# How to configure sssd on SLES 12 to connect to Windows 2012 R2 AD

**Environment**

Windows 2012 R2 w/ Active Directory

Suse Enterprise Linux Server 12

**Situation**

Configure SLES 12 server to resolve and authenticate users located in the Active Directory on Window 2012 R2

**Resolution**

SSSD (System Security Service Daemon)

Provides:

- Identity resolution - NSS module

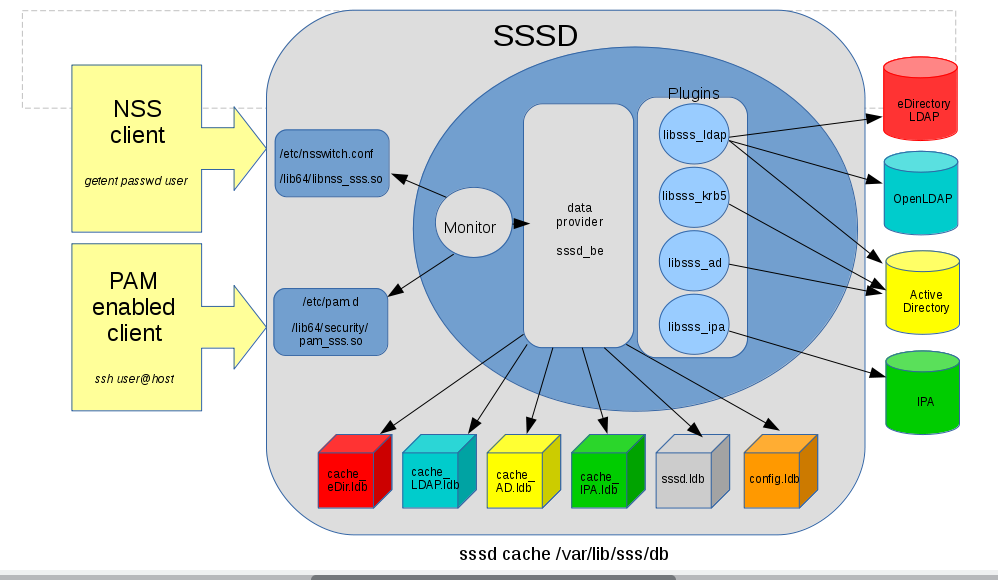
- Authenication - PAM module

-  Caching for offline access and reduced database processing

- Multiple sources in single configuration

(common sources: LDAP, AD, KRB)

SSSD Functionality Diagram



Sample Windows AD Information

Domain = AD.DOMAIN.COM

Windows Server Name = WIN2012SRV

Windows Server IPADDRESS = 192.168.157.131

AD Administrator = cn=Administrator.users.ad.domain.com

Create test user = Jane Doe / jdoe

Steps to configure SLES 12 to resolve and authenticate users in Active Directory using the AD backend plugin

1.  Join SLES 12 server to Active Directory domain

- Install krb5-client and samba client

zypper ref

zypper in krb5-client

zypper in samba-client

- Configure /etc/krb5.conf

[libdefaults]

        default\_realm = AD.DOMAIN.COM

        dns\_lookup\_realm = false

        dns\_lookup\_kdc = false

        ticket\_lifetime = 24h

        renew\_lifetime = 7d

        forwardable = true

        rdns = false

[realms]

        AD.DOMAIN.COM = {

                 kdc = win2012srv.ad.domain.com

                 master\_kdc = win2012srv.ad.domain.com

                 admin\_server = win2012srv.ad.domain.com

        }

[logging]

        kdc = FILE:/var/log/krb5/krb5kdc.log

        admin\_server = FILE:/var/log/krb5/kadmind.log

        default = SYSLOG:NOTICE:DAEMON

[domain\_realm]

        .ad.domain.com = AD.DOMAIN.COM

        ad.domain.com = AD.DOMAIN.COM

- Configure /etc/samba/smb.conf

[global]

        workgroup = AD

        printing = cups

        printcap name = cups

        printcap cache time = 750

        cups options = raw

        map to guest = Bad User

        include = /etc/samba/dhcp.conf

        logon path = \\%L\profiles\.msprofile

        logon home = \\%L\%U\.9xprofile

        logon drive = P:

        usershare allow guests = No

        idmap gid = 10000-20000

        idmap uid = 10000-20000

        realm = AD.DOMAIN.COM

        security = ADS

        template homedir = /home/%u

        template shell = /bin/bash

        winbind refresh tickets = yes

        winbind use default domain = yes

        kerberos method = secrets and keytab

        client signing = yes

        client use spnego = yes

- Configure /etc/hosts

192.168.157.131  win2012srv win2012srv.ad.domain.com ad ad.domain.com

- Join the SLES 12 Server to the AD domain

kinit Administrator

net ads join -k

-  Test GSSAPI connectivity with ldapsearch

/usr/bin/ldapsearch -H ldap://win2012srv.ad.domain.com/ -Y GSSAPI -N -b "dc=ad,dc=domain,dc=com" "(&(objectClass=user)(sAMAccountName=jdoe))"

2. Configure SSSD

-  Install sssd and sssd-ad

zypper ref

zypper in sssd

zypper in sssd-ad

-  Modify /etc/sssd/sssd.conf

[sssd]

config\_file\_version = 2

debug\_level = 6

services = nss, pam

domains =  AD

[nss]

filter\_users = root

filter\_groups = root

[domain/AD]

debug\_level = 6

id\_provider = ad

auth\_provider = ad

ad\_domain = ad.domain.com

ad\_server = win2012srv.ad.domain.com

ad\_hostname = win2012srv.ad.domain.com

ldap\_id\_mapping = True

override\_homedir = /home/%u

ldap\_schema = ad

3. Configure NSS

- Modify  /etc/nsswitch.conf

passwd:  files  sss

group:   files sss

-  Modify  /etc/nscd.conf

enable-cache   passwd    no

enable-cache   group      no

-  restart nscd

systemctl restart nscd

-  start sssd

systemctl start sssd

4. Configure PAM

/etc/pam.d/common-auth

auth    sufficient        pam\_sss.so     use\_first\_pass

/etc/pam.d/common-account

account   sufficient      pam\_sss.so    use\_first\_pass

/etc/pam.d/common-session

session    sufficient     pam\_sss.so     use\_first\_pass

session    sufficient   pam\_mkhomedir.so

/etc/pam.d/common-password

password     sufficient     pam\_sss.so

5.  Test Resolution and Authentication

Resolution

  id  <userid>

getent passwd <userid>

Authentication

ssh <userid>@localhost