Notes for cyrus-imap, openldap with sendmail and smtp-auth on OpenBSD

Notes for installing cyrus-imap with sendmail and smtp-auth on OpenBSD to provide a virtual e-mail service, using a simpler approach for setting up ldap authentication.

Last edited 05 November 2006, per request by mail list users, this information is posted for historical reference.

> This information is distributed in the hope that it will be useful, with the understanding that the information presented is from various sources and application experiences, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
> These notes are have not been audited, and are provided per request for others to reference. We expect some typos and maybe a missing step and a less than optimum approach. Your input welcome! Some of the LDAP implementation can certainly be improved like the access list setup, binding with more secure user, and so on, but the concept of using directories for each domain name with users under each is working. Apologies up front but something is better than nothing so here it is!

For documentation examples: We use the domain of ispforexample.com for the hosting server and a domain that need not have email go to cyrus-imap. For examples of virtual hosting the domains example1.com and example2.com

Cyrus-Imap will provide the pop3, imap and mail boxes. The use of LDAP for the directory storage of passwords and authentication is common and better supported than using SQL. The applications Sendmail and Cyrus-Imap through Cyrus-sasl2 support LDAP authentication. A search on the Internet will find significant documentation for setting up Cyrus, however these notes approach using Sendmail. An administrator will need experience with Sendmail configuration to consider this approach.

Several port packages we will endeavor to use include openldap, cyrus-imap, cyrus-sasll. Other packages like db (berkely db) may be useful also.

The preference is to use OpenLDAP package with the "bdb" flavor because the OpenLDAP developers strongly recommends using Sleepycat Software's Berkeley DB as the data storage mechanism for an OpenLDAP deployment.
Note that LDAP is not a database, but a protocol for accessing and managing data. However for OpenBSD 4.4 the openldap port flavor bdb is broken.

You may want to go ahead and try to install.

```
cd /usr/ports/mail/cyrus-imap
make package/
```

cd /usr/ports/security/cyrus-sasl2
env FLAVOR=ldap make package

cd /usr/ports/databases/openldap/
env SUBPACKAGE=ldap FLAVOR=bdb make package

If you are using a 'i386' platform your packages should be saved to the directory /usr/ports/packages/i386/all/

If you have a conflict because you already have the package loaded with a different FLAVOR or without, you may can use pkg_add with the "-r" option.

*You'll probably need to go back and also install the package with cyradm, example: pkg_add /usr/ports/packages/i386/cyrus-imapd-perl-**

For sendmail, the installed sendmail may not support smtp-auth and ldap. After you have the cyrus-sasl2 package installed and you have edited /etc/mk.conf you may need to recompile sendmail from the source. Assuming you have the source for OpenBSD under /usr/src and you have room for /usr/obj the following method could be used:

```
echo "WANT_LDAP=yes" >> /etc/mk.conf
echo "WANT_SMTPAUTH=yes" >> /etc/mk.conf
## either drop down to the sendmail src directories and make or make build the user land.
cd /usr/src
## could use this opportunity to update the source,
#cvs update -Pd
make obj && make build
```

You will need to prepare your Sendmail configuration files to support your ldap setup, virtual hosting, and a tweak to be able to do virtusertable before mailertable. We could have arranged to have our Sendmail tables in LDAP also, but for our example we are just putting the username, realm and password for authentication in LDAP. Here are some features and options you can consider for your Sendmail *.mc file, some may or may not be necessary, try to research these lines to verify they are appropriate for your setup and versions before using for production:

Prior to make with m4 macros edit necessary files. According to the documentation by Cyrus-imap to support virtual hosting we will need to modify the mailer/cyrus2 file provided by Sendmail. Reference the document http://cyrusimap.web.cmu.edu/imapd/install-virtdomains.html **[1]**

Edit /usr/share/sendmail/mailer/cyrus2.m4 accordingly.

