OpenLDAP

Install OpenLDAP

Install OpenLDAP

```
# apt-get install slapd
```

You will be prompted for an administrative password. This will be the LDAP administrator password and will be used anywhere that write permission to LDAP is required. This will get set again in the next step when we reconfigure OpenLDAP.

Reconfigure OpenLDAP

Debian's default configuration for OpenLDAP is sometimes not quite what you might want. If you want to use an LDAP base DN based off something other than the domain name used when configuring the host you will need to reconfigure the package.

```
# dpkg-reconfigure slapd
```

The reconfiguration script will allow you to change the LDAP base DN to be based on a different domain name. For example, "myhub.org" would become "dc=myhub,dc=org".

The reconfiguration script will then ask for the organization to use. This isn't important to us and can be set arbitrarily.

You will then be asked to enter a password for the admin account. You will need to remember this password for later configuration steps.

Accept the default "HDB" database backend type.

Do not remove database when slapd is purged. Sometimes during maintenance it can be useful to reinstall slapd without wiping out the database.

Move the old database out of the way.

Don't allow LDAPv2 protocol.

Install nscd

The Name Service Cache (nscd) will used later so we go ahead and install it here.

```
# apt-get install nscd
```

Install HUBzero LDAP Schema

```
# apt-get install hubzero-openldap
```

To enable this new schema edit **/etc/ldap/slapd.conf** and add the following line as the last "include" statue under the "Schema and objectClass definitions" comment toward the beginning of the file.

```
include         /etc/ldap/schema/hub.schema
```

Then restart OpenLDAP

```
# /etc/init.d/slapd restart
```

Initialize OpenLDAP Database

Several entries are expected to be prepopulated in OpenLDAP.

There is a script to do this, but the script has to be manually configured.

```
# cp /usr/lib/hubzero/openldap/HUB-INIT-SLAPD.tmpl HUB-INIT-SLAPD
```

Modify HUB-INIT-SLAPD and edit the five configuration lines near the beginning of the file:

```
base_dn=""
admin_pass=""
hubadmin_passhash=""
hubrepo_passhash=""
home_dir=""
```

- **base_dn** should be the base DN of your LDAP (e.g., "dc=myhub,dc=org")

- **admin_pass** should be the clear text password you set for the LDAP administrator.
- **hubadmin_passhash** should be the hashed password for the about to be created hubadmin account. You can hash a password using '/usr/sbin/slappasswd'
- **hubrepo_passhash** should be the hashed password for the about to be created hubrepo account. You can hash a password using '/usr/sbin/slappasswd'
- **home_dir** should be the home directoy you created earlier (eg., "/home/myhub").

Then run the configuration script

```
# sh ./HUB-INIT-SLAPD
```

This should prepopulate the databae enough to bootstrap HUBzero.

Configure PAM to use LDAP

```
# apt-get install libpam-ldap
```

- Use "ldap://127.0.0.1" as the URI
- Set the base DN to match how you configured OpenLDAP (eg., "dc=myhub,dc=org")
- Use LDAP v3
- Accept making local root data admin
- LDAP does not require login
- Specify the DN for the LDAP admin user (eg., "cn=admin,dc=myhub,dc=org")
- Enter admin password for LDAP

Modify **/etc/pam.d/common-auth** by commenting out the existing configuration then adding rules to allow authentication against LDAP.

```
#auth required pam_unix.so nullok_secure

auth sufficient pam_unix.so nullok_secure
auth sufficient pam_ldap.so try_first_pass
auth required pam_deny.so
```

Modify **/etc/pam_ldap.conf** by adding the following section (other mappings in this file should already be commented out).

```
# HUBzero Mappings
nss_base_passwd ou=users,?one
nss_base_shadow ou=users,?one?host=web
pam_filter host=web
pam_password crypt
```

```
nss_map_attribute uniqueMember member
nss_base_group ou=groups,dc=myhub,dc=org?sub
```

Be sure the BASEDN in the above matches that used by your configuration.

/etc/pam_ldap.secret contains the LDAP admin password and should only be readable by root.

Configure NSS to use OpenLDAP

```
# apt-get install libnss-ldap
```

- Specify the DN for the ldap admin account
- Specify the password for the ldap admin account

Modify **/etc/libnss-ldap.conf** by adding the following section. (other mappings in this file should already be commented out).

```
# HUBzero Mappings
nss_base_passwd ou=users,?one
nss_base_shadow ou=users,?one?host=web
pam_filter host=web
pam_password crypt
nss_map_attribute uniqueMember member
nss_base_group ou=groups,dc=myhub,dc=org?sub
```

Be sure the BASEDN in the above matches that used by your configuration.

Modify **/etc/nsswitch.conf**

```
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
```

/etc/libnss-ldap.secret contains the LDAP admin password and should only be readable by root.

Test

```
# getent passwd
```

To test configuration. You should see entries for users 'hubrepo' and 'apps' toward the end of the list if everything is working correctly.

Troubleshooting

If you have a problem with the system apparently not recognizing up to date account or group information (eg., in the next section some people report receiving an error about unknown username 'hubadmin') you can nscd to flush it data cache and restart using the following commands:

```
# nscd -i passwd
# nscd -i group
# /etc/init.d/nscd restart
# getent passwd
```

If you still don't see the hubadmin account listed then re-read the instructions and check your work very carefully. These instructions assume a fresh install, if you are working with an existing LDAP/PAM/NSS installation you will have to do more advanced troubleshooting outside the scope of this documentation.

Create home directories

Create a home directory for the apps user

```
# mkdir /home/myhub/apps
# chown apps.public /home/myhub/apps
# chmod 0700 /home/myhub/apps
```