

AD Beitritt Ubuntu 26.04 LTS

Hier ist eine **komplette, kopierfertige Anleitung** für **Ubuntu 26.04 LTS (Resolute Raccoon, erschienen im April 2026)** mit **SSSD + Realmd** für **AD-Integration inkl. Offline-Login – ohne Winbind**, da SSSD zuverlässiger für Offline-Szenarien ist. Ubuntu **24.04 LTS** bleibt ebenfalls kompatibel.

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

Voraussetzungen:

- Ubuntu **26.04 LTS** (auch Ubuntu **24.04 LTS** bleibt kompatibel) (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 full-upgrade -y

# Benötigte Pakete installieren
sudo apt install -y realmd sssd-ad sssd-tools libnss-sss libpam-sss adcli samba-common-bin krb5-user packagekit
odmjob odmjob-mkhomedir

# Zeitsynchronisation aktivieren und Status prüfen
sudo timedatectl set-ntp true
timedatectl status

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

Hinweis zu den Paketen: `sssd-ad` ist das für Active Directory benötigte SSSD-Backend; das allgemeine Metapaket `sssd` ist dafür nicht erforderlich. `pam_krb5` ist ein RHEL-Paketname und unter Debian/Ubuntu nicht verfügbar. Das veraltete Paket `ntp` ist zudem nicht mehr im Ubuntu-Archiv; die Zeitsynchronisation erfolgt hier über `systemd-timesyncd` via `timedatectl`. Alternativ kann `chrony` installiert und der Domänencontroller als Zeitquelle konfiguriert werden (z. B. `sudo apt install -y chrony`).

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.domaene.lan
        admin_server = dc1.beispiel.domaene.lan
    }

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

3 DNS prüfen & anpassen

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

# DNS des DC dauerhaft über Netplan setzen
sudo vi /etc/netplan/01-netcfg.yaml
```

Beispielinhalt:

```
network:
  version: 2
  ethernets:
    enp1s0:
      dhcp4: true
      dhcp4-overrides:
        use-dns: false
      nameservers:
        addresses: [192.168.1.10]
        search: [beispiel.domaene.lan]
```

“ Ersetze `enp1s0` durch den tatsächlichen Interface-Namen. Ab Ubuntu 24.04/26.04 sollten Netplan-Dateien nicht für normale Benutzer lesbar sein:
`sudo chmod 600 /etc/netplan/01-netcfg.yaml` .

```
sudo chmod 600 /etc/netplan/01-netcfg.yaml
sudo netplan apply
resolvectl status
```

→ **Wichtig:** `/etc/resolv.conf` ist unter Ubuntu üblicherweise ein Symlink auf `/run/systemd/resolve/stub-resolv.conf`. Direkte manuelle

Änderungen daran überleben einen Neustart nicht; `systemd-resolved` daher nicht deaktivieren.

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`

Beitritt prüfen:

```
sudo realm list
id testuser@beispiel.domaene.lan
```

5 `□` SSSD für Offline-Login konfigurieren

```
sudo vi /etc/sss/sss.conf
```

Folgende Konfiguration einfügen:

```
[sss]
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@domaene.lan")
fallback_homedir = /home/%u
access_provider = ad
entry_cache_timeout = 1209600  # Cache-Gültigkeit: 14 Tage
account_cache_expiration = 14  # Account-Cache: 14 Tage
```

“ **Hinweis:** `account_cache_expiration` ist nur zusammen mit `krb5_store_password_if_offline = true` sinnvoll. Die Datei muss `root:root` gehören und die Rechte `600` haben.

SSSD und Benutzerzugriff verifizieren:

```
sudo sssctl domain-status BEISPIEL.DOMAENE.LAN
sssctl user-checks <user>
```

Berechtigungen setzen:

```
sudo chown root:root /etc/sss/sss.conf
sudo chmod 600 /etc/sss/sss.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  
id testuser@beispiel.domaene.lan # FQDN-Notation prüfen  
klist -l      # Sollte gecachte Tickets zeigen
```

Fehlersuche (falls nötig)

Problem	Befehl zur Diagnose
Anmeldung fehlgeschlagen	<code>journalctl -u sssd -f</code>
Keine Benutzer auflösbar	<code>getent passwd testuser</code>
Kerberos-Fehler	<code>kinit testuser</code> (manueller Test)
<code>Unable to locate package pam_krb5</code> / <code>ntp</code>	Nicht installieren: Paketnamen sind unter Ubuntu nicht verfügbar; <code>sssd-ad</code> verwenden und Zeitsynchronisation mit <code>timedatectl</code> (alternativ <code>chrony</code>) einrichten.
DNS-Probleme	<code>dig dc1.beispiel.domaene.lan</code>
SSSD-Cache löschen	<code>sudo systemctl stop sssd; sudo rm -f /var/lib/sss/db/cache_*.ldb;</code> <code>sudo systemctl start sssd</code>

📌 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	☐ <code>realmd</code> 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! ☐☐

☐☐ Änderungsnotiz

Stand: August 2026 – aktualisiert für Ubuntu 26.04 LTS

- Paketinstallation auf `sssd-ad`, `samba-common-bin` und aktuelle Ubuntu-Pakete angepasst; `pam_krb5` und `ntp` entfernt.
- Zeitsynchronisation und DNS-Konfiguration für Ubuntu 24.04/26.04 aktualisiert.
- Domänenbeispiele auf ASCII-FQDN `beispiel.domaene.lan` vereinheitlicht und SSSD-/Verifikationsprüfungen ergänzt.

Revision #2

Created 15 August 2026 06:39:09 by Stefan Mechler

Updated 15 August 2026 06:39:56 by Stefan Mechler