Table of Contents

RHEL 7 Active Directory LDAP with SSSD

Configure DNS with Active Directory IP address.

```
nmcli con mod eth0 ipv4.dns-search dominio.local
hostnamectl set-hostname ldap.dominio.local
yum install sssd realmd oddjob oddjob-mkhomedir samba-common-tools krb5-
workstation sssd-ad
realm join dominio.local
authconfig --update --enablesssd --enablesssdauth --enablemkhomedir
```

RHEL 6

You must have configured NTP and DNS.

File /etc/hosts correctly configure for example:

```
192.168.75.166 servidor servidor.2008r2.example.com
```

Install packages:

```
yum install ntp sssd samba-common krb5-workstation
```

Edit /etc/krb5.conf:

```
includedir /var/lib/sss/pubconf/krb5.include.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = 2008R2.EXAMPLE.COM
 dns_lookup_realm = true
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 2008R2.EXAMPLE.COM = {
 }

[domain_realm]
 .2008r2.example.com = 2008R2.EXAMPLE.COM
 2008r2.example.com = 2008R2.EXAMPLE.COM
```

Edit /etc/samba/smb.conf:

```
[global]
   workgroup = 2008R2
   client signing = yes
   client use spnego = yes
   kerberos method = secrets and keytab
   log file = /var/log/samba/%m.log
   realm = 2008R2.EXAMPLE.COM
   security = ads
```

Create kerberos ticket:

```
kinit Administrator
net ads join -k
authconfig --enablesssd --enablesssdauth --enablelocauthorize --
enablemkhomedir --update
```

Create /etc/sssd/sssd.conf:

```
echo >/etc/sssd/sssd.conf
chmod 600 /etc/sssd/sssd.conf
```

With this content:

```
[domain/2008r2.example.com]
id_provider = ad
access_provider = ad
default_shell=/bin/bash
fallback_homedir=/home/%u
debug_level = 0

[sssd]
services = nss, pam
config_file_version = 2
domains = 2008r2.example.com

[nss]

[pam]
```

Restart sssd:

```
service sssd restart
```

AD user access filter

Edit /etc/sssd/sssd.conf and configure in a similar way:

```
access_provider = simple
simple_allow_users = user1,user2
```

Restart sssd:

```
systemctl restart sssd
```

AD groups access filter

Edit /etc/sssd/sssd.conf and configure in a similar way:

```
access_provider = simple
simple_allow_groups =
linuxusers@administrativos.ice.com,linuxusers@sucursales.ice.com
```

Restart sssd:

```
systemctl restart sssd
```

Configure AD groups with sudo

Use visudo to add this lines:

```
%linuxusers@administrativos.ice.com     ALL=(ALL)       ALL
```

Configure home dir

Change line:

```
fallback_homedir=/home/%u@%d
```

Referencias

- https://access.redhat.com/solutions/2710131
- https://access.redhat.com/articles/3023951
- https://access.redhat.com/solutions/715173
- http://www.thinkplexx.com/learn/howto/linux/system/allow-user-sudo-but-exlude-some-privileges-run-shells-etc