

## Gestionar cuentas de equipo de terminales Linux en un controlador de dominio Windows.

Realizaremos los siguientes pasos en modo comando ya que conocemos de unidades anteriores como trabajar con el entorno gráfico, seguiremos el ejemplo para un dominio “infoalislal.local” controlado en un servidor Windows con nombre equipo “*distancia*” y con la IP:192.168.1.174, el cliente Linux tiene como nombre de host “*serverlinux*” y una IP:192.168.1.23:

1. El terminal Linux tendrá configurado los parámetros de **configuración TCP/IP** de forma que pertenezcan a la misma red que el servidor Windows y su IP del servidor DNS será la de equipo que tenga instalado el servicio (posiblemente la del controlador de Dominio Windows, ya que se instalara de forma predeterminada si no se dispone de este servicio en la red que estemos administrando. Para ellos editamos el fichero de configuración del interfaz de red y configuramos las valores:

carlos@serverlinux:~\$ *sudo gedit /etc/network/interfaces*



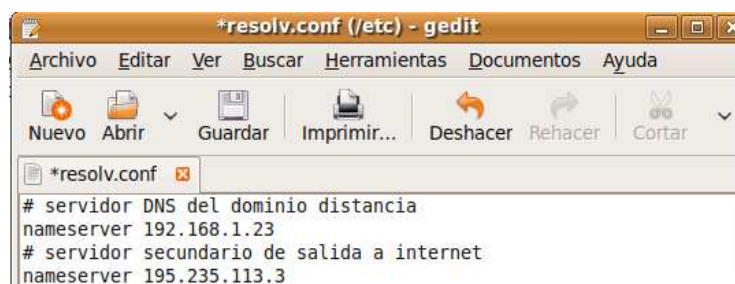
```
*interfaces (/etc/network) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Nuevo Abrir Guardar Imprimir... Deshacer Rehacer Cortar Copiar Pegar Buscar Reemplazar
*interfaces
#auto lo
#iface lo inet loopback
#iface eth0 inet dhcp debemos comentar estas líneas
#Agregar al archivo por ejemplo interfaz eth0 con la IP 192.168.1.174 con una máscara 255.255.255.0
# con una puerta de enlace 192.168.1.1. |
# Configurar IP estatica en eth0
auto eth0
iface eth0 inet static
address 192.168.1.110
gateway 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
```

Una vez más guardamos el archivo reiniciamos los servicios de red ejecutando:

carlos@serverlinux:~\$ *sudo /etc/init.d/networking restart*

Seguidamente **configuramos los servidores DNS de búsqueda**, deberemos incluir el servidor DNS de nuestro dominio de la red, editamos el siguiente fichero:

carlos@serverlinux:~\$ *sudo gedit /etc/resolv.conf*



```
*resolv.conf (/etc) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Nuevo Abrir Guardar Imprimir... Deshacer Rehacer Cortar
*resolv.conf
# servidor DNS del dominio distancia
nameserver 192.168.1.23
# servidor secundario de salida a internet
nameserver 195.235.113.3
```

2. Instalación de las siguientes aplicaciones necesarias para configurar el servicio:

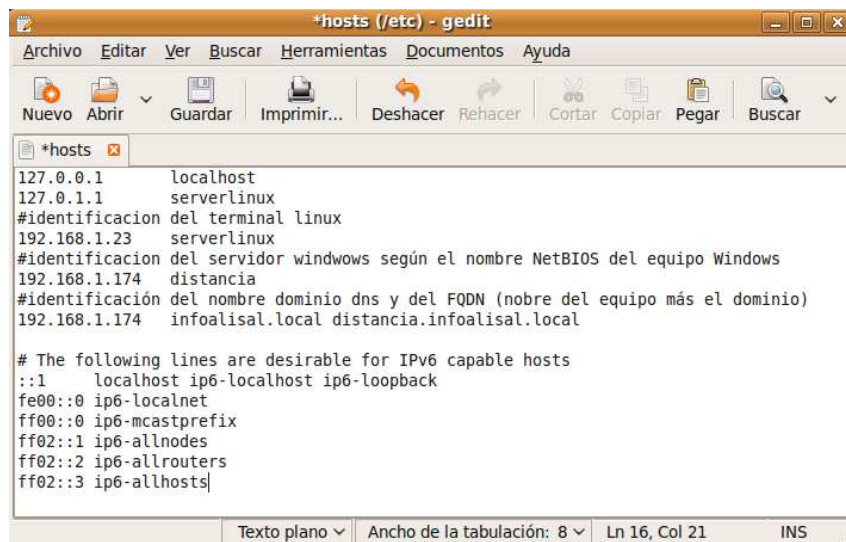
carlos@serverlinux:~\$ *sudo apt-get install samba smbclient winbind krb5-user krb5-config*

En esta tabla vemos la para que sirve cada programa:

<b>samba</b>	Permiten instalar la aplicación cliente para que Linux pueda comunicarse con el
<b>smbclient</b>	Servidor para acceder a recursos compartido en el controlador de dominio Windows. Ofrecerá una interfaz similar a la del servicio ftp
<b>Winbind</b>	Necesario para autentificar de acceso de los usuarios Linux hacia un servidor Windows
<b>Krb5-user</b>	Sistema Kerberos utilizado por Windows para validar la claves de acceso de clientes,
<b>Krb5-config</b>	se instalara un protocolo de autenticación segura entre dos equipos de una red.

3. Editar el fichero `/etc/hosts` para **configurar la para resolver nombres de los equipo**, añadimos al final de ficheros los nombres de los equipos que forman parte del dominio en red junto con sus direcciones IPs, por lo menos el del servidor Windows y el del terminal Linux. Según el ejemplo:

carlos@serverlinux:~\$ `sudo gedit /etc/hosts`

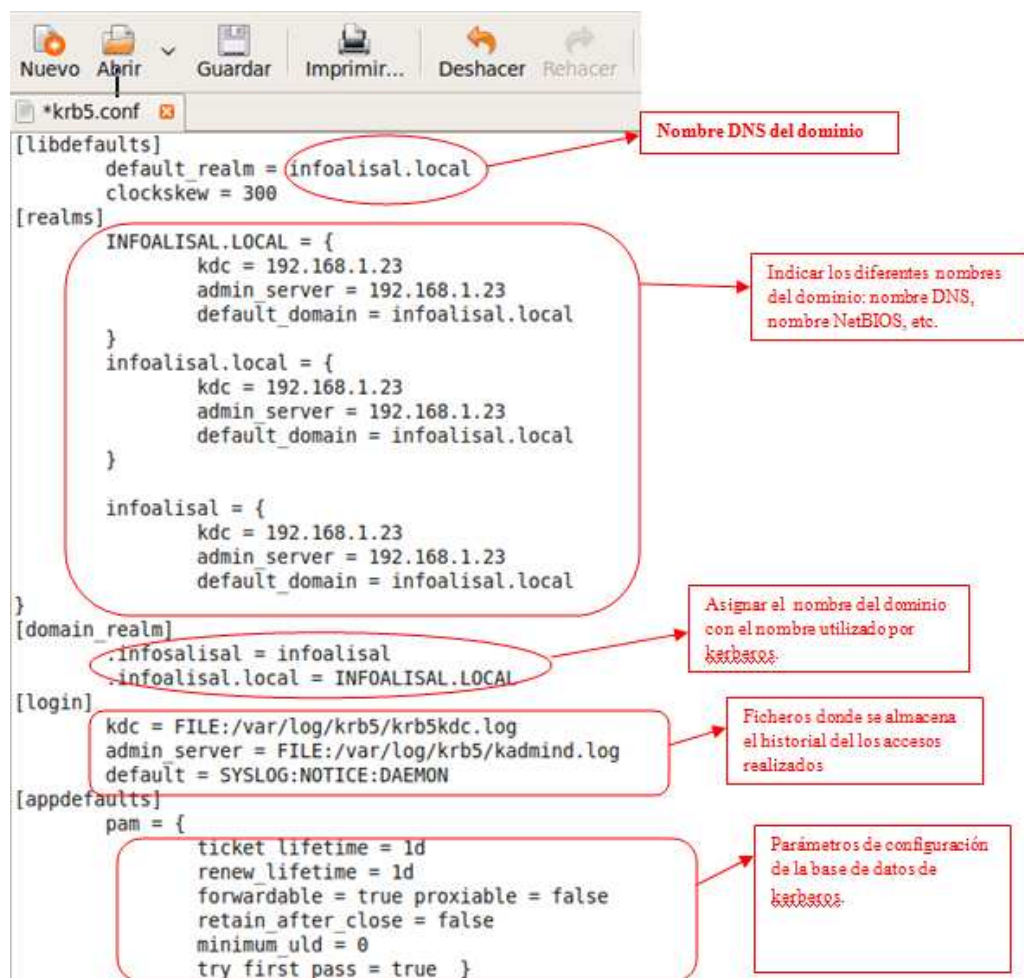


```
*hosts (/etc) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Nuevo Abrir Guardar Imprimir... Deshacer Rehacer Cortar Copiar Pegar Buscar
*hosts
127.0.0.1 localhost
127.0.1.1 serverlinux
#identificacion del terminal linux
192.168.1.23 serverlinux
#identificacion del servidor windows según el nombre NetBIOS del equipo Windows
192.168.1.174 distancia
#identificación del nombre dominio dns y del FQDN (nobre del equipo más el dominio)
192.168.1.174 infoalisal.local distancia.infoalisal.local

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
Texto plano Ancho de la tabulación: 8 Ln 16, Col 21 INS
```

Configurar la validación de clientes en el controlador de dominio Windows mediante **Kerberos**, para ello se editará el fichero de configuración `/etc/krb5.conf`:

carlos@serverlinux:~\$ `sudo gedit /etc/krb5.conf`



```
*krb5.conf
[libdefaults]
    default_realm = infoalisal.local
    clocks skew = 300
[realms]
    INFOALISAL.LOCAL = {
        kdc = 192.168.1.23
        admin_server = 192.168.1.23
        default_domain = infoalisal.local
    }
    infoalisal.local = {
        kdc = 192.168.1.23
        admin_server = 192.168.1.23
        default_domain = infoalisal.local
    }
    infoalisal = {
        kdc = 192.168.1.23
        admin_server = 192.168.1.23
        default_domain = infoalisal.local
    }
}
[domain_realm]
    .infoalisal = infoalisal
    .infoalisal.local = INFOALISAL.LOCAL
[login]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON
[appdefaults]
    pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true proxiable = false
        retain_after_close = false
        minimum_uld = 0
        try_first_pass = true
    }
```

Nombre DNS del dominio

Indicar los diferentes nombres del dominio: nombre DNS, nombre NetBIOS, etc.

Asignar el nombre del dominio con el nombre utilizado por kerberos.

Ficheros donde se almacena el historial de los accesos realizados

Parámetros de configuración de la base de datos de kerberos.

4. En el siguiente paso vamos a **configurar el servicio Samba** para que el terminal de Linux se pueda comunicar como cliente del servidor de dominio Windows (en unidades anteriores aprendimos a configurar el protocolo como controlador de dominio). Para ello editamos el fichero `/etc/smb.conf` y modificamos las líneas según el ejemplo que tratamos:

```
carlos@serverlinux:~$ sudo gedit /etc/smb.conf
```

```
#Modificación del fichero smb.conf, las líneas que empiezan por # son comentarios del programa
[global]

security = ads
netbios name = serverlinux
realm = INFOALISAL.LOCAL
password server = 192.168.1.23
workgroup = INFOALISAL
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
# El demonio winbindd usa este parámetro para asignar el directorio personal para ese usuario
# Si la cadena %D está presente, se sustituye por el dominio del usuario. Si la cadena %U está #Presente, se sustituye
por el nombre de usuario en Windows.
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
domain master = no
server string = terminal del dominio infoalisal
encrypt passwords = yes

#Configuramos la sección homes para que cuando se conecte un usuario pueda acceder a su #directorio personal de
Linux, %S nombre del servicio actual
[homes]

comment = Home Directories
valid users = %S
browseable = No
read only = No
inherit acls = Yes

#configuramos el lugar donde se guarda el perfil del usuario
# %H es directorio home raíz de la cuenta del usuario %u.
[profiles]
comment = Network Profiles Service
path = %H
read only = No
store dos attributes = Yes
create mask = 0600
directory mask = 0700

##compartir una carpeta para los usuarios
[users]
comment = All users
path = /home
read only = No
inherit acls = Yes
veto files = /aquota.user/groups/shares/
```

5. Creamos el directorio para los usuarios del dominio:

```
carlos@serverlinux:~$ sudo mkdir /home/INFOALISAL
```

6. Editamos y configuramos el fichero /etc/nsswitch.conf para **controlar la resolución de nombres de usuarios y grupos de dominio**; esto le indica al sistema dónde buscar contraseñas y grupos. Modificamos o añadimos las siguientes líneas:

<i>passwd:</i>	<i>files winbind</i>
<i>group:</i>	<i>files winbind</i>
<i>shadow:</i>	<i>files winbind</i>
<i>hosts:</i>	<i>files dns winbind</i>

Seguidamente deberemos de configurar que todos los usuarios del dominio puedan acceder desde el entorno gráfico de Linux, para ello deberemos de editar y modificar como root los ficheros de **configuración pam** (son programas que permiten a los usuarios acceder al sistema verificando la identidad de cada usuario a través de un proceso llamado autenticación). A cada fichero agregamos o modificamos las siguientes líneas y eliminamos, si existen, las líneas en rojo:

FICHERO	LÍNEAS
/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 <i>auth optional pam_smbpass.so migrate missingok</i>
/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

7. Estando en sesión como usuario root **creamos los tickets Kerberos** (nos pide la contraseña del administrador del dominio) y configurar la **sincronización de la hora** entre el ordenador cliente y el servidor.

```
root@serverlinux:~# kinit administrador@infoalislal.local
```

```
Password for administrador@infoalislal.local:
```

```
root@serverlinux:~# net time set
```

8. **Reiniciamos todos los servicios samba y winbind:**

```
root@serverlinux:~# /etc/init.d/samba restart
```

```
root@serverlinux:~# /etc/init.d/winbind restart
```

9. **Unir el terminal Linux al dominio Windows** con el comando siguiente:

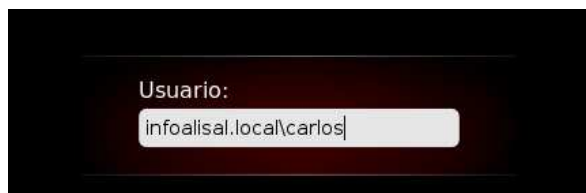
```
root@serverlinux:~# net ads join -U administrador -S distancia.infoalislal.local
```

Nos solicitará la contraseña del administrador del dominio ya que no la hemos indicado directamente en la orden con el parámetro `%clave_administrador` después del nombre del usuario administrador.




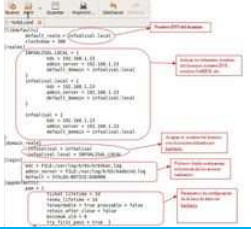
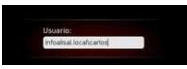
**Existe la herramienta gráfica Likewise** que nos facilita la unión de equipos Linux a Active Directory de Windows. Para más información consultar el siguiente enlace:

<http://110n.ubuntu.tla.ro/ubuntu-docs-jaunty/html/serverguide/es/likewise-open.html#likewise-open-ms-dns>

10. Si no se ha producido ningún error (encaso contrario repasar los pasos y ficheros de configuración), ya podemos iniciar sesión con usuarios locales o del dominio de Active Directory Windows en nuestro Linux. Para **iniciar sesión** con un usuario del dominio en la ventana de login deberemos de teclear nombre de dominio el signo indicado en el parámetro *winbind* separador del fichero *smb.conf* (en nuestro caso “\”) junto al nombre de usuario (por ejemplo: *infoalisal.local\carlos*) y posteriormente la contraseña. Tenemos que cumplir la regla de que los usuarios del dominio no pueden ser usuarios locales del terminal de Linux.



## Anexo de licencias

Imagen	Credenciales	Imagen	Credenciales
	Título: ISO07_AUXR05_R01_pantalla1.png Autoría: Linux Ubuntu Tipo de licencia: GNU GPL (Cita). Procedencia: Captura pantalla de Linux Ubuntu		Título: ISO07_AUXR05_R02_pantalla2.png Autoría: Linux Ubuntu Tipo de licencia: GNU GPL (Cita). Procedencia: Captura pantalla de Linux Ubuntu
	Título: ISO07_AUXR05_R03_pantalla3.png Autoría: Linux Ubuntu Tipo de licencia: GNU GPL (Cita). Procedencia: Captura pantalla de Linux Ubuntu		Título: ISO07_AUXR05_R04_pantalla4.png Autoría: Linux Ubuntu Tipo de licencia: GNU GPL (Cita). Procedencia: Captura pantalla de Linux Ubuntu
	Título: ISO07_AUXR05_R05_pantalla5.png Autoría: Linux Ubuntu Tipo de licencia: GNU GPL (Cita). Procedencia: Captura pantalla de Linux Ubuntu		