Configurando Ldap y Samba como PDC(Primary Domain Controller) en CentOS 4.4

Autores:

- Roberth Figueroa
- Camilo Solis

INDICE

1. **Requisitos**
2. **Configurando LDAP :**
3. **Configurando Samba:**

1. Requisitos

En nuestro caso utilizamos paquetes rpm para nuestra configuracion, a continuacion detallamos todos los paquetes necesarios para tener exito en el trabajo.

- **Paquetes necesarios para OpenLdap**

  nss_ldap-226-13
  php-ldap-4.3.9-3.15
  openldap-devel-2.2.13-6.4E
  openldap-servers-sql-2.2.13-6.4E
  python-ldap-2.0.1-2
  compat-openldap-2.1.30-6.4E
  openldap-servers-2.2.13-6.4E
  openldap-clients-2.2.13-6.4E
  openldap-2.2.13-6.4E
  mod_authz_ldap-0.26-2

- **Paquetes necesarios para Samba**
  samba-client-3.0.10-1.4E.9
  samba-common-3.0.10-1.4E.9
  samba-3.0.10-1.4E.9
  samba-swat-3.0.10-1.4E.9
  system-config-samba-1.2.21-1

- Como informacion adicional cabe senalar que utilizamos la distribucion Centos 4.4 con Kernel 2.6.9-42.ELsmp.
- Una vez instalado todos los paquetes necesarios comenzaremos nuestra configuracion, paso a paso y con mucha paciencia para tener exito.

2. Configurando LDAP :

Luego de tener completa los requisitos, editamos el archivo slapd.conf que incluya las librerias del schema, hacemos un vi al archivo siguiente:

 # vi /etc/openldap/slapd.conf

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/misc.schema
```

Ademas cambiamos el suffix, rootdn y el rootpw, como a continuacion lo mostramos y guardamos los cambios:

