añadir Linux AD net ads tutorial

dominio patosa.com

Controlador de dominio
winser2012AD → 172.16.0.201
cliente linux
clienteWin2012 → 172.16.0.110

Lo primero de todo le ponemos nombre a la maquina:

hostnamectl set-hostname clienteWin2012

instalamos resolvconf para poder establecer el controlador de dominio como DNS y que no nos lo machaque otro programa

apt install resolvconf

y configuramos nuestro DNS

cat /etc/resolvconf/resolv.conf.d/head
domain patosa.com
search patosa.com
nameserver 172.16.0.201
nameserver 8.8.8.8

cat /etc/resolv.conf
Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
domain patosa.com
search patosa.com
nameserver 172.16.0.201
nameserver 8.8.8.8
nameserver 192.168.0.1

iniciamos servicio, por defecto estará habilitado pero no levantado
systemctl status resolvconf.service
systemctl start resolvconf.service

comprobamos que ha modificado nuestro archivo /etc/resolv.conf

modificamos el archivo /etc/hosts

cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 clienteWin2012.patosa.com clienteWin2012
172.16.0.201 winser2012AD.patosa.com winser2012AD

The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

Establecemos ip estatica:

cat /etc/network/interfaces
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet static
address 172.16.0.110/24

reiniciamos la red:
systemctl restart networking

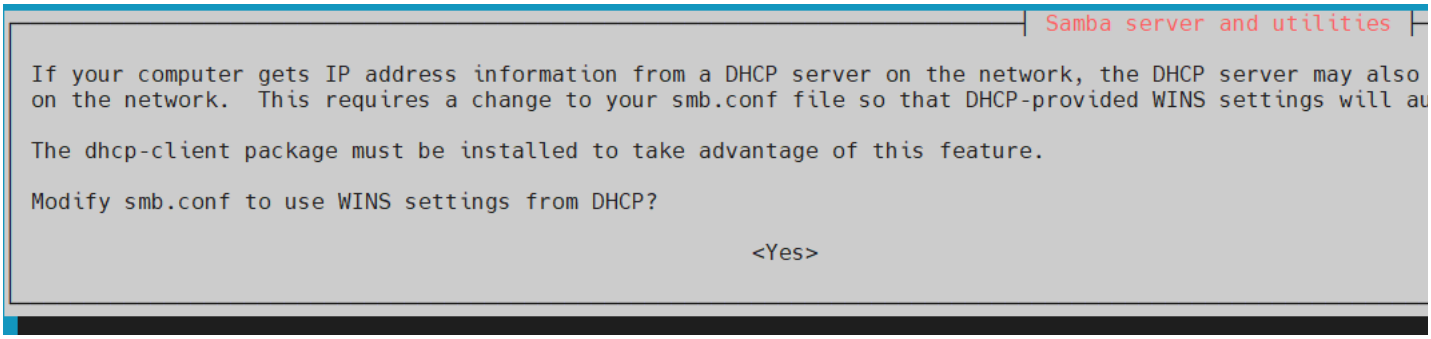
comprobamos la ip
ip address

comprobamos que podemos acceder al controlador de dominio

ping winser2012AD

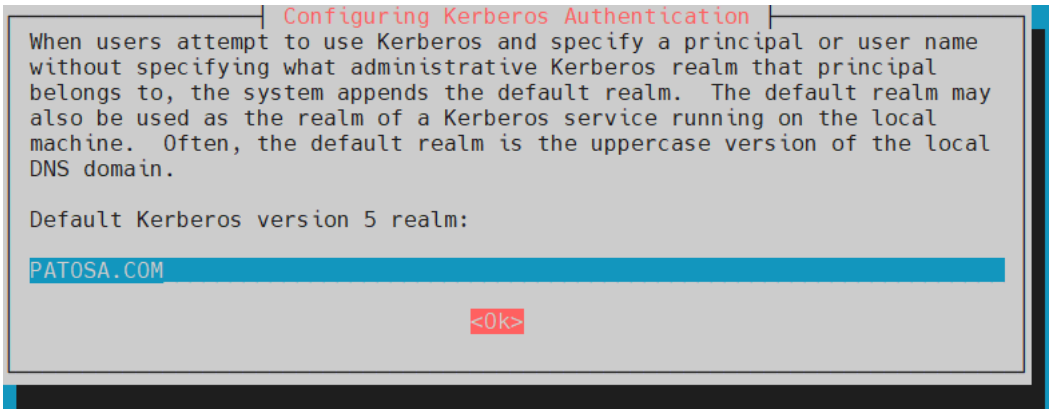
actualizamos lista paquetes
apt update

instalamos software necesario:
apt-get -y install ntp vim ntpdate winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user



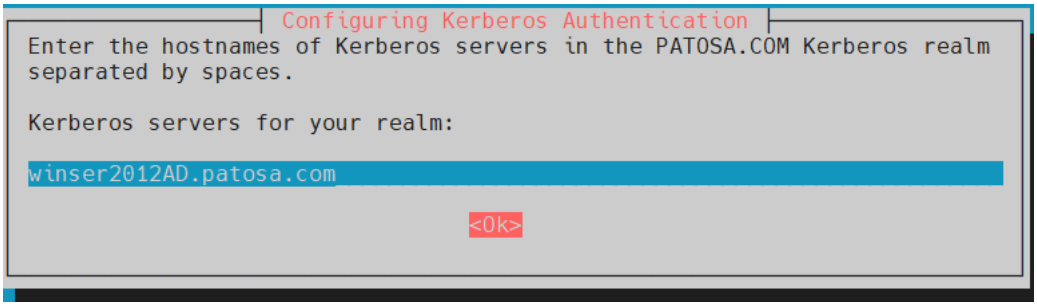
no queremos recuperar información de ningun DHCP

Nos preguntará sobre la configuración de kerberos:



ponemos nuestro dominio patosa.com en mayúsculas

También nos preguntará por el kerberos server (nuestro controlador de dominio)



igual cuando nos pregunte por el kdc server