You'll have to use the Cyrus mailer in LMTP mode, and you'll have to change the mailer flags so that it provides the full domain while communicating LMTP. Specifically these changes:

S=EnvFromSMTP/HdrFromSMTP, R=EnvToSMTP

Edit your file you use to make your sendmail m4 macro from and here are some lines that may be critical for your settings
(read also head of /usr/share/sendmail/cf/Makefile)

```
dnl if you aren't using Sendmail 8.12, you might need to remove dnl
dnl the following feature. its in the carnegie example dnl
dnl http://cyrusimap.web.cmu.edu/imapd/cyrusv2.mc dnl
FEATURE(`preserve_local_plus_detail')dnl
dnl
dnl --- not sure if we need this enabled, seems to work okay with it --- dnl
FEATURE(`nocanonify')dnl
dnl
dnl -- for using the virtusertable feature before mailertable we may need the follong? dnl
define(`_VIRTUSER_STOP_ONE_LEVEL_RECURSION_',`true')dnl
define(`_NEED_MACRO_MAP_',`1')dnl
dnl
dnl Many features also use the access db feature so we list this early in macros dnl
dnl --- for some of the virtual hosting we need to add domain and RELAY dnl
dnl --- because we have to configure sendmail to accept email for the domains dnl
dnl --- we remap in mailertable, but we can't put it in local-host-names dnl
FEATURE(access_db, `hash -T<TMPF> /etc/mail/access')dnl
dnl

dnl Do what you need to do to setup SMTP-AUTH, something like.... dnl
define(`CERT_DIR', `MAIL_SETTINGS_DIR`'certs')
define(`confCACERT_PATH', `CERT_DIR')
define(`confCACERT', `CERT_DIR/xyz.ca-bundle')
define(`confSERVER_CERT', `CERT_DIR/xyz.pem')
define(`confSERVER_KEY', `CERT_DIR/xyz.mailkey.nopassphrase.pem')
define(`confCLIENT_CERT', `CERT_DIR/xyz.mailcert.pem')
define(`confCLIENT_KEY', `CERT_DIR/xyz.mailkey.nopassphrase.pem')
define(`confAUTH_MECHANISMS', `PLAIN')dnl
TRUST_AUTH_MECH(`PLAIN LOGIN')dnl
dnl

dnl We do not have to use virtusertable mapping but it is helpful. If the virtusertable dnl
dnl is enabled and VIRTUSER_DOMAIN or VIRTUSER_DOMAIN_FILE is used, dnl
dnl this feature will cause addresses to be searched in the map if their domain parts are dnl
dnl subdomains of elements in class dnl {VirtHost}. To clarify... dnl
dnl --- You will need to user VIRTUSER_DOMAIN for each domain you will map or dnl
dnl --- put them in one file with VIRTUSER_DOMAIN_FILE dnl
FEATURE(`virtusertable', `hash -T<TMPF> /etc/mail/virtusertable')dnl
VIRTUSER_DOMAIN(example1.com)dnl
VIRTUSER_DOMAIN(example2.com)dnl
dnl
dnl You can still enable support for /etc/mail/local-host-names to have hostnames that dnl
dnl should be considered local.and not directed to Cyrus lmtp socket dnl
FEATURE(`use_cw_file')nk
dnl
dnl
dnl Will need to enable support for /etc/mail/mailertable to put mappings to Cyrus lmtp socket
dnl
FEATURE(`mailertable', `hash -o /etc/mail/mailertable')
dnl
```

```
dnl We can tell the server its local name which probably should not be a domain mapped to lmtp
dnl
LOCAL_DOMAIN(`mail.ispforexample.com')dnl
dnl

dnl
MAILER(`smtp')dnl
dnl
MAILER(`local')dnl
dnl
define(`confLOCAL_MAILER',`cyrusv2')dnl
MAILER(`cyrusv2')
dnl
```

Configure the file /usr/local/lib/sasl2/Sendmail.conf
Example: cat /usr/local/lib/sasl2/Sendmail.conf

```
pwcheck_method: saslauthd
```

Take appropriate steps to make your sendmail.cf file and implement.

Setup other files used by sendmail (assuming we used files not maps in LDAP).

