HowTo LDAP einrichten

(Proxmox + LDAP Vorlage)

Aktualisiert: Juli 2026 | napp-it.org | CC-BY-SA 2.0

Dieser Guide behandelt LDAP-Verzeichnisschemata, die für die Windows/SMB-Authentifizierung relevant sind (POSIX, Samba, Active-Directory-Modus), wann welches Schema sinnvoll ist, und wie ein LDAP-Server auf Proxmox als napp-it cs Backend-Member eingerichtet wird.

Inhaltsverzeichnis

TL;DR — Kurzfassung

Windows-Clients sollen sich mit Benutzername/Passwort gegen ein zentrales Verzeichnis anmelden? Nutze OpenLDAP + das Samba-Schema (NT4-Stil) für einfache NTLM-Authentifizierung, oder Samba 4 als vollständigen AD Domain Controller, wenn zusätzlich Kerberos-SSO und Gruppenrichtlinien benötigt werden. Empfohlener Weg: Proxmox-LXC-Container mit dem TurnKey-LDAP-Appliance-Template, danach das Samba-Schema importieren und diesen Host als napp-it cs Backend-Member hinzufügen.

1. Die drei LDAP-Schema-Modi

POSIX / RFC2307 — klassisches Linux-LDAP

Speichert Linux-UIDs, GIDs, Home-Verzeichnisse und (mit dem separaten openssh-lpk-Schema) SSH-Public-Keys. Allein kann es keine NTLM-Hashes für Windows-SMB-Logins verarbeiten.

Samba-Schema (sambaSamAccount)

Erweitert das Linux-LDAP-Schema um Attribute wie sambaNTPassword, damit Samba Windows-Clients per NTLM ohne Kerberos authentifizieren kann. Dies ist das klassische "NT4-Style-Domain"-Modell.

Hinweis: Die klassische NT4-Style-Domain-Controller-Unterstützung (Samba PDC/BDC) ist in aktuellen Samba-Versionen (4.11+) veraltet (deprecated). Neue Setups sollten in der Regel den Active-Directory-Modus unten bevorzugen, außer es gibt einen konkreten Grund, beim Legacy-Modell zu bleiben.

Active-Directory-Modus (Samba 4 AD DC)

Der LDAP-Server verhält sich für Windows-Clients weitgehend wie ein Microsoft Windows Domain Controller — er integriert Kerberos, DNS und LDAP in einem Paket. Er ist sehr kompatibel, aber keine Byte-für-Byte-Nachbildung jeder AD-Funktion.

Modus / Schema	OpenLDAP (pur)	OpenLDAP + Samba3-Schema	Samba 4 AD DC
1. POSIX / RFC2307 (nativ Linux/Unix)	Ja	Ja	Ja (--use-rfc2307)
2. Samba-Schema (NTLM für SMB)	Nein	Ja	anders gehandhabt*
3. Active-Directory-Modus (KDC / Kerberos / GPO)	Nein	Nein	Ja

* Samba 4 AD DC benötigt keinen Import des klassischen sambaSamAccount-Schemas — es unterstützt intern weiterhin NTLM für Legacy-Clients, speichert den Hash aber anders (unicodePwd / supplementalCredentials im eigenen AD-Schema).

2. Warum reines OpenLDAP kein vollständiges Active Directory bieten kann

Ein echtes Active Directory ist weit mehr als ein Verzeichnisdienst — es ist ein eng integriertes Ökosystem mehrerer Dienste:

- **Integrierter Kerberos-KDC** (Key Distribution Center) — stellt Ticket-Granting-Tickets (TGTs) aus
- **Microsoft-spezifische LDAP-Erweiterungen** — z. B. Global Catalog auf Port 3268, das MS-DRSR-Replikationsprotokoll
- **SMB/RPC-Server** — für Group Policy Objects (GPOs), NETLOGON- und SYSVOL-Freigaben
- **DNS-Server** — BIND-DLZ oder Samba-interner DNS für die Kerberos-SRV-Records, die Clients benötigen

OpenLDAP ist ein exzellenter, extrem schneller und sehr flexibler reiner LDAP-Server. Aber von Haus aus fehlen ihm der Kerberos-KDC, die SYSVOL-Netzwerkfreigaben für Gruppenrichtlinien und die Microsoft-spezifischen RPC-Schnittstellen, die ein Windows-Client nach dem Domainbeitritt erwartet.

3. Wann was verwenden

OpenLDAP wählen, wenn...

- primär Linux/Unix-Clients, macOS oder Webanwendungen (Nextcloud, GitLab, VPN) zentral authentifiziert werden sollen
- ein klassisches Samba-3-Setup ("NT4-Style-Domain") mit samba.schema für Windows-SMB-Freigaben betrieben wird
- maximale Kontrolle über das Verzeichnisschema und extrem schnelle Abfragen bei sehr vielen Einträgen benötigt werden

Samba 4 (Active Directory DC) wählen, wenn...

