

OpenLDAP Samba Share

Diese Anleitung geht davon aus, dass die folgenden Schritte bereits durchgeführt wurden und alles funktioniert:

<https://www.howtoforge.de/anleitung/so-installierst-du-openldap-unter-ubuntu-22-04/>

Installation der notwendigen Pakete:

Installiere Samba und die LDAP-Unterstützungspakete:

```
sudo apt update
sudo apt install samba smbldap-tools libnss-ldap libpam-ldap
```

Konfiguration von NSS und PAM für LDAP:

Während der Installation wirst du aufgefordert, die LDAP-Konfiguration bereitzustellen. Gib dabei die Details deines OpenLDAP-Servers an, wie z.B. die Basis-DN und den LDAP-Server-URI.

Bearbeite die Datei `/etc/nsswitch.conf`, um LDAP in die Namensauflösung einzubeziehen:

```
sudo nano /etc/nsswitch.conf
```

Ändere die Zeilen `passwd`, `group` und `shadow` wie folgt:

```
# /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
networks:  files
```

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

netgroup:    nis
```

Konfiguration von Samba für LDAP:

Erstelle eine Sicherungskopie der aktuellen Samba-Konfigurationsdatei:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Bearbeite die Samba-Konfigurationsdatei:

```
sudo nano /etc/samba/smb.conf
```

Füge oder passe folgende Parameter im `[global]`-Abschnitt an:

```
[global]
workgroup = test.local
security = user
passdb backend = ldapsam:ldap://ldap.test.local
ldap admin dn = cn=admin,dc=test,dc=local
ldap suffix = dc=test,dc=local
ldap user suffix = ou=Sales
ldap group suffix = ou=group
ldap machine suffix = ou=Computers
ldap passwd sync = yes
ldap ssl = no
```

Einrichten des Samba-Administrators:

Füge den LDAP-Administrator als Samba-Benutzer hinzu:

```
sudo smbpasswd -W
```

```
ldapadd -Q -LLL -Y EXTERNAL -H ldapi:/// -f /usr/share/doc/samba/examples/LDAP/samba.ldif
```

Gib das Passwort des LDAP-Administrators ein.

Erstellen eines Samba-Shares:

Füge am Ende der Datei `/etc/samba/smb.conf` folgenden Abschnitt hinzu:

```
[shared]
    path = /srv/samba/shared
    browseable = yes
    writable = yes
    guest ok = no
    valid users = john.doe
```

Erstelle das Verzeichnis und setze die Berechtigungen:

```
sudo mkdir -p /srv/samba/shared
sudo chown -R nobody:nogroup /srv/samba/shared
sudo chmod -R 777 /srv/samba/shared
```

User Konfigurieren:

Der User sollte schlussendlich eine ähnliche konfiguration wie die folgende haben.

```
root@ldap:~# ldapsearch -x -H ldap://ldap.test.local -b "uid=john.doe,ou=Sales,dc=test,dc=local"
dn: uid=john.doe,ou=Sales,dc=test,dc=local
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: posixAccount
cn: John Doe
sn: Doe
mail: john.doe@test.local
uid: john.doe
sambaPasswordHistory: 0000000000000000000000000000000000000000000000000000000000000000
00000000
sambaAcctFlags: [U      ]
loginShell: /bin/bash
homeDirectory: /home/john.doe
uidNumber: 15258
gidNumber: 4549
sambaPwdLastSet: 1731871539
sambaSID: S-1-5-21-1055546307-1221338049-756278767-1001
```

```
sambaNTPassword: A9FDFA038C4B75EBC76DC855DD74F0DA
```

sambaSID: Kann über den folgenden befehl generiert werden. (muss hintendran noch eine 4 Stellige nummer konfiguriert werden)

```
root@ldap:~# net getlocalsid
```

```
SID for domain LDAP is: S-1-5-21-1055546307-1221338049-756278767
```

sambaNTPassword: To make the NT Password you can use the following Site:

<https://www.browserling.com/tools/ntlm-hash>

Machen würde man es mit dem folgenden Idif file:

```
dn: uid=john.doe,ou=Sales,dc=test,dc=local
changetype: modify
add: objectClass
objectClass: sambaSamAccount
objectClass: posixAccount
-
add: loginShell
loginShell: /bin/bash
-
add: homeDirectory
homeDirectory: /home/john.doe
-
add: uidNumber
uidNumber: 15258
-
add: gidNumber
gidNumber: 4549
-
add: sambaSID
sambaSID: S-1-5-21-1055546307-1221338049-756278767-1001
-
add: sambaNTPassword
sambaNTPassword: A9FDFA038C4B75EBC76DC855DD74F0DA
```

Um das File dann auszuführen benutzen sie dann denn folgenden befehl:

```
ldapmodify -x -D "cn=admin,dc=test,dc=local" -W -H ldap://ldap.test.local -f modify_john_doe.ldif
```

```
smbpasswd -a john.doe
```

Neustart der Dienste

Starte die Samba-Dienste neu, um die Änderungen zu übernehmen:

```
sudo systemctl restart smb nmbd
```

Testen

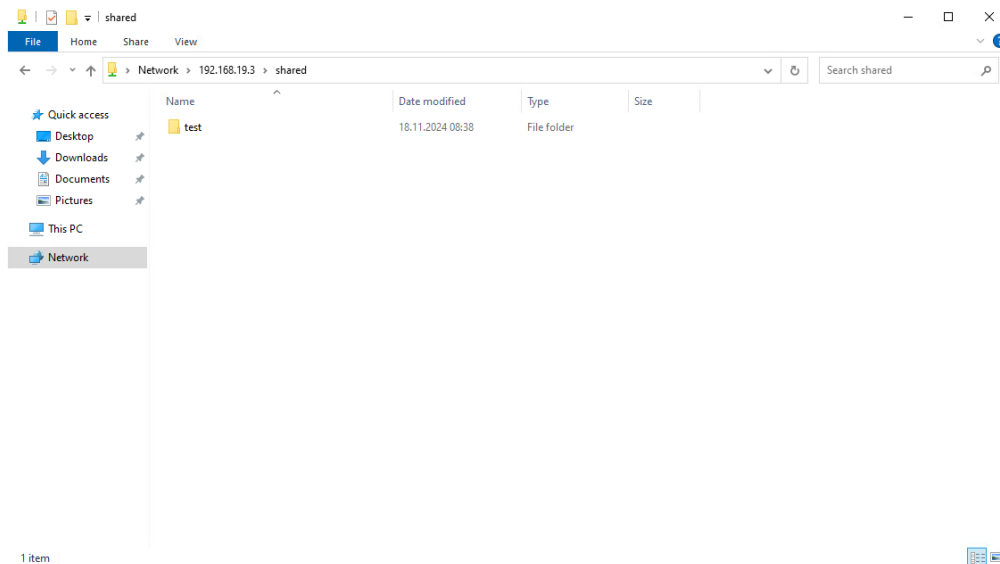
Linux

```
smbclient //192.168.19.3/shared -U john.doe
```

```
root@ldap:~# smbclient //192.168.19.3/shared -U john.doe
Password for [TEST.LOCAL\john.doe]:
Try "help" to get a list of possible commands.
smb: \> mkdir test
smb: \> ls
.                D            0  Mon Nov 18 07:38:32 2024
..               D            0  Mon Nov 18 07:38:32 2024
test             D            0  Mon Nov 18 07:38:32 2024

24050032 blocks of size 1024. 14773196 blocks available
smb: \> |
```

Windows



Revision #7

Created 17 November 2024 17:43:48 by Manuel Regli

Updated 9 December 2024 12:47:19 by Manuel Regli