In the file /etc/mail/local-host-hames We don't want example1.com, nor other domains that are to use cyrus-imap for mailboxes, but we can have a domain for local mail like mail.ispforexample.com

In the file /etc/mail/access We want to make sure Sendmail accepts email so we could add lines like:

```
To:exampe1.com RELAY
To:example2.com RELAY
```

In the file /etc/mail/mailertable we need to map the virtual domains to the socket used by cyrus. Example:

```
example1.com cyrusv2:/var/imap/socket/lmtp
example2.com cyrusv2:/var/imap/socket/lmtp
```

We do not have to use /etc/mail/virtusertable but it can be useful in many ways. Here is and example of an alias of numberone for user1@example1.com and a redirect from exampe2 and putting and error message to quickly say we only accept user1 and user2 emails at example2.com
(note may need to test the example2.com trickery - has not been verified that it will not loop or drop user1@example2.com)

numberone@example1.com user1@example1.com
user1@example2.com user1@example2.com
user2@example2.com someuser@gmail.com
@example2.com error:nouser 550 No such user

Setup configuration file for ssalauthd. Example cat /etc/saslauthd.conf

ldap_servers: ldap://ldap.xxx/ [2]
ldap_bind_dn: o=salsauth,dc=ispforexample,dc=com
ldap_bind_pw: secret
ldap_search_base: o=%r,o=hosting,dc=ispforexample,dc=com
ldap_filter: (&(uid=%u)(accountStatus=active))
ldap_password_attr: userPassword
ldap_auth_method: custom

Looking at the documentation for sendmail and cyrus what is being asked during the sasl2 authentication is these items:

%u Username whose properties are being fetched/stored.

%p Name of the property being fetched/stored. This could technically be anything, but SASL authentication will try userPassword and cmusaslsecretMECHNAME (where MECHNAME is the name of a SASL mechanism).

%r Realm to which the user belongs. This could be the kerberos realm, the FQDN of the computer the SASL application is running on or whatever is after the @ on a username. (read the realm documentation).

So it would follow that we need a directory service that would hold account information like username, realm, userPassword and maybe cmusaslsecret. That will be the job for openldap.

Setup OpenLDAP. Good Luck to the novice. It took the author a few tries to wrap his mind around the fact that LDAP is not like SQL. Of serious note, their is a heck of a lot of documentation on the internet that can cause you to make things harder then they have to be. Much of the documentation using Postfix or Qmail with LDAP uses a different approach to storing the usernames and passwords in LDAP. After looking and reading it became apparent that to apply the KISS principle in the simplest case we just need ldap to resolve a password against and email account. The core and cosine schemas have something called "simpleSecurityObject" and that may suffice instead of doing some loopy courier or qmail schema with required entries like home directory which we do not want nor need and would have to fill with fluff.

Prepare to run the slapd daemon by editing /etc/openldap/slapd.conf

In preparation you can make an encrypted password to paste into the slapd.conf or use a plain text password and do it latter, use the slpappasswd command and save the results

```
man slappasswd
slappasswd
```

Example slapd.conf file using bdb database instead of ldbm database (requires package to have bdb FLAVOR. cat /etc/openldap/slapd.conf

```
### See slapd.conf(5) for details on configuration options.
### This file should NOT be world readable.
###
### If we need to debug:
# loglevel config 4095

include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
### the following may not be necessary but if you want, include them.
#include /etc/openldap/schema/nis.schema
#include /etc/openldap/schema/misc.schema
#include /etc/openldap/schema/inetorgperson.schema
#include /etc/openldap/schema/sendmail.schema

### Schema check allows for forcing entries to
### match schemas for their objectClasses's
### Do we want this on or off ???
#schemacheck on
pidfile /var/run/slapd.pid
argsfile /var/run/slapd.args

### TLS keys and certificates
### for our example the slapd is on the same server as cyrus
### so we don't need to encrypt the traffice on localhost.

### Some examples set limits like
#sizelimit 262144
#timelimit 300

### Some Access Control
### mostly set from looking at other config files,
### this example probably can be better and tighter.
access to attrs=userPassword
by dn="cn=Manager,dc=ispforexample,dc=com" write
by anonymous auth
by self write
by dn="o=saslauth,dc=ispforexample,dc=com" read
by * none
```

```
access to dn.base="" by * read

access to *
by dn="cn=Manager,dc=ispforexample,dc=com" write
by dn="o=saslauth,dc=ispforexample,dc=com" read
by self write
by * read

### Using berkeley sleeping cat for database,
### more effort to setup, but said to be better
database bdb

suffix "dc=ispforexample,dc=com"
rootdn "cn=root,dc=ispforexample,dc=com"
### Cleartext passwords, especially for the rootdn, should
### be avoid. See slappasswd(8) and slapd.conf(5) for details.
rootpw secretphrase
#rootpw {SSHA}xxxxxxxxxxxxxxx
#
### The database directory MUST exist prior to running slapd AND
### should only be accessible by the slapd and slap tools.
### Mode 700 recommended.
directory /var/openldap-data

### To speed up searches, here are indexes for commonly searched attributes:
index objectClass pres,eq
index mail,cn eq,sub

### DB_CONFIG Settings - For SleepyCat Berkeley DB
### these settings copied from another config file, may want to check them.
dbconfig set_cachesize 0 10485760 0
dbconfig set_lg_regionmax 262144
dbconfig set_lg_bsize 2097152

### EOF ###
```