editamos /etc/ntp.conf
cambiamos todos los pool por:
pool winser2012AD.patosa.com

service ntp restart

modificamos nuestro fichero de configuración de kerberos:

cp /etc/krb5.conf /etc/krb5.conf_original

Lo editamos y dejamos como sigue:

[libdefaults]
default_realm = PATOSA.COM
dns_lookup_realm = true
dns_lookup_kdc = true
renew_lifetime = 7d

[realms]

PATOSA.COM = {
kdc = winser2012AD.PATOSA.COM:88
admin_server = winser2012AD.PATOSA.COM:464
default_domain = PATOSA.COM

}

[domain_realm]
.PATOSA.COM = winser2012AD.PATOSA.COM
PATOSA.COM = winser2012AD.PATOSA.COM
[appdefaults]
pam = {
debug = true

ticket_lifetime = 36000
renew_lifetime = 36000
forwadable = true
krb4_convert = false
}
[loggin]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmin.log

comprobamos que nos podemos autenticar con un usuario del active directory:
kinit administrador
Password for administrador@PATOSA.COM:

Si no nos da error, es que ha ido todo bien.

Si ejecutamos klist, comprobamos que se nos ha creado un ticket:
klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrador@PATOSA.COM

Valid starting Expires Service principal
02/03/21 07:32:04 02/03/21 17:32:04 krbtgt/PATOSA.COM@PATOSA.COM

renew until 09/03/21 07:31:38

modificamos la configuracion de nuestro samba:
cp /etc/samba/smb.conf /etc/samba/smb.conf_original

dejamos la sección [global] como sigue:
[global]
workgroup = PATOSA
security = ADS
realm = PATOSA.COM
encrypt passwords = yes
idmap config * : backend = tdb
idmap config * : range = 2000-3000
winbind trusted domains only = no
winbind use default domain = yes
winbind enum users = yes
winbind enum groups = yes
winbind refresh tickets = 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
idmap uid = 2000-29999
idmap gid = 2000-29999
dedicated keytab file = /etc/krb5.keytab
kerberos method = secrets and keytab
winbind refresh tickets = yes

winbind nss info = rfc2307

modificamos el archivo nsswitch.conf

cat /etc/nsswitch.conf
passwd: compat winbind
group: compat winbind
shadow: compat winbind
gshadow: files
.
.
.

