

Samba+LDAP+LAM 管理工具应用

作者 : gavin

电子邮箱 : gavin.zhou@gmail.com msn : gavin_zhm@msn.com

主页地址 : blog.yepn.net

建立日期 : 2008 年 04 月 11 日, 最后修改日期 : 2008 年 04 月 11 日

版本 : 0.1

版权说明 : 本文基于创作共用约定, 内容归作者所有, 欢迎大家转载, 但要请保留作者的完整信息和出处, 谢谢!

本文参考 : RedHat Enterprise Linux Server 4.3 + OpenLDAP + DNS + Samba + Postfix + OpenWebmail 作者 Fandy

<http://bbs.chinaunix.net/thread-805302-1-1.html>

使用 OpenLDAP 集中管理用户帐号 作者 Mike O'Reilly IBM

<http://www.ibm.com/developerworks/cn/linux/l-openldap/#author>

OpenLDAP 2.1 管理员指南 翻译 NTKO

http://i18n.linux.net.cn/others/OpenLDAP2.htm#_Toc14210017

作者 注 :

由于公司使用的文件服务器空间不足 (只有 750G), 所以准备新装一台服务器。另外, 小弟现在管理公司网络, 每新来一名员工就要建 6-7 个 ID, 网络认证 ID, Samba ID, 邮件 ID, SNS ID, Desknet ID 等等, 让日常维护工作量大大增加, 所以打算在公司应用 LDAP 服务器, 也可以借这次新的 Samba 服务器, 先把 SambaID 导出到 LDAP 中。

小弟在服务器构筑过程中也有很多很多的问题多用 GOOGLE 是最好的方法, 如果能找到高人请教也是一种方法, 不过总有效的还是 GOOGLE 一下, 这样对自己也是一种学习过程。另外, 对于一些 LINUX 前辈写的文章要仔细阅读特别是安装文件的版本号, 往往很小的细节会让你浪费一天的时间。

文章分为

I.OS 准备确认

II.OpenLDAP 和 SAMBA 安装设置

III.Samba 用户和组导入 (smbldap-tool 使用例)

IV.LAM 软件安装和应用

服务器环境

1.CentOS 5.0 Linux server 2.6.18-53.1.14.el5

安装后先配置一下 yum 再升级一下, Centos 带的 yum 站点好像没有 REDHAT 家的好用, 有可能是个人感觉, 不过我还是按照 Centos 网站上写的添加了一下装了一下 RPMforge

```
#yum install yum-priorities
#vi /etc/yum/pluginconf.d/priorities.conf
[main]
enabled=1
#vi /etc/yum.repos.d/
priority=N    #我设置的 N=1
#wget
http://apt.sw.be/redhat/el5/en/i386/RPMS.dag/rpmforge-release-0.3.6-1.el5.rf.i386.rpm
#rpm -ivh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
#yum check-update    #升级一下
```

2.Apache 2.2.6 Released (现在 2.2.8 已经 Released 了)

源码包安装

```
./configure && make && make install
```

安装后 Document Root 为

```
/usr/local/apache2/htdocs
```

3.PHP Version 5.2.5

源码包安装

```
./configure --with-apxs2=/usr/local/apache2/bin/apxs --enable-mbstring --with-zlib
--with-gd --with-jpeg-dir --with-png-dir --with-mysql --with-mcrypt --with-xsl
--with-gettext --with-ldap --with-mhash --with-imap --with-imap-ssl && make && make
install
```

对于参数有不明白的朋友可以 GOOGLE 一下, 讲的会比我写的明白。

PHP 安装后要设置 Apache 的配置文件 httpd.conf, 内容请参考 PHP 源码包中的 INSTALL

文件，我就是按上面写的。

4.OpenLDAP 和 Samba 安装都用的 yum 安装，如果想用源码包安装的话，需要自己安装一些 LIB 等文件，详细说明请参考我的 WIKI 网站 <http://wiki.yepn.net> 中 OpenLDAP 中有详细的源包码说明。上面提到的 Apache 和 PHP 源码包安装也有详细的说明。

5.对于 Samba 和 LDAP 用户管理需要 smbldap-tool 这个工具用起来很方便。一样用 yum 安装

```
#yum -y install smbldap-tool
```

=====华丽的分划线=====

OpenLDAP 配置文件说明

```
vi /etc/openldap/slapd.conf
```

特别注意：下面的配置文件使用时请去掉注释，LDAP 对配置文件格式有严格要求。

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema
#这个 samba.schema 文件，如果用 yum 安装后可以在
/usr/share/doc/samba-3.0.25b/LDAP/下找到复制到上面指定的目录

include /etc/openldap/schema/corba.schema
include /etc/openldap/schema/misc.schema

# Allow LDAPv2 client connections. This is NOT the default.
allow bind_v2
```

#允许使用 bind v2 有些设备需要用到 Samba 用 V3

Do not enable referrals until AFTER you have a working directory

service AND an understanding of referrals.

#referral ldap://root.openldap.org

pidfile /var/run/openldap/slapd.pid

argsfile /var/run/openldap/slapd.args

#loglevel 296

#调试的时候加的 LOG 配置文件，运行正常后去掉了，不想生成大量的 LOG 文件

access to attrs=userPassword

by self write

by anonymous auth

by dn="uid=admin,ou=Users,dc=yepn,dc=com" write

by * none

access to *

by self write

by dn="uid=admin,ou=Users,dc=yepn,dc=com" write

by * read

#上面是配置访问权限

对于 userPassword 字段自己可以改写，用户 admin 可以改写，匿名用户可以认证，其他拒绝。

自己可以写自己 dc 中的所有权限，admin 用户可以写全部，所有人可读。

上面 ACL 的顺序也很重要，调换的话会出现 PAM 认证问题。

database bdb

suffix dc=yepn,dc=yepn

rootdn cn=root,dc=yepn,dc=com

directory /var/lib/ldap

index objectClass eq,pres

index ou,cn,mail,surname,givenname eq,pres,sub

index uidNumber,gidNumber,loginShell eq,pres

index uid,memberUid eq,pres,sub

```
index nisMapName,nisMapEntry          eq,pres,sub
index sambaSID,sambaSIDList,sambaGroupType    eq,pres
```

```
# Replicas of this database
repllogfile /var/lib/ldap/openldap-master-replog
#replica host=172.30.4.91:389 starttls=critical
replica host=172.30.4.91:389
    binddn="cn=root,dc=yepn,dc=com"
    credentials=111111
    bindmethod=simple
```

#上段为从 LDAP 服务器，只有一台 LDAP 服务器的网络配置不太稳定，万一 LDAP 服务器坏掉，会出现很多系统不能登陆的问题。

```
rootpw 000000    #密码名文, 过后会把 ROOT 从配置文件中删除, 用 admin 用户管理 LDAP
```

配置文件确认无误后启动 LDAP

```
#service ldap start
```

看到下面的信息说明你的 LDAP 正常启动了

```
Checking configuration files for slapd:  config file testing succeeded
Starting slapd:                          [ OK ]
Starting slurpd:                          [ OK ]
```

=====华丽的分划线=====

Samba 安装可以参考 Fandy 的 RedHat Enterprise Linux Server 4.3 + OpenLDAP + DNS + Samba + Postfix + OpenWebmail 这篇文章我的 Samba 配置配置是按照他上面写的配置的。

下面是我的配置文件，简单说明一下，因为原文的作者写的很细。

```
# Global parameters
# Version 2008-03-28-01
[global]
    workgroup = YEPN
    netbios name = vanilla
    security = user
    server string = Samba Server 7T %v
```

```
    encrypt passwords = Yes
    obey pam restrictions = No
    ldap passwd sync = yes
#与 LDAP 密码同步
    log level = 3
    syslog = 0
    log file = /var/log/samba/log.%m
    max log size = 100000
    time server = Yes
    socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
    mangling method = hash2
    Dos charset = UTF-8
    Unix charset = UTF-8
    logon script = %U.bat
    logon drive = H:
    domain logons = Yes
    os level = 65
    preferred master = Yes
    passdb backend = ldapsam:ldap://127.0.0.1/
#指定 LDAP 服务器
    ldap admin dn = uid=root,dc=yepn,dc=net
#可以管理员用户
    ldap suffix = dc=yepn,dc=net
#搜索域
    ldap group suffix = ou=Groups
#用户级的检索字段
    ldap user suffix = ou=Users
#用户检索字段
    add user script = /usr/sbin/smbldap-useradd -a -m "%u"
#添加用户
    ldap ssl = off
    ldap delete dn = Yes
    delete user script = /usr/sbin/smbldap-userdel -r "%u"
#删除用户
    add group script = /usr/sbin/smbldap-groupadd -a -p "%g"
#添加组
```

```
delete group script = /usr/sbin/smbldap-groupdel "%g"
#删除组
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
#把用户加到指定组
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
#从组中删除用户
set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
#设定用户的属组
#以上配置是跟 LDAP 相关的, 其他对于共享目录等控制可以自行添加
```

[homes]

```
comment = Home Directories %U, %u
browseable = no
writeable = yes
read only = no
force create mode = 0700
force directory mode = 0700
directory mode = 0700
create mode = 0700
inherit acls = yes
guest ok = no
printable = no
```

#homes 目录的定义, 其实这个作用已经不大了, 因为建立目录的时候会通过 smbldap-tool

Samba 配置完后启动一下

```
#service smb start
```

```
Starting SMB services: [ OK ]
```

```
Starting NMB services: [ OK ]
```

显示上面的说明正常启动, 第二个服务说明一下是 NETBIOS 服务

```
#smbpasswd -w 111111
```

#把 LDAP 的管理员密码加到 Samba 中, 这个一定要做, 让 Samba 对 LDAP 有权修改。

====华丽的分划线=====

写在 Samba 安装之前

Samba 服务器安装之前，需要修改服务器的 PAM 认证，让系统用户通过 LDAP 认证，具体内容可以参考《使用 OpenLDAP 集中管理用户帐号》这篇文章写的很细。如果你的系统可以通过 LDAP 认证登陆了，请继续向下看，如果不行，不要向下进行。

Samba 用户和组导入

原来的 Samba 用户和组采用系统帐号，现在导入起来也比较方便。

很多文章介绍用 MigrationTools 这个工具导入，我用的是 smbldap-tools 这个工具导入的用户和组。

在用 smbldap-tool 之前先要配置一下，下面是我的配置文件，会说明一下。

用 yum 安装后配置文件在下面的目录可以找到

```
# ls /etc/smbldap-tools/  
smbldap_bind.conf  smbldap.conf  
#vi smbldap_bind.conf  
slaveDN="cn=root,dc=yepn,dc=com"  
slavePw="111111"  
masterDN="cn=root,dc=yepn,dc=com"  
masterPw="111111"  
#这部分要与前面你配置的 LDAP 服务器的管理员相同
```

然后是 smbldap.conf 配置文件，这个文件在建立用户时比较重要

```
SID="S-1-5-21-1153389650-4125104348-4025214935"  
#SID 每台服务器特有的 ID 号用下面命令生成，这个一定要修改，不然 Samba 通过 LDAP  
建立的用户会有问题，我开始就因为这个地方困惑了好久。  
#net getlocalsid  
  
sambaDomain="YEPN"  
#改成自己的 Samba 域  
  
slaveLDAP="127.0.0.1"  
slavePort="389"  
masterLDAP="127.0.0.1"  
masterPort="389"  
#LDAP 服务器设置
```

```
ldapTLS="0"
```

#LDAP 认证时候加密码，因为在公司内部网络使用，我又不想弄 SSL 所以没加密，如果有需要的朋友可以参考《使用 OpenLDAP 集中管理用户帐号》这篇文章做一下 TLS，这个地方的参数改成 1

