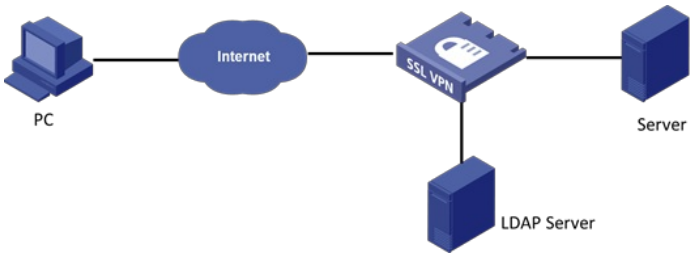
SSL VPN基于LDAP认证的配置

SSL VPN　张泷文　2015-05-05 发表

搭建LDAP服务器：这里使用Windows Server 2003的AD服务器。AD服务器的搭建请参考其他文档。

LDAP服务器及用户信息查看方式：推荐使用ldap browse查看。



1. LDAP服务器配置

在Users目录下新建用户（如用户test）

用户密码设置

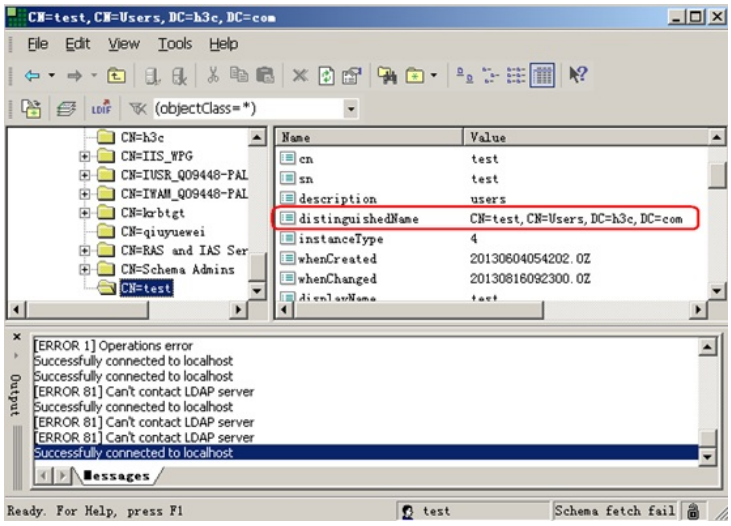
2. SSL VPN设备LDAP认证页面的配置

LDAP认证页面整体配置，红色框中“用户组LDAP属性”需要填写相应的本地用户组名称。

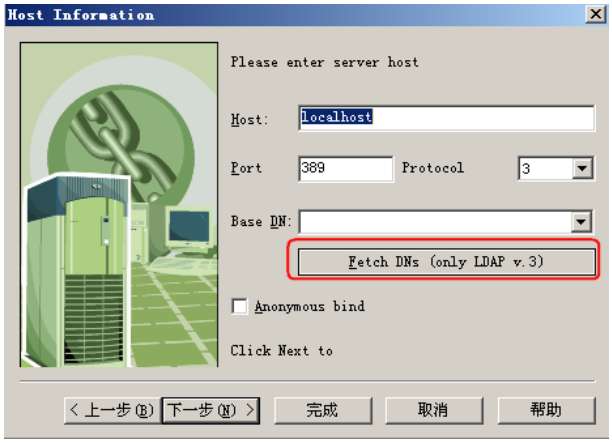
LDAP配置参数说明：

“用户组LDAP属性”，对应LDAP服务器上的用户（如test）的描述信息。
设备提取该描述信息作为认证用户所属的组信息。

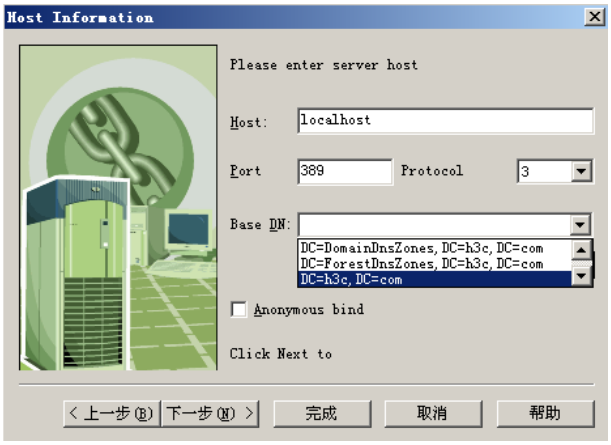
“管理员DN”，即管理员用户的distinguished name，出于安全性考虑，这里管理员用户一般用AD服务器Users组下的一个用户，而不是LDAP服务器的管理员administrator。在ldap browse中可以看到用户的DN值，将该值copy过来即可。



“搜索库DN”，表示从哪个目录节点开始查询，一般写LDAP目录树的根就可以了。在ldap browse中新建Profile也可以看到：
点击红色框中的按钮：



会出现LDAP服务器上的所有“基准DN”，选择用户所在的域h3c.com即可。



“搜索查询模板”，如果LDAP服务器上的用户账号是基于cn的，则填写为“cn=%logon%”；如果账号是基于uid（User ID），那就需要写为“uid=%logon%”。

CN, OU, DC 都是 LDAP 连接服务器的端字符串中的区别名称（DN, distinguished name），LDAP连接服务器的连接字串格式为：ldap://servername/DN。LDAP 目录类似于文件系统目录。

下列目录：

DC=redmond,DC=wa,DC=microsoft,DC=com

如果我们类比文件系统的话，可被看作如下文件路径:

Com/Microsoft/Wa/Redmond