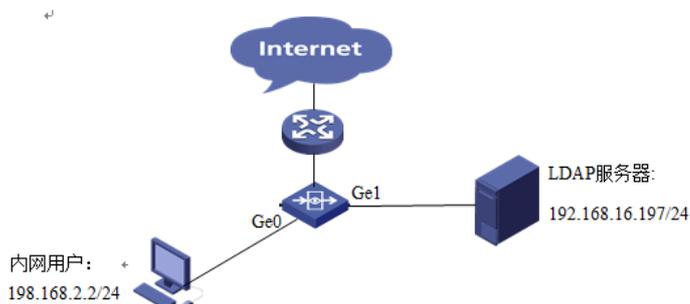


知 ACG1060结合LDAP服务器做WEB认证

ACG1000 认证 刘嘉炜 2016-05-19 发表

某局点想要对内网用户进行登录管理，使用ACG1060设备进行结合LDAP服务器的WEB认证。

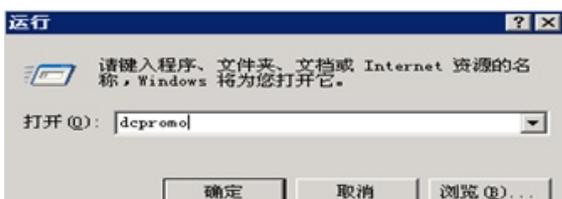


LDAP简介:

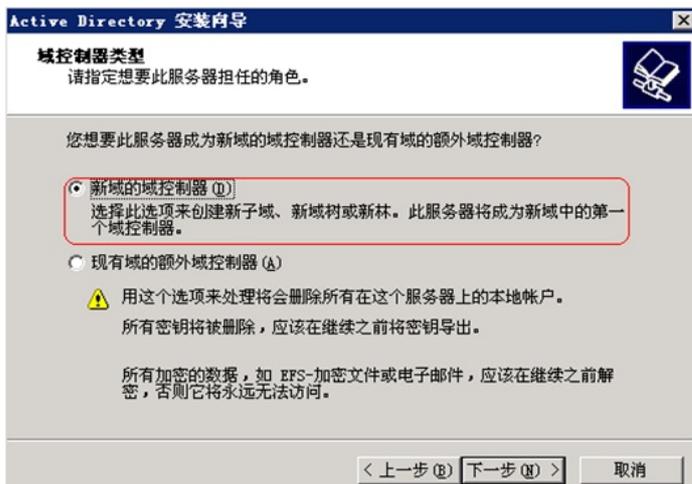
LDAP是一种基于TCP/IP的目录访问协议，用于提供跨平台的、基于标准的目录服务。LDAP协议的典型应用是用来保存系统的用户信息，如Microsoft的Windows操作系统就使用了Active Directory Server来保存操作系统的用户、用户组等信息，用于用户登录Windows时的认证和授权。LDAP的目录服务功能建立在Client/Server的基础之上，所有的目录信息存储在LDAP服务器上。LDAP服务器就是一系列实现目录协议并管理存储目录数据的数据库程序。目前，Microsoft的Active Directory Server、IBM的Tivoli Directory Server和Sun的Sun ONE Directory Server都是常用的LDAP服务器软件。

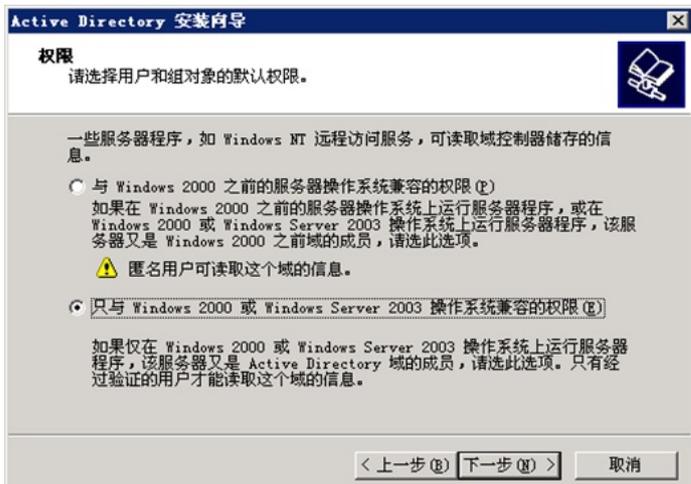
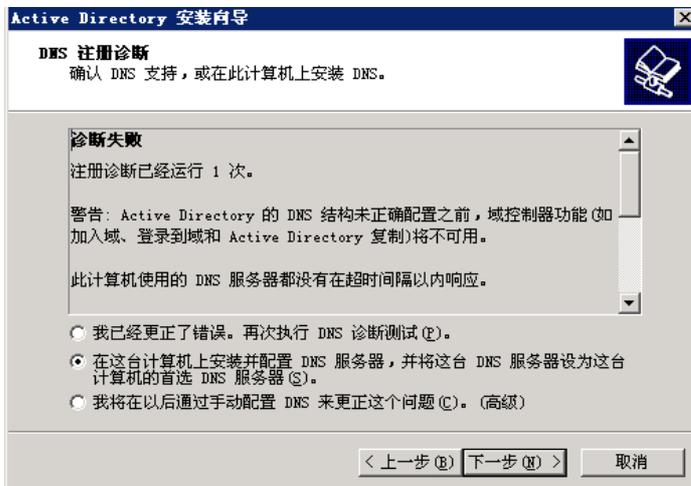
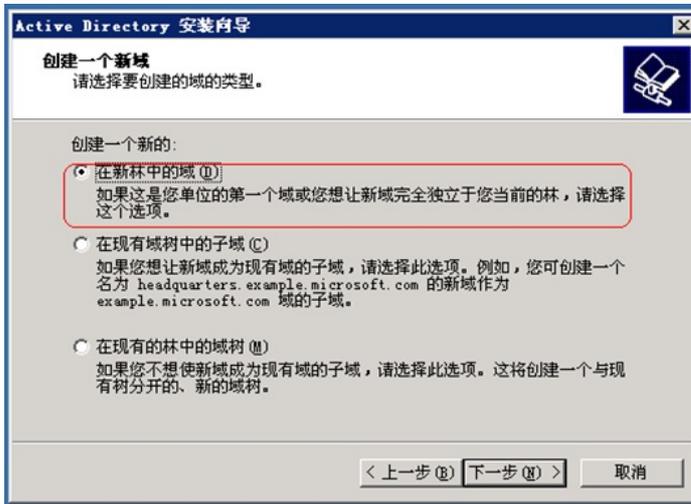
LDAP服务器设置:

- 1、在服务器界面点击“开始”在运行中输入“dcpromo”。

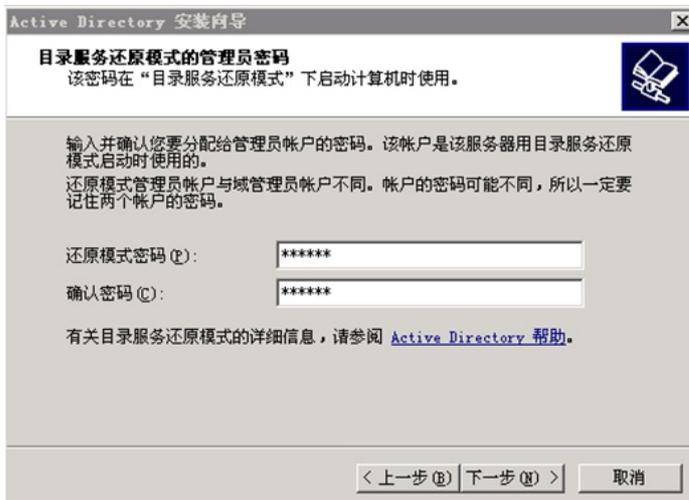


- 2、按照下面步骤配置服务器





下图中管理员密码可以不填。这个密码在卸载AD时使用。



设置完成后需要重启服务器AD域才能生效。

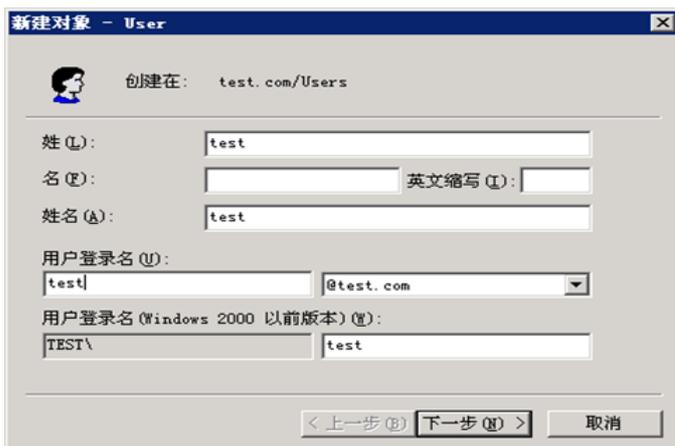
3. 配置登录认证时的用户

点击电脑“开始”-“管理工具”-“Active Directory用户和计算机”。

在test.com中users目录下去创建新用户。



新建用户登录名为“test”域为“test.com”



设置登录用户的密码



ACG1060设备侧的配置:

4、配置与内网和服务器连接的接口IP地址

接口名称	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1 ge0	192.168.16.100/24		3c:8c:40:4e:2f:79	route	full	100	up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2 ge1	192.168.2.1/24		3c:8c:40:4e:2f:7a	route	full	1000	up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3 ge2			3c:8c:40:4e:2f:7b	route	full	1000	down	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

5、新建用户LDAP认证用户



6、配置用户策略



7、设置LDAP的认证服务器



这里的区别名中: cn表示common name 通用名也就是这里的“users”

DC: Domain Component: DC类似于dns中的每个元素, 例如test.com, “.”符号分开的两个单词可以看成两个DC,

8. 配置全局设置



实验验证:

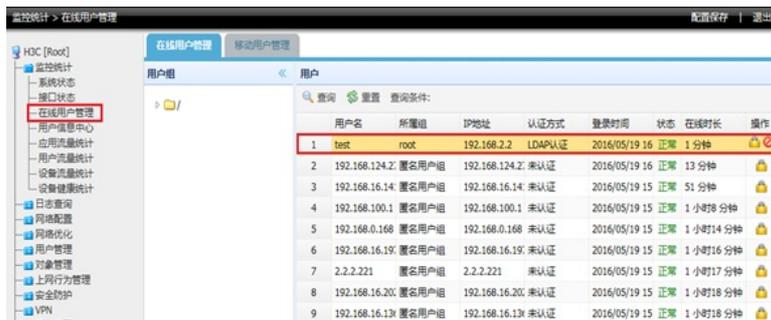
浏览器输入任意地址后出现登录界面: 网页被重定向到登录界面。



客户端登陆后出现登陆成功界面:



在设备上也可以看到对应的用户在线信息。



1、正确的安装LDAP服务器，并且在对应目录下创建用户。

2、客户端使用LDAP的认证，其实是设备和LDAP服务器之间交互查询报文，所以配置中一定保证设备和服务器之间是可达的。