```
suffix "dc=duke,dc=com"
rootdn "cn=Manager, dc=duke, dc=com"
rootpw secret
```

Despues cambiamos el directorio de la herramienta de migracion y migramos todos los datos de

autenticacion a LDAP en migrate_common.ph, ubicado en: /usr/share/openldap/migration/migrate_common.ph

Cambiamos las variables con nuestro
$DEFAULT_MAIL_DOMAIN = "duke.com";
$DEFAULT_BASE = "dc=duke,dc=com";

Haga una prueba corriendo el **migrate_all_offline.sh**
Antes de cada migracion debera borrar todos del **/var/lib/ldap.**
./migrate_all_offline.sh
Baya a vi /etc/protocols y comente el protocolo **tp++**, luego al vi /etc/services y comente **whois++** (ambos udp,tcp) y finalmente comente el **echo 4/ddp**

Cree el archivo netgroup: touch /etc/netgroup, realice:
rm -f /var/lib/ldap/*
./migrate_all_offline.sh
Liste los archivos y cambiar los permisos si es necesario:
ls -l /var/lib/ldap
chown -R ldap.ldap /var/lib/ldap
Comienza el servicio ldap:
service ldap start
chkconfig ldap on
tail /var/log/messages

Finalmente veras el servicio funcionando con exito(sucessful)
Ahora la autenticacion con LDAP
authconfig

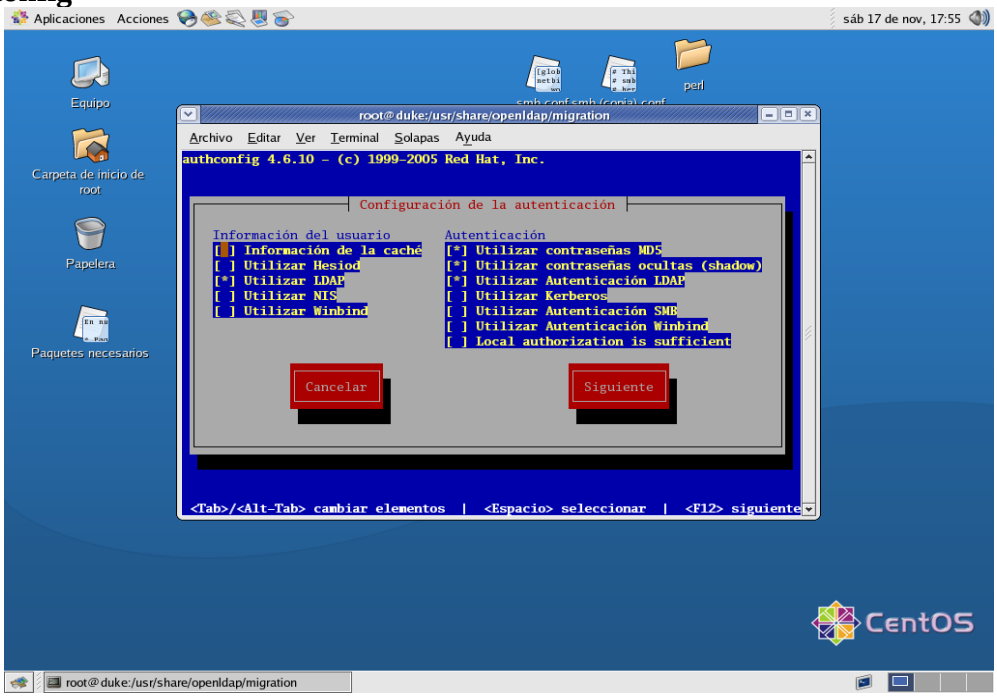

Figura 1: authconfig (asiganacion de permisos LDAP)

Aqui la pantalla
y prueba el servicio con un usurio (en nuestro caso fue tux1)

Login: tux1
Password: tux1

Aqui una prueba con su [tu usuario]. Puedes utilizar otra consola

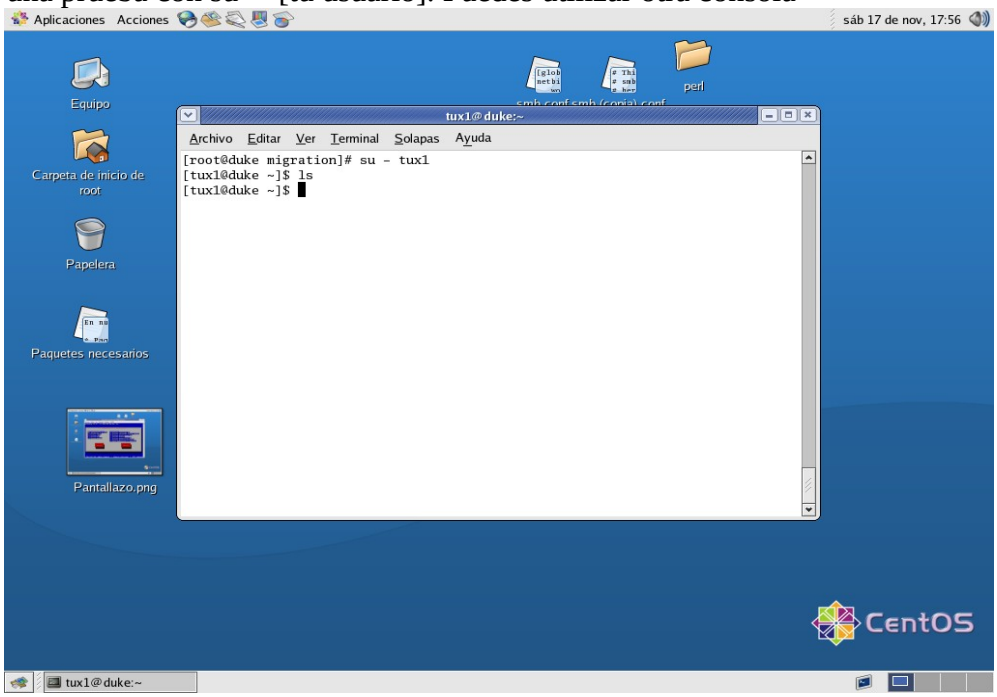

Figura 2: prueba de ldap (comando su - ***usuario***)

3. Configurando Samba:

En este inicio asumimos que no tienes instalado ningun servidor samba previo, si este es el caso, deberas utilizar los siguientes comandos para eliminar los usuarios, el grupo y no tener inconvenientes.

Borramos los usuarios y removemos el contenido de los respectivos directorios:
userdel -r samba1
userdel -r samba2
rm -fr /home/samba*
rm -fr /home/profiles/samba*
vi /etc/samba/smbusers

Ademas deberas remover el grupo(si existiere), utilizando el siguiente comando:
groupdel samba

Como primer paso deberas detener el servicio de Ldap
service ldap stop
Deberas instalar modulos perl adicionales Net::LDAP , ademas de los siguientes RPMs:
perl-Convert-ASN1
perl-Authen-SASL
perl-IO-Socket
perl-Net-SSLeay
perl-Digest-SHA1 (viene incluido en la distro)
perl-Digest-HMAC (viene incluido en la distro)

Copiar el esquema Samba Ldap al directorio correcto:
cd /usr/share/doc/samba-version/LDAP
cp samba.schema /etc/openldap/schema

Instalar el smbldap-tools:
fedora/redhat# cd /usr/share/doc/samba-version/LDAP/smbldap-tools
cp smbldap* /usr/local/sbin
chmod 750 /usr/local/sbin/smbldap*.pl
cd mkntpwd
make
cp mkntpwd /usr/local/sbin

Configuramos el Servidor OpenLdap para el correcto esquema de usuarios Ldap:
slappasswd -h {MD5}
password: **xx**
nuevamente colocar el password**: xx**
{MD5}JVjCcT8HpBD5QpncQEv/tg== (el resultado, deberas copiar y pegarlo como en rootpw se indica)
vi /etc/openldap/slapd.conf
Anadimos la linea:
include /etc/openldap/schema/samba.schema
Colocamos el control de acceso:
access to attrs=SambaLMPassword,SambaNTPassword
by dn="cn=duke,dc=lx26,dc=com" write
by * none
access to *
by dn="cn=Manager,dc=duke,dc=com" write
by * read
Configuramos el suffix:
suffix "dc=duke,dc=com"
rootdn "cn=Manager,dc=lx26,dc=com"
schemacheck off (si usas OpenLdap 2.2)
Pegamos la password encriptada asi:
rootpw {MD5}JVjCcT8HpBD5QpncQEv/tg==
Adicionamos los indices:
index sambaSID eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
index default sub
Asegurate que el /var/lib/ldap directorio este vacio:
ls /var/lib/ldap
rm -f /var/lib/ldap/*
Reiniciamos el servicio:
service ldap start
tail -50 /var/log/messages
chkconfig ldap on

Configuramos el OpenLDAP clientes:
vi /etc/openldap/ldap.conf

