

[zurück](#)

Samba mit LDAP oder Active Directory

Diese Anleitung zeigt, wie du Samba in ein zentrales Verzeichnisdienst-System integrierst – wahlweise über **OpenLDAP** oder **Active Directory (AD)**. Dadurch entfällt die lokale Benutzerpflege auf dem Linux-Server.

□ Ziel

- zentrale Benutzer- und Gruppenverwaltung für Samba-Zugriffe
- konsistente Anmeldung für Windows- und Linux-Clients
- optional: Benutzerverwaltung über LDAP Account Manager (LAM)

□ Voraussetzungen

- Samba ist installiert
- LDAP- oder AD-Server existiert (z. B. [openldap](#) oder Windows AD)
- Der Linux-Server kann die LDAP-Quelle auflösen und erreichen (z. B. per `ldapsearch`)

□ OpenLDAP-Anbindung (Idapsam)

1. Benötigte Pakete

```
```bash apt install samba libnss-ldap libpam-ldap nscd
```

### 2. smb.conf Ergänzungen

```
passdb backend = ldapsam:ldap://ldap.mash4077.local ldap admin dn =
cn=admin,dc=mash4077,dc=local ldap suffix = dc=mash4077,dc=local ldap user suffix = ou=Users
ldap group suffix = ou=Groups ldap machine suffix = ou=Computers ldap ssl = start_tls
```

### 3. LDAP-Struktur (Beispiel)

```
dc=mash4077,dc=local |— ou=Users | — uid=lars |— ou=Groups | — cn=smbgroup
```

### 4. Benutzer mit smbldap-tools oder LAM einpflegen

Siehe: [openldap](#) und: [lam\\_setup](#)

## ☐ Active Directory-Anbindung (ADS-Modus)

### 1. Voraussetzungen

- Domain Controller mit DNS (z. B. dc1.mash4077.local)
- Zeit synchronisiert (NTP)
- FQDN auflösbar (ping dc1.mash4077.local)
- Kerberos korrekt konfiguriert (/etc/krb5.conf)

### 2. smb.conf Beispiel für ADS

workgroup = MASH security = ADS realm = MASH4077.LOCAL

idmap config \* : backend = tdb idmap config \* : range = 3000-7999 idmap config MASH : backend =  
rid idmap config MASH : range = 10000-999999

winbind use default domain = yes winbind enum users = yes winbind enum groups = yes

### 3. Domain-Join durchführen

net ads join -U Administrator

### 4. Testen

wbinfo -u # AD-Benutzer anzeigen getent passwd # Benutzerauflösung testen

## ☐ Rechtevergabe in Samba-Freigaben

valid users = MASH\\lars

Oder bei LDAP:

valid users = @smbgroup

## ☐ Hinweise

- Bei ADS ist Kerberos entscheidend – ohne funktionierendes Ticket kein Login
- Bei LDAP sollte smbldap-tools oder LAM verwendet werden
- Prüfe /var/log/samba/log.smbd bei Problemen

## ☐ Weiterführend

- `[[linux:samba_mischfreigabe|Zurück zur Hauptanleitung]]`
- `[[linux:samba_acl|ACLs für Gruppenfreigaben]]`
- `[[linux:openldap|OpenLDAP einrichten]]`
- `[[linux:lam_setup|LDAP Account Manager (LAM)]]`

Bereit für den nächsten Punkt? Dann folgt als Nächstes:

☐ `docker:traefik_setup` - Samba + Traefik + HTTPS + Subdomain-Zugriff

Los?

From:

<http://wiki.nctl.de/dokuwiki/> - ☐ **Veni. Vidi. sudo rm -rf / vici.**

Permanent link:

[http://wiki.nctl.de/dokuwiki/doku.php?id=linux:samba\\_active\\_directory&rev=1752143287](http://wiki.nctl.de/dokuwiki/doku.php?id=linux:samba_active_directory&rev=1752143287)

Last update: **10.07.2025 12:28**

