So far, i've discovered.

* **SSSD( System Security Services Daemon)**
* **Samba/Winbind**
* **Native LDAP and Kerberos PAM and NSS modules**
* **MY HEAD HURTS ALL THESE DIFFERENT METHODS USE THE SAME AUTHENTICATION METHODS. HOW WILL I KNOW WHICH METHOD IS BEING IMPLEMENTED?**
* **lksajdlaksjdlksajdalsjdlasd**

### **Samba/ Winbind DEBIAN/ UBUNTU BOTNET**

So with samba/winbind, there is a mixture of kerberos and pam authentication, according to arch wiki, debian wiki and redhat guides. samba/winbind steps for all these distros are very similiar. Will start with debian.. ubuntu(they are different) … centos and arch.

**Packages needed**

Winbind 2:3.6.6-3

Samba 2:3.6.6-3

Krb5-user 1.10.1+dfsg-2

Libpam-krb5 4.6-1

libpam-winbind

libnss-winbind

**Check /etc/hosts .**

**#** this must be able to resolve to authenticate. Back this up too

127.0.0.1 linux.test.server.com localhost linux

If its authenticating using Keberos. You should see what port its listing on and what box its being pointed too. What is in purple will show you how it is trying to authenticate.

**/etc/krb5.conf**

[logging]

Default = FILE:/var/log/krb5.log

[libdefaults]

ticket\_lifetime = 24000

clock-skew = 300

default\_realm = test.server.com

# dns\_lookup\_realm = false

# dns\_lookup\_kdc = true

[realms]

test.example.com = {

**kdc = example.test.server.com:88**

**admin\_server = example.test.server.com:464**

**default\_domain = test.server.com**

}

[domain\_realm]

.server.com = test.server.com

server.com = test.server.com

**Test configuration by requesting a ticket using the kinit command**

root@linux:~# kinit [Administrator@test.server.com](mailto:Administrator@test.server.com)

Password for Administrator@test.server.com : \*\*\*

**Should output to something like this if it worked.**

root@linux:~# klist

Ticket cache: File: /tmp/krb5cc\_0

Default principal: Administrator@test.server.com

Valid starting Expires Service principal

05/16/07 10:30:42 05/16/07 20:30:01

Krbtgt/test.server.com@test.server.com

renew until 05/16/07 10:30:42

KERBEROS should be configured before anyone joins AD

Now that it works. 1st step is that someone has to join the domain. This is where samba comes in. kerberos simply authenticates credentials. And samba syncs up the the user accounts with AD.

**Default samba config /etc/samba/smb.conf**

security = ads

realm = LAB.EXAMPLE.COM (SOME.CCDC.SITE)

# If the system doesn't find the domain controller automatically, you may need the following line

# password server = 10.0.0.1

# note that workgroup is the 'short' domain name

workgroup = LAB

# winbind separator = +

idmap uid = 10000-20000

idmap gid = 10000-20000

winbind enum users = yes

winbind enum groups = yes

template homedir = /home/%D/%U

template shell = /bin/bash

client use spnego = yes

client ntlmv2 auth = yes

encrypt passwords = yes

winbind use default domain = yes

restrict anonymous = 2

The "winbind use default domain" parameter is useful in single-domain enterprises and causes winbind to treat any username that isn't qualified with a domain name as a username in the domain to which winbind is joined. Omit this parameter if you are concerned about confusion between local accounts on your systems and accounts in the default domain. The "winbind separator" directive is optional, and the default value is the usual backslash "\" Domain and User separator. You can use "+" if you know of a specific reason "\" will not work in your environment.

Restarting Windbind, Samba

root@linux:~# /etc/init.d/winbind stop

root@linux:~# /etc/init.d/samba restart

root@linux:~# /etc/init.d/winbind start

**Request Kerberos TGT for an account**

$sudo kinit Administrator@EXAMPLE.COM

$sudo net ads join

Using short domain name – LAB

Joined 'linuxwork' to realm 'LAB.EXAMPLE.COM'

You might get an error like

**kinit(v5): Cannot resolve network address for KDC in realm LAB.EXAMPLE.COM while getting initial credentials**

even though nslookup win2k3 and host 10.0.0.1 would both return the correct entries.

