01.--> Introducción

A continuación se presenta una guía de todos los pasos que seguí para unir Debian GNU/Linux a un dominio de Active Directory de Windows Server 2003. Para referirnos al equipo Debian GNU/LINUX, de aquí en adelante lo llamaremos "Linux", al equipo con Windows Server 2003 con Active Directory de aquí en lo adelante lo llamaremos "Server".

02.-->Información con la que contamos

Contamos con los siguientes datos:

```
        - Dominio:                      pruebas.local
        - Nombre del Server AD:         ad = ad.pruebas.local
        - IP del Server AD:             192.168.1.254
        - Nombre del Cliente Linux:     debian
        - Ip del Cliente Linux:         192.168.1.20
```

NOTA: En los archivos de configuración utilizaremos estos datos por lo que usted deberá sustituirlos por los apropiados.

03.--> Configurar parámetros de red

Antes de continuar asegúrese de que el equipo con Linux cuente con la siguiente configuración:

```
        - IP del mismo rango que el Server Active Directory
        - DNS utilizado por el Server Active Directory
        - Debe responder el ping a ad.pruebas.local
```

04.--> Instalar la paquetería necesaria:

```
 # aptitude install samba smbclient winbind krb5-user krb5-config
```

05.--> Resolver equipos de la red

Agregar la IP de nuestro equipo Linux y la del Server Active Directory a "/etc/hosts":

```
       192.168.1.20    debian.pruebas.local    debian
       192.168.1.254   ad.pruebas.local         ad
```

06.--> Configurar el cliente kerberos

Para configurar el cliente kerberos agregamos/modificamos las siguientes lineas a "/etc/krb5.conf":

```
[libdefaults]
        default_realm = PRUEBAS.LOCAL
        clockskew = 300

[realms]
        PRUEBAS.LOCAL = {
                kdc = 192.168.1.254
                default_domain = pruebas.local
                admin_server = 192.168.1.254
        }
        pruebas.local = {
```

```
                kdc = 192.168.1.254
                default_domain = pruebas.local
                admin_server = 192.168.1.254
        }
        pruebas = {
                kdc = 192.168.1.254
                default_domain = pruebas
                admin_server = 192.168.1.254
        }

[logging]
        kdc = FILE:/var/log/krb5/krb5kdc.log
        admin_server = FILE:/var/log/krb5/kadmind.log
        default = SYSLOG:NOTICE:DAEMON

[domain_realm]
        .pruebas = pruebas
        .pruebas.local = PRUEBAS.LOCAL

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

07.--> Crear tickets Kerberos

Para crear los tickets kerberos ejecutamos el siguiente comando:

```
# kinit administrador@pruebas.local
```

Nos pedirá el password de la cuenta administrador del dominio. Puede utilizarse cualquier cuenta con permisos administrativos en el dominio.

08.--> Configurar samba

Editamos "/etc/samba/smb.conf" quedando algo parecido a lo siguiente:

```
[global]
 security = ADS
 netbios name = debian
 realm = PRUEBAS.LOCAL
 password server = ad.pruebas.local
 workgroup = PRUEBAS
 log level = 1
 syslog = 0
 idmap uid = 10000-29999
 idmap gid = 10000-29999
 winbind separator = +
 winbind enum users = yes
 winbind enum groups = yes
 winbind use default domain = yes
 template homedir = /home/%D/%U
```

```
  template shell = /bin/bash
  client use spnego = yes
  domain master = no
  server string = linux como cliente de AD
  encrypt passwords = yes

##compartir el home del usuario solo para él cuando se encuentre en otro equipo de la red
  [homes]
         comment = Home Directories
         valid users = %S
         browseable = No
         read only = No
         inherit acls = Yes
  [profiles]
         comment = Network Profiles Service
         path = %H
         read only = No
         store dos attributes = Yes
         create mask = 0600
         directory mask = 0700
##compartir una carpeta para todos los usuarios
  [users]
         comment = All users
         path = /alguna/carpeta
         read only = No
         inherit acls = Yes
         veto files = /aquota.user/groups/shares/
##compartir carpeta solo para el usuario spruebas
[UnUsuario]
         comment = prueba con usuario del dominio
         inherit acls = Yes
         path = /ruta/de/alguna/carpeta/
         read only = No
         available = Yes
         browseable = Yes
         valid users = pruebas+spruebas
```

09.--> Reiniciamos samba:

```
         # testparm
         # /etc/init.d/samba restart
```

10.--> Agregar Linux al dominio:

```
         # net ads join -S ad.pruebas.local  -U administrador
```

Nos deberá mostrar un mensaje como el siguiente:

```
         Using short domain name -- PRUEBAS
         Joined 'DEBIAN' to realm 'PRUEBAS.LOCAL'
```

Si nos llega a mostrar un error como el siguiente:

```
Administrador's password:
[2007/08/25 16:58:33, 0] libsmb/cliconnect.c:cli_session_setup_spnego(785)
Kinit failed: Clock skew too great
Failed to join domain!
```

El problema puede ser que la hora del equipo con Linux no este configurada correctamente. Kerberos es muy estricto con la hora. Para solucionarlo, corregimos la hora manualmente o ejecutamos el siguiente comando:

```
# ntpdate pool.ntp.org
```

Después de hacer esto ya se debería de poder unir al dominio.

11.--> Resolver nombres de usuarios y grupos de dominio

Editar "/etc/nsswitch.conf" y modificar las siguientes lineas dejándolas así:

```
passwd:         files winbind
group:          files winbind
shadow:         files winbind
hosts:          files dns winbind
```

Gracias a las lineas anteriores los usuarios y grupos del dominio pueden ser resueltos.

12.--> Reiniciamos winbind:

```
 # /etc/init.d/winbind restart
```

13.0--> Hacer pruebas para ver si todo salio bien

13.1.--> Verificar la integración del dominio:

- *"net rpc testjoin"* muestra si esta correctamente integrada al dominio:

```
Join to 'PRUEBAS' is OK
```

- *"net ads info"* muestra información del dominio:

```
LDAP server: 192.168.1.254
LDAP server name: ad.pruebas.local
Realm: PRUEBAS.LOCAL
Bind Path: dc=PRUEBAS,dc=LOCAL
LDAP port: 389
Server time: dom, 26 ago 2007 14:57:04 MDT
KDC server: 192.168.1.254
Server time offset: 11
```

- *"net rpc info -U Usuario_de_dominio"* muestra el dominio al que pertenece,
numero de usuarios, grupos, etc:

```
Domain Name: PRUEBAS
Domain SID: x-x-x-xx-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxx
Sequence number: xx
Num users: xx
Num domain groups: xx
Num local groups: xx
```

13.2.--> Verificar que winbind este funcionando:

- *"wbinfo -u"* lista usuarios del dominio.

- *"wbinfo -g"* lista grupos del dominio.

- *"getent passwd"* muestra usuarios locales y del dominio.

- *"getent group"* muestra grupos locales y del dominio.

* *"su usuario-de-dominio"* nos convertimos en usuario-de-dominio.

Si todo lo anterior funciona vamos por buen camino.

14.--> Configurar la autenticación

Para configurar el acceso a usuarios del dominio a nuestro Linux mediante el entorno gráfico hay que configurar pam. Para ello editamos los siguientes archivos y agregamos/modificamos las siguientes lineas:

```
/etc/pam.d/common-account
        account sufficient      pam_winbind.so
        account required        pam_unix.so try_first_pass
/etc/pam.d/common-auth
        auth    sufficient      pam_winbind.so
        auth    required        pam_unix.so nullok_secure try_first_pass
/etc/pam.d/common-password
        password   sufficient   pam_winbind.so
        password   required     pam_unix.so nullok obscure min=4 max=8 md5 try_first_pass
/etc/pam.d/common-session
        session required        pam_mkhomedir.so skel=/etc/skel/ umask=0022
        session sufficient      pam_winbind.so
        session required        pam_unix.so try_first_pass
```

El modulo "pam_winbind.so" le indica a pam que los usuarios y grupos los obtenga mediante winbind. El modulo "pam_mkhomedir.so" nos crea el directoriohome del usuario en caso de no existir.

15.--> Creamos el directorio "/home/PRUEBAS" (Nombre del dominio en MAYÚSCULA) que es donde tendrán sus home los usuarios:

```
        # mkdir /home/PRUEBAS
```

16.--> Comentarios finales

- Ya podemos iniciar sesión con usuarios locales o del dominio de Active Directory en nuestro Linux.

- Para iniciar sesión con un usuario del dominio se hace tecleando solo el nombre de usuario o especificando el dominio+usuario(ejemplo: pruebas+usuariopruebas).

- La guía anterior ha sido probada con éxito en un equipo con Debian GNU/Linux como cliente y en un Windows Server 2003 con Active Directory.

- En el WinServer2003 no fue necesario instalar ninguna aplicación para que en el Administrador de "Usuarios y equipos de Active Directory" en las propiedades de un usuario aparezca la pestaña "Atributos UNIX". La pestaña "Atributos UNIX" no es necesaria.

- No fue necesario configurar nada sobre LDAP.