Wenn man, wie bei vielen Arbeitsplätzen schon vorhanden, eine Nutzerauthentifizierung über Active Directory hat, wäre es doch schön, sich auch bei Linux-Rechnern über die AD authentifizieren zu können.

Installation benötigter Pakete

```
yum install realmd oddjob oddjob-mkhomedir sssd ntpdate
```

Zeitabgleich

Bei einer Domänenanmeldung ist es wichtig, dass die Zeiten übereinstimmen.
Ob die sychronisierung jetzt mit ntp oder chrony stattfindet, ist eigentlich völlig egal. Hier die chrony-Variante

```
systemctl stop chrony
ntpdate <NTP-Server> (Meist AD-Server)
sytemctl enable chrony
systemctl start chrony
```

Zeitgleichheit sieht man über die Übersicht `chronyc sources`

Authentifizierung gegenüber AD

```
realm join --computer-ou=OU=Linuxrechner,DC=<domain> --
user=<username>@<domain> <domain>
```

Der User sollte berechtigt sein, Rechner in die Domäne aufzunehmen (Domänenadmin)

Wenn die anbidung funktiert hat, kann man sich mit dem Befehl `realm list` alle einstellungen lassen.

Ab sofort kann man sich per SSH auf dem Rechner mit seinem Domänen-Namen anmelden:
Format: <username>@<domain>

Abkürzung des Anmeldenahmens

Um nicht bei jeder SSH-Anmeldung <username>@<domain> angeben zu müssen, emfiehlt es sich, die Domäne automisch hinzufügen zu lassen

In der Datei `/etc/sssd/sssd.conf` im Globalen Teil folgendes eintragen

```
[sssd]
...
default_domain_suffix = USERS.EXAMPLE.COM
```

Um alle Änderungen am SSSD zu übernehmen, muss der Dienst jetzt noch neugestartet werden

```
systemctl restart sssd
```

Einschränkung des Nutzerkreises

Wenn sich nur eine Bestimmete Person oder Gruppe per AD authentifizieren darf, kann man dies einschränken

In der Datei `/etc/sssd/sssd.conf` im Domänen-Teil folgendes eintragen

```
[domain/Domain]
...
access_provider = simple
simple_allow_users = <username1>,<username2>
simple_allow_groups = <Gruppenname>
```

die User- und Gruppennamen findet man heraus, indem man sich diese mit `id <username | sed -e 's/,/\n/g'` anzeigen lässt.

Um alle Änderungen am SSSD zu übernehmen, muss der Dienst jetzt noch neugestartet werden

```
systemctl restart sssd
```

AD-Verbindung trennen

Nicht immer soll eine sssd-Verbindung von bestand bleiben. \ Um den Rechner wieder aus der Domäne zu bekommen, empfiehlt sich der folgende Weg

```
realm leave --user=<username>@<domain> <domain>
```

Debugging

GSSAPI funktioniert nicht?

Loglevel erhöhen

```
LogLevel DEBUG1
```

SSH neu starten und unter `/var/log/secure` den Fehler identifizieren

Quellen

1. https://fedorahosted.org/sssd/wiki/Configuring_sssd_with_ad_server#no1

1. http://www.hexblot.com/blog/centos-7-active-directory-and-samba
2. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/introduction.html
3. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/SSSD-Introduction.html
4. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sssd-user-ids.html
5. https://docs.fedoraproject.org/en-US/Fedora/18/html/System_Administrators_Guide/config-sssd-domain-access.html
6. https://www.freeipa.org/images/c/cc/FreeIPA33-sssd-access-control.pdf
7. https://fedorahosted.org/sssd/wiki/DesignDocs/ActiveDirectoryAccessControl