www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

Authenticating Linux users using Active Directory

1. First, you will need to install Samba and Winbind on your target Linux machine. This would be obtained by either using yum if on a RHEL/CentOS distribution or apt-get on a Debian/Ubuntu distribution.

For example:

```
# yum install samba
# yum install winbind
```

2. Once these packages are installed, we'll now configure the Linux system. First, we need to modify the file /etc/nsswitch.conf. Typically this file has something like this for password authentication:

```
passwd: files
shadow: files
group: files
```

Basically, this is saying to use local files on the system to authenticate users. We need to change these lines to use winbind in addition to local files. That way local users like root can still authenticate and login to the system. Change those lines to read as follows:

```
passwd: files winbind
shadow: files winbind
group: files winbind
```

3. Now we need to configure Winbind to play nicely with Active Directory. Modify the /etc/samba/smb.conf file to read something like this:

```
[global]
winbind separator = +
winbind cache time = 10
workgroup = <DOMAIN>
password server = <DOMAIN CONTROLLER1> <DOMAIN CONTROLLER2>
winbind use default domain = yes
realm = <DOMAIN.TLD>
security = ads
encrypt passwords = yes
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
```

www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

template shell = /bin/bash
template homedir = /home/%D/%U

In the above example, set your workgroup to be your domain, domain controller1 and domain controller2 should be the IP address of your domain controllers. You could also use host names, but I prefer to use IP addresses in case DNS fails for some reason. The realm parameter needs to be your domain suffix. (e.g. company.com or company.net)

4. After that, now you will need to join the Linux server to the domain as a computer. This is an important step, as Active Directory will disregard requests for authentication for computers not joined to the domain. NOTE: You will need to have a Domain Administrator account to perform this action.

net ads join –U <username>

You will be prompted for your Windows password. Enter that, and then you should see a confirmation message that the machine has been joined to the domain.

5. Now you can start winbind. Typically this is done by using the “/etc/init.d/winbind start” command or the “service winbind start” command depending on which Linux distribution you are using.

6. Next, backup your /etc/pam.d directory, as we will be making changes to the PAM authentication configuration and it’s important to back up what you currently have. If you make a mistake, there’s a possibility that no one will be able to login to the machine, so having a backup can save you a lot of work!

7. Now insert the following lines into any service that you want to control with AD Authentication:

auth sufficient pam_winbind.so
account sufficient pam_winbind.so
password sufficient pam_winbind.so use_authtok

And also, if you want home directories to be created automatically when a user first logins into the system, add this line to /etc/pam.d/system-auth:

session required pam_mkhomedir.so skel=/etc/skel umask=0022

8. That’s it! Users should be able to login to the Linux system using their Windows Active Directory account and if you have the automatic home directory configuration installed, it will create a directory in /home/DOMAIN/username for them. Make sure you have created the /home/DOMAIN directory first!