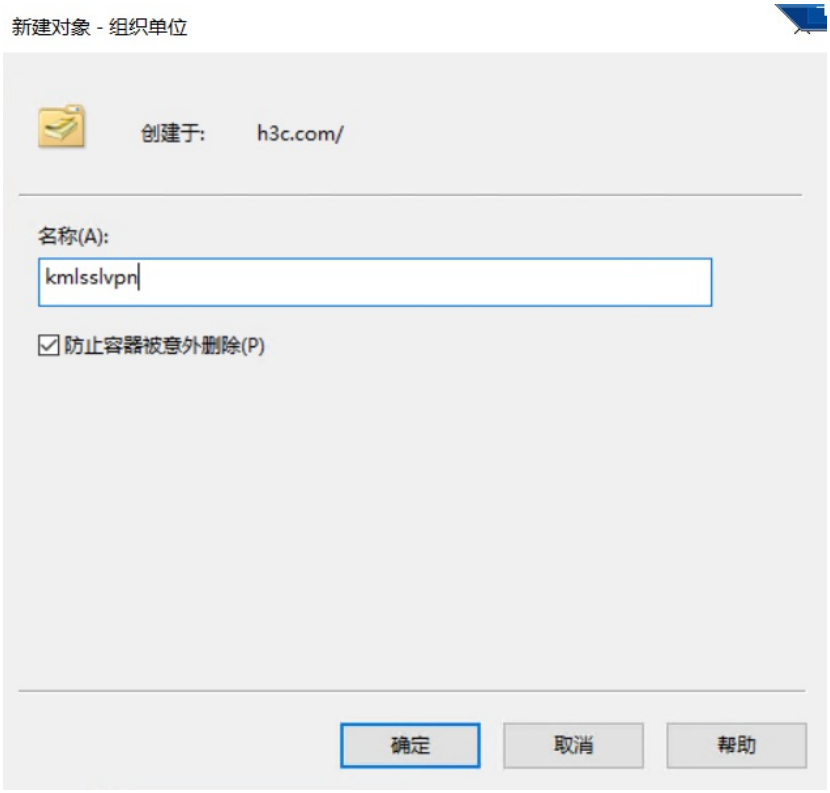
（1）【目录下命名不支持中文】LDAP的根目录是h3c.com，翻译过来就是 DC=h3c，DC=com。



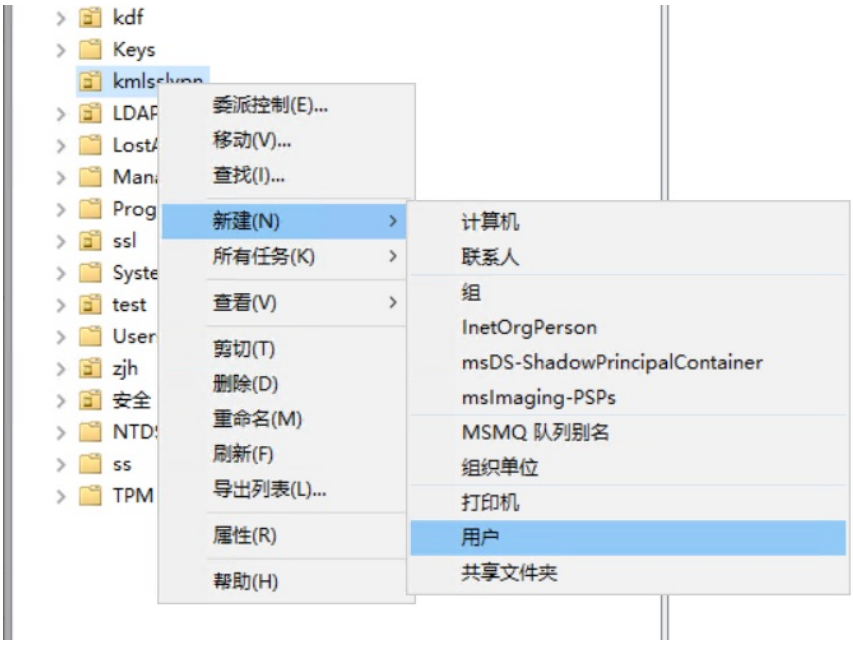
（2）新建kmlsslvpn组织单元。鼠标放在h3c.com上，右键一直选择到组织单元，左键点击



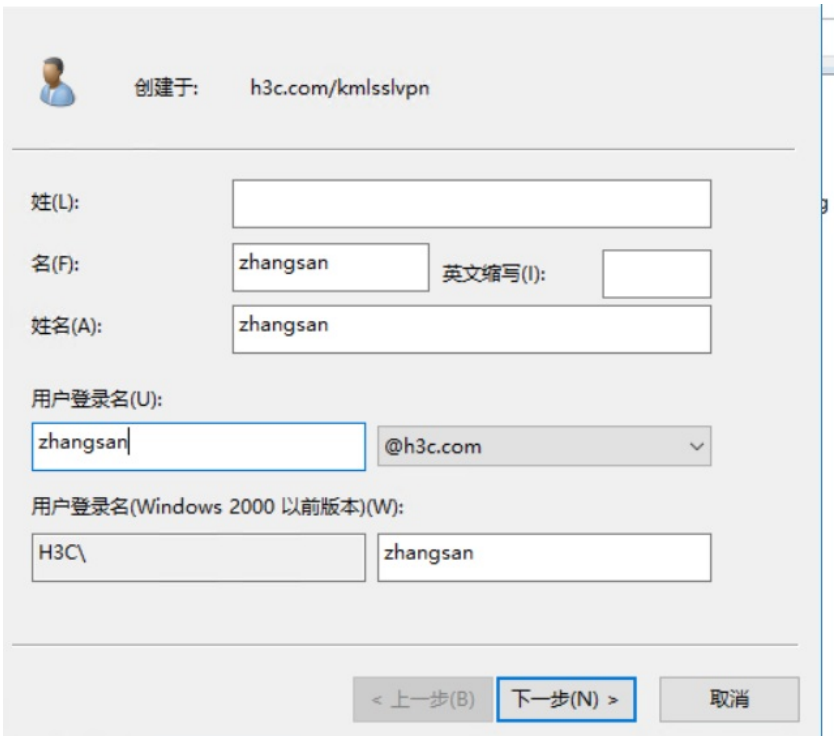
输入组织单元的名字kmlsslvpn，然后点击确定，创建成功；



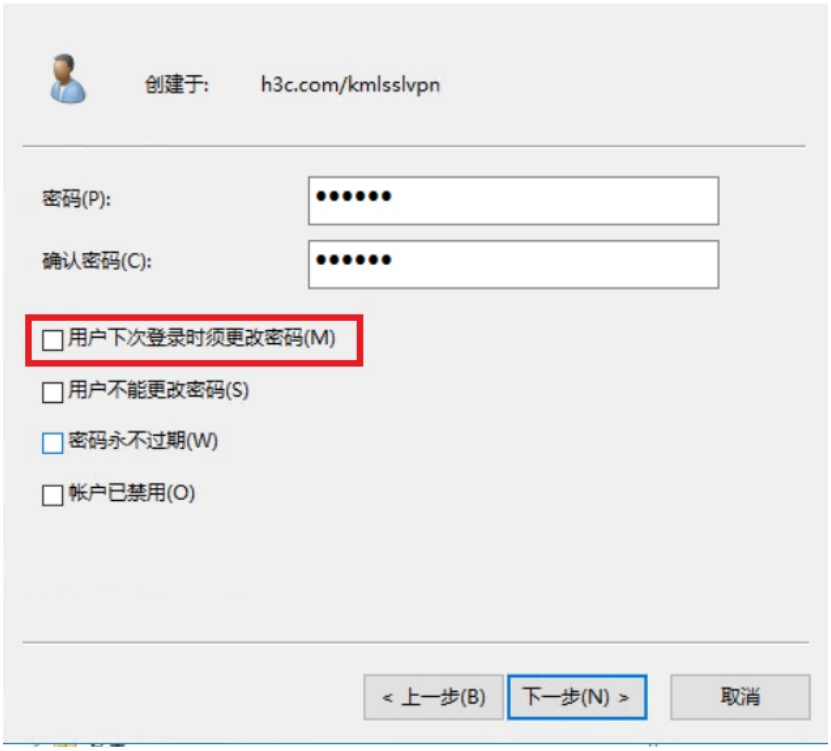
（2）新建用户zhangsan。右键kmlsslvpn，新建用户

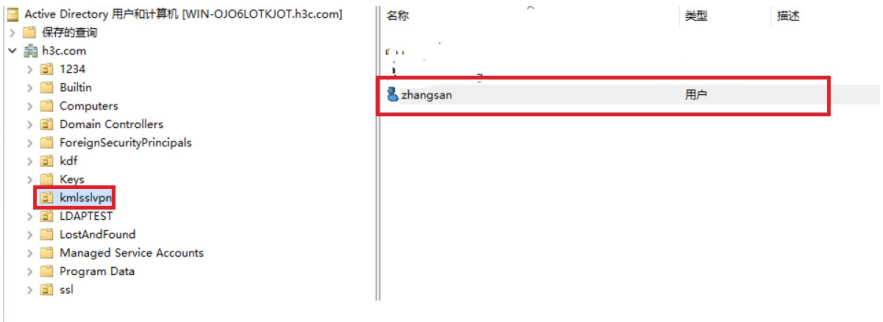


新建用户输入名字zhangsan

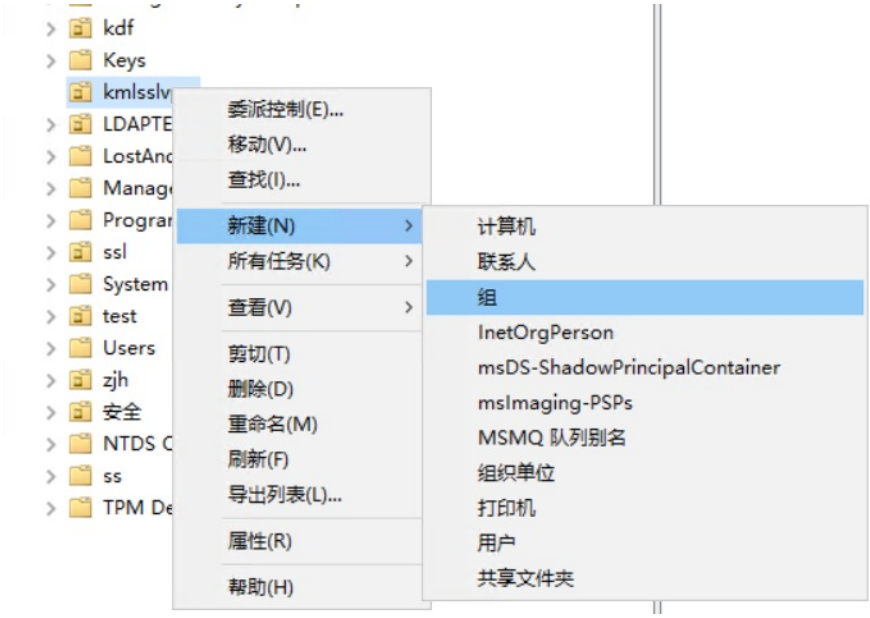


点击下一步，然后输入密码，勾选掉【用户下次登陆时必须更改密码】，点击确定，kmlsslvpn下创建zhangsan用户成功。