Start LDAP and see if it running

Per the man page for slapd, to test whether the configuration file is correct or not, type:

```
/usr/local/libexec/slapd -Tt
```

To start the OpenLDAP server, its just /usr/local/libexec/slapd. However you may want to use some of the options, like -4 for tcp4 if you are not configured to support tcp6 and maybe limit access with the -h option. And maybe setup /etc/pf.conf to block it also for localhost use. For testing you may want to remove the -h option till you know it works.

```
/usr/local/libexec/slapd -4 -h ldap:/// -d 384
```

Now to proceed with putting information into the LDAP directories

Example of.a search of the naming connect to see what directory information is already there

before we import.

ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts

We are going to use OpenLDAP server to store all user settings. Some of Sendmail's features support LDAP and you could also use the OpenLDAP server to store maps, aliases and other lookups. We use the LDAP tree of our organization dc=ispforexample,dc=net and create a subtree for all our accounts. You can think of the subtrees being containers for data, mainly accounts.

We will need to use LDAP object classes and attributes to make our directories. The attributes we use will need to be in the included schemas. The schema defines which attributes an entry can have by defining object classes.

The first step is to create directory tree structure with our root node, the hosting organization and an entry for the rootdn. Create a file called base.ldif with the following contents. Be careful not to have spaces before lines or openldap may try to concatenate lines as it reads the configuration. Not sure we really need the Manager directory at the moment, but it is typical to create it. We will create "saslauth" as an account we can have the saslauthd use when accessing, and then we could setup access list to appropriately allow or restrict saslauth..

```
dn: dc=ispforexample,dc=com
objectClass: dcObject
objectClass: organization
o: AUTH-cyrus-smtp LDAP Server
dc: ispforexample

dn: cn=Manager,dc=ispforexample,dc=com
objectClass: organizationalRole
cn:Manager

dn: o=sasluth,dc=ispforexample,dc=com
o:saslauth
objectClass:top
objectClass:ogranization

dn: o=hosting, dc=ispforexample,dc=com
o:hosting
objectClass:top
objectClass:organization
```

Now use ldapadd, binding as the root account, to add this LDIF:

```
ldapadd -x -D "cn=root,dc=ispforexample,dc=com" -w secret -f base.ldif
```

Domains to be used for virtual email can be added under the hosting tree. Each domain needs to have postmaster and abuse users (entries) at minimum. To make a tree for example1.com and a tree for another virtual host example2.com, create a file called virtualhosts.ldif with the following contents: Note we do not have to setup CourierMailAlias because we are not using it, and Sendmail has it's own approaches to mail aliases with or without ldap.

```
dn: o=example1.com,o=hosting,dc=ispforexample,dc=com
objectClass: top
objectClass: organization
o:example1.com

dn: o=example2.com,o=hosting,dc=ispforexample,dc=com
objectClass: top
objectClass: organization
o:example2.com
```

Add this domain with the following command:

```
ldapadd -x -D "cn=root,dc=ispforexample,dc=com" -w secret -f virtualhost.ldif
```

Now, let's add an account with an e-mail user1@example1.com. and also setup a user cyrus on both domains for use by cyradm later. Create a user.example.ldif with the following contents:

```
dn: uid=user1,o=example1.com,o=hosting,dc=ispforexample,dc=com
uid: user1
userPassword:secret
objectClass: account
objectClass: simpleSecurityObject
objectClass: top

dn: uid=cyrus,o=example1.com,o=hosting,dc=ispforexample,dc=com
uid: user1
userPassword:verysecret
objectClass: account
objectClass: simpleSecurityObject
objectClass: top

dn: uid=cyrus,o=example2.com,o=hosting,dc=ispforexample,dc=com
uid: user1
userPassword:verysecret
objectClass: account
objectClass: simpleSecurityObject
objectClass: top
```

The first section adds a new entry under the directory example.com with user user1

```
/usr/local/bin/ldapadd -x -D "cn=root,dc=ispforexample,dc=com" -w secret -f
user.example.ldif
```

Other domains and accounts can be added with similar LDIF files or through a web interface that administrates LDAP like the project phpldapadmin [3] is said to be very helpful and you should benefit by setting up your web server to support it. Note we have not setup username and password for user2@example2.com above, you can try doing that with another LDIF or through phpldapamin.