Es posible que al reiniciar los servicios de samba
service smbd restart
service nmbd restart
service winbind restart
nos aparezca el siguiente error:

cat /var/log/samba/log.smbd
.
.
ERROR: failed to setup guest info.

resolucion
groupadd nobody
net -s /dev/null groupmap add sid=S-1-5-32-546 unixgroup=nobody type=builtin
Successfully added group nobody to the mapping db as a wellknown group

nos unimos al dominio

net join ads -U administrador

es posible que nos aparezca el error:

Failed to join domain: failed to find DC for domain ads - {Operation Failed} The requested operation was unsuccessful.

en ese caso ejecutamos:

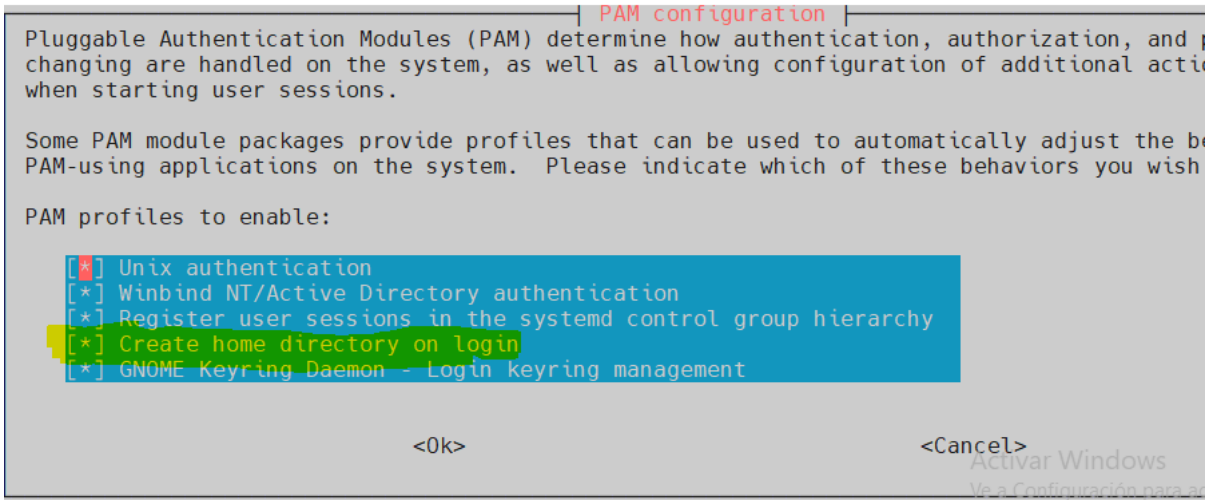
net join ads -U administrador -S winser2012AD.patosa.com

podemos ir a nuestro controlador de dominio y comprobar que nos ha creado la maquina

root@clienteWin2012:~# **wbinfo -g**
could not obtain winbind interface details: WBC_ERR_WINBIND_NOT_AVAILABLE
could not obtain winbind domain name!
failed to call wbcListGroups: WBC_ERR_WINBIND_NOT_AVAILABLE
Error looking up domain groups

ejecutamos:

pam-auth-update



reiniciar los servicios de samba
service smbd restart
service nmbd restart
service winbind restart

wbinfo -g
winrmremotewmiusers__
equipos del dominio
controladores de dominio
administradores de esquema
administradores de empresas
.
.

wbinfo -u
administrador
invitado
krbtgt
jernesto
usuariodominio

en estos momento es muy probable que no nos deje loguearnos en modo grafico, rebotamos la máquina y probamos: