

# PROYECTO INTEGRADO

El proyecto consiste en integrar una maquina unix en un dominio de windows para ello necesitaremos una maquina windows 2003 server y un cliente unix en este caso debian lenny, utilizaremos autenticación con kerberos para aportar seguridad a la conexión.

Un **dominio** es un conjunto de ordenadores conectados en una red que confían a uno de los equipos de dicha red (controlador de dominio) la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.

En la maquina que actúa como servidor montaremos un windows 2003 server sp2 e instalaremos un servidor dhcp para que adjudique direcciones ip a los equipos clientes de nuestro dominio, un servidor dns para la asignación de nombre de dominio a direcciones ip y active directory (LDAP) para guardar los atributos de los usuarios y maquinas o dispositivos. Además tendremos que instalar unos paquetes que harán que podamos introducir en el active directory atributos de maquinas unix como directorio de home que en el caso de windows no existiría.

## **Instalación del servidor:**

### **Para comenzar la instalación:**

- 1.- Insertar el cd de windows server 2003.
- 2.- Reiniciar el equipo e iniciar desde el cd.
- 3.- Crea una partición del tamaño necesario en este caso 20 GB.
- 4.- Selecciona formatear la partición creada anteriormente utilizando el sistema de archivos NTFS.

### **Asistente de instalación de windows 2003**

- 5.- Realizar los cambios necesarios en la configuración regional y el idioma.
- 6.- Escriba su nombre y organización.
- 7.- Escriba la clave del producto.
- 8.- Configure el nombre del equipo y la contraseña de administrador.
- 9.- Configure fecha y hora.
- 10.- En la ventana configuración de la red seleccione configuración típica.
- 11.- En la ventana de grupo de trabajo o dominio seleccionad no por defecto, mas adelante se indicara el dominio.
- 12.- La instalación de windows 2003 continuara asta finalizar.

## **Configuración de la red**

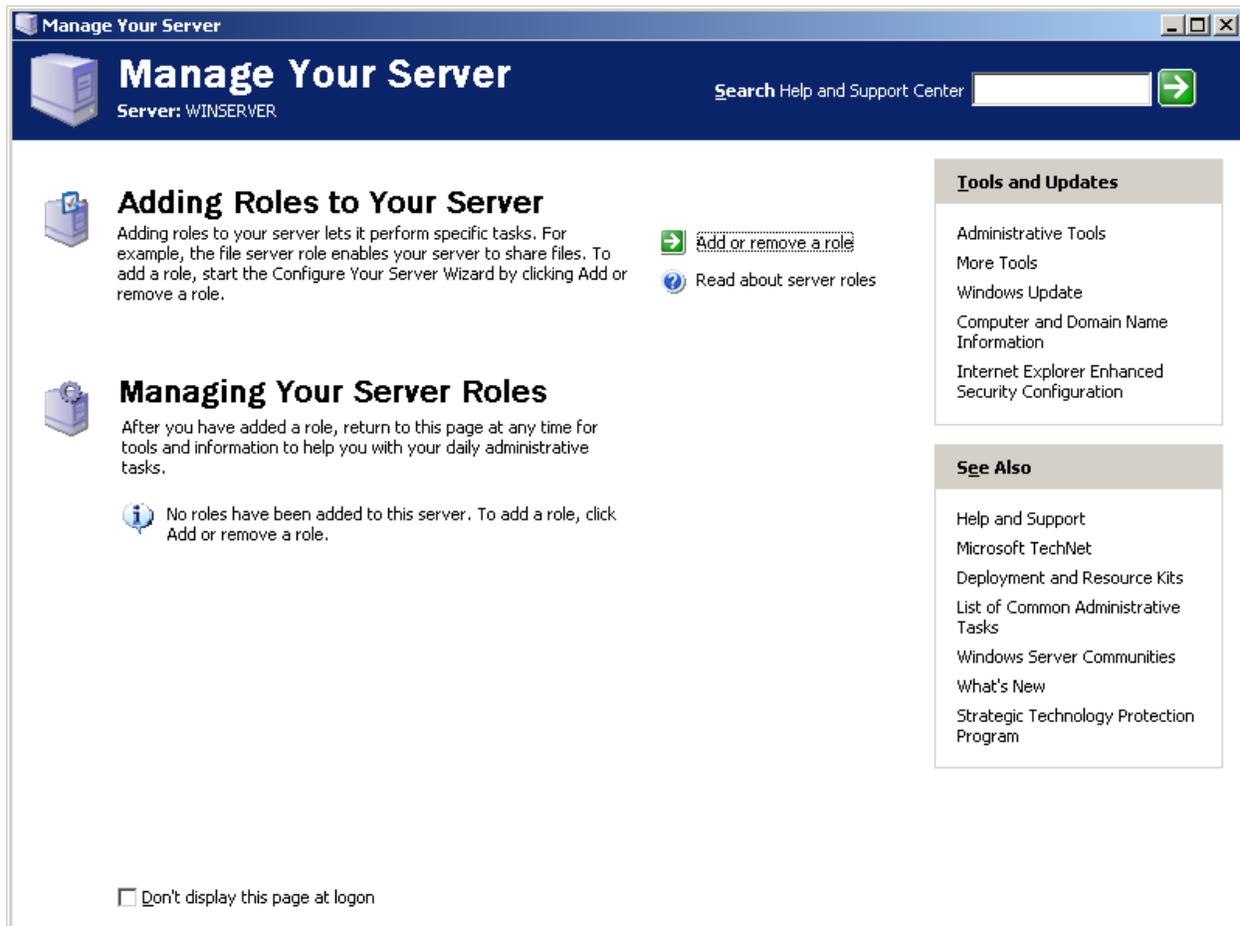
En nuestro caso nuestro servidor solo tiene una interfaz de red, una tarjeta ethernet la configuraremos con los siguientes parametros:

