

INSTALACION SERVIDOR SAMBA ACTIVE DIRECTORY.

S.O: OpenSuSE 10.1

Hardware: Dell PowerEdge 850, Intel Dual Core 3,00 Ghz, 1024 RAM, 2x160 SATA RAID 0

1.-Via Yast instalamos todos los paquetes samba a excepción del samba-vscan y el cliente kerberos.

2.-Resolución de nombres-IP

Según recomendación de Microsoft para una instalaciones de Active Directory (AD) es necesario tener definido un DNS donde resolver los nombre a direcciones IP (para este instructivo consideramos que no tenemos DNS) es por ello que debemos modificar el /etc/hosts e incluir las IP de la maquina que es servidor de dominio (mail-server) y la maquina cliente que en este caso es mi maquina (dataserver)

```
192.168.1.80  dataserver dataserver.prueba
192.168.1.81  mail-server mail-server.prueba
```

3.- Configuración cliente kerberos. Como root, editaremos /etc/krb5.conf para que quede similar a esto:

```
[libdefaults]
    default_realm = PRUEBA.LOCAL
    clockskew = 300
    ticket_lifetime = 24000
    dns_lookup_realm = false
    dns_lookup_kdc = false
[realms]
PRUEBA.LOCAL = {
    kdc = 192.168.1.81
    default_domain = prueba.local
    admin_server = 192.168.1.81
}
prueba.local = {
    kdc = 192.168.1.81
    default_domain = prueba.local
    admin_server = 192.168.1.81
}

prueba = {

    kdc = 192.168.1.81
    default_domain = prueba
    admin_server = 192.168.1.81
}
[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON
[domain_realm]
    .prueba = prueba
    .prueba.local = PRUEBA.LOCAL
[appdefaults]
```

```
pam = {  
    ticket_lifetime = 1d  
    renew_lifetime = 1d  
    forwardable = true  
    proxiable = false  
    retain_after_close = false  
    minimum_uid = 0  
    try_first_pass = true  
}
```

4.- Creamos los tickets kerberos. En la opción **[libdefaults]** del fichero anterior se ha añadido **ticket_lifetime = 24000** que prolonga la vida del ticket kerberos.

```
kinit Administrador@prueba
```

Nos pide el password del dominio.

Errores comunes:

"Clock skew" : Debemos sincronizar los relojes de ambos servidores. En este punto es recomendable sincronizar con `rdate` los relojes, por ejemplo con el servidor de rediris: `hora.rediris.es`

```
5.-linux-xse1:/ #
```

```
[root@dataserver] klist
```

```
Ticket cache: FILE:/tmp/krb5cc_0
```

```
Default principal: Administrador@PRUEBA.LOCAL
```

```
Valid starting Expires Service principal
```

```
09/14/06 10:25:33 09/14/06 20:25:36 krbtgt/PRUEBA.LOCAL@PRUEBA.LOCAL
```

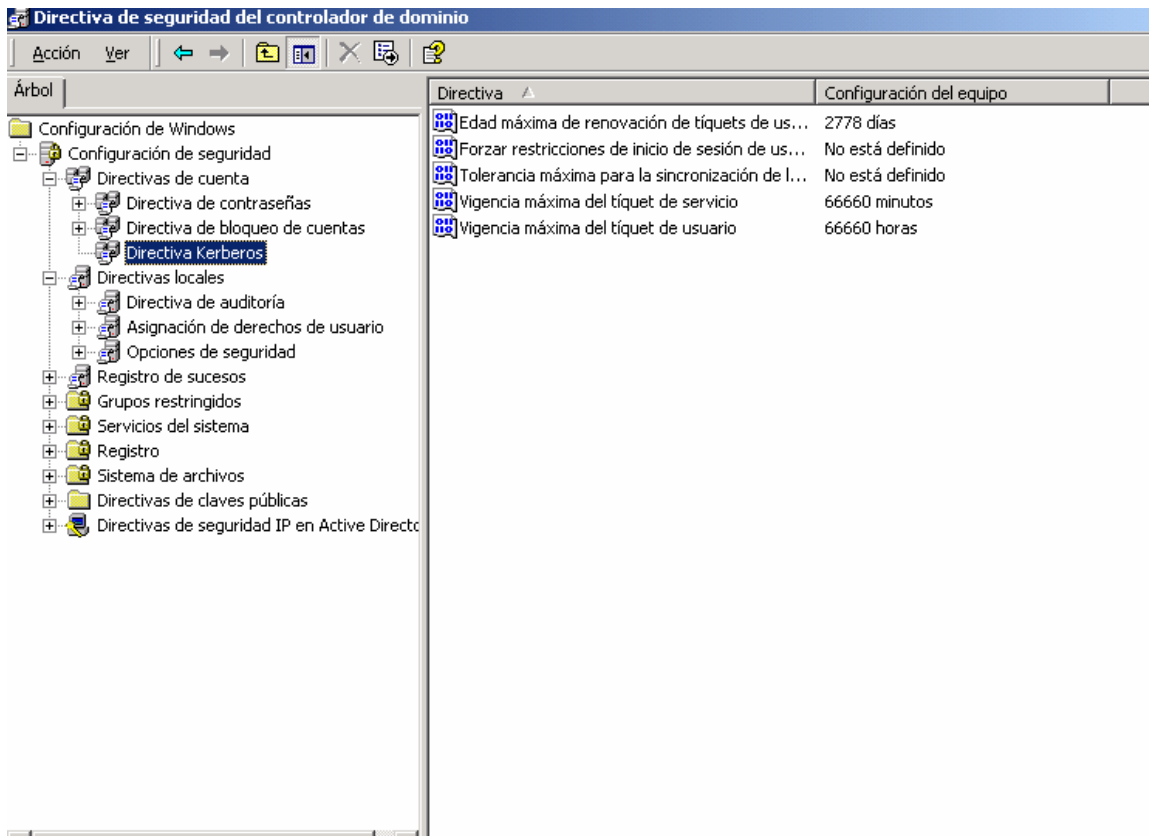
```
renew until 09/15/06 10:25:33
```

```
Kerberos 4 ticket cache: /tmp/tkt0
```

```
klist: You have no tickets cached
```

Ahora podemos ver los tickets kerberos.

Me he encontrado con un problema a la hora de renovar los tickets Kerberos. Por defecto Windows 2000 envía tickets por 10 horas, con lo cual, pasado ese tiempo, debemos pedir otro ticket, impidiendo el acceso al Servidor Linux que hemos configurado. ¿Cómo solucionamos este tema? En el servidor Windows 2000, nos vamos a Inicio/Programas/Herramientas Administrativas/Directiva de Seguridad de Controlador de Dominio, y cambiamos los parámetros por unos similares a los que podemos ver en esta captura de pantalla:



Aparte del comando **kinit**, existe otro llamada **kdestroy** que elimina los **tickets kerberos**. He eliminado el que tenía con kdestroy. A continuación he pedido de nuevo tickets pero con el parámetro **-l** (que indica el lifetime) :

```
[root@dataserver] kdestroy
```

```
[root@dataserver] kinit -l 365d administrador@PRUEBA.LOCAL
```

Los parámetros de kinit y kdestroy vienen en el man, pero si no lo teneis instalado, os dejo unos links que me han ayudado:

<http://www.die.net/doc/linux/man/man1/kinit.1.html>

<http://www.die.net/doc/linux/man/man1/kdestroy.1.html>

6.- Winbind, para poder autenticarnos contra el dominio active directory, en el fichero /etc/nsswitch.conf, debemos tener algo como esto:

```
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be #
sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an # entry
should stop if the search in the previous entry turned # up nothing. Note
that if the search failed due to some other reason # (like no NIS server
responding) then the search continues with the # next entry.
#
# Legal entries are:
#
#         compat                Use compatibility setup
#         nisplus               Use NIS+ (NIS version 3)
#         nis                   Use NIS (NIS version 2), also called YP
#         dns                   Use DNS (Domain Name Service)
#         files                 Use the local files
#         [NOTFOUND=return]     Stop searching if not found so far
#
# For more information, please read the nsswitch.conf.5 manual page.
#

# passwd: files nis
# shadow: files nis
# group:  files nis

passwd:    compat winbind
group:     compat winbind
shadow:    compat winbind
hosts:     files dns winbind
networks:  files

services:  files
protocols: files
rpc:       files
ethers:    files
netmasks: files
netgroup:  files nis
publickey: files

bootparams: files
automount:  files nis
aliases:    files
```

7.- Samba.

Fichero smb.conf

```
[global]
unix charset = LOCALE
workgroup = prueba
server string = dataserver
security = domain
auth methods = winbind
```

Validación Samba contra Active Directory -- Version Beta

```
update encrypted = yes
obey pam restrictions = yes
password server = 192.168.1.81
username map = /etc/samba/smbusers
log level = 1
syslog = 0
log file = /var/log/samba/log.%m
max log size = 0
add user script = /usr/sbin/useradd -m '%u'
add group script = /usr/sbin/groupadd '%g'
add machine script = /usr/bin/useradd -M '%u'
os level = 0
preferred master = no
domain master = no
dns proxy = no
idmap uid = 10000-29999
idmap gid = 10000-29999
winbind separator = +
winbind use default domain = yes
winbind cache time = 10
template shell = /bin/bash
template home dir = /home/%D/%U
invalid users = root
[homes]
comment = Directorios Home
read only = no
browseable = yes
```

En consola y como root , reiniciamos los servicios.

```
[root@dataserver] rcsmb restart
```

```
[root@dataserver] rcnmb restart
```

8.- PAM

Al realizar esta instalación me he topado con la necesidad de crear automáticamente los directorios /home de cada usuario en el primer inicio de sesión. Ya que por motivos que no puedo explicar en esta receta, a la hora de crear el usuario dentro del Active Directory del Windows 2000 Server, necesitaba que automáticamente, se crease su directorio personal en el servidor Linux. Para ello utilizaremos PAM.

PAM, del inglés ``Pluggable Authentication Modules'', o Módulos de Autenticación Enlazables, permite al administrador del sistema establecer una política de autenticación sin la necesidad de recompilar los programas de autenticación. Mediante PAM, Ud. controla cómo los módulos se conectan a los programas editando un fichero de configuración.

En OpenSuSE 10.1, los ficheros de configuración PAM se localizan en /etc/pam.d. En este caso modificaremos el fichero common-session, y añadimos la siguiente línea.

```
session required          pam_mkhome.so skel=/etc/skel umask=0022
```

Ahora el fichero /etc/pam.d/common-session queda como sigue

```
#
# /etc/pam.d/common-session - session-related modules common to all
# services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive). The default is pam_unix2.
#
session required          pam_limits.so
session required          pam_unix2.so
session required          pam_mkhome.so skel=/etc/skel umask=0077
```

9.- Añadimos la máquina al dominio de Active Directory

```
net ads join -S PRUEBA -U administrador
```

Debemos asegurarnos que winbind está corriendo, lo reiniciamos

```
[root@dataserver] rcwinbind restart
```

Con el comando **wbinfo -u** listamos los usuarios del dominio. Los terminados en \$ son máquinas del dominio.

```
[root@dataserver]wbinfo -u
user
Administrador
Invitado
TsInternetUser
IUSR_MAIL-SERVER
IWAM_MAIL-SERVER
krbtgt
opensuse-dataserver$
ZD8000$
data-server$
```

Validación Samba contra Active Directory -- Version Beta

```
linux-xsel$  
MAIL-SERVER$
```

Con el comando **wbinfo -g** listamos los grupos del dominio.

```
[root@dataserver]wbinfo -g  
Equipos del dominio  
Controladores de dominio  
Administradores de esquema  
AdministraciA  
Publicadores de certificados  
Admins. del dominio  
Usuarios del dominio  
Invitados de dominio  
Propietarios del creador de directivas de grupo  
DnsUpdateProxy  
prueba
```

10.- Creo que no se me olvida nada. Por si acaso he reiniciado el server.

MIRAR: Tema del WINS.

LINKS

http://www.wikilearning.com/autenticacion_de_usuarios_mediante_pam-wkccp-9645-55.htm

http://es.opensuse.org/Active_Directory_Integracion

<http://www.mcpmag.com/columns/article.asp?EditorialsID=858#findit>

<http://www.die.net/doc/linux/man/man1/kinit.1.html>

<http://www.die.net/doc/linux/man/man1/kdestroy.1.html>