Useful note, the slapcat program is used to dump the database to an LDIF file. This can be useful when you want to make a human-readable backup of your database or when you want to edit your database off-line. The program is invoked like this:

```
man slapcat
/usr/local/sbin/slapcat -f /etc/openldap/slapd.conf -l /tmp/ldapdump.`date
+%Y%m%d%H%M`.ldif
```

We setup Sendmail and Open-LDAP, now we need to setup Cyrus-imap. Recommend reading the Cyrus-imap documentation, http://cyrusimap.web.cmu.edu/imapd/ **[4], especially the web pages:**

- http://cyrusimap.web.cmu.edu/imapd/install-configure.html [5]
- http://cyrusimap.web.cmu.edu/imapd/install-virtdomains.html [1]
- http://cyrusimap.web.cmu.edu/imapd/faq.html [6]
- It may also be helpful to read docs under /usr/local/share/doc/sasl2/ like the doc /usr/local/share/doc/sasl2/options.html

Like Sendmail, it may be necessary to create a salsauthd application file for Cyrus.

```
echo "pwcheck_method: saslauthd" > /usr/local/lib/sasl2/Cyrus.conf
```

Edit the /etc/services file and make sure inetd configuration file does not call pop3 nor imap

Edit the configuration file /etc/imapd.conf Here is an example:

```
configdirectory: /var/imap
defaultdomain: ispforexample.com
postmaster: postmaster
partition-default: /var/spool/imap
sievedir: /var/sieve
sendmail: /usr/sbin/sendmail
admins: cyrus cyrus@exampl1.com [7] cyrus@example2.com [8]
virtdomains: userid
reject8bit: no
quotawarn: 90
timeout: 30
poptimeout: 10
dracinterval: 0
drachost: localhost
sieve_maxscriptsize: 32
sieve_maxscripts: 5
sasl_pwcheck_method: saslauthd
sasl_mech_list: PLAIN
```

```
#unixhierarchysep: yes
### example TLS stuff
tls_ca_file: /etc/mail/certs/xyz.ca-bundle
tls_cert_file: /etc/mail/certs/xyz.mailcert.pem
tls_key_file: /etc/mail/certs/xyz.mailkey.nopassphrase.pem
```

Start cyrus by running it's "master."

```
/usr/local/libexec/cyrus-imapd/master &
```

Now we have an authentication for user1@example1.com, but we don't have a mail box. Setting up mail boxes for Cyrus-imap for virtual hosting is achievable, but the perl tool cyradm for the author and others was a royal pain to authenticate.

To use cyradm you ideally login as an admin, in our example imapd.conf file cyrus. If you login as say cyrus@example1.com as admin, you can only manage accounts under the domain example1.com. If you login as and admin with an unqualified address (without domain) like cyrus then you can manage accounts on all the domains.

According to the documentation you could login with cyaradmin and create the mail box like this:

```
cyradm> cm user1@example1.com [9]
```

*If you cannot locate cyradm, you'll probably need to go back and also install the package with cyradm, example: pkg_add /usr/ports/packages/i386/cyrus-imapd-perl-**

Here comes a cyradm FUBAR. When your login with an unqualified address the cyradmin chooses the domain for you. According to the documentation it is suppose to choose a domain by the IP address, thus you could edit localhost or appropriate name for IP in /etc/hosts. However the author's experience was that when using saslauthd with ldap it would leave the realm blank regardless! Funny thing was it would choose a realm when were testing saslauthd with mysql. It really seems to be either a bug or a feature of cyrus not using realm if realm is defaultdomain. Maybe with a future release that problem will go away. Check the log files like /var/log/authlog and watch what realm is used and see if this happens for you also. If you have this problem also, it may require you to do something like temporarily hack the /etc/saslauthd to allow cyrus to login without a domain.

Here is a possible work around that will mess up pop3/imap connections tempoarily.
Change your /etc/saslauthd.conf file to
declare the domain in ldap_search_base setting:

```
###ldap_search_base: o=%r,o=hosting,dc=ispforexample,dc=com
```

```
ldap_search_base: o=example1.com,o=hosting,dc=ispforexample,dc=com
```

Then use cyradmn to login as cyrus, create one sample user in each email account, thus making the /var/imap/spool/domain/* folders.

```
/usr/local/bin/cyradm --user cyrus --server localhost --auth login
> cm user1@example1.com
> cm user1@example2.com
```

As soon as you can quit cyradm, edit /etc/saslauthd.conf back to change ldap_search_base back to using realm to authenticate. Now you can use a qualified admin per domain, so long as you have it in the ldap directory with username and password under domain. example:

```
/usr/local/bin/cyradm --user cyrus@example1.com--server localhost --auth login
> cm user2@example1.com

/usr/local/bin/cyradm --user cyrus@example2.com--server localhost --auth login
> cm user2@example2.com
```

Apologies, the above seems very 'hack', we expect as we go along a reader will send corrections or better advice, or the cyradm was the culprit and will get fixed.

You may also want to some lines for /etc/rc.local to start the daemons like:

```
### start ldap
echo "start openldap, slapd "
/usr/local/libexec/slapd
echo ""

echo '\nMay need saslauthd to support smtp-auth. '
if [ -x /usr/local/sbin/saslauthd ]; then
echo 'Starting cyrus-sasl support for smtp-auth.'
echo -n ' saslauthd'; /usr/local/sbin/saslauthd -a ldap
else
echo '\nWARNING, could not find saslauthd to start for smtp-auth support.'
fi
echo ""

echo '\nSTART cyrus-imapd/master for CYRUS-IMAP support. '
/usr/local/libexec/cyrus-imapd/master &
echo ""
```

Got imap, Got Web Interface? For a web interface that supports password changes you will need find one that supports editing ldap and most likely have to hack it to use the ldap search base with realm.

The author was able to get Squirrelmail **[10]** working with the change_ldappass **[11] plugin**, but had to

hack the functions.php to split the username then use the realm in the ldap search base
http://www.squirrelmail.org/ [10]
http://www.squirrelmail.org/plugin_view.php?id=26 [11]

In functions.php for change_ldappass after the function loads config.php you may can hard code variables and do something like:

```
// load config
include(SM_PATH . 'plugins/change_ldappass/config.php');
list ( $usernameuser, $usernamerealm ) = split ( "@" ,$username);
$ldap_base_dn = "o={$usernamerealm},o=hosting,dc=ispforexample,dc=com";
```

Then later in functions.php for the actual search replace $username with $usernameuser

```
// Hide ldap_search notices
$sr=@ldap_search($ds,$ldap_base_dn,"($ldap_user_field=$usernameuser)",array('dn'));
```

Another plugin that will be very helpfull for virtual hosting is the SquirrelMail plugin **Vlogin**.
http://www.squirrelmail.org/plugin_view.php?id=47 [12]
Just enabling the default had email logins like user1@example1.com working.

Additional configuration of the plugin would help set a default domain so
if user logged in as user1 it could make imap connection as user1@example.com

Only the localhost needs access to the ldap server for the above example. To be paranoid, it may be a good idea to also block the port in pf.conf

```
############ block ldap port from external interface
block in log on $ext_if proto {tcp,udp} from any to any port {389}
```

We hope the above gives readers some of the missing pieces and is of help.

OTHER:

Wish list for this document and things we received email on that would be nice to include, resources permitting, but would turn the document into a thick book ;)

- More information on how to use LDAPS and IMAPS. New users find it somewhat complicated to implement.
- There are quite a few gotchas when using clients like Microsoft Outlook
  (not Outlook Express, surprisingly) with OpenLDAP.
  It would be nice to have that also documented and explained clearly.

Useful websites for LDAP

- http://www.zytrax.com/books/ldap/ [13] LDAP for Rocket Scientists
  This Open Source Guide is about LDAP and (mostly) OpenLDAP 2.x on Linux

(REDHAT Versions 7.x) and the BSD's (FreeBSD, OpenBSD and NetBSD).
It is meant for newbies, Rocket Scientist wannabees and anyone in between.

