实验目标：samba+ldap实现共享登陆单用户认证

实现的功能：可基于组实现共享权限的认证，基于S1账号登陆，权限更安全更可控。

环境：两台Centos5.5，一台作为LDAP服务器（IP：172.16.27.223）、一台作为samba服务 器（IP：172.16.27.224）

安装软件：LDAP服务器上安装openldap\*、samba

SAMBA服务器安装samba\*、openldap-clients\*

实验步骤：

LDAP服务器配置：

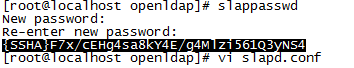
1. 关闭selinux,更改主机名，实验主机名为：localhost

2. cp /etc/openldap/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

chown -R ldap:ldap /var/lib/ldap/

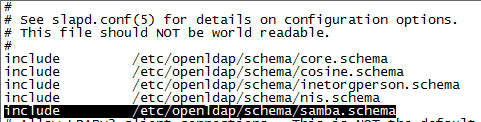
3. cp /usr/share/doc/samba-3.0.33/LDAP/samba.schema /etc/openldap/schema/

4. slappasswd //生成管理员Manager密码，如图：

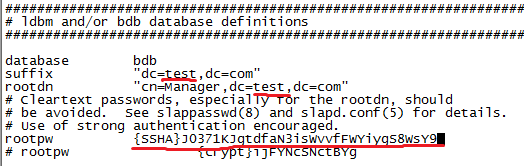


5. vi slapd.conf 更改如下

增加：samba.schema,让ldap支持samba，如图：



更改域名并添加密码，如图：



6. 编辑migrate\_common.ph

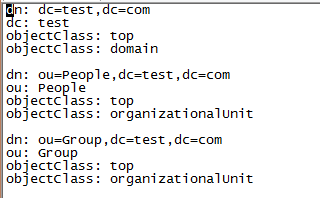
2.png

更改为：$DEFAULT\_BASE = "dc=test,dc=com"；

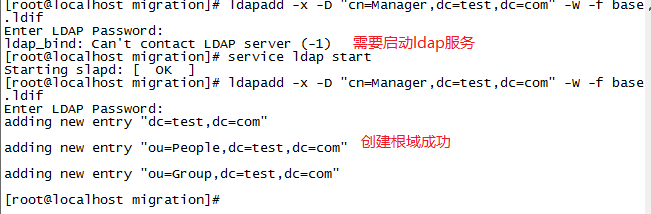
7. 调用脚本执行，如图：

3.png

仅保留如下图：



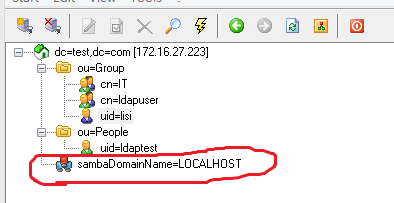
8. 创建根域，如图：



迁移组和用户，可任意新建一个组和用户，如图：

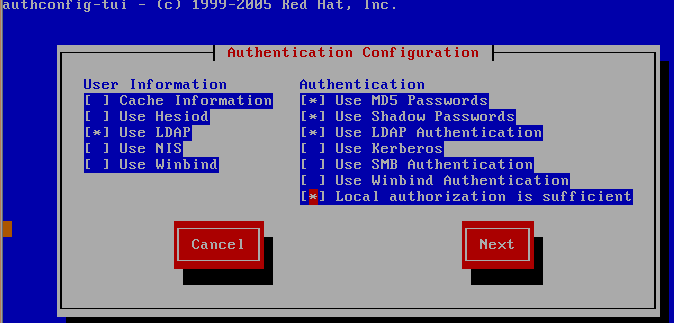


登陆域，可看见：如图：



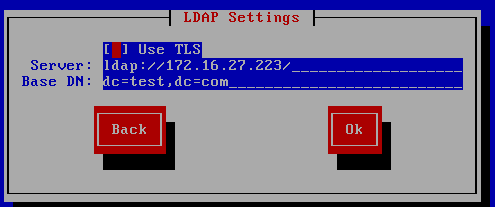
SAMBA服务器配置：

1. 输入命令setup ，如图：



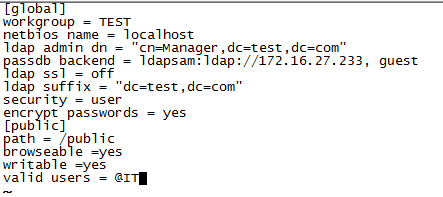
勾选：Use LDAP 、Use MD5 Passwords 、 Use Shadow passwords 、Use LDAP Authentication 、Local authorization is sufficient

点击Next，如图：



不勾选Use TLS ，设置ldap服务器IP地址，设置域名。点击OK

2. 备份smb.conf文件，重新编辑smb.conf,如图：



上图定义了一个IT组，有写入权限。

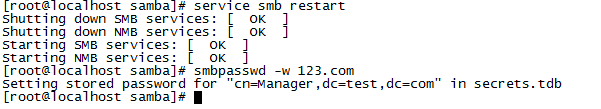
建立共享目录

mkdir /public

chown -R root:IT /public 更改属组为IT组

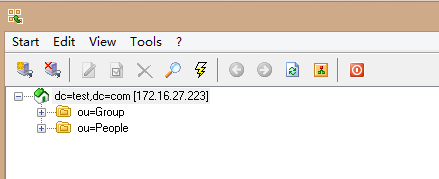
chmod -R 771 /public 更改目录读写权限

3. 写入LDAP服务器的Manager密码，如图：



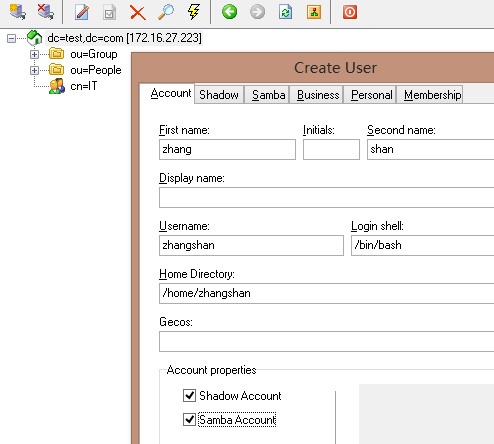
最后测试：

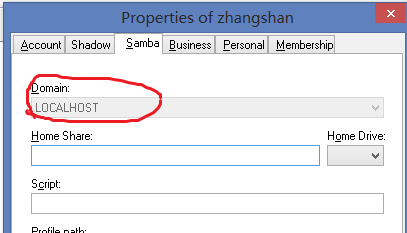
1.启动ldapadmin.exe,连接域test.com.如图：



连接成功。

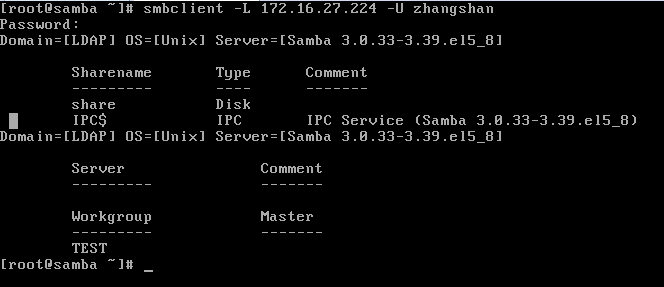
2.新建用户，如图：





此处的LOCALHOST即为上面所示的。没有此处选项，无法实现用户调用LDAP认证。

测试结果：如图：



顶我，就访问我的淘宝：jfaner.taobao.com,赚点人气哦，谢谢！