

Wenn man wie bei vielen Arbeitsstellen 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 Synchronisierung jetzt mit ntp oder chrony stattfindet, ist eigentlich völlig egal. Hier die chrony-Variante

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

Zeitgleichheit sieht man über die Übersicht chronyc sources

## Authentifizierung gegenüber AD

```
realmd --join --user=<username>@<domain> <domain>
```

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

Wenn die Anbindung funktioniert hat, kann man sich mit dem Befehl realmd list alle Einstellungen lassen.

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

## Abkürzung des Anmeldenamens

Um nicht bei jeder SSH-Anmeldung <username>@<domain> angeben zu müssen, empfiehlt es sich, die Domäne automatisch 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 bestimmte 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
```

## Quellen

1. [https://fedorahosted.org/sssd/wiki/Configuring\\_sssd\\_with\\_ad\\_server#no1](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](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](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](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](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>

From:  
<https://wiki.da-checka.de/> - PSwiki



Permanent link:  
<https://wiki.da-checka.de/doku.php/wiki/centos/ad-anbindung?rev=1432707506>

Last update: **2015/05/27 08:18**