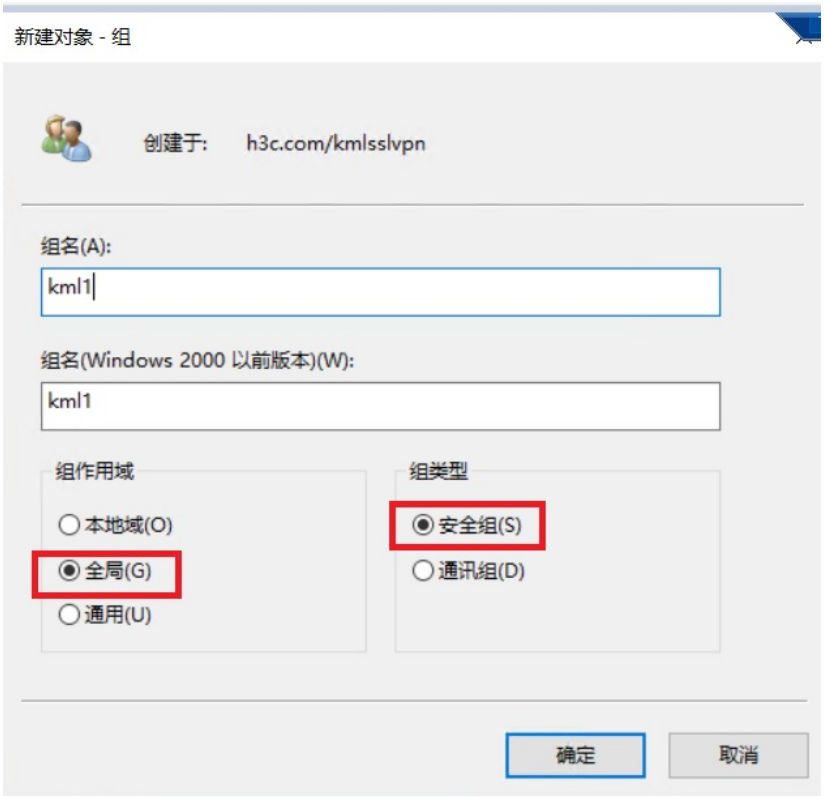


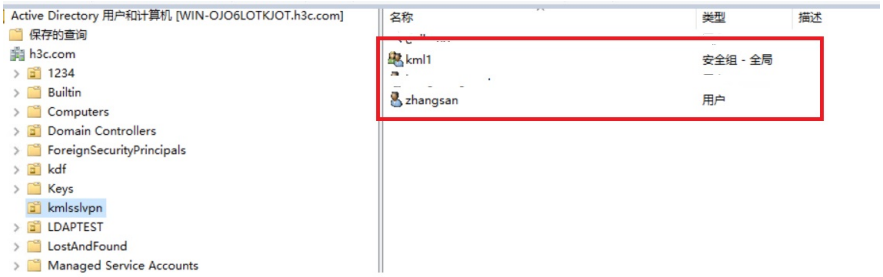


（3）创建安全组kml1。右键kmlsslvpn，找到新建组

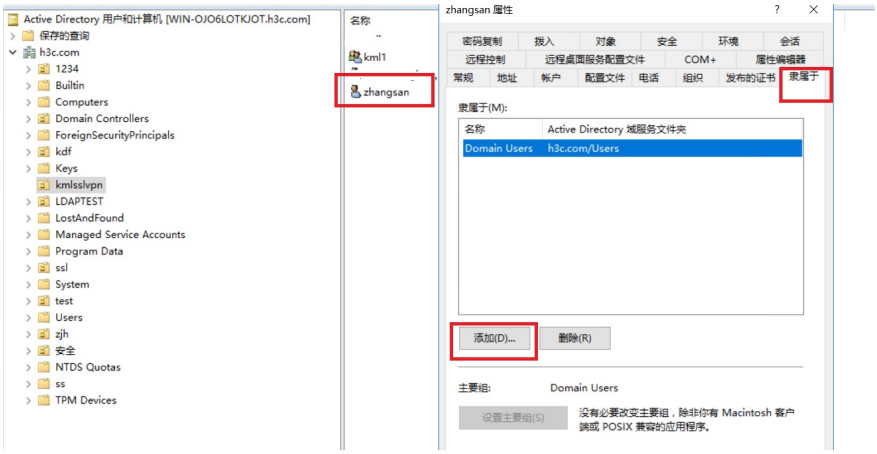


点击确认，新建安全组kml1，然后点击确定。

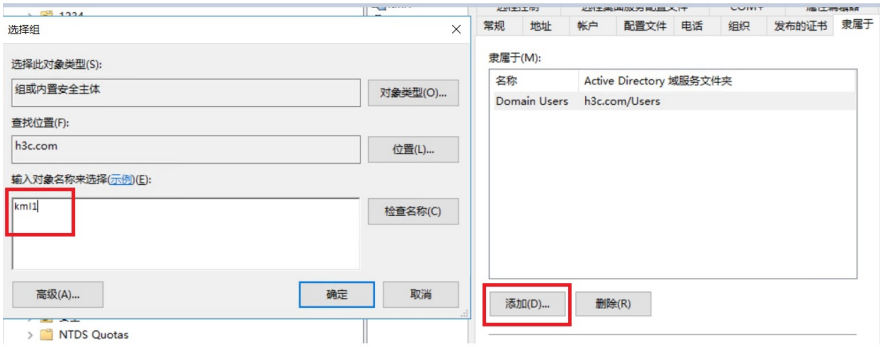




（4）将用户zhangsan归属安全组kml1。右键zhangsan,点击属性，跳出下面的框，点击隶属于，默认的Domain Users不用管，点击添加



在弹出的框中的【输入对象名称来选择】中输入刚创建的安全组kml1,点击确定。



自此SSL VPN+LDAP的认证配置完成，可以使用inode拨号测试是否正常。

配置中解释，

（1）LDAP中创建的安全组kml1,在防火墙上相对应的是：

```
# user-group kml1
 authorization-attribute sslvpn-policy-group pg1
#
```

两者的名字要严格的对应，保持一致。

（2）LDAP中的目录或者用户很多的时候，搜索开始的范围写的太多很浪费设备的性能，甚至导致检索失败，建议精细化

例如本案例中可以写成

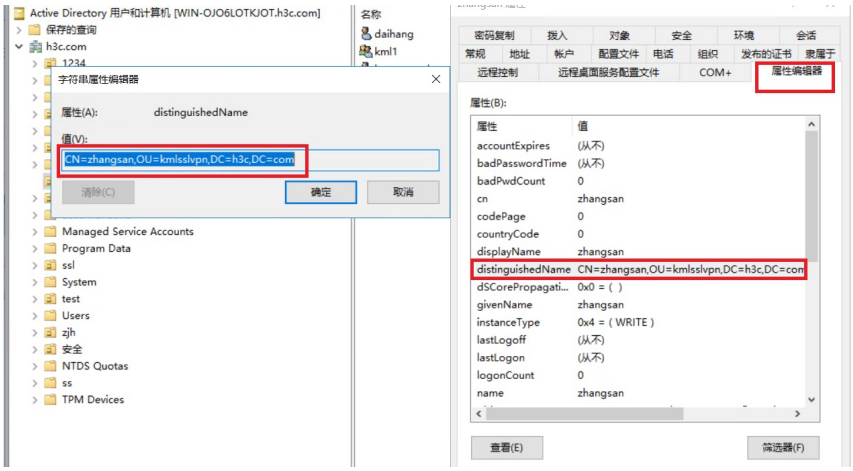
```
 search-base-dn ou=kmlsslvpn,dc=h3c,dc=com
```

也可以写成

```
 search-base-dn dc=h3c,dc=com
```

后者明显搜索的范围很大，怎样快速写出这个用户比较简单的路径呢？

右键zhangsan,属性，弹框中属性编辑器，双击distinguisheNamme，再弹框中，除了CN这个字段，从OU开始，就可以作为搜索开始的路径了



SSL VPN+LDAP还有异常的话，建议通过debug和抓包确认故障点。
需要debug的命令：
debugging sslvpn error
debugging sslvpn event
debugging sslvpn aaa
debugging ldap all