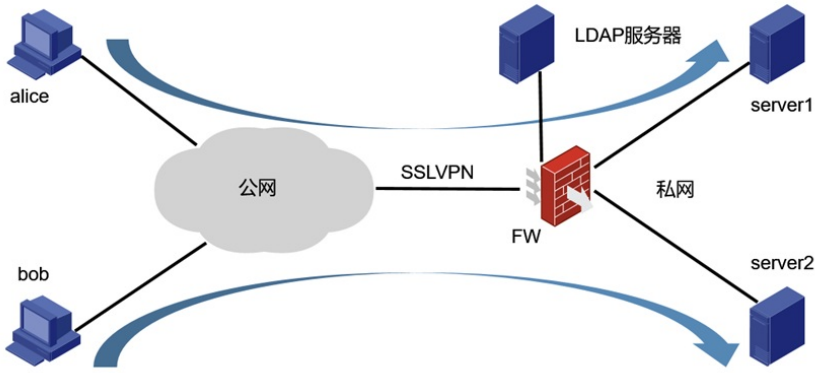
防火墙SSL VPN结合LDAP认证和授权-1.0

SSL VPN AAA 胡伟 2022-02-17 发表

组网及说明

如下图组网，用户alice和bob需要通过防火墙提供的SSL VPN网关接口来访问内网的服务器资源，防火墙使用第三方LDAP服务器进行用户认证，且授权用户alice只能访问server1，用户bob只能访问server2。



关于LDAP服务器的组织架构和基本原理，需要事先了解好DN、DC、OU和CN等相关概念，否则会对配置过程产生困难。LDAP服务器目前通常使用微软的Active Directory，参考资料：

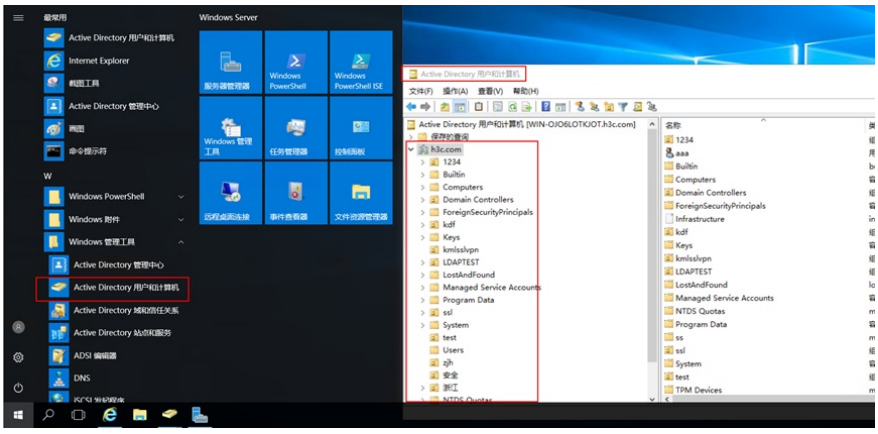
1，https://blog.csdn.net/jfyy/article/details/86070119 Active Directory的基本概念

2，https://blog.csdn.net/qq_38684504/article/details/88125773域服务的建立与测试

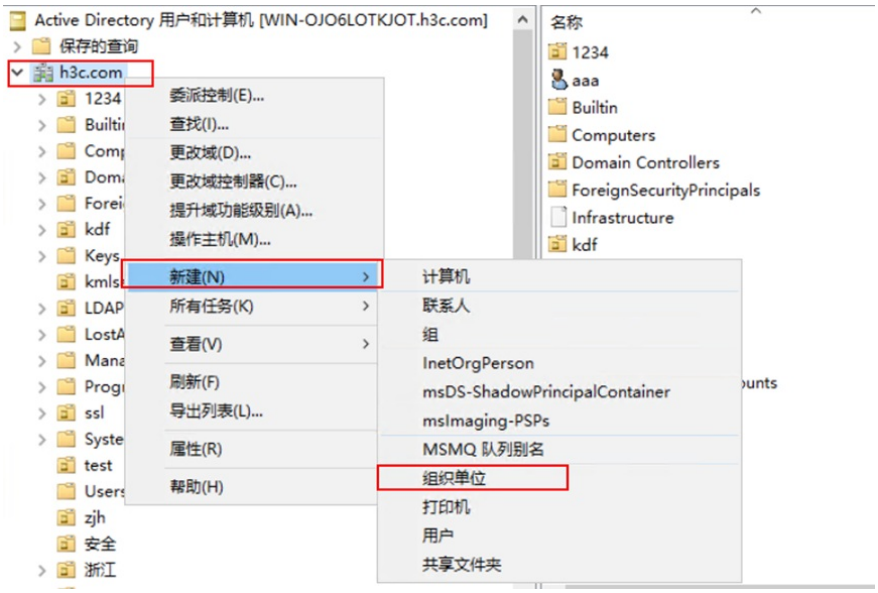
配置步骤

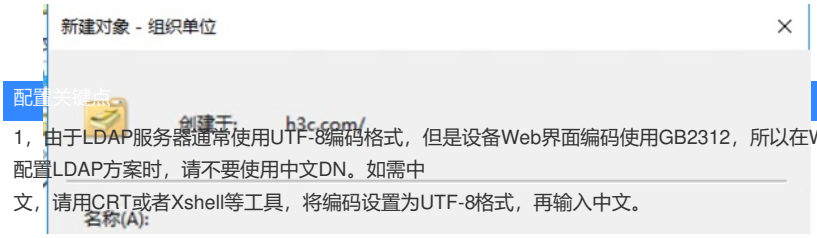
一，配置LDAP服务器

1，登录Windows Server，打开【**Active Directory用户和计算机**】界面，可以查看到系统对应的目录结构信息，比如这里的根目录DN为DC=h3c,DC=com，即h3c.com。



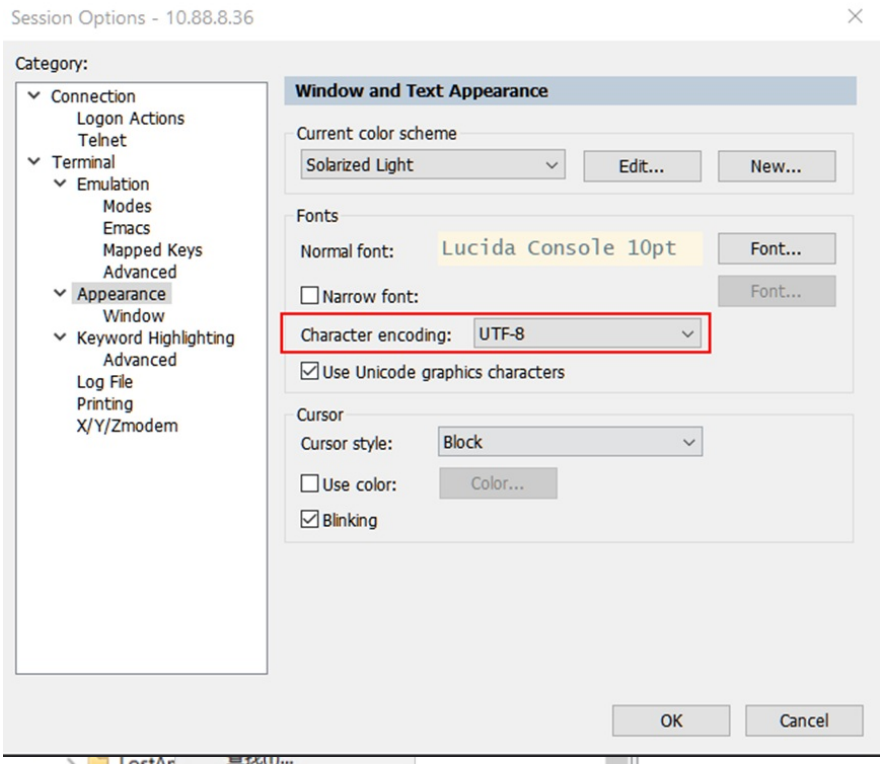
2，在对应的目录下右键新建所需【**组织单位**】（即OU），名称为sslvpn或者使用其他名称。



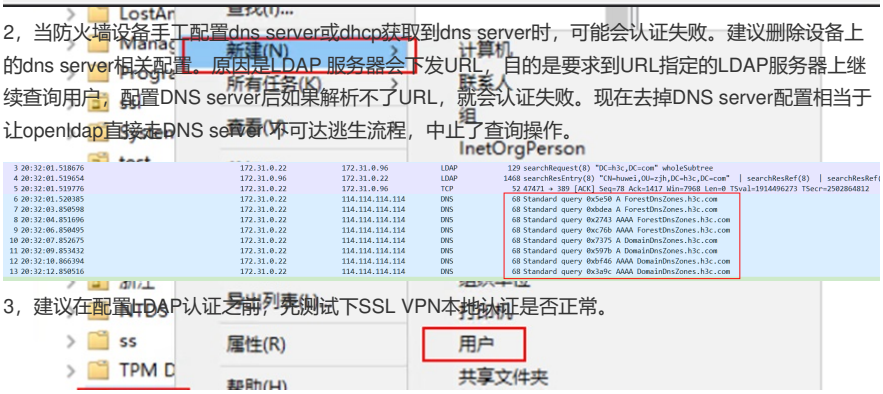


配置关键点

1，由于LDAP服务器通常使用UTF-8编码格式，但是设备Web界面编码使用GB2312，所以在Web界面配置LDAP方案时，请不要使用中文DN。如需中文，请用CRT或者Xshell等工具，将编码设置为UTF-8格式，再输入中文。



2，当防火墙设备手工配置dns server或dhcp获取到dns server时，可能会认证失败。建议删除设备上的dns server相关配置。原因是LDAP 服务器会下发URL，目的是要求到URL指定的LDAP服务器上继续查询用户，配置DNS server后如果解析不了URL，就会认证失败。现在去掉DNS server配置相当于让openldap直接去DNS server不可达逃生流程，中止了查询操作。



3，建议在配置LDAP认证之前，先测试下SSL VPN本地认证是否正常。