Linux System zu AD hinzufügen

Allgemeines

Es gibt zwar eine relativ einfache Methode einer AD Domäne beizutreten. Dies ist hier sehr gut beschrieben. Wer jedoch die volle Funktionalität von AD nutzen möchte, kommt bei der Methode sehr schnell an seine Grenzen. Unter Open Suse 15.x / Tubleweed ist das kein Problem. Yast auf und Domäne beitreten wählen. Etwas warten, die Admin Benutzerdaten eingeben und schon ist die Sache erledigt. Bei Ubuntu ist die Sache nicht ganz so simpel. Dieser Artikel bezieht sich auf Ubuntu 20.04 und 21.04. Sollte so aber auch in späteren Versionen funktionieren.

Pakete installieren

```
sudo apt-get install -y krb5-user libpam-krb5 winbind  samba  smbclient libnss-winbind libpam-winbind
```

Während der Installation wird nach dem Realm für Kerberos 5 gefragt. Dieser ist der Domänen Name von Active Directory. Wenn der Rechner als **rechner01.ad.einedomain.org** lautet ist der Realm **einedomain.org**.

Kerberos einrichten

In der Datei **/etc/krb5.conf** mit folgendem Inhalt versehen, wobei **ad.eigenedomain.org** wieder der bei der Installation eingegebene Name ist. Bitte auch auf die Großschreibung achten, da MIT Kerberos da ein kleinwenig heikel ist:

```
[logging]
    default = FILE:/var/log/krb5.log
```

```
[libdefaults]
    ticket_lifetime = 24000
    clock_skew = 300
    default_realm = AD.EIGENEDOMAIN.ORG

[realms]
    EXAMPLE.COM = {
        kdc = pdc.eigenedomain.org:88
        admin_server = pdc.eigenedomain.org:464
        default_domain = AD.EIGENEDOMAIN.ORG
    }

[domain_realm]
    .ad.eigenedomain.org = AD.EIGENEDOMAIN.ORG
    ad.eigenedomain.org = AD.EIGENEDOMAIN.ORG
```

Sobald die Datei gespeichert ist kann dies getestet werden. Auch hier wieder auf die groß geschriebene Domain achten:

```
kinit administrator@AD.EIGENEDOMAIN.ORG
```

Sollte jetzt keine Ausgabe kommen, war die Operation erfolgreich. Wenn jedoch eine Meldung wie die kommt:

```
kinit: KDC-Antwort entsprach nicht den Erwartungen bei Anfängliche Anmeldedaten werden geholt.
```

ist etwas schief gelaufen. In den meisten Fällen ist der Fehler dann entweder ein Fehler in den Rechnernamen oder dass der Realm entweder bei kinit oder in der Konfiguration nicht groß geschrieben waren.

Samba konfigurieren

Als nächstes bringen wird die bestehende Beispielkonfiguration in Sicherheit (diese behalte ich ganz gerne, weil in den Dateien sehr viel Dokumentiert ist):

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.sample
```

Nun legen wird die Datei **/etc/samba/smb.conf** neu an:

```
[global]
  security = ads
  realm = AD.EIGENEDOMAIN.ORG
  password server = IPADRESSE     #IP des Domain Controllers
  workgroup = AD
  idmap uid = 10000-20000
  idmap gid = 10000-20000
  winbind enum users = yes
  winbind enum groups = yes
  winbind cache time = 10
  winbind use default domain = yes
  template homedir = /home/%U
  template shell = /bin/bash
  client use spnego = yes
  client ntlmv2 auth = yes
  encrypt passwords = yes
  restrict anonymous = 2
  domain master = no
  local master = no
  preferred master = no
  os level = 0
```

Jetzt kann der Rechner der Domäne hinzugefügt werden:

```
sudo net ads join -U administrator
```

Sollte hier die Fehlermeldung kommen, dass der DNS Eintrag nicht aktualisiert werden konnte, ist das nicht schlimm. Hierzu die Datei **/etc/hosts** aktualiesieren, dass die den vollen Domain Namen enthält:

```
192.168.1.2          rechner01.eigenedomain.org        rechner01
```

Nun müssen die RPC Dienste noch verbunden werden:

```
sudo net rpc join -U administrator
```

Um die Änderungen zu übernehmen muss nun Winbind neu gestartet werden:

```
sudo systemctl restart winbind
```

Um zu prüfen ob alles wie gewünscht funktioniert können nun anfragen an den AD Server gestellt werden. Mit volgendem Befehl werden alle Benutzer aufgelistet:

```
wbinfo -u
```

System Auth konfigurieren

Kerberos und Winbind laufen jetzt. Jetzt muss das System noch dazu überredet werden, die Auth über Winbind laufen zu lassen. Dazu muss die Datei **/etc/nsswitch.conf** bearbeitet werden.

```
passwd:         compat winbind
group:          compat winbind
shadow:         compat
```

Nun muss Winbind wieder neu gestartet werden:

```
sudo systemctl restart winbind
```

PAM Konfiguration

Zuletzt muss ein Domänen Benutzer noch in die Lage versetzt werden mit dem System zu interagieren. Hierzu folgende Zeile in die Datei **/etc/security/group.conf** einfügen:

```
* ; * ; * ; Al0000-2400 ; floppy, audio, cdrom, video, usb, plugdev, users
```

Nun noch dafür sorgen, dass die Home Verzeichnisse angelegt werden. dazu folgenden Befehl ausführen und den Eintrag "Create home directory on login" aktivieren:

```
sudo pam-auth-update
```

Die folgenden abschließenden Befehle sorgen für die Übernahme der letzten Änderungen:

```
sudo systemctl stop winbind
sudo systemctl restart smbd
sudo systemctl start winbind
```

Einhängen von Netzlaufwerken mit Benutzerrechten

Dazu müssen noch weitere Pakete installiert werden:

```
sudo apt-get install libpam-mount cifs-utils
```

Abschliesende Arbeiten

Damit Domänenbenutzer **sudo** verwenden können, müssen diese entweder in die entsprechende Gruppe, oder es muss eine Datei im Ordner **/etc/sudoers.d/** angelegt werden. Ein Beispiel:

```
%wksadmins      ALL=(ALL:ALL)     ALL
"%domain admins"    ALL= (ALL:ALL) ALL
```

Die WKSAdmins Gruppe verwende ich um den Benutzern auf den lokalen Maschinen Admin Rechte zu geben ohne, dass sie diese in der Domain hätten ;).

Auch wenn das nicht unbedingt notwendig ist, sollte nun der Rechner neu gestartet werden. Dann sollten die Domänen Benutzer in der Lage sein, sich anzumelden. Ein guter Artikel zu dem Thema kann hier gefunden werden.

Revision #4
Created 14 August 2025 16:41:40 by Stefan Mechler
Updated 14 August 2025 18:06:49 by Stefan Mechler