

LDAP

The Lightweight Directory Access Protocol (LDAP /'ɛldæp/) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.[1] Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.[2] As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

- Use iRedMail's OpenLDAP database for Unix user authentication
- Make Samba work with iRedMail's OpenLDAP database backend

Use iRedMail's OpenLDAP database for Unix user authentication

iRedAdmin

Create user in iRedAdmin or with iRedMail tools!

Stop mail services

```
service sogo stop
service dovecot stop
service postfix stop
service iredapd stop
service clamav-daemon stopservice amavis stop
```

File operations

Create users home directory

```
mkdir /home/usersmkdir /home/users/username
```

Move mail directories

```
mv /var/vmail/vmail1/domain/u/s/e/username@domain.com/* /home/user/username/
```

If the user never logged in and changed his settings in webmail the sieve directory wont exists.

```
mkdir /home/users/username/sieve
```

Set up OpenLDAP

The easiest way to make the changes is to use phpLDAPAdmin.

Create group for domain

```
{ou=Groups,domainName=domain.com,o=domains,dc=domain,dc=com}
```

new child->posixGroup

```
rdn=cn  
gid=5000cn=DOMAIN-GROUP
```

Set up the user

```
{ou=Users,domainName=domain.com,o=domains,dc=domain,dc=com}
```

objectClass->(new entry)->posixAccount

```
homeDirectory=/home/users/username  
shadowLastChange=-1
```

new attribute->loginShell

```
loginShell=/bin/bash
```

Add the user to the group

```
{ou=Groups,domainName=domain.com,o=domains,dc=domain,dc=com}
```

new attribute->memberUID

```
memberUID=username
```

Set up permissions

```
chown username:DOMAIN-GROUP /home/user/username -R  
chown username:username /home/user/username/MailDir/ -R  
chown vmMail:vmMail /home/user/username/sieve/ -R  
chmod 00700 /home/user/username/MailDir/chmod 00700 /home/user/username/sieve/
```

Set up sshd

Edit the `/etc/ssh/sshd_conf` file

```
UsePAM yes
```

Enable password change of the user

Edit `/etc/pam.d/common-password`

Add this line to the file

```
# here are the per-package modules (the "Primary" block)password
requisite                pam_pwquality.so retry=3password
sufficient                pam_ldap.so try_first_passpassword      [success=3
default=ignore]          pam_unix.so obscure use_authtok use_first_pass sha512password
sufficient                pam_sss.so use_authtok use_first_pass# here's the fallback if no
module succeeds

password      requisite                pam_deny.so# prime the stack with a positive
return value if there isn't one already;# this avoids us returning an error just because nothing
sets a success code

# since the modules above will each just jump aroundpassword
required                pam_permit.sopassword      optional
pam_smbpass.so nullok use_authtok use_first_pass# and here are more per-package modules (the
"Additional" block)# end of pam-auth-update config
```

Edit `/etc/ldap/slapd.conf`

Add shadowLastChange to allow user to change own password

```
# Access Control
```

```
# Allow users to change their own passwords and mail forwarding addresses.access to
attrs="userPassword,shadowLastChange,mailForwardingAddress,storageBaseDirectory,homeDirectory,mail
    by anonymous      auth
    by self           write
    by dn.exact="cn=vmail,dc=domain,dc=com"    read    by
dn.exact="cn=vmailadmin,dc=domain,dc=xom"    write
    by users          none
```

Set up the connection

Install the necessary packages

```
apt-get install ldap-utils libpam-ldap libnss-ldapd nslcd sssd
```

Edit the `/etc/nslcd.conf` file

```
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.
# The user and group nslcd should run as.
uid nslcd
gid nslcd
# The location of which the LDAP server(s) should be reachable.
uri ldap://127.0.0.1:389
# The search base that will be used for all queries.
base dc=domain,dc=com
# The LDAP protocol version to use.
ldap_version 3
# The DN to bind with for normal lookups.
binddn cn=vmail,dc=domain,dc=com
```

```
bindpw *****SECRETLDAPPASSWORD*****
# The DN used for password modifications by root.
# rootpwmoddn cn=admin,dc=example,dc=com
# SSL options
#ssl off
#tls_reqcert never
tls_cacertfile /etc/ssl/certs/ca-certificates.crt
# The search scope.
```

Edit the `/etc/nsswitch.conf` file

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.# If you have the `glibc-doc-
reference' and `info' packages installed, try:# `info libc "Name Service Switch"' for
information about this file.
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap
gshadow:     files
hosts:       files mdns4_minimal [NOTFOUND=return] dns
networks:    files
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files
netgroup:    nissudoers      files
```

Enable start `nsld` at boot

```
update-rc.d nsld enable
```

Restart `nscd` service

```
/etc/init.d/nscd restart
```

Edit `/etc/sss/sss.conf` file

```
[sss]
  config_file_version = 2
  services = nss,pam
domains = LDAP
[nss]
filter_users = root,named,avahi,haldaemon,dbus,radiusd,news,nscd
[pam]
[domain/LDAP]
  ldap_search_base = dc=domain,dc=com
  ldap_access_filter = objectClass=posixAccount
  id_provider = ldap
  auth_provider = ldap
  chpass_provider = ldap
  access_provider = ldap
  ldap_schema = rfc2307
  ldap_uri = ldap://127.0.0.1
  ldap_user_name = uid
  ldap_user_search_base = o=domains,dc=domain,dc=com
  ldap_group_search_base = o=domains,dc=domain,dc=com
  ldap_default_bind_dn = cn=vmail,dc=domain,dc=com
  ldap_default_authtok_type = password
  ldap_default_authtok = *****SECRETLDAPPASSWORD*****
  enumerate = true
  cache_credentials = true
  ldap_tls_reqcert = never
```


Start `sssd` service

```
service sssd start
```

Start mail services

```
service slapd restart  
service amavis start  
service dovecot start  
service postfix start  
service iredapd start  
service clamav-freshclam restart  
service clamav-daemon startservice sogo start
```

Troubleshoot

Start `sssd` in debug mode and try to login via ssh

```
/usr/sbin/sssd -i -d7
```

Check if users and groups exists

```
getent passwdgetent group
```

Check log files while trying to log in

```
tailf /var/log/auth.logtailf /var/log/syslog□
```

Make Samba work with iRedMail's OpenLDAP database backend

First you should follow the steps in this howto to use iRedMail's OpenLDAP database for Unix user authentication!

Generate SambaSID

Create sidgenerator.sh file

Create the sidgenerator.sh file with the following content:

```
#!/bin/sh
sambaSID=
for num in 1 2 3 ;do
    randNum=$(od -vAn -N4 -tu4 < /dev/urandom | sed -e 's/ //g')
    if [ -z "$sambaSID" ]; then
        sambaSID="S-1-5-21-$randNum"
    else
        sambaSID="${sambaSID}-${randNum}"
    fi
done
```

```
done
echo $sambaSID
exit 0
```

This script is created by naterator

Make it executable

```
chmod +x sidgenerator.sh
```

Generate sid

```
bash ./sidgenerator.sh
```

Set up Samba

Install samba

```
apt-get install samba smbldap-tools -y
```

Edit `/etc/samba/smb.conf`

We use root dn because we want to allow samba to create the `sambaDomainName=SERVERNAME` entry.

```
[global]
...
netbios name = SERVERNAME
```

```
...  
passdb backend = ldapsam:ldap://127.0.0.1  
ldap ssl = no  
ldap admin dn = cn=Manager,dc=domain,dc=com  
ldap suffix = dc=domain,dc=com ...
```

Set LDAP password for Samba

Enter the password of `ldap admin dn`

```
smbpasswd -w *****SECRETPASSWORD*****
```

Restart Samba

```
service smb restart
```

Set up OpenLDAP

Add the needed Samba settings to the domain group

```
{ou=Groups,domainName=domain.com,o=domains,dc=domain,dc=com}
```

```
objectClass->(new entry)->sambaGroupMapping
```

```
sambagrouptype=2sambaSID=YOU-NEED-GENERATE-WITH-SCRIPT
```

Valid numbers for `sambagrouptype` entry

```
SID_NAME_USE_NONE=0,  
SID_NAME_USER=1,  
SID_NAME_DOM_GRP=2,  
SID_NAME_DOMAIN=3,  
SID_NAME_ALIAS=4,  
SID_NAME_WKN_GRP=5,  
SID_NAME_DELETED=6,  
SID_NAME_INVALID=7,  
SID_NAME_UNKNOWN=8, SID_NAME_COMPUTER=9
```

Set up user

```
{ou=Users,domainName=domain.com,o=domains,dc=domain,dc=com}
```

```
objectClass->(new entry)->sambaSamAccount
```

Create the following entries under the user

```
(new attribute)->sambaGroupMapping
```

```
sambaSID=SID-OF-THE-SAMBA-SERVER-3000 # Increment the 3000 partsambaAcctFlags=[U]  
sambaLMPassword=*****SAMBAPASSWORD*****  
sambaNTPassword=*****SAMBAPASSWORD*****sambaPrimaryGroupSID=SID-OF-THE-  
CREATED-GROUP- # Add '-' character to the end of the group sidsambaPwdLastSet=-1
```

Troubleshoot

Samba

1. Troubleshooting Samba

OpenLDAP

1. Troubleshooting OpenLDAP