AD Beitritt Ubuntu LTS

Hier ist eine **komplette, kopierfertige Anleitung für Ubuntu (22.04 LTS / 24.04 LTS)** mit **SSSD + Realmd** für **AD-Integration inkl. Offline-Login** – **ohne Winbind**, da SSSD zuverlässiger für Offline-Szenarien ist.

□□ Ubuntu AD-Integration mit Offline-Login (SSSD + Realmd)

Voraussetzungen:

- Ubuntu **22.04 LTS oder 24.04 LTS** (frisch installiert)
- Domänenname: `BEISPIEL.DOMAENE.LAN` (ersetzen!)
- AD-Admin-Benutzer: `Administrator` (oder anderer berechtigter Benutzer)
- Netzwerkverbindung zum **Domänencontroller (DC)**

1□ Pakete installieren & System vorbereiten

```
# System aktualisieren
sudo apt update && sudo apt upgrade -y

# Benötigte Pakete installieren
sudo apt install -y realmd sssd sssd-tools adcli krb5-user packagekit oddjob oddjob-mkhomedir pam_krb5 libnss-sss libpam-sss ntp

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

2□ Kerberos konfigurieren

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

Inhalt ersetzen durch:

```
[libdefaults]
    default_realm = BEISPIEL.DOMAENE.LAN
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false

[realms]
    BEISPIEL.DOMAENE.LAN = {
        kdc = dc1.beispiel.domäne.lan
        admin_server = dc1.beispiel.domäne.lan
    }

[domain_realm]
    .beispiel.domäne.lan = BEISPIEL.DOMAENE.LAN
    beispiel.domäne.lan = BEISPIEL.DOMAENE.LAN
```

---

3 DNS prüfen & anpassen

```
# Testen, ob der DC erreichbar ist
ping dc1.beispiel.domäne.lan
nslookup dc1.beispiel.domäne.lan

# Falls DNS nicht funktioniert, manuell anpassen:
sudo vi /etc/resolv.conf
```

Inhalt ersetzen durch:

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

→ **Wichtig:** Falls `systemd-resolved` aktiv ist:

```
sudo systemctl disable --now systemd-resolved
sudo systemctl enable --now NetworkManager
```

---

4 Domäne mit `realmd` beitreten

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

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

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

---

5 SSSD für Offline-Login konfigurieren

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

Folgende Konfiguration einfügen:

```
[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  # Kurze Benutzernamen (z. B. "user" statt "user@domäne.lan")
fallback_homedir = /home/%u
access_provider = ad
```

```
entry_cache_timeout = 1209600     # Cache-Gültigkeit: 14 Tage
account_cache_expiration = 14     # Account-Cache: 14 Tage
```

Berechtigungen setzen:

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

---

6 PAM für Home-Verzeichnisse & Offline-Login anpassen

```
# Automatische Home-Verzeichnisse aktivieren
sudo pam-auth-update --enable mkhomedir

# Manuell prüfen (falls nötig)
sudo vi /etc/pam.d/common-session
```

Folgende Zeile hinzufügen (falls nicht vorhanden):

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

---

7 Dienste neu starten

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

---

8 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`.

---

9 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
```

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`
SSSD-Cache löschen	`sudo systemctl stop sssd; sudo rm -f /var/lib/sss/db/cache_*.ldb; sudo systemctl start sssd`

Fertig!

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

Optional: Automatische Ticket-Erneuerung

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
```

□□ Warum SSSD statt Winbind?

Kriterium	SSSD	Winbind
Offline-Login	□ Zuverlässig (cached credentials)	□ Oft problematisch
Kerberos-Integration	□ Voll unterstützt	⚠ Teilweise manuelle Konfiguration nötig
Performance	□ Schneller (lokaler Cache)	⚠ Langsamer (mehr DC-Abfragen)
Gruppenrichtlinien (GPO)	□ Nicht unterstützt	□ Teilweise möglich
Einfachheit	□ `realmd` macht viel automatisch	⚠ Manuelle Konfiguration nötig

---

□□ Fazit

- **SSSD + Realmd** ist die **beste Wahl für Ubuntu mit Offline-Login**.
- **Winbind** ist nur nötig, wenn **GPOs** oder **Samba-Freigaben** im Vordergrund stehen.
- **Smartcards?** → Dann zusätzlich `pam_pkcs11` installieren und konfigurieren.

Falls du **Samba-Freigaben** oder **Gruppenrichtlinien** brauchst, lass es mich wissen – dann ergänze ich die Anleitung! □□

Revision #1
Created 14 September 2025 07:47:43 by Stefan Mechler
Updated 14 September 2025 07:48:07 by Stefan Mechler