AD Beitritt Open Suse 16

Hier ist eine **kompakte, kopierfertige Anleitung** für die **Domänenintegration mit Offline-Login** unter **openSUSE Leap 16 / SLE 16**. Einfach **Schritt für Schritt abarbeiten** – von der Installation bis zum Test der Offline-Anmeldung.

□□ Anleitung: openSUSE Leap 16 in Active Directory einbinden (mit Offline-Login)

Voraussetzungen:

- Domänenname: `BEISPIEL.DOMAENE.LAN` (ersetzen!)
- Domänen-Admin: `Administrator` (oder anderer Berechtigter)
- Netzwerkverbindung zum Domänencontroller (DC)

1□ Pakete installieren

```
sudo zypper refresh
sudo zypper install --no-confirm realmd sssd sssd-ad sssd-tools adcli krb5-client oddjob oddjob-mkhomedir
pam_krb5 pam_winbind samba-client
```

2□ Hostname und DNS prüfen

```
# Hostname setzen (muss im AD eindeutig sein)
sudo hostnamectl set-hostname client1.beispiel.domäne.lan

# DNS prüfen (muss den DC auflösen können)
ping dc1.beispiel.domäne.lan
nslookup dc1.beispiel.domäne.lan
```

→ Falls DNS nicht funktioniert:

```
sudo vi /etc/resolv.conf
```

Eintrag hinzufügen:

```
nameserver 192.168.1.10  # IP des DC
search beispiel.domäne.lan
```

3️⃣ Domäne mit `realmd` beitreten

```
# Domäne entdecken (Test)
sudo realm discover BEISPIEL.DOMAENE.LAN

# Domäne beitreten (Passwort des AD-Admins eingeben)
sudo realm join -U Administrator BEISPIEL.DOMAENE.LAN --verbose
```

→ **Erwartete Ausgabe:** `Successfully enrolled machine in realm`

4️⃣ SSSD für Offline-Login konfigurieren

```
sudo vi /etc/sssd/sssd.conf
```

Folgende Zeilen anpassen/ergänzen:

```
[sssd]
domains = BEISPIEL.DOMAENE.LAN
config_file_version = 2
services = nss, pam, sudo, ssh

[domain/BEISPIEL.DOMAENE.LAN]
ad_domain = BEISPIEL.DOMAENE.LAN
krb5_realm = BEISPIEL.DOMAENE.LAN
realmd_tags = manages-system joined-with-adcli
cache_credentials = true          # Offline-Login aktivieren
```

```
krb5_store_password_if_offline = true
default_shell = /bin/bash
ldap_id_mapping = true
use_fully_qualified_names = false  # Anmeldung mit "benutzername" statt "benutzername@domäne.lan"
fallback_homedir = /home/%u
access_provider = ad
entry_cache_timeout = 1209600     # Cache-Gültigkeit: 14 Tage (in Sekunden)
account_cache_expiration = 14     # Account-Cache: 14 Tage
```

Berechtigungen setzen:

```
sudo chmod 600 /etc/sssd/sssd.conf
```

5️⃣ PAM für Home-Verzeichnis und Offline-Login konfigurieren

```
# Automatische Erstellung von Home-Verzeichnissen aktivieren
sudo pam-config --add --mkhomedir

# PAM-Konfiguration prüfen
sudo vi /etc/pam.d/common-session
```

Folgende Zeile hinzufügen (falls nicht vorhanden):

```
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

6️⃣ Dienste neu starten

```
sudo systemctl restart sssd
sudo systemctl enable --now oddjobd
```

7️⃣ Test: Online-Anmeldung (Cache füllen)

```
# Testbenutzer anmelden (ersetze "testuser" mit einem AD-Benutzer)
su - testuser
exit

# Kerberos-Ticket prüfen
klist
```

→ **Erwartet:** Ein gültiges Ticket für `testuser@BEISPIEL.DOMAENE.LAN`.

---

8 Test: Offline-Login

```
# Netzwerk trennen (z. B. Kabel ziehen oder WLAN deaktivieren)
sudo systemctl stop NetworkManager

# Offline-Login testen
su - testuser  # Sollte funktionieren!
id testuser    # Sollte Benutzerdaten anzeigen
klist -l       # Sollte gecachte Tickets zeigen
```

---

9 Fehlersuche (falls nötig)

Problem	Befehl zur Diagnose
Anmeldung fehlgeschlagen	`journalctl -u sssd -f`
Keine Benutzer auflösbar	`getent passwd testuser`
Kerberos-Fehler	`kinit testuser` (manueller Test)
DNS-Probleme	`dig dc1.beispiel.domäne.lan`

Wichtige Dateien & Befehle im Überblick

Zweck	Datei/Befehl
SSSD-Konfiguration	`/etc/sssd/sssd.conf`
Kerberos-Einstellungen	`/etc/krb5.conf`

Zweck	Datei/Befehl
PAM-Konfiguration	`/etc/pam.d/common-session`
Cache löschen	`sudo systemctl stop sssd; sudo rm -f /var/lib/sss/db/cache_*.ldb; sudo systemctl start sssd`
Ticket-Cache prüfen	`klist -l`
Benutzerdaten prüfen	`id testuser`

Fertig!

- Der Rechner ist jetzt in der Domäne und unterstützt **Offline-Login**.
- **Wichtig:** Jeder Benutzer muss sich **mindestens einmal online anmelden**, bevor er offline arbeiten kann.

Optional: Automatische Ticket-Erneuerung konfigurieren

Falls Kerberos-Tickets zu schnell ablaufen:

```
sudo vi /etc/krb5.conf
```

Folgende Zeilen anpassen:

```
[libdefaults]
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
```

Dann **SSSD neu starten**:

```
sudo systemctl restart sssd
```

Tipp: Falls **Smartcards** oder **Zertifikatsauthentifizierung** benötigt werden, muss zusätzlich `pam_pkcs11` oder `sssd` mit `certificate`-Backend konfiguriert werden. Lass es mich wissen, falls du das brauchst!

Viel Erfolg!

Revision #1
Created 14 September 2025 07:44:40 by Stefan Mechler
Updated 14 September 2025 07:45:16 by Stefan Mechler