Dirección IP: 192.168.1.2  
Mascarada de red: 255.255.255.0  
Puerta de enlace: 192.168.1.1

1er DNS: 127.0.0.1

## El siguiente paso es instalar y configurar el servidor DHCP

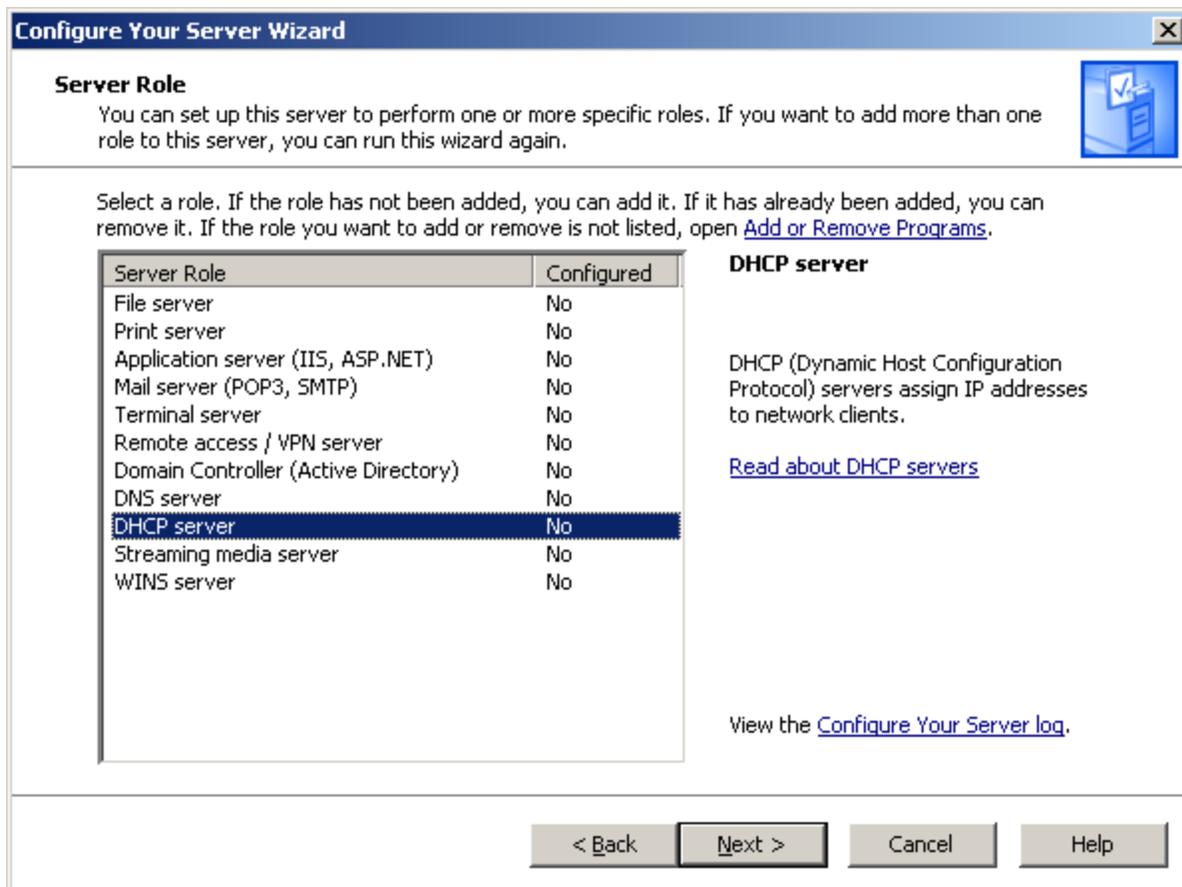
1.- En inicio, herramientas administrativas, administrar su servidor, hacer clic en agregar o quitar función.



2.- En el asistente para configurar su servidor, hacer clic en siguiente.

3.- Hacer clic en configuración personalizada, hacer clic en siguiente.

4.- En la ventana función del servidor, hacer clic en servidor DHCP y luego en siguiente.



5.- Para nombre de ámbito escriba "ámbito directorio" y hacer clic en siguiente.

6.- Para el rango de direcciones que va a dar escribir como inicial 192.168.1.100 y como final 192.168.1.200, hacer clic en siguiente.

**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 1 . 100

End IP address: 192 . 168 . 1 . 200

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back   Next >   Cancel

7.- En la ventana de las direcciones ip excluidas, no indicar ninguna ip, hacer clic en siguiente.

8.- Establecer la duración de las concesiones, por defecto 8 días, hacer clic en siguiente.

9.- Para definir las opciones de configuración de DHCP, hacer clic en siguiente.

10.- En la ventana enrutador (puerta de enlace predeterminada), escriba 192.168.1.1 para dirección ip, hacer clic en siguiente.

**New Scope Wizard**

**Router (Default Gateway)**  
 You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

11.- En la ventana nombre de dominio y servidores DNS, escriba para dominio primario directorio.com para direccion ip 192.168.1.2 que es la dirección de nuestro servidor windows 2003.

**New Scope Wizard**

**Domain Name and DNS Servers**  
 The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

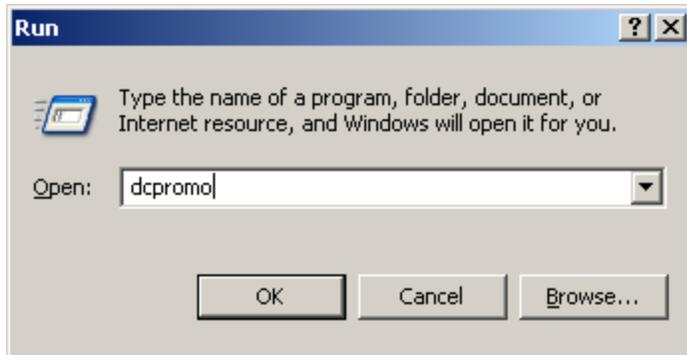
IP address:

12.- En la ventana de configuración del servidor WINS, elegir la opción desactivado ya que no vamos a usar WINS.

13.- hacer clic en finalizar.

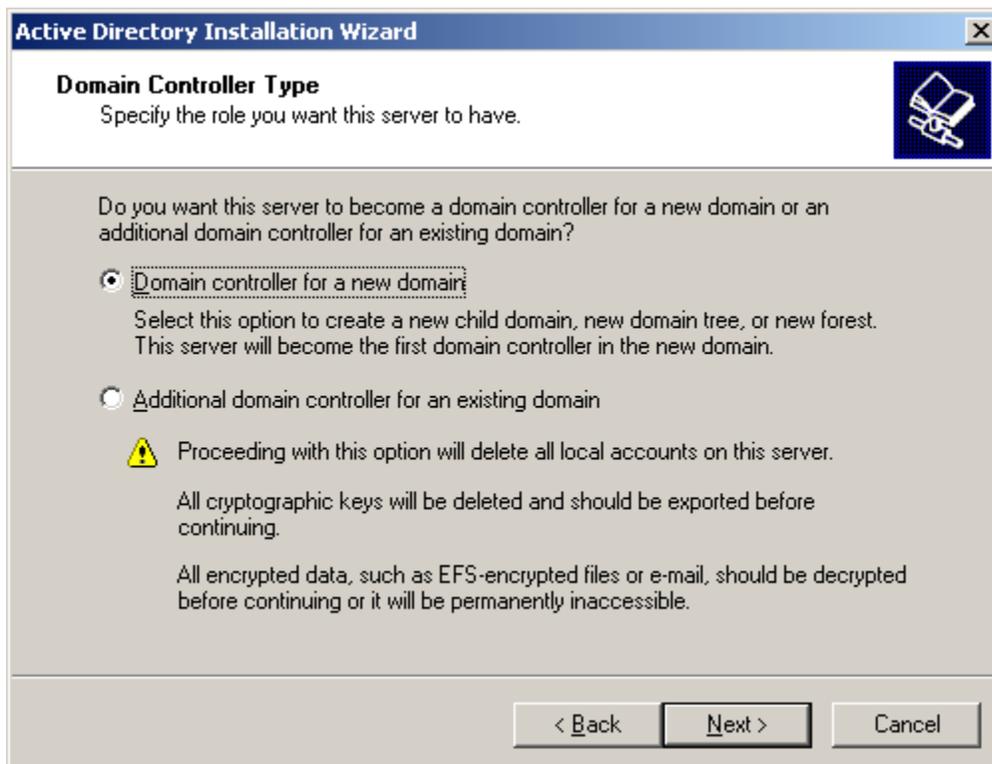
## Configurar el servidor como controlador de dominio

1.- Hacer clic en inicio, ejecutar y escribir dcpromo y pulsar darle a aceptar.

