Linux Active Directory Anbindung

1 Einleitung

Mit dieser Anleitung kann ein Linux-Client an das Active-Directory der Uni Stuttgart angebunden werden, so dass eine Anmeldung am Client mit AC-Accounts möglich ist. Diese Anleitung wurde mit einem aktuellen Ubuntu Desktop (Version 16.04.1) durchgeführt. Mit älteren Versionen ist das bisher nicht gelungen.

Dem TIK stehen nicht die Ressourcen zur Verfügung um für diese Anleitung Support zu leisten. Fragen und Anregungen zur Anbindung von Linux Rechner können Sie gerne an windows-support@tik.uni-stuttgart.de senden. Wir können zu diesem Thema aber keine zeitnahe Rückmeldung garantieren.

2 Voraussetzungen

2.1 Benötigte offene Ports

- TCP & UDP port 88 for Kerberos Authentication
- TCP & UDP 389 for LDAP
- TCP & UDP 445 for SMB/CIFS/SMB2
- TCP and UDP port 464 for Kerberos Password Change
- TCP Port 3268 & 3269 for Global Catalog

2.2 Domaincontroller erreichbar

Mindestens ein Domaincontroller der Active Directory Domäne UNI-STUTTGART.DE (USADR) muss per DNS auflösbar und erreichbar sein.

```
>ping adserv01.uni-stuttgart.de
PING ADSERV01.uni-stuttgart.de (141.58.101.243) 56(84) bytes of data.
64 bytes from adserv01.uni-stuttgart.de (141.58.101.243): icmp_seq=1 ttl=128 time=1.26 ms
>ping adserv02.uni-stuttgart.de
PING adserv02.uni-stuttgart.de (129.69.4.2) 56(84) bytes of data.
64 bytes from adserv02.uni-stuttgart.de (129.69.4.2): icmp_seq=1 ttl=128 time=0.756 ms
>ping adserv03.uni-stuttgart.de
PING adserv03.uni-stuttgart.de (129.69.19.3) 56(84) bytes of data.
64 bytes from adserv03.uni-stuttgart.de (129.69.19.3): icmp_seq=1 ttl=128 time=0.672 ms
```

2.3 Korrekte Uhrzeit

Die Uhrzeit des anzubindenden Systems muss korrekt gesetzt sein.

3 Installation

Die nötigen Pakete müssen installiert werden:

```
>sudo apt-get update
>sudo apt-get install winbind samba cifs-utils smbclient libnss-winbind libpam-winbind
```

In dieser Anleitung wurden folgende Paketversionen verwendet:

Paket	winbind	samba	cifs-utils	smbclient	libnss-winbind	libpam-winbind
Version	4.3.9	4.3.9	6.4	4.3.9	4.3.9	4.3.9

4 Konfiguration

4.1 Computername ändern

```
>sudo gedit /etc/hostname
```

Den in der Datei angegebenen Computernamen nach den Vorgaben des TIK ändern, also in der Form <*Instkürzel*>-<Bezeichnung>, z.B. IXY-PC04.

```
>sudo gedit /etc/hosts
```

Hier die IP-Adresse und den Computernamen anpassen.

Computer neu starten:

```
>sudo reboot
```

4.2 Samba konfigurieren

Groß-/Kleinschreibung ist hier relevant. Insbesondere sind Domain-/Realm-Namen immer groß zu schreiben.

Den Inhalt der Datei smb.conf ersetzen:

```
>sudo gedit /etc/samba/smb.conf
```

```
[global]
security = ads
realm = UNI-STUTTGART.DE
# If the system doesn't find the domain controller automatically, you may need the following line
# password server = 141.58.101.243
# note that workgroup is the 'short' domain name
workgroup = USADR
# winbind separator = +
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

```
>sudo /etc/init.d/winbind stop
>sudo /etc/init.d/samba restart
>sudo /etc/init.d/winbind start
```

Jetzt sollte der Rechner in der Lage sein einen Active Directory Domaincontroller zu finden:

```
>sudo net ads info
LDAP server: 129.69.19.3
LDAP server name: adserv03.uni-stuttgart.de
Realm: UNI-STUTTGART.DE
Bind Path: dc=UNI-STUTTGART,dc=DE
LDAP port: 389
Server time: Fri, 23 Sep 2016 08:39:59 CEST
KDC server: 129.69.19.3
Server time offset: 0
```

4.3 Der Domäne beitreten (domain join)

Für den folgenden Schritt braucht der Account, mit dem der Beitritt durchgeführt werden soll, die Rechte um ein Computerobjekt in der angegeben Organisational Unit (OU) zu erzeugen. Das sind normalerweise die Institut-Administratoren mit ihrem jeweiligen Admin-Account (ADxxxxxx). Mit folgendem Befehl wir das Computerobjekt in der OU „uni-stuttgart.de/test/TestInst“ erzeugt:

```
>sudo net ads join createcomputer="test/TestInst" -U acXXXXXX
Enter acXXXXXX's password:
Using short domain name -- USADR
Joined 'UBUNTU' to dns domain 'uni-stuttgart.de'
No DNS domain configured for ubuntu. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
```

Die Fehlermeldung bezüglich des DNS Updates ist zu ignorieren. Ob der Domänenbeitritt erfolgreich war, kann wie folgt geprüft werden:

```
>sudo net ads testjoin
Join is OK
```

4.4 Login konfigurieren

Den Inhalt der Datei nsswitch.conf ersetzen:

```
>sudo gedit /etc/nsswitch.conf
passwd: compat winbind
group: compat winbind
shadow: compat
```

Das PAM Modul konfigurieren und dabei das automatische erzeugen von Homeverzeichnissen einschalten:

```
>sudo pam-auth-update
[*] Unix authentication
[*] Winbind NT/Active Directory authentication
[*] Register user sessions in the systemd control group hierarchy
[*] Create home directory on login
[*] GNOME Keyring Daemon - Login keyring management
```

Jede Domäne braucht ein Verzeichnis in /home/.

```
>sudo mkdir /home/USADR
```

Den Inhalt der Datei common-auth ersetzen:

```
>sudo gedit /etc/pam.d/common-auth
auth sufficient pam_unix.so nullok_secure
auth sufficient pam_winbind.so use_first_pass
auth requisite pam_deny.so
auth required pam_permit.so
auth optional pam_ecryptfs.so unwrap
```

Winbind neu starten

```
>sudo /etc/init.d/winbind restart
```

Jetzt sollte der Login für geschützte (SIAM-)Accounts an der Konsole funktionieren. Nur den Accountnamen eingeben, ohne Zusätze:

```
tik-sas-301 login: acXXXXXX
Password:
```

Eingabe des Login-Namens in der Grafischen Anmeldung ermöglichen:

```
>sudo gedit /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf
```

die Zeile

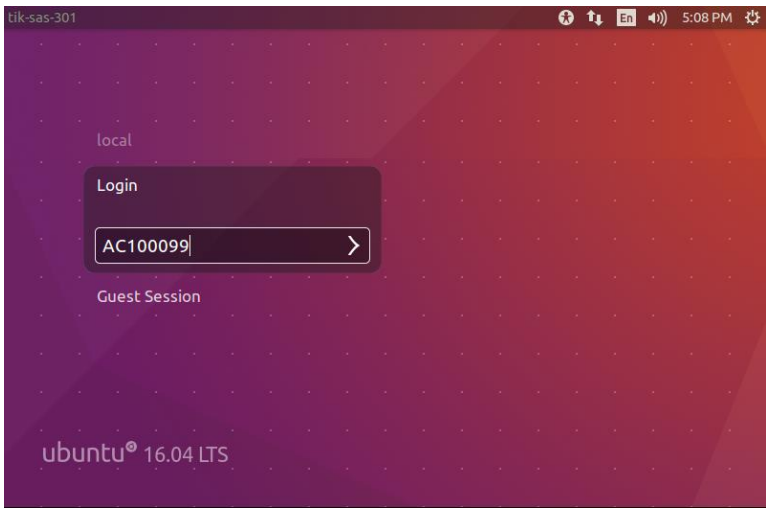
```
greeter-show-manual-login=true
```

hinzufügen.

Computer neu starten:

```
>sudo reboot
```

Nun kann an der grafischen Login-Oberfläche ein Username eingegeben werden:



5 Referenzen

[1] ActiveDirectoryWinbindHowto,
https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto