LDAP-Client Ubuntu

Hauseigenes Apt-Repo: https://apt.iteas.at 

Betrifft Ubuntu Version 16.04, 18.04 und 19.04.

```
export SUDO_FORCE_REMOVE=yes
apt-get install ldap-auth-client libnss-ldapd sudo-ldap libpam-ldap
#ldap-auth-config ist optional
#für KDE:
apt install apturl-kde kdesudo ubuntu-minimal
```

Man kann den darauf folgenden Assistenten durchgehen und die Daten ausfüllen. Hat eine sehr einfache Konfiguration wird das funktionieren. Ansonsten muss man nach der Installation die Dateien manuell bearbeiten. Bei der Installation wird auch der Dienst „nscd“ mit installiert. Wer diesen nicht haben möchte einfache mit apt deinstallieren oder das service mit systemd deaktivieren. (systemctl disable nscd && systemctl stop nscd)

Relevante Dateien sind:

```
/etc/ldap.conf/etc/ldap/ldap.conf
/etc/nsswitch.conf
/etc/pam.d/common-session
/etc/nslcd.conf
```

Möchte man das ein Home mit sämtlichen Daten von „/etc/skel“ beim Ersten Login angelegt wird muss man Pam konfigurieren.

```
nano /etc/pam.d/common-session
Folgende Zeile anfügen:
session         required        pam_mkhomedir.so skel=/etc/skel umask=0077
```

Folgendes Service muss laufen damit man sich gegenüber LDAP authentifizieren kann.

```
systemctl status nslcd.service
● nslcd.service - LSB: LDAP connection daemon
   Loaded: loaded (/etc/init.d/nslcd; bad; vendor preset: enabled)
   Active: active (running) since Fre 2016-04-22 22:35:58 CEST; 20h ago
     Docs: man:systemd-sysv-generator(8)
   CGroup: /system.slice/nslcd.service
           └─1474 /usr/sbin/nslcd
```

Konfigbeispiele

/etc/ldap.conf: Diese Konfig ist mit einem ausgestellten Zertifikat von Startssl versehen.

```
suffix                  "dc=tux,dc=local"
bind_policy             soft
#bind_timelimit          2
ldap_version            3
nss_base_group
ou=usergroups,ou=group,ou=specialpage,ou=wifi,ou=organisationname,ou=messagi
ng,ou=homepages,dc=tux,dc=local
nss_base_hosts          ou=machines,dc=tux,dc=local
nss_base_passwd
ou=users,ou=people,ou=specialpage,ou=wifi,ou=organisationname,ou=messaging,o
u=homepages,dc=tux,dc=local
nss_base_shadow
ou=users,ou=people,ou=specialpage,ou=wifi,ou=organisationname,ou=messaging,o
u=homepages,dc=tux,dc=local
sudoers_base            ou=SUDOers,ou=Anwendungen,dc=tux,dc=local
pam_filter              objectclass=posixAcclount
pam_filter              |(host=darkbox)(host=\*)
pam_check_host_attr     yes
pam_login_attribute     uid
pam_member_attribute    memberUid
pam_password            exop
scope                   two
timelimit               20
uri                     ldap://slave01.tux.local ldap://master.tux.local
ldap://slave02.tux.local
ssl                     start_tls
tls_checkpeer           yes
tls_cacertfile          /etc/ldap/ssl/startTLSCAcert.pem
nss_reconnect_tries 4                   # number of times to double the
sleep time
nss_reconnect_sleeptime 1               # initial sleep value
nss_reconnect_maxsleeptime 16   # max sleep value to cap at
nss_reconnect_maxconntries 2    # how many tries before sleeping
nss_initgroups_ignoreusers #www-data,apache,apt-cacher-ng,avahi,avahi-
autoipd,backup,bin,clamav,clickpkg,colord,daemon,davfs2,debian-spamd,debian-
tor,dnsmasq,festival,games,geoclue,gnats,hplip,irc,kernoops,landscape,libuui
d,libvirt-dnsmasq,libvirt-
qemu,lightdm,list,lp,mail,man,mediatomb,messagebus,minidlna,motion,mysql,nag
ios,news,nvidia-
persistenced,openldap,portage,postfix,proxy,pulse,puppet,root,rtkit,saned,sm
okeping,speech-
dispatcher,sshd,statd,sync,sys,syslog,tftp,usbmux,usermetrics,uucp,vde2-
net,vdradmin-am,whoopsie,www-data
```

/etc/ldap/ldap.conf

```
BASE    dc=tux,dc=local
URI     ldap://slave.tux.local ldap://master.tux.local
ldap://slave01.tux.local
```

```
sudoers_base            ou=SUDOers,ou=Anwendungen,dc=tux,dc=local
TLS_REQCERT     demand
TIMELIMIT       2
TLS_CACERT      /etc/ldap/ssl/startTLSCAcert.pem
```

/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 dns mdns6
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
sudoers:        files ldap
```

/etc/nslcd.conf

```
# /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 at which the LDAP server(s) should be reachable.
uri ldap://slave.tux.local ldap://master.tux.local ldap://slave01.tux.local

# The search base that will be used for all queries.
base dc=tux,dc=local

# The LDAP protocol version to use.
#ldap_version 3

# The DN to bind with for normal lookups.
#binddn cn=annonymous,dc=example,dc=net
#bindpw secret

# 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/ldap/ssl/startTLSCAcert.pem

# The search scope.
#scope sub
```

Zertifikateinfo

- never: no certificate will be requested or checked;
- allow: a certificate will be requested, but it is not required or checked;
- try: a certificate will be requested and checked, but if no certificate is provided, it is ignored
- demand: a certificate will be requested, required, and checked.