```
verify="require"
```

```
cafile="/etc/smbldap-tools/ca.pem"
```

```
clientcert="/etc/smbldap-tools/smbldap-tools.pem"
```

```
clientkey="/etc/smbldap-tools/smbldap-tools.key"
```

#以上为安装后默认设置没改动过

```
suffix="dc=yepn,dc=com"
```

#前面配置 LDAP 时说过，不再解释了

```
usersdn="ou=Users,${suffix}"
```

#用户的检索字段

```
#computersdn="ou=Computers,${suffix}"
```

#我不用 Samba 做 PDC，所以去掉了这项

```
groupsdn="ou=Groups,${suffix}"
```

#用户组的检索字段

```
hash_encrypt="SSHA"
```

#Password 的加密方式

#以下为建立 UNIX 用户时的参数

```
userLoginShell="/bin/false"
```

#我不需要用户登陆服务器

```
userHome="/home/%U"
```

#用户的 home 目录，Samba 的 homes 用这个

Default mode used for user homeDirectory

```
userHomeDirectoryMode="700"
```

#HOME 目录的权限

```
# Gecos
userGecos="System User"

# Default User (POSIX and Samba) GID
defaultUserGid="513"
#用户属组 ID 是 SAMBA 用户

defaultMaxPasswordAge="45"
#默认值

#下面是 Samba 用户配置参数
userSmbHome="%PDC-SRV%U"
#homes 目录

userProfile="%PDC-SRV%Uprofiles%U"
userHomeDrive="H:"
userScript="logon.bat"
mailDomain="yepn.net"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
#以上除邮件域名外没有修改
```

smbldap-tool 配置完成, fandy 介绍了一种用 smbldap-tools 自带的 configure.pl 脚本创建 smbldap.conf 配置文件, 我没用这个, 感觉还是自己改的比較快。

=====华丽的分划线=====

现在用 smbldap-tool 初始化 LDAP, 很简单运行一下面的命令

```
#smbldap-populate
```

Populating LDAP directory for domain yepn (你自己服务器的 SID 号, 这个一定要修改)
(using builtin directory structure)

```
adding new entry: dc=yepn,dc=net
adding new entry: ou=Users,dc=yepn,dc=net
adding new entry: ou=Groups,dc=yepn,dc=net
adding new entry: ou=Computers,dc=yepn,dc=net
adding new entry: ou=Idmap,dc=yepn,dc=net
adding new entry: uid=root,ou=Users,dc=yepn,dc=net
adding new entry: uid=nobody,ou=Users,dc=yepn,dc=net
adding new entry: cn=Domain Admins,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Domain Users,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Domain Guests,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Domain Computers,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Administrators,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Account Operators,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Print Operators,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Backup Operators,ou=Groups,dc=yepn,dc=net
adding new entry: cn=Replicators,ou=Groups,dc=yepn,dc=net
adding new entry: sambaDomainName=yepn,dc=yepn,dc=net
```

Please provide a password for the domain root:

Changing password for root

New password : 111111 (root 的 ldap 管理密码)

Retype new password : 111111 (root 的 ldap 管理密码)

介绍一下用 `smbldap-tool` 来管理帐号

详细操作 :

```
# smbldap-useradd -a -m test (添加一个 samba 帐号并创建主目录)
```

```
# smbldap-groupadd -a -m yepn (添加一个 samba 组帐号)
```

注 : fancy 的文章中没有加 `-a` 这个参数, 这个参数 `smbldap-tool` 帮助中说明 `-a` 这个参数为

add an automatic Security ID for the group (SID).

The rid of the group is calculated from the gidNumber of the group as $rid=2*gidNumber+1001$. Thus the resulted SID of the group is `$$SID-$rid` where `$$SID` and `$rid` are the domain SID and the group rid

所以我感觉还是加上好, 这个地方添加用户组的时候一定加 `-a`, 这个不会在改变用户属组后看

不到共享文件

