

1-9 : LDAP协议

作者：曾垂鑫

课程地址：http://edu.51cto.com/lecturer/index/user_id-639838.html

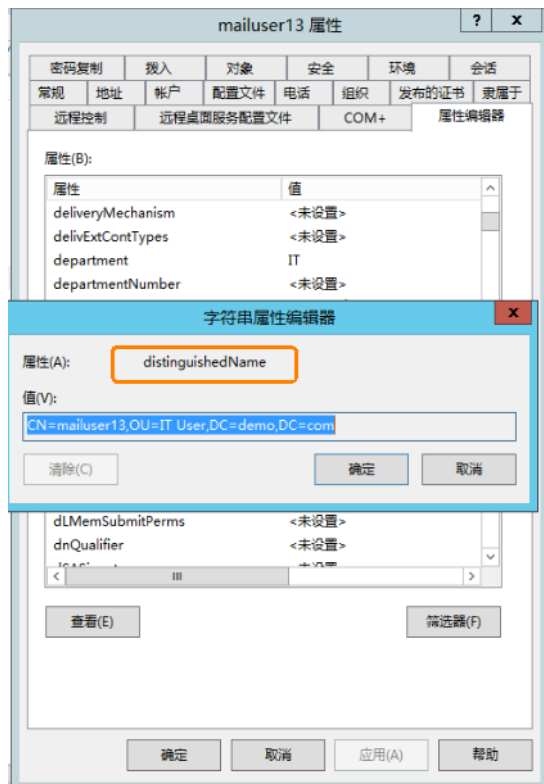
LDAP

lightweight directory access protocol轻型目录访问协议

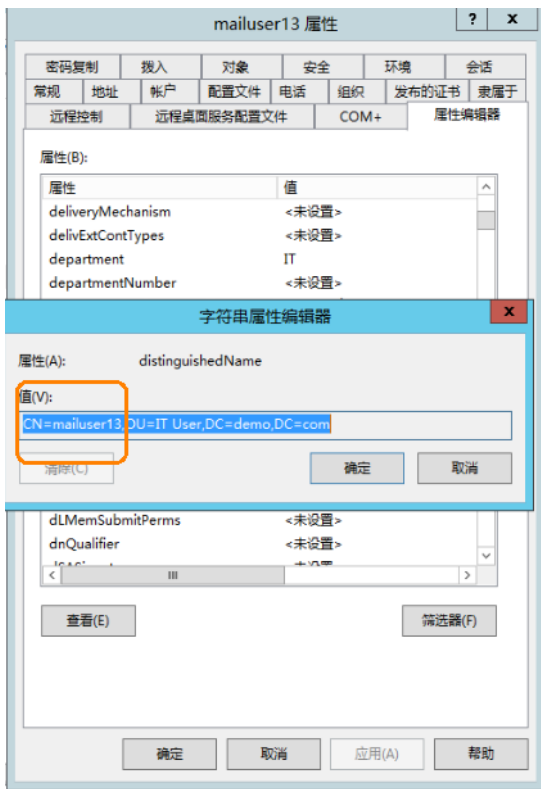
ADDS利用LDAP名称路径来描述对象在ADDS内的位置，以便使用它来访问ADDS对象。

LDAP名称路径

DN名称：它是对象在ADDS内的完整路径



RDN (relative DN) 相对DN：用来代表DN完整路径名称中的部分路径。



GUID: global unique identificatier: 系统会自动为每一个对象指定唯一的128位的GUID。对象的名称会变，但是GUID是永远不会变的。

例如：账户删除后，新建同名的账户，虽然账户名称一样，但是GUID不同了。

```
PS C:\Users\Administrator> Get-ADUser -Identity zengchuixin ! fl
DistinguishedName : CN=zengchuixin,OU=IT User,DC=demo,DC=com
Enabled           : True
GivenName        :
Name             : zengchuixin
ObjectClass      : user
ObjectGUID       : ff6128f3-3bd0-4d84-abd7-d1f6b001f0d8
SamAccountName   : zengchuixin
SID              : S-1-5-21-1248245699-3737697923-1929772546-1244
Surname          : zengchuixin
UserPrincipalName : zengchuixin@demo.com
```

UPN名称 (user principal name) 用户主体名称

在登录域的时候，可以输入域\用户名形式，也可以输入用户名@域的格式。

```
PS C:\Users\Administrator> Get-ADUser -Identity zengchuixin ! fl
DistinguishedName : CN=zengchuixin,OU=IT User,DC=demo,DC=com
Enabled           : True
GivenName        :
Name             : zengchuixin
ObjectClass      : user
ObjectGUID       : ff6128f3-3bd0-4d84-abd7-d1f6b001f0d8
SamAccountName   : zengchuixin
SID              : S-1-5-21-1248245699-3737697923-1929772546-1244
Surname          : zengchuixin
UserPrincipalName : zengchuixin@demo.com
```

SPN (service principal name) 服务主体名称，主要用于服务交互，SPN用来代表某台计算机所支持的服务，它让其他计算机可以通过SPN来与这台计算机的服务进行交互。

例如SCOM部署完成后，SCOM的服务账户会有多个SPN关联到SQL。

C:\Windows\system32>setspn -l letv\scomadmin

Registered ServicePrincipalNames 用于 CN=scomadmin,OU=公用帐号,DC=demo,D

C=com:

MSSQLSvc/SCOM.DEMO.COM:1433

MSSQLSvc/SCOM.DEMO.COM:51669

MSSQLSvc/SCOM.DEMO.COM:SCOMSQLSERVER