LDAP

Lightweight Directory Access Protocol

User names and passwords are kept on a Windows Server.

The Windows Server is set to provide LDAP.

A Unix box may be configured to use the LDAP protocol to access the user names and passwords.

This causes and account on the Windows Server to also become an account on the Unix box.

Useful in adding a Unix machine to a Windows based environment.

The Components

Utility procedures (system calls).
Used by LDAP client programs.
Used by programs that the "name switch",
(`nsswitch.conf`)
like password and group (login).

LDAP client libraries.
Where the utility procedures are implemented.

LDAP client programs.
These are mostly useful for testing to see if your install is working.

LDAP client daemons.
These maintain connections with the ldap server.

LDAP server daemons.
You only need these if you are providing ldap to other machines.

Your install details vary with the Linux release you use.

Your windows server (active directory) must provide ldap.

Ubuntu Install

Load the following libraries:

`libpam-ldap`: `/lib/security/pam_ldap.so`
`libpam-smbpass`: `/lib/security/pam_smbpass.so`
`winbind`: `/lib/security/pam_winbind.so`

If you use the Ubuntu package install utility you will be asked for the *uri* and *base*
if not, you edit them into the config files.

The package install utility will start `winbind`,
otherwise start it by hand.

Configuration Files

`ldap.conf`

Because many facilities (ldap server, ldap client browsers) use this file it has much in it that is ignored. It also needs to be able to compensate for the way your Windows domain controllers are set up. You may also find more than one of these files with different parts "missing".

```
base cn=users,dc=ad,dc=example,dc=com
```

The PDC does active directory in a subdomain called `ad`.
We are interested in `users`, that is logins.

```
uri ldap://192.168.1.1  ldap://192.168.1.2
host 192.168.1.1  192.168.1.2
#port 389
```

Some facilities use the uri format;
some use the host:port format.
Recommendation: use numbers and not names.
The port defaults to 389.
You may specify the port as part of the uri or host name (use `:398` following the internet number)

```
ldap_version 3
```

Options are 2 or 3, 2 is legacy.

```
binddn padl@ad.example.com
bindpw somepassword
```

Entries shown assume you are using the PADL version of ldap on your windows machine.
It logs into the PDC with the account name and password shown.
If the `binddn` is omitted it logs in anonymously and ignores the `bindpw`.

```
#scope sub
```

Do subtree lookups (for the logins).
(Under the "`users`" subtree.)


```
pam_login_attribute msSFU30Name
pam_password md5
nss_base_passwd cn=users,dc=ad,dc=example,dc=com?one
nss_base_group cn=users,dc=ad,dc=example,dc=com?one
nss_map_objectclass posixAccount User
nss_map_attribute uid msSFU30Name
nss_map_attribute uidNumber msSFU30UidNumber
nss_map_attribute gidNumber msSFU30GidNumber
nss_map_attribute loginShell msSFU30LoginShell
nss_map_attribute gecos name
nss_map_attribute userPassword msSFU30Password
nss_map_attribute homeDirectory msSFU30HomeDirectory
nss_map_attribute posixGroup Group
nss_map_attribute uniqueMember posixMember
nss_map_attribute cn sAMAccountName
```

Maps Windows/LDAP fields to Linux fields.
All these have defaults (`RFC 2307`, 1998)
so they may not be necessary for your configuration.

ldap.conf

`nss_initgroups_ignoreusers bin,daemon,lp, mail,syslog`

These users should never log in,
don't bother to check the PDC, just deliver a failed.
Note: important if you check `ldap` before `files`

`#ssl no`

You may use ssl to connect to the server, the default is not to.
Not all client libraries support ssl.

Configuration Files

/etc/nsswitch.conf

For the `passwd`, `group` and `shadow` entries:
add `ldap`

Example:

`passwd files ldap`

Home Directories

You are logging into the Unix machine,
not the Windows Domain.

You must create the home directories on the Unix machine
(they can be on an NFS mount)

Testing

`ldapsearch -x -b "cn=users,dc=ad,dc=example,dc=com" "uid=bob"`
You should see information for the user bob.

`echo ~bob`
You should get `/home/bob` or whatever bob's home directory is set to.

`login bob`
bob should be able to login