HOST 127.0.0.1
BASE dc=duke,dc=com

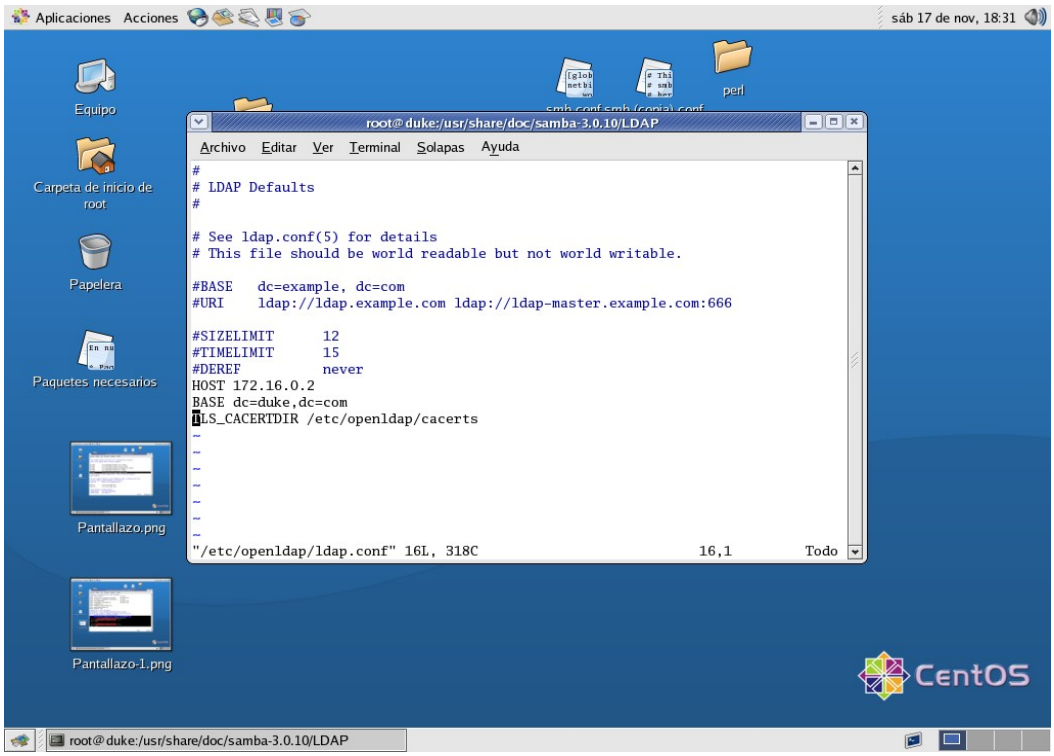

Figura 3: Vista de pasos anteriores del archivo ldap.conf

Configuramos el smbldap-tools:

/usr/local/sbin
net getlocalsid
seleccionas el SID
vi smbldap_conf.pm y adicionar los cambios que siguen:
$suffix = "dc=duke,dc=com";
$usersou = q(People);
$computersou = q(Computers);
$groupsou = q(Groups);
$bindpassword = "xx";
$_userLoginShell = q(/bin/bash);
$_userHomePrefix = q(/home);
$_userGecos = q(Samba User);
$_userSmbHome = q(\\\\duke\\homes);
$_userProfile = q(\\\\duke\\profiles\\);
$_userHomeDrive = q(H:);
chmod 640 smbldap_conf.pm (damos permisos)
Poblamos la base de LDAP
smbldap-populate.pl
vemos que todos archivos existan:

slapindex -f /etc/openldap/slapd.conf

Modificamos el uidNuember del Admistrador a 0 y colocamos el grupo secundario a 512 y 544, colocamos el password del Admistrador en **xx**

smbldap-usermod.pl -u 0 Administrator
smbldap-usermod.pl -G 512,544 Administrator
smbldap-passwd.pl Administrator
password**:xx**
reiteramos el password:**xx**
Verificamos los contenidos de Ldap
slapcat | less
ldapsearch -x -LLL "(uid=Administrator)"(deberias ver la cuenta Administrator)
Vemos que existan la autenticacion de LDAP:
authconfig (como en la Figura 1)
modificamos las siguientes lineas con nuestros datos en /etc/ldap.conf:
vi /etc/ldap.conf
nss_base_passwd dc=duke,dc=com?sub
nss_base_shadow dc=duke,dc=com?sub
nss_base_group ou=Groups,dc=duke,dc=com?one

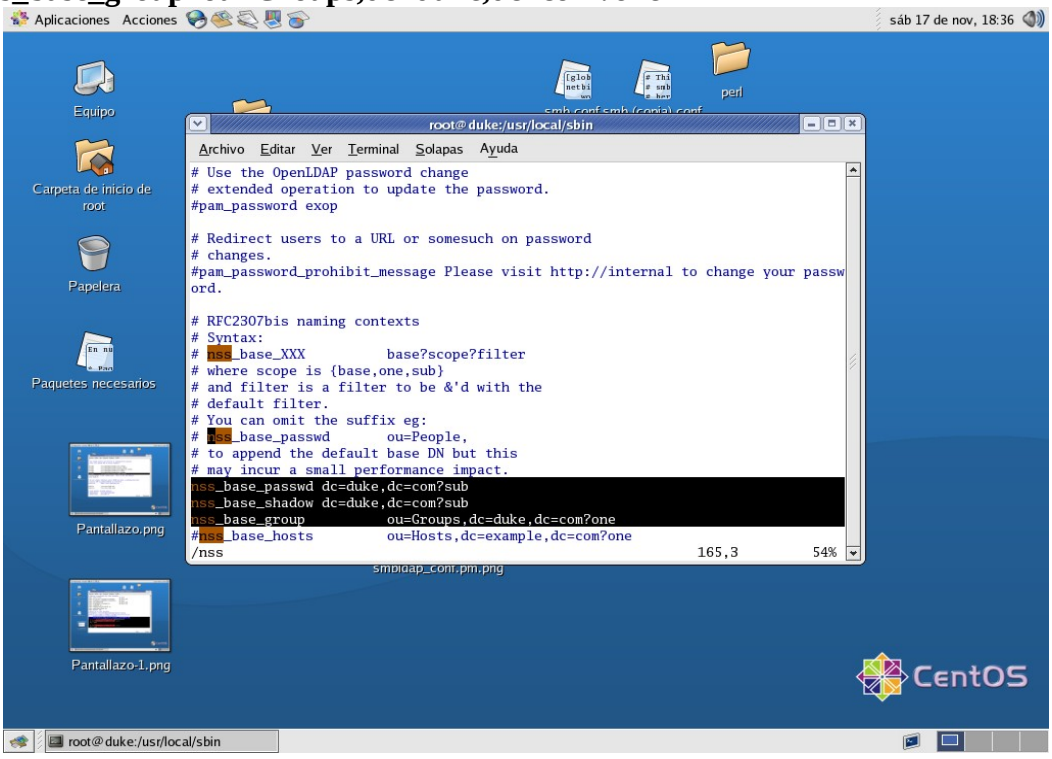

Figura 4. Modificando archivo /etc/ldap.conf

Verificamos que la autenticacion utilice LDAP
cat /etc/passwd (No verias la cuenta Administrator y nobdy)
getent passwd (Deberias ver las cuentas Administrator y nobdy)

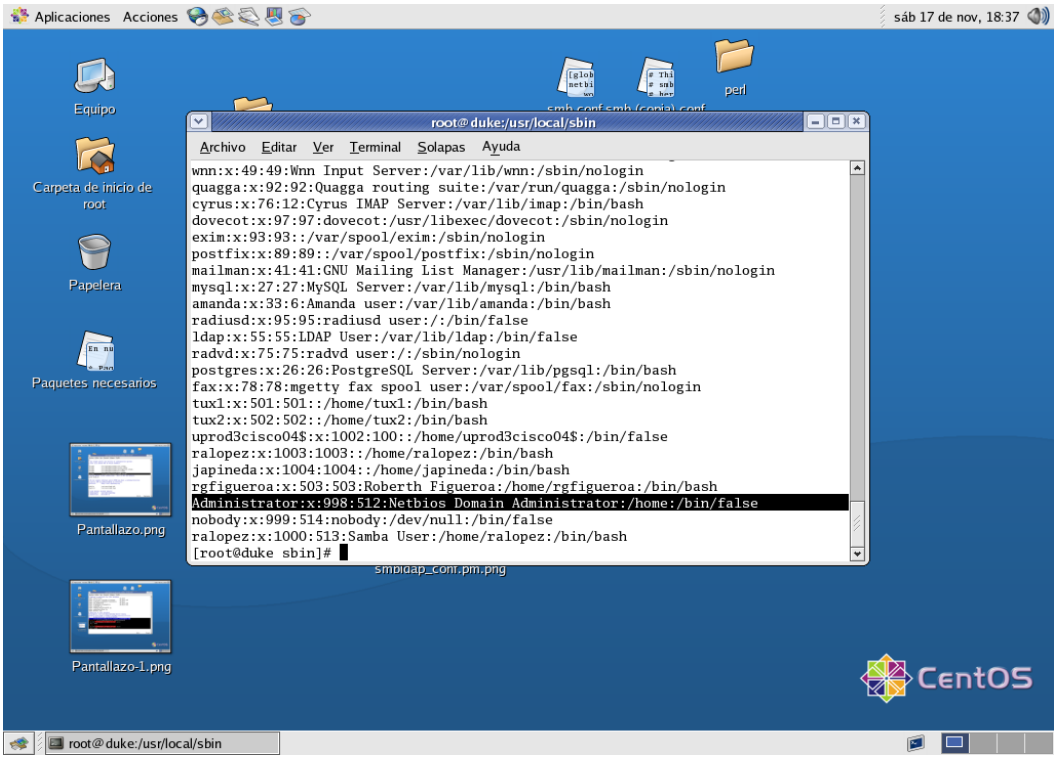

Figura 5. Ejecucion comando **getent**

Adicionamos las cuentas a samba con:

smbldap-useradd.pl -a -m samba1
smbldap-useradd.pl -a -m ralopez
smbldap-passwd.pl samba1
smbldap-passwd.pl samba2

Logearse en otra consola como samba1

Login: samba1
Password: samba1

Configuramos Samba para usar LDAP

vi /etc/samba/smb.conf
eliminar **username map smbpasswd file**

Adicionamos en la seccion [global]:

ldap admin dn = "cn=Manager,dc=duke,dc=com"
ldap ssl = none
passdb backend = ldapsam:"ldap://duke"
ldap delete dn = no
ldap suffix = dc=duke,dc=com
ldap user suffix = ou=People
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers

Adicionamos los comandos relacionados para anadir y eliminar cuentas de usuario, grupo y maquinas:

**add machine script = **

/usr/local/sbin/smbldap-useradd.pl -w %u
**add user script = **
/usr/local/sbin/smbldap-useradd.pl -m %u
**delete user script = **
/usr/local/sbin/smbldap-userdel.pl %u
**set primary group script = **
/usr/local/sbin/smbldap-usermod.pl -g %g %u
**add group script = **
/usr/local/sbin/smbldap-groupadd.pl %g
**delete group script = **
/usr/local/sbin/smbldap-groupdel.pl %g
**add user to group script = **
/usr/local/sbin/smbldap-groupmod.pl -m %u %g
**delete user from group script = **
/usr/local/sbin/smbldap-groupmod.pl -x %u %g

Luego probamos la sintaxis con:
testparm
Almacenamos el password del Openldap a Samba in el archivo secrets.tdb, ejecutando el
smbpasswd -w ibmlnx

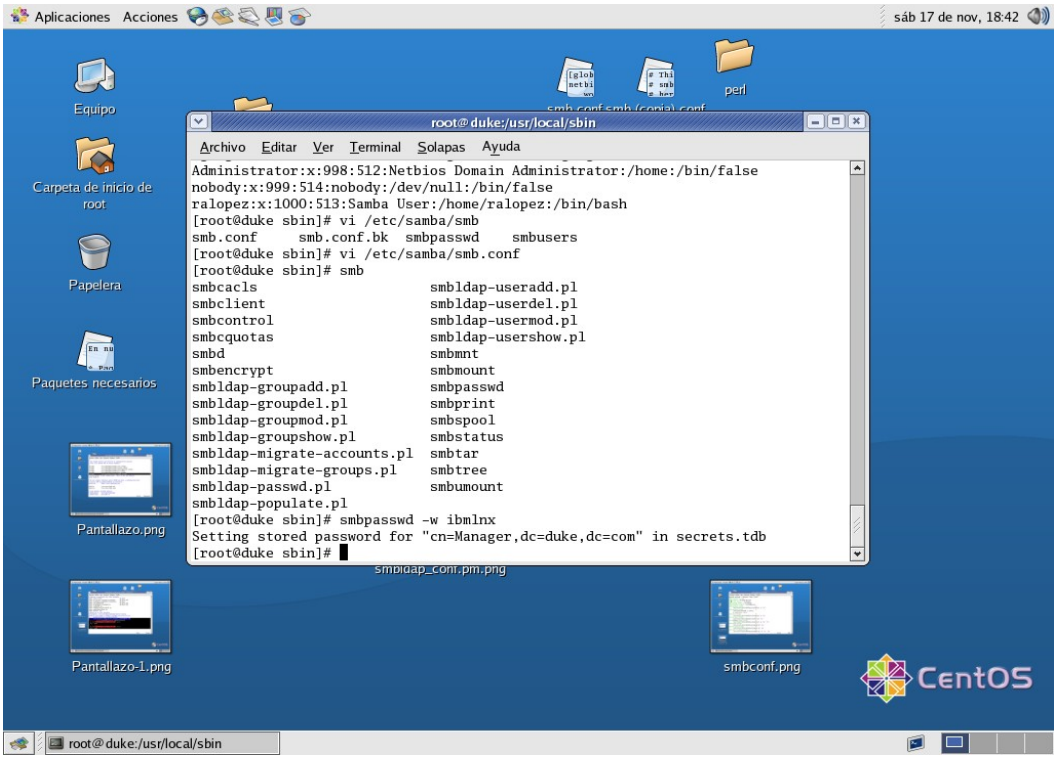

Figura 5. Ejecucion comando **smbpasswd -w ibmlnx**

Reiniciamos el servicio de Samba
service smb restart
Opcionalmente podemos verificar la instalcion con:
Probamos la instalacion de Samba con:
pdbedit -Lv ralopez

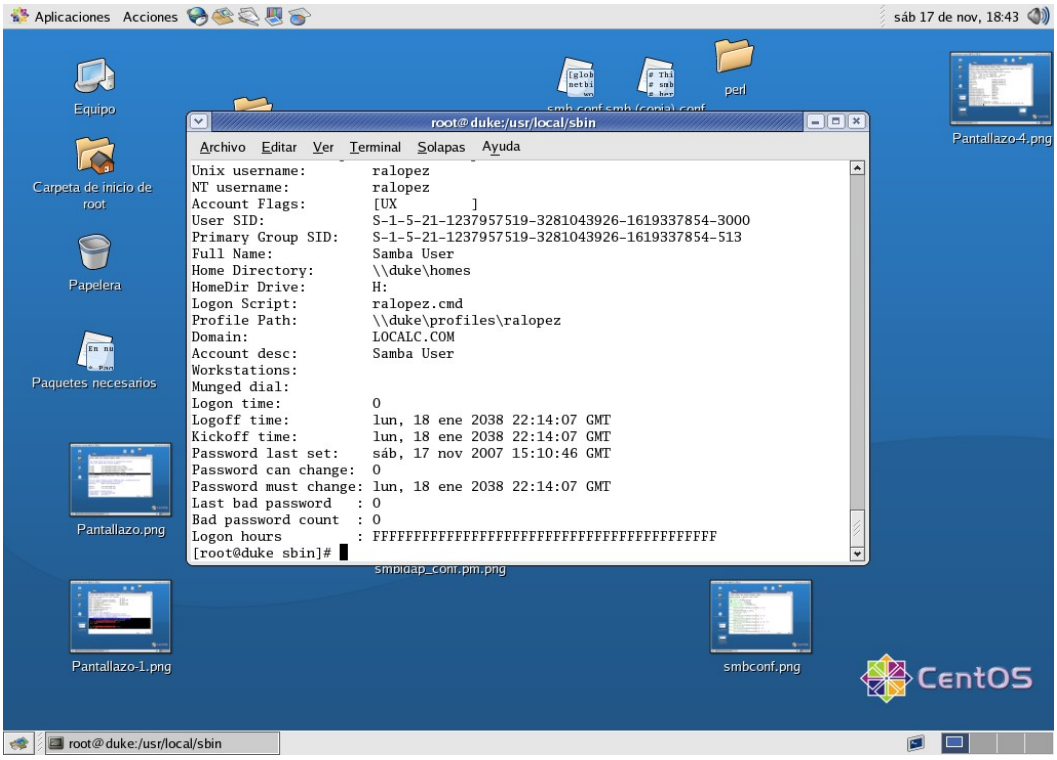

Figura 6. Visualizacion de informacion del usuario ralopez

smbclient -L localhost -U samba1%samba1

Si todo esta bien, podras probarlos desde cualquier otro sistema y anadirse a tu dominio PDC.