

Práctica 15b. Implantación del AD en Linux¹

Previamente crearemos un **clon enlazado** de **Debian-Plantilla** que llamaremos **Debian-AD**.

Añadiremos dos tarjetas una en modo NAT y otra en modo Red Interna. La configuración para cada una serán:

Tarjeta	IP	Red	NetMask	Puerta Enlace
NAT	192.168.0.100	-	-	-
Red Interna	192.168.0.101	192.168.0.0	255.255.255.0	192.168.0.100

Instalamos el siguiente servicio para tener la hora correcta en todo momento.

```
# apt-get install ntp
```

```
filegen clockstats file clockstats type day enable
# Specify one or more NTP servers.
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 0.es.pool.ntp.org
server 1.es.pool.ntp.org
server 2.es.pool.ntp.org
server 3.es.pool.ntp.org
# Use Ubuntu's ntp server as a fallback
```

A continuación instalamos Samba4

```
# apt-get install build-essential libacl1-dev python-dev libldap2-dev pkg-config gdb libgnutls-dev
libreadline-dev libattr1-dev python-dnspython libpopt-dev libbsd-dev attr docbook-xsl libcups2-dev
git
```

Luego las fuentes necesarias y compilamos

```
# git clone git://git.samba.org/samba.git /usr/src/samba4/
```

```
# sudo ./configure --enable-debug
```

```
# make
```

```
# make install
```

1 [enlace](#)

y añadiremos el path de las carpeta bin y sbin de samba:

```
# export PATH="/usr/local/samba/sbin:/usr/local/samba/bin:$PATH"
```

Comenzamos el proceso de configuración (ver imagen)

```
root@server:/usr/src/samba4# /usr/local/samba/bin/samba-tool domain provision
Realm: casa.local
Domain [casa]: CASA
Server Role (dc, member, standalone) [dc]: dc
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.2.1]:
Administrator password:
Retype password: _
```

En nuestro caso sera como nombre del dominio *minombre.local*.

A continuación editaremos el archivo **smb.conf** (cuidado, que en lugar de /etc/samba/, lo tenemos en /usr/local/samba/etc!!) y añadimos la opción que los clientes puedan actualizar su registro dns.

```
GNU nano 2.2.6 Archivo: /usr/local/samba/etc/smb.conf Modificado
# Global parameters
[global]
workgroup = CASA
realm = CASA.LOCAL
netbios name = SERVER
server role = active directory domain controller
dns forwarder = 192.168.2.1
allow dns updates = True_
[netlogon]
path = /usr/local/samba/var/locks/sysvol/casa.local/scripts
read only = No
[sysvol]
path = /usr/local/samba/var/locks/sysvol
read only = No
```

A continuación reiniciamos la máquina y cuando iniciamos sesión iniciamos el servicio de samba:

```
# /usr/local/samba/sbin/samba start
```

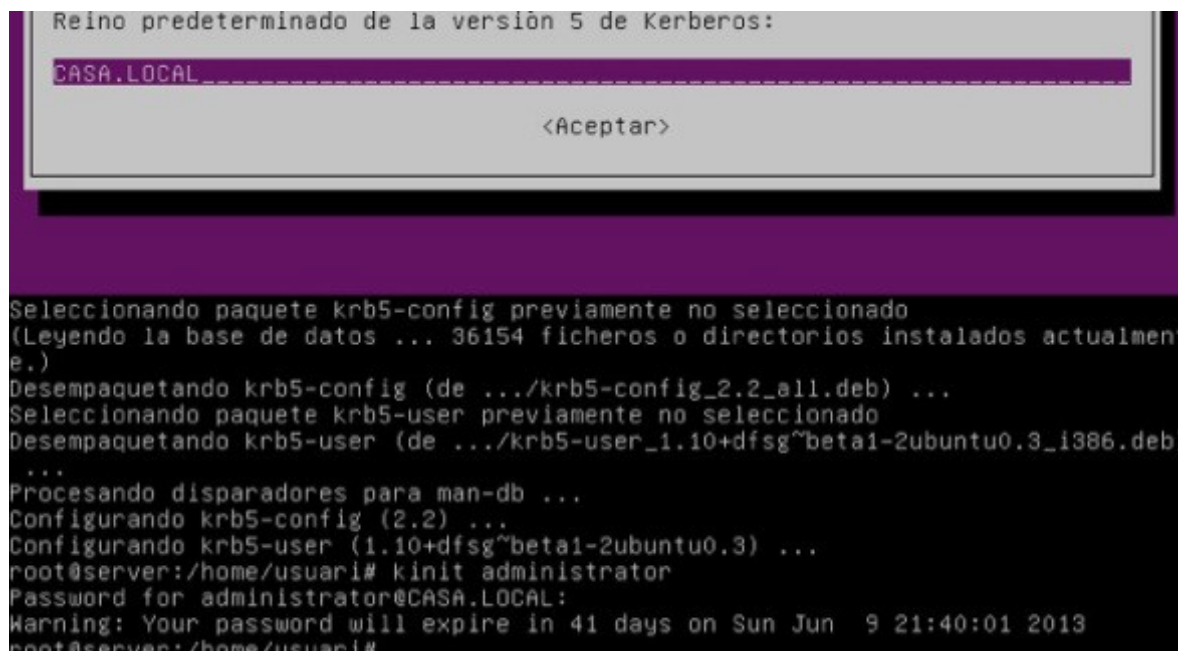
Probamos que todo funciona:

```
root@server:/home/usuario#
root@server:/home/usuario#
root@server:/home/usuario# host -t SRV _ldap._tcp.casa.local.
_ldap._tcp.casa.local has SRV record 0 100 389 server.casa.local.
root@server:/home/usuario# _
```

Ahora probaremos el servicio Kerberos, para ello instalaremos la utilidad de cliente:

```
# apt-get install krb5-user
```

Cuando nos pida el reino Kerberos, deberemos poner el que hemos elegido, **pero muy importante en mayúsculas**. Una vez instalado podemos testear por ejemplo la password de administrador:



The image shows a terminal window with a grey dialog box at the top. The dialog box has a title bar that says "Reino predeterminado de la versión 5 de Kerberos:". Inside the dialog, the text "CASA.LOCAL" is entered in a purple field, followed by a dashed line. Below the field is a button labeled "<Aceptar>". Below the dialog, the terminal shows the following output:

```
Selecionando paquete krb5-config previamente no seleccionado
(Leyendo la base de datos ... 36154 ficheros o directorios instalados actualment
e.)
Desempaquetando krb5-config (de ../krb5-config_2.2_all.deb) ...
Selecionando paquete krb5-user previamente no seleccionado
Desempaquetando krb5-user (de ../krb5-user_1.10+dfsg~beta1-2ubuntu0.3_i386.deb)
...
Procesando disparadores para man-db ...
Configurando krb5-config (2.2) ...
Configurando krb5-user (1.10+dfsg~beta1-2ubuntu0.3) ...
root@server:/home/usuario# kinit administrator
Password for administrator@CASA.LOCAL:
Warning: Your password will expire in 41 days on Sun Jun  9 21:40:01 2013
root@server:/home/usuario#
```

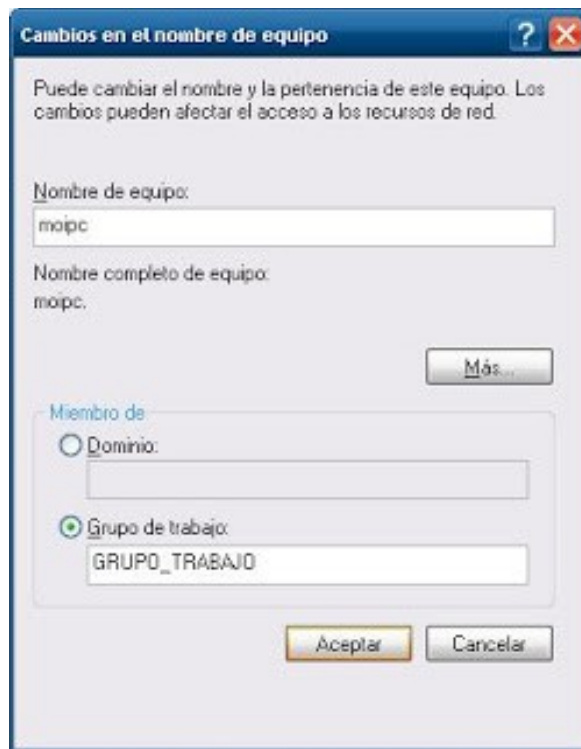
Si todo funciona sin problemas, podemos seguir, pero si tenemos algún problema deberemos reiniciar el proceso, para ello borraremos el archivo smb.conf y procederemos a repetir el proceso de crear el dominio, pero muy importante añadiendo el argumento `-use-ntvfs` al final y configurando directamente con el comando los argumentos, por ejemplo:

```
# samba-tool domain provision --realm casa.local --domain CASA --adminpass P@ssword --server-  
role=dc --use-ntvfs
```

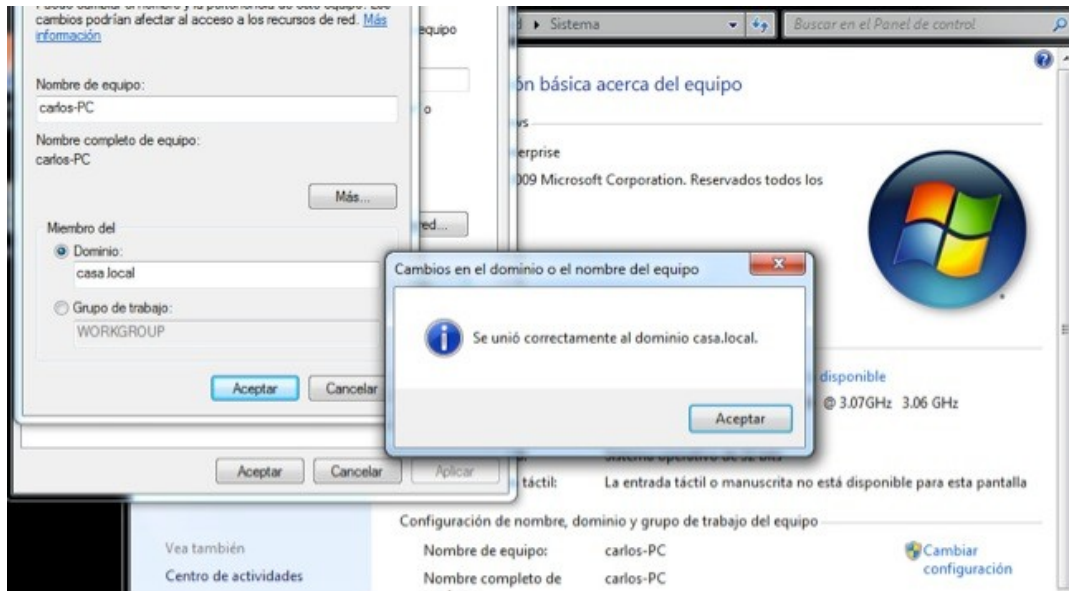
Posteriormente en el archivo smb.conf añadiremos el dns forwarder y la opción de update de los clientes.

- **Como añadir un Equipo a Directorio Activo**

En el **equipo cliente**, indicamos el Dominio:



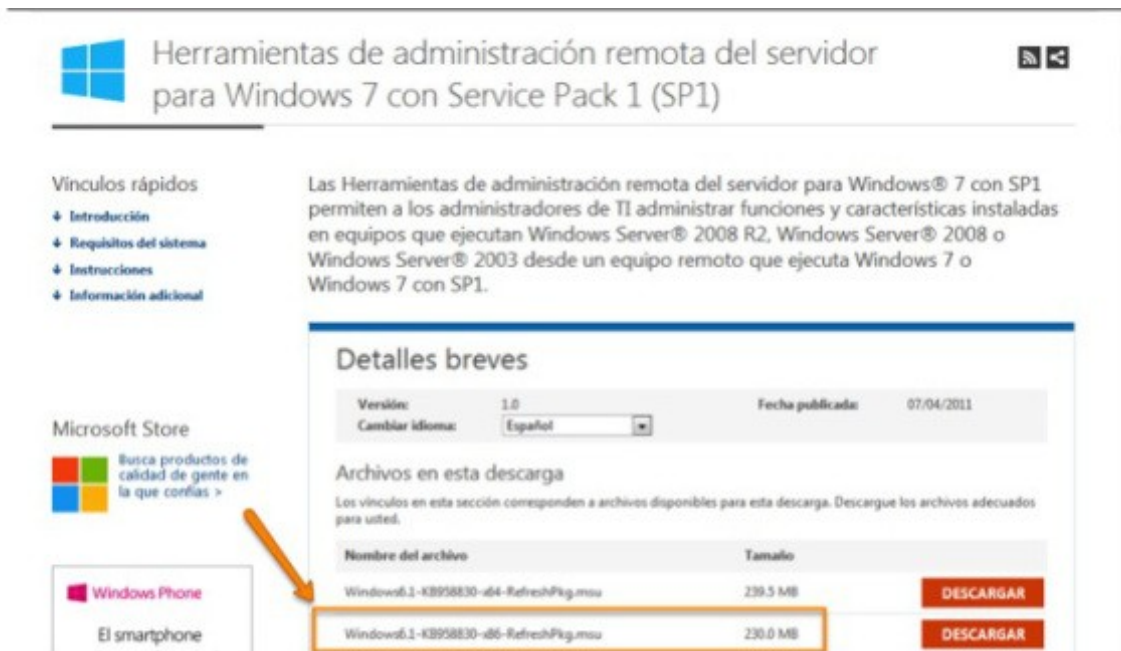
Nos muestra el panel para el logueo con el usuario que anteriormente creamos personalmente para él, reiniciamos la máquina y ya pertenecemos al nuevo dominio.



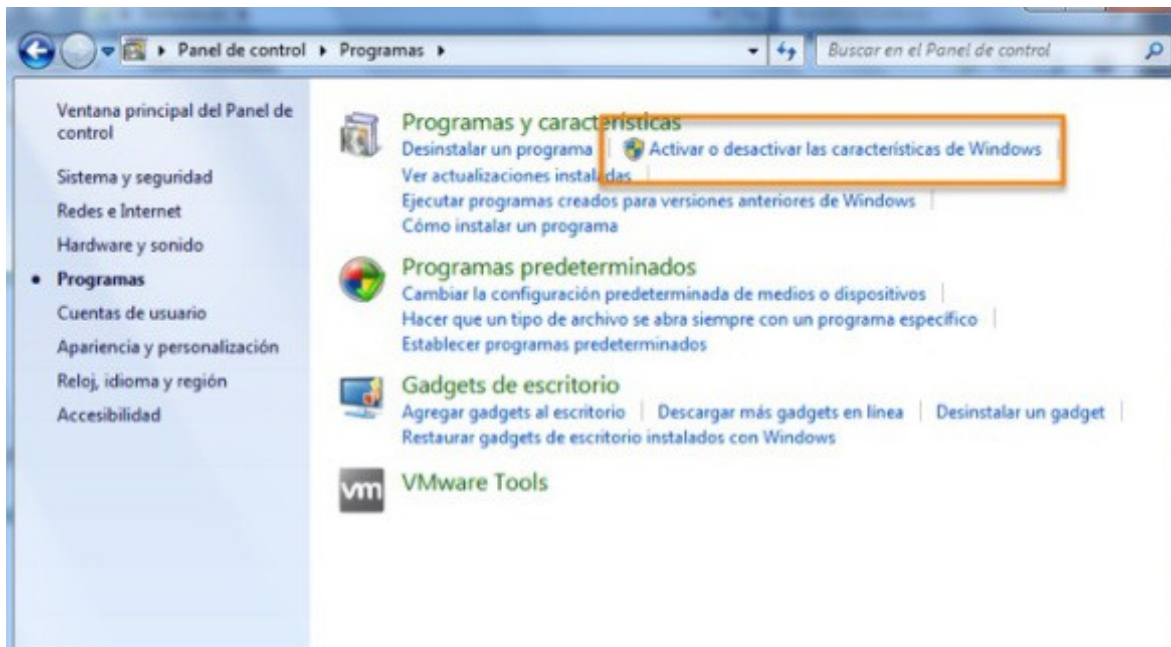
Como dar de alta un Usuario en el AD

Para ello hay que instalar previamente la herramientas RAST que se descarga desde la página de

Microsoft adecuada a un equipo cliente **ya unido al dominio**.

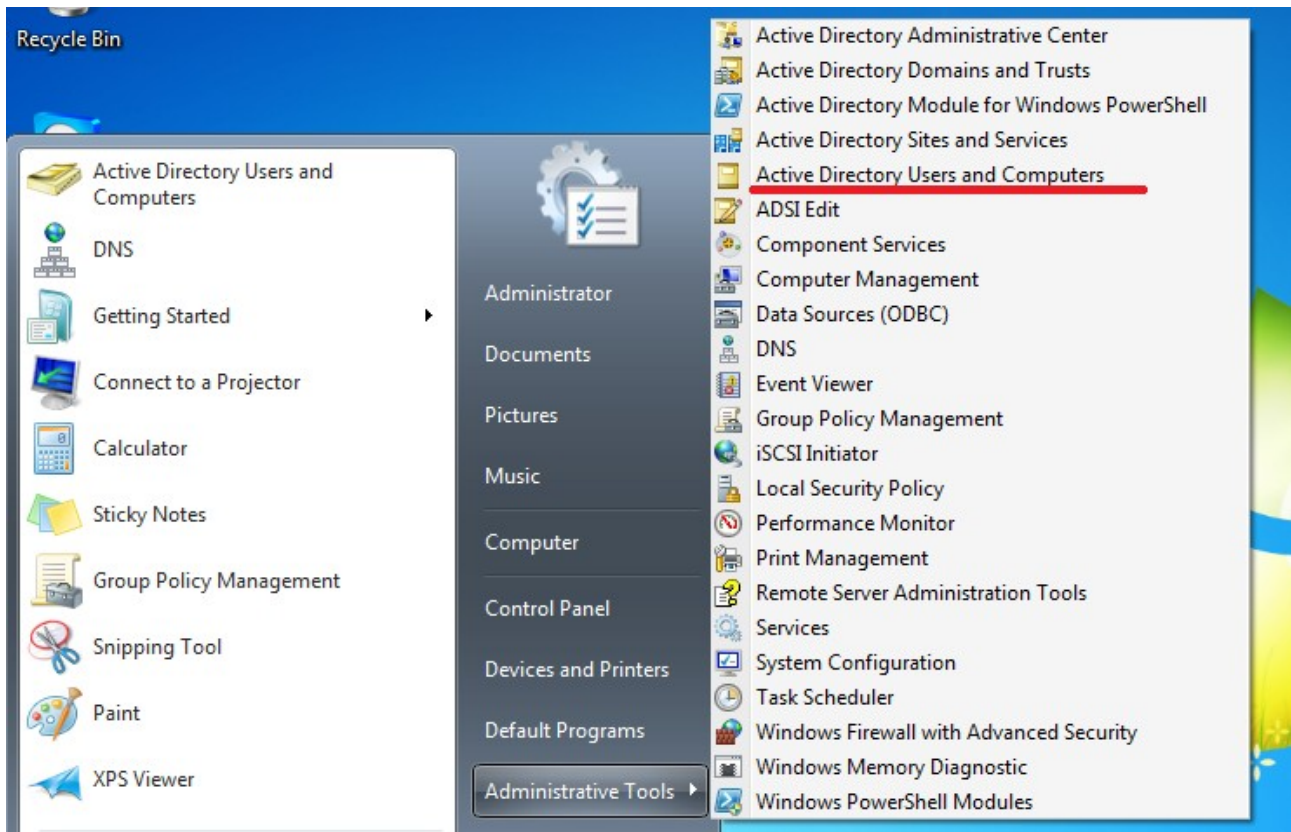


Una vez instalado el paquete de herramientas, procederemos a habilitar aquellas que necesitemos, para ello deberemos ir a *Panel de Control, Programas y características, Activar características de Windows*:



Aquí activaremos las herramientas de administración que sean necesarias, en nuestro caso tendremos suficiente con la administración básica del AD y la administración de políticas de grupo. Si posteriormente se necesitan herramientas adicionales, siempre se pueden activar.

Una vez hemos activado las diferentes herramientas, vamos a comenzar a administrar nuestro dominio. En primer lugar, abrimos *Usuarios y Equipos de Active Directory*. En esta consola podemos crear OU, grupos, usuarios y preaprovisionar máquinas al dominio.



Nos vamos a "Usuarios y equipos de Directorio Activo". Botón Derecho/Nuevo/Usuario

A screenshot of the 'Nuevo objeto: Usuario' (New Object: User) dialog box in Active Directory. The dialog is titled 'Nuevo objeto: Usuario' and has a close button (X) in the top right corner. It shows the creation path 'Crear en: prueba.com/Users'. The fields are filled with the following information: 'Nombre de pila' (First Name) is 'Prueba', 'Iniciales' (Initials) is empty, 'Apellidos' (Last Name) is empty, 'Nombre completo' (Full Name) is 'Prueba', 'Nombre de inicio de sesión de usuario' (User logon name) is 'prueba@prueba.com', and 'Nombre de inicio de sesión de usuario (anterior a Windows 2000)' (User logon name (pre-Windows 2000)) is 'PRUEBA\prueba'. At the bottom, there are three buttons: '< Atrás' (Back), 'Siguiente >' (Next), and 'Cancelar' (Cancel).

Nuevo objeto: Usuario

Crear en: prueba.com/Users

Contraseña: [.....]

Confirmar contraseña: [.....]

El usuario debe cambiar la contraseña en el siguiente inicio de sesión

El usuario no puede cambiar la contraseña

La contraseña nunca expira

La cuenta está deshabilitada

< Atrás Siguiente > Cancelar

A continuación veremos las actividades a realizar.

a) Establecer un dominio en la MV **DebianServer-AD**. El nombre del dominio será **tunombre.local**. Por ejemplo, *carlosperez.local*. Los datos de la red ya se han dado al principio del documento.

b) Añade un equipo al dominio. Para ello tenemos que clonar un MV de **Window7/10-Plantilla** con el nombre **Win7/10-AD**. Los datos que le daremos son:

Nombre del Equipo: **Equipo1**

IP: **192.168.0.10**

c) Da de alta los siguientes usuarios (todos con la contraseña *abc123*):

En **administracion**: *Gerente, AuxAdm1*

En almacen: *Capataz, Mozouno, Mozodos, RepartoUno, RepartoDos*

Comprobar en Usuario y Equipos del AD que tanto los usuarios como el equipo aparecen.