- Windows-Clients nativ einer Domain beitreten sollen (Win-Taste + Pause → Domain beitreten)
- Gruppenrichtlinien (GPOs) auf Windows-Clients angewendet werden sollen
- nahtloses Kerberos-Single-Sign-On (SSO) über Windows-, Linux- und Mac-Clients im Netzwerk gewünscht ist

Gut zu wissen: Samba 4 bringt einen eigenen integrierten LDAP-Server mit. Sobald Samba 4 als Active-Directory-Domain-Controller (AD DC) eingerichtet ist, wird OpenLDAP gar nicht mehr benötigt — Samba 4 beantwortet LDAP-, Kerberos- und SMB-Anfragen vollständig selbst.

4. Empfohlener Installationsweg (Proxmox + TurnKey LDAP)

- Proxmox-Host mit einem LXC-Container, der das TurnKey-LDAP-Appliance-Template nutzt
- Container starten und als Master (read/write) installieren

Samba-Schema installieren:

```
apt update
apt install smbldap-tools

# Samba-Schema in die OpenLDAP-Konfiguration importieren
ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/share/doc/samba/examples/LDAP/samba.ldif

# Samba selbst installieren
apt update && apt install -y samba
```

Import prüfen:

```
ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=schema,cn=config" "(cn=*samba*)" dn
```

Sobald eine Zeile wie `dn: cn={X}samba,cn=schema,cn=config` in der Ausgabe erscheint, stehen alle Samba-Attribute in OpenLDAP und phpLDAPadmin zur Verfügung.

Test: https://ldap-ip im Browser öffnen (napp-its eigener webserver.pl darf hier NICHT gestartet sein — er würde mit phpLDAPadmin auf demselben Port kollidieren). Es sollte die phpLDAPadmin-Verwaltungsoberfläche erscheinen.

5. Samba-Attribute pro Benutzer

Wichtig: Das Samba-Schema in OpenLDAP wird für JEDEN Benutzer benötigt, der sich per SMB/NTLM von Windows (oder Linux-SMB-Clients) anmelden soll.

Warum ein normaler LDAP-Passworteintrag nicht ausreicht:

- **Format-Mismatch:** OpenLDAP speichert Passwörter standardmäßig als gewöhnliche Hashes (z. B. SHA-256, SSHA oder Bcrypt). Windows sendet bei einem SMB/NTLM-Login jedoch kein Klartext-Passwort — es erwartet, dass der Server den Login anhand eines speziellen NTLM-Hashes (sambaNTPassword) verifiziert.
- **Fehlendes Attribut:** Das OpenLDAP-Kernschema hat gar kein sambaNTPassword-Feld. Erst das Hinzufügen der Objektklasse sambaSamAccount aus dem Samba-Schema gibt einem Benutzer dieses Feld in LDAP.
- **Kerberos vs. NTLM:** In einer vollständigen Active-Directory/Kerberos-Umgebung würde die Authentifizierung über Tickets laufen. Da hier NTLM ohne Kerberos verwendet wird, muss der Samba-Server (z. B. als Fileserver) diesen sambaNTPassword-Hash aus LDAP lesen, um den Windows-Login zu bestätigen.

Was das für den Workflow bedeutet:

Sobald das Schema importiert ist, benötigt jeder Benutzer, der sich per SMB anmelden darf:

- die Objektklasse sambaSamAccount hinzugefügt
- mindestens diese Pflichtattribute gesetzt: sambaSID (eine eindeutige Security-ID des Benutzers) und sambaNTPassword (der generierte NTLM-Hash des Passworts)

Tipp: Wird das Passwort in phpLDAPadmin oder der Konsole geändert, wird der NTLM-Hash oft nicht automatisch aktualisiert — außer bei Verwendung spezieller Overlays (z. B. smbk5pwd) oder Tools wie smbldap-tools / smbpasswd.

6. napp-it cs: LDAP-Server als Backend-Member

napp-it cs auf dem LDAP-Container als Backend-Member einrichten (Autostart über `perl /opt/csweb-gui/autobackend.pl`). Dies startet beim Boot NUR server.pl und monitor.pl — bewusst NICHT webserver.pl, da napp-its eigene Web-GUI mit phpLDAPadmin auf demselben Port kollidieren würde. Die eigentliche Web-GUI bleibt ein manueller Schritt, falls sie auf diesem Host direkt benötigt wird.

```
perl /opt/csweb-gui/autobackend.pl 1   # Backend-Autostart aktivieren, sofort starten
```

Anschließend diesen Host in napp-it cs als Member hinzufügen: System-Menü › Container per IP hinzufügen, über den Standard-Member-Join-Ablauf.

7. Ausblick: NTLM-Deprecation

Sollte ein zukünftiges Windows-Release das einfache NTLM-Modell standardmäßig nicht mehr unterstützen und stattdessen das sicherere Kerberos verlangen, gibt es zwei Optionen:

- NTLM per Windows-Registry-Richtlinie wieder zulassen, oder
- auf Samba als vollständigen AD DC mit DNS/DHCP und Kerberos umsteigen (deutlich mehr Aufwand)