

Installation

Als erstes müssen mir folgende Pakete installieren. Je nach Anwendungsgebiet müssen Useflags angepasst werden.

```
emerge cups dev-python/pycups dev-perl/Net-CUPS openldap net-print/cups-windos sys-auth/pam_ldap
```

Danach muss man den LDAP eine Ersteinrichtung verpassen, die nicht wirklich kompliziert ist. Als ersters passen wir hierzu die Schemas an. Zur Info, hat man ein Schema einkommentiert das nicht existiert, lässt sich der LDAP auch nicht starten. Jetzt entpacken wir das „ldapns.schema.bz2“. Es ist für die Hostzuweisung nötig.

```
cd /etc/openldap/schema/  
unp /usr/share/doc/pam_ldap-183/ldapns.schema.bz2
```

Danach holen wir wir uns das „openssh-lpk.schema“. Es ist für die Verteilung öffentlicher SSH-Schlüssel mittels LDAP zuständig. Downloaden kann man es direkt unter <http://code.google.com/p/openssh-lpk/downloads/list> Zwei verschiedene Kopien sind auf dieser Seite im Anhang. Jetzt bearbeiten wir die „slapd.conf“

```
nano /etc/openldap/slapd.conf
```

```
include /etc/openldap/schema/core.schema  
include /etc/openldap/schema/cosine.schema  
include /etc/openldap/schema/inetorgperson.schema  
include /etc/openldap/schema/samba.schema  
include /etc/openldap/schema/collective.schema  
include /etc/openldap/schema/nis.schema  
include /etc/openldap/schema/corba.schema  
include /etc/openldap/schema/duaconf.schema  
include /etc/openldap/schema/dyngroup.schema  
include /etc/openldap/schema/java.schema  
include /etc/openldap/schema/pmi.schema  
include /etc/openldap/schema/misc.schema  
include /etc/openldap/schema/openldap.schema  
include /etc/openldap/schema/ppolicy.schema  
include /etc/openldap/schema/ldapns.schema  
include /etc/openldap/schema/openssh-lpk.schema
```

Offlinekonfiguration (empfohlen)

Jetzt erstellen wir eine Datenbankkonfigurationsdatei. Und starten LDAP.

```
cp /var/lib/openldap-data/DB_CONFIG.example /var/lib/openldap-data/DB_CONFIG  
/etc/init.d/slapd start
```

Jetzt müssen wir noch den Ldapbaum generieren. Hier für erstellen wir eine ganz einfach LDIF, und fügen sie in unserem LDAP ein.

```
nano /etc/openldap/ldap.ldif

# before|||02.03.09|||olli|||OpenLDAP|||LDAP DNs for basic structure. Insert
this file with <pre>ldapadd -x -D cn$
# after
# Base DN
dn: dc=osit,dc=cc
#dc: osit.cc
objectClass: top
objectClass: domain
```

Einfügen der LDIF und ersten suchen im LDAPbaum.

```
ldapadd -x -D cn=Manager,dc=osit,dc=cc -W -f ldap.ldif

ldapsearch -x -b dc=osit,dc=cc '(objectclass=*)'
```

Onlinekonfiguration

Die Onlinekonfiguration ermöglicht es einem die LDAP-Konfiguration zu bearbeiten ohne den Server neu starten zu müssen. Da diese Art der Konfig wesentlich komplexer ist, und auch nur für Hochverfügbarkeitssysteme benötigt wird, gehe ich hier auch nicht näher darauf ein.

```
cp /var/lib/openldap-data/DB_CONFIG.example /var/lib/openldap-data/DB_CONFIG
mkdir /etc/openldap/slapd.d
/usr/lib/openldap/slapd -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
kill -s 15 `pidof slapd`
chown -R ldap:ldap /etc/openldap/slapd.d
/etc/init.d/slapd start
```

Einfügen der LDIF und ersten suchen im LDAPbaum.

```
nano /etc/openldap/ldap.ldif

ldapadd -x -D cn=Manager,dc=osit,dc=cc -W -f ldap.ldif
```

Clientkonfiguration

```
cp -r /root/.nano* /etc/skel/.
emerge -qak sudo pam_ldap nss_ldap

nano /etc/nsswitch.conf
```

```

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

visudo
%wheel ALL=(ALL) ALL

nano /etc/ldap.conf
suffix              "dc=osit,dc=cc"
bind_policy         soft
bind_timelimit     2
ldap_version       3
nss_base_group     ou=usergroups,ou=group,dc=osit,dc=cc
nss_base_hosts     ou=machines,dc=osit,dc=cc
nss_base_passwd    ou=users,ou=people,dc=osit,dc=cc
nss_base_shadow    ou=users,ou=people,dc=osit,dc=cc
pam_filter         objectclass=posixAccount
pam_login_attribute uid
pam_member_attribute memberid
pam_password       exop
scope              one
timelimit          2
uri                ldap://itmgmt.osit.cc/
#ssl               start_tls

nano /etc/openldap/ldap.conf
BASE      dc=osit,dc=cc
URI      ldap://itmgmt.osit.cc/

#SIZELIMIT      12
#TLS_REQCERT    allow
TIMELIMIT      2
#DEREF         never

cp /etc/pam.d/system-auth /etc/pam.d/system-auth.orig
nano /etc/pam.d/system-auth
auth          required      pam_env.so
auth          sufficient    pam_unix.so try_first_pass likeauth nullok
auth          sufficient    pam_ldap.so use_first_pass
auth          required      pam_deny.so

account       sufficient    pam_ldap.so
account       required      pam_unix.so

password      required      pam_cracklib.so difok=2 minlen=8 dcredit=2
ocredit=2 retry=3
password      sufficient    pam_unix.so try_first_pass use_authtok
nullok sha512 shadow
password      sufficient    pam_ldap.so use_authtok use_first_pass
password      required      pam_deny.so

```

```
session      required      pam_limits.so
session      required      pam_env.so
session      required      pam_unix.so
session      required      pam_mkhomedir.so skel=/etc/skel umask=0077
session      optional     pam_ldap.so

nano /etc/pam.d/su
auth         sufficient      pam_rootok.so
auth         required      pam_wheel.so group=wheel use_uid
auth         include       system-auth

account      include       system-auth

password     include       system-auth

session      include       system-auth
session      required      pam_env.so
session      optional     pam_xauth.so
```

Links

* [openssh-lpk_openssl.schema](#)

From:
<https://deepdoc.at/dokuwiki/> - DEEPDOC.AT - enjoy your brain

Permanent link:
https://deepdoc.at/dokuwiki/doku.php?id=ldap-server_unter_gentoo&rev=1330611571

Last update: **2025/11/29 22:06**