To correct this problem, edit

**/etc/hosts file**

10.0.0.1 win2k3.lab.example.com(SOME CCDCWINBOX)

**If your Active Directory server is not running DDNS as well (eg. if you're running a separate DNS server) you may get the error:**

sudo net ads join

Failed to join domain: failed to find DC for domain LAB.EXAMPLE.COM

To fix this, specify the AD server to the "net join" command:

sudo net ads join -S WIN2K3 -U <username>%<password>

You'll get a warning about not being able to update DNS, but you will successfully join the AD!

**Setup Authentication**

**#NSS SWITCH**

#A system administrator usually configures the operating system's name services using the file #/etc/nsswitch.conf. This lists databases (such as passwd, shadow and group) and one or more #sources for obtaining that information. Examples for sources are files for local files, ldap for the #Lightweight Directory Access Protocol, nis for the Network Information Service, nisplus for NIS+, #and wins for Windows Internet Name Service. Dont forget to restert nsswitch.

nsswitch Location: **/etc/nsswitch.conf**

passwd: compat winbind

group: compat winbind

shadow: compat

**PAM**

**/etc/pam.d/common-account**

account sufficient pam\_winbind.so

account required pam\_unix.so

**/etc/pam.d/common-auth**

auth sufficient pam\_winbind.so

auth sufficient pam\_unix.so nullok\_secure use\_first\_pass

auth required pam\_deny.so

**/etc/pam.d/common-auth**

session required pam\_unix.so

session required pam\_mkhomedir.so umask=0022 skel=/etc/skel

**Location: /etc/pam.d/sudo**

Auth sufficient pam\_winbind.so

Auth sufficient pam\_unix.so use\_first\_pass

Auth required pam\_deny.so

@include common-account

#<https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto>

Okay so now that im arelaxed. I guess not matter which way AD is authenticated. Its always going to use either PAM or kebereos or both. Then comes windbind or SSSD or any other thing they throw at us. Here is how to set up SSSD on REDHAT/Fedora

/etc/sssd/sssd.conf

**Example sssd.conf configuration**

[sssd]

config\_file\_version = 2

domains = ad.example.com

services = nss, pam

[domain/ad.example.com]

# Uncomment if you need offline logins

# cache\_credentials = true

id\_provider = ad

auth\_provider = ad

access\_provider = ad

# Uncomment if service discovery is not working

# ad\_server = server.ad.example.com

# Uncomment if you want to use POSIX UIDs and GIDs set on the AD side

# ldap\_id\_mapping = False

# Comment out if the users have the shell and home dir set on the AD side

default\_shell = /bin/bash

fallback\_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available

# ldap\_sasl\_authid = host/client.ad.example.com@AD.EXAMPLE.COM

# Comment out if you prefer to user shortnames.

use\_fully\_qualified\_names = True

**Set the file ownership and permissions on sssd.conf**

chown root:root /etc/sssd/sssd.conf

chmod 0600 /etc/sssd/sssd.conf

restorecon /etc/sssd/sssd.conf

**NSS/PAM Configuration**

Depending on your distribution you have different options how to enable SSSD.

**Fedora/RHEL**

Use authconfig to enable SSSD, install oddjob-mkhomedir to make sure home directory creation works with SELinux:

authconfig --enablesssd --enablesssdauth --enablemkhomedir --update

**Debian/Ubuntu**

Install libnss-sss and libpam-sss to have SSSD added as NSS/PAM provider in /etc/nsswitch.conf and /etc/pam.d/common-\* configuration files. Add pam\_mkhomedir.so to PAM session configuration manually. Restart SSSD after these changes.

**Configure NSS/PAM manually**

Manual configuration can be done with the following changes. The file paths for PAM in the example below are from Debian/Ubuntu, in Fedora/RHEL corresponding manual configuration should be done in /**etc/pam.d/system-auth** and **/etc/pam.d/password-auth.**

**/etc/pam.d/common-auth**

Right after the pam\_unix.so line, add

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

**/etc/pam.d/common-account**

Right after the pam\_unix.so line, add

account [default=bad success=ok user\_unknown=ignore] pam\_sss.so

**/etc/pam.d/common-password**

Right after the pam\_unix.so line, add

password sufficient pam\_sss.so use\_authtok

**/etc/pam.d/common-session**

Just before the pam\_unix.so line, add

session optional pam\_mkhomedir.so

**Right after the pam\_unix.so line, add**

session optional pam\_sss.so