- http://www.openldap.org/lists/openldap-software/ [14]
  Search the OpenLDAP Software Mailing List Archives
- http://www.padl.com/OSS/MigrationTools.html [15] Migration Tools
  The Migration Tools are a set of Perl scripts for migrating users, groups, aliases, hosts, netgroups, networks, protocols, RPCs, and services from existing nameservices (flat files, NIS, and NetInfo) to LDAP. The tools require the ldapadd and ldif2dbm commands

LINKS related that maybe helpful to understand openldap- cyrus - sendmail

- http://openbsd-wiki.org [16]
  OpenBSD WIKI
- http://www.abstrakt.ch/unix/MINI-HOWTO-openbsd-cyrus.html [17]
- http://www.sendmail.org/m4/readme.html [18]
  Sendmail Configuration Files, The file cf/README for Sendmail has some LDAP information that may be helpful if not misleading, because it is more for mapping information used by features or routing.
- http://yolinux.com/TUTORIALS/LinuxTutorialLDAP.html [19]
  YoLinux LDAP Tutorial: Deploying OpenLDAP - Directory,
- http://www.linuxjournal.com/article/8374 [20]
  Single Sign-on and the Corporate Directory, Part I
- http://www.brennan.id.au/20-Shared_Address_Book_LDAP.html [21]
  Shared Address Book (LDAP)
- http://linuxgazette.net/124/pfeiffer.html [22]
  Migrating a Mail Server to Postfix/Cyrus/OpenLDAP
- http://www.linuxjournal.com/article/5917 [23] Large-Scale Mail with Postfix, OpenLDAP and Courier
- http://www.owlriver.com/projects/exchange/www.arrayservices.com [24]
  /projects/Exchange-HOWTO/html/x354.html [24]
  Sendmail configuration for Exchange Server Replacement
- http://www.linuxjournal.com/article/6266 [25]
  OpenLDAP Everywhere, Step-by-step instructions for sharing e-mail directories, having a unified login and sharing files in a mixed environment.
- http://www.crt.realtors.org/projects/email-redir/ [26]
  paper-html/implementation.html [26]
  Virtual Mailserver using Postfix, OpenLDAP, and Courier HOWTO
- http://www.afp548.com/article.php?story=20040824063737872 [27] cyrus-imap repair backup mailbox
- http://cyrusimap.web.cmu.edu/twiki/bin/view/Cyrus/Backup [28] wiki for backup

Source URL: https://cocoavillagepublishing.com/development/tools/openbsd/tips/cyrus-imapd

Links
[1] http://cyrusimap.web.cmu.edu/imapd/install-virtdomains.html
[2] ldap://ldap.xxx/
[3] http://phpldapadmin.sourceforge.net/
[4] http://cyrusimap.web.cmu.edu/imapd/
[5] http://cyrusimap.web.cmu.edu/imapd/install-configure.html
[6] http://cyrusimap.web.cmu.edu/imapd/faq.html
[7] mailto:cyrus@exampl1.com
[8] mailto:cyrus@example2.com

[9] mailto:user1@example1.com
[10] http://www.squirrelmail.org/
[11] http://www.squirrelmail.org/plugin_view.php?id=26
[12] http://www.squirrelmail.org/plugin_view.php?id=47
[13] http://www.zytrax.com/books/ldap/
[14] http://www.openldap.org/lists/openldap-software/
[15] http://www.padl.com/OSS/MigrationTools.html
[16] http://openbsd-wiki.org/
[17] http://www.abstrakt.ch/unix/MINI-HOWTO-openbsd-cyrus.html
[18] http://www.sendmail.org/m4/readme.html
[19] http://yolinux.com/TUTORIALS/LinuxTutorialLDAP.html
[20] http://www.linuxjournal.com/article/8374
[21] http://www.brennan.id.au/20-Shared_Address_Book_LDAP.html
[22] http://linuxgazette.net/124/pfeiffer.html
[23] http://www.linuxjournal.com/article/5917
[24] http://www.owlriver.com/projects/exchange/www.arrayservices.com/projects/Exchange-HOWTO/html/x354.html
[25] http://www.linuxjournal.com/article/6266
[26] http://www.crt.realtors.org/projects/email-redir/paper-html/implementation.html
[27] http://www.afp548.com/article.php?story=20040824063737872
[28] http://cyrusimap.web.cmu.edu/twiki/bin/view/Cyrus/Backup