```
# smbldap-groupmod -m test yepn (添加 user2 用户帐号到 acc 帐号中)
adding user test to group yepn
```

更改 test 帐号的密码：

详细操作：

```
# smbldap-passwd test
```

```
# smbpasswd test
```

#以上两个密令都可以个改 Samba 密码, 不同的是 smbldap-passwd 会连 unix 的密码一起修改, 为什么要用 smbpasswd 修改密码, 或许你需要 unixpasswd 用做别的系统的密码, 比如邮件, 证书认证等。

Changing password for test

New password : test (用户密码)

Retype new password : test (确认用户密码)

添加 test 帐号的信息：

#可以再修改帐号的信息, 默认是 smbldap.conf 中的配置

详细操作：

```
# smbldap-userinfo test
```

查看 test 帐号的信息：

详细操作：

```
# smbldap-usershow test
```

test 帐号建立后可以测试一下, 看看能不能看到共享文件

```
# smbclient -L localhost -U test
```

Password:

如果下面能正常显示共享信息, 说明你的 Samba 服务器已经通过 LDAP 认证了。

下面会介绍管理 LDAP 和 Samba 的工具 LAM

=====华丽的分划线=====

把原来的 Samba 用户和组信息导入到 LDAP 服务器

很多文章介绍 MigrationTools 这个工具导入, 如果你也想用这个导入, 可以 GOOGLE 一下, 这里不做介绍。

因为 MigrationTools 工具导入用户时没有 Samba 用户的相关信息, 所以我用的是 smbldap-tools 这个工具导入的用户和组。

先拿到原来 Samba 服务器上的 passwd 和 group 文件

passwd 文件删除系统帐号只留下 Samba 帐号

```
#awk -F: '{print $1,$3,$4}' passwd > userlist
```

这样导出来的数据结构是: 用户名 UID GID

group 文件删除系统帐号只留下 Samba 组

```
#awk -F: '{print $1,$3,$4}' group > grouplist
```

这样导出来的数据结构是: 组名 GID 用户列表

有了这两个文件后写一个很简单的脚本文件, 通过 smbldap-useradd 添加用户

```
#more useradd.sh
```

```
#!/bin/bash
```

```
while read name uid gid
```

```
do
```

```
  /usr/sbin/smbldap-useradd -a -u $uid -g $gid -m $name
```

```
done < userlist
```

很简单, 都能看明白不解释了, 对于 smbldap-useradd 不明白的朋友可以, man smbldap-useradd 看一下各个参数。

建立组用户也一样

```
#more groupadd.sh
```

```
#!/bin/bash
```

```
while read name gid member
```

```
do
```

```
  /usr/sbin/smbldap-groupadd -a -g $gid $name
```

```
done < grouplist
```

再来就是把用户加到指定组中，只是把上面的文件小小修改一下就可以，通过

```
smbldap-groupmod
```

```
#more groupmember.sh
```

```
#!/bin/bash
```

```
while read name gid member
```

```
do
```

```
    /usr/sbin/smbldap-groupmod -m "$member" $name
```

```
done < grouplist
```

到上面为止用户和组都已经导入，而且设定好了用户的属组。不过 Samba 用户的密码还都没有设置，这个还是需要设置一下的

在设置密码时，我没找到什么好方法，所以用了 `expect` 这个命令，如果有更好的办法，希望能补充一下。

CentOS 默认 `expect` 这个是没有安装的，安装很简单直接 `yum`

```
#yum -y install expect
```

先写个改密码的脚本

```
#more chpass.exp
```

```
#!/usr/bin/expect
```

```
spawn /usr/sbin/smbldap-passwd [lindex $argv 0]
```

```
set password [lindex $argv 1]
```

```
expect "*password:"
```

```
#sleep .1
```

```
send "$password\u2199n"
```

```
expect "*password:"
```

```
send "$password\u2199n"
```

```
expect eof
```

再用 `smbldap-passwd` 来改用户密码

```
#more userpasswd.sh
```

```
#!/bin/bash
```

```
while read name uid gid
```

```
do
```

```
/usr/bin/expect chpass.exp $name 123456
done < userlist
```

#这个需要等一段时间，我用户不多只有 100 多个，如果你用户多的话，可以时间更长

到这里 Samba 用户全都迁移到 LDAP 认证了，以后建立用户删除都可以用 `smbldap-tool` 来完成。

因为我公司里只有我自己一个人管理这个服务器，如果我休息的时候对于非技术人员来管理 LDAP 服务器和 Samba 服务器来说用这个密码会有些麻烦，所以我还要向下写，找了两个 GUI 的工具来解决

=====华丽的分界线=====

Samba 管理工具 Webmin，这个不用多介绍网上文章一大片，GOOGLE 一下很多，也不是我介绍的重要，通过这个管理 Samba 服务器会很方便，不过用 Webmin 管理 LDAP 服务器的用户和组我没有设置成功，如果有调协成功的朋友，想请教一下

下面介绍 LDAP Account Manager（以下简称 LAM）这个 GUI 的管理工具，这个可以管理 LDAP 和 Samba 的用户，对我来说特别重要的是可以建立 home 目录，这点对于非技术人员管理 LDAP 和 Samba 服务器相当重要。当然你也可以说用 Webmin 建立 home 目录，不过那样会让非技术者相当麻烦。

相信有很多人用 `phpldapadmin` 来维护 LDAP，我开始也是用这个工具来维护 LDAP 服务器，而且也感觉这个会比 LAM 来维护 LDAP 更简单一些，不过对于 Samba 来说 `phpldapadmin` 不能管理这点有些不足，所以改用 LAM。LAM 的安装很简单也是 PHP 的 GUI，如果你以前装过 `phpldapadmin` 的话那么 LAM 复制到 `apache` 的 `Document Root` 目录下就可以运行了。安装过程请参看 LAM 压缩包中的 `INSTALL` 文件。

在 LAM 的 `config` 需要修改一下 `lam.conf` 的配置文件，LAM 也提供了 GUI 的修改页面，这个很方便，下面是我用的配置文件

```
#more lam.conf
```

```
ServerURL: ldap://localhost:389
```

```
Admins: uid=admin,ou=Users,dc=yepn,dc=com
```

#这个地方很重要，如果你希望用 LAM 来建立 home 目录，就需要给系统建立一个 admin 帐号，所以这个地方不能设 LDAP 的 root 帐号，而且这个 admin 帐号必需是 unix 系统中存在的用户。

Passwd: {SSHA}DrIFykO6wONLf65+jmLeif8nbCA= buvDNg==

treesuffix: dc=yepn,dc=net

defaultLanguage: en_GB.utf8:UTF-8:English (Great Britain)

#这个地方的语言配置可以选中文，这点很方便

scriptPath: /usr/local/apache2/htdocs/lam/lib/lamdaemon.pl

#这个是非常关键的建立 home 目录用的脚本文件

Server of external Script

scriptServer: localhost

scriptRights: 750

cachetimeout: 5

Module settings

modules: posixAccount_minUID: 1000

modules: posixAccount_maxUID: 3000

modules: posixAccount_minMachine: 5000

modules: posixAccount_maxMachine: 6000

modules: posixGroup_minGID: 1000

modules: posixGroup_maxGID: 2000

modules: posixGroup_pwdHash: SSHA

modules: posixAccount_pwdHash: SSHA

activeTypes: user,group

types: suffix_user: ou=Users,dc=yepn,dc=net

types: attr_user: #uid:#givenName:#sn:#uidNumber:#gidNumber

types: modules_user: inetOrgPerson,posixAccount,sambaSamAccount

types: suffix_group: ou=Groups,dc=yepn,dc=net

types: attr_group: #cn:#gidNumber:#memberUID:#description

types: modules_group: posixGroup,sambaGroupMapping

#types: suffix_smbDomain: ou=domains,dc=yepn,dc=net

#types: attr_smbDomain: sambaDomainName:Domain name;sambaSID:Domain SID

#types: modules_smbDomain: sambaDomain

```
# Access level for this profile.
accessLevel: 100
modules: sambaSamAccount_timeZone: 9
types: suffix_host:
types: attr_host: #cn:#description:#uidNumber:#gidNumber
types: suffix_smbDomain:
types: attr_smbDomain: #sambaDomainName:#sambaSID
```

改成你自己用 LDAP 域就 OK 了

现在登陆 LAM 就可以管理 LDAP 和 Samba 用户，但是还不能建立 home 目录

=====华丽的分划线=====

下面是 lamdaemon.pl 的安装，这个小脚本折腾了我两天，记我非常的郁闷。

前面刚说过运行 lamdaemon 脚本需要一个真实的系统用户，我建立了一个 admin 用户，但是需要让 admin 远程登陆之后能用 1.sudo 这个命令来执行 lamdaemon 这个脚本，所以需要修改 sudoers 这个配置文件

添加内容如下：

```
admin All= NOPASSWD: /usr/local/apache2/htdocs/lam/lib/lamdaemon.pl
```

对于 sudoers 的说明请 GOOGLE，简单说一下，就是让 admin 用户可以不要密码，通过 sudo 运行 /usr/local/apache2/htdocs/lam/lib/lamdaemon.pl

2.需要让 Perl 支持 Quota，这个比较简单去 <http://cpan.org/> 上搜索一下，装上就 OK 了

3.需要让 PHP 支持 libssh2

libssh2 可以到 <http://www.libssh2.org> 下载 libssh2 0.13 一定要这个版本，最少在我前面写的那个系统环境下，这个版本我测试通过了，最新的 0.18 让我非常郁闷，怎么都是不成，PHP 是可以支持 ssh2，但是 lamdaemon 这个脚本就是不行。

libssh2 安装之后去 php 的主页上下载 php5-ssh2 0.10 这个版本，让 PHP 支持 ssh2，这两个版本我测试过没问题，其他版本我都没有成功。对于 php3-ssh2 0.10 的安装说明一下，通过 phpize 安装。

```
#tar -zxvf ssh2-0.10.tgz
```

```
#cd ssh2-0.10
#phpize && ./configure --with-ssh2 && make
#cp modules/ssh2.so /usr/local/lib
#我的 PHP 指定库在这个目录下，你不一定在这个目录，要看你的 php.ini 文件中的 PATH
```

```
#echo extension=ssh2.so >> /usr/local/lib/php.ini
#把 ssh2.so 添加到你的 php.ini 文件中
```

最好再修改一下 SSH 的配置文件

```
#vi /etc/ssh/sshd_config
```

```
PasswordAuthentication yes
#原来是被注释掉的
```

到这里 LAM 的 lamdaemon.pl 的配置脚本也设置完了，如果上面这些配置你都没有报名信息出现的话，下面可以测试一下你的脚本安装是否成功。GOOD LUCK !!!

登陆到 LAM 里左上角有 TOOLS→TEST→Lamdaemon test

如果一共都 OK, 那说明你的 Lamdaemon 安装正常了, 如果只是最后一项 Lamdaemon: read quotas 报错的话, 你的 LAM 也可以正正常建立 home 目录。

=====最后的分划线=====

到这里 Samba 和 LDAP 的管理工具都配置完成了，如果有其他的朋友有更好的方法介绍，希望来信告诉我或是加我的 MSN 一起讨论，现在只是把 Samba 和 LDAP 整合了，离我要完成的目标，还有些差距，前天 openpne 的认证也可以通过 LDAP 了，但是用户迁移是个问题。或许再等等 PNE 会有更成熟的版本推出。

下面两个工作是以后要做的，如果有作过经验的朋友希望和我联系一下，有问题请教

- 1.Qmail 用户迁移到 Postfix+LDAP 中
- 2.Net'Attest EPS 认证服务器用户整合到 LDAP 中

注：以后会慢慢整理和完善这份文档