

CentOS7 Servers aan LDAP koppelen

Deze instructies resulteren in dat de betreffende server voor de authenticatie de LDAP server met IP nummer 192.168.1.230 raadpleegt.

Via pam-ldap

Let wel op, autorisatie wordt dus niet gedaan, iedereen in de ldap kan inloggen.

Installeer software

```
yum install -y openldap-clients nss-pam-ldapd
```

Configureer de authenticatie module

```
authconfig --enableldap --enableldapauth --ldapserver=ldap://192.168.1.230\  
--ldapbasedn=dc=voorbeeld,dc=lan --enablemkhomedir --updateall
```

in het geval van een IPA server moet de ldapbasedn worden aangepast met een cn=compat in ons voorbeeld wordt dit dus:

```
authconfig --enableldap --enableldapauth --ldapserver=ldap://192.168.1.230\  
--ldapbasedn=cn=compat,dc=voorbeeld,dc=lan --enablemkhomedir --updateall
```

```
systemctl restart nslcd
```

En test: `getent passwd testuser`

```
testuser:x:1000:1000:testuser:/home/testuser:/bin/bash
```

Hierna kan je als testuser proberen in te loggen.

via sssd

log in als root op de te koppelen client. Installeer de nodige software:

```
yum install -y openldap-clients sssd
```

Copieer het certificaat van de IPA of LDAP server of de CA naar de client en plaats deze in `/etc/openldap/cacerts`

En gebruik authconfig om sssd te configureren:

```
authconfig --enablesssd --enablesssdauth --enableldap --enableldapauth --  
enablemkhomedir
```

```
--ldapserver=ldap://192.168.1.230 --ldapbasedn="dc=voorbeeld,dc=lan" --  
enablelocauthorize --update
```

```
chmod 600 /etc/sss/sss.conf  
systemctl restart sssd
```

De resulterende sssd.conf file ziet er daarna als volgt uit:

```
[domain/default]  
autofs_provider = ldap  
cache_credentials = True  
ldap_search_base = dc=voorbeeld,dc=lan  
id_provider = ldap  
auth_provider = ldap  
chpass_provider = ldap  
ldap_uri = ldap://192.168.1.230  
ldap_id_use_start_tls = True  
ldap_tls_cacertdir = /etc/openldap/cacerts  
  
[sss]  
config_file_version = 2  
services = nss, pam, autofs  
domains = isae_ldap  
  
[nss]  
  
[pam]  
  
[domain/voorbeeld_ldap]  
id_provider = ldap  
auth_provider = ldap  
chpass_provider = ldap  
ldap_uri = ldap://192.168.1.230  
ldap_search_base = dc=voorbeeld,dc=lan  
ldap_id_use_start_tls = True  
ldap_tls_reqcert = never  
ldap_tls_cacertdir = /etc/openldap/certs/  
ldap_tls_cacert = /etc/openldap/cacerts/voorbeeld.pem  
[autofs]
```

Bronnen

<https://jackiechen.org/2014/08/15/setup-ldap-authentication-in-centos-openldapsssd/>

https://fedoraproject.org/wiki/QA:Testcase_freeipa_use_nss_pam_ldapd_to_give_access_to_trusted_domain_users

From:
<https://wiki.auriel.nl/> -

Permanent link:
https://wiki.auriel.nl/doku.php?id=werkinstructies:centos_servers_aan_ldap_koppelen&rev=1522134666 

Last update: **2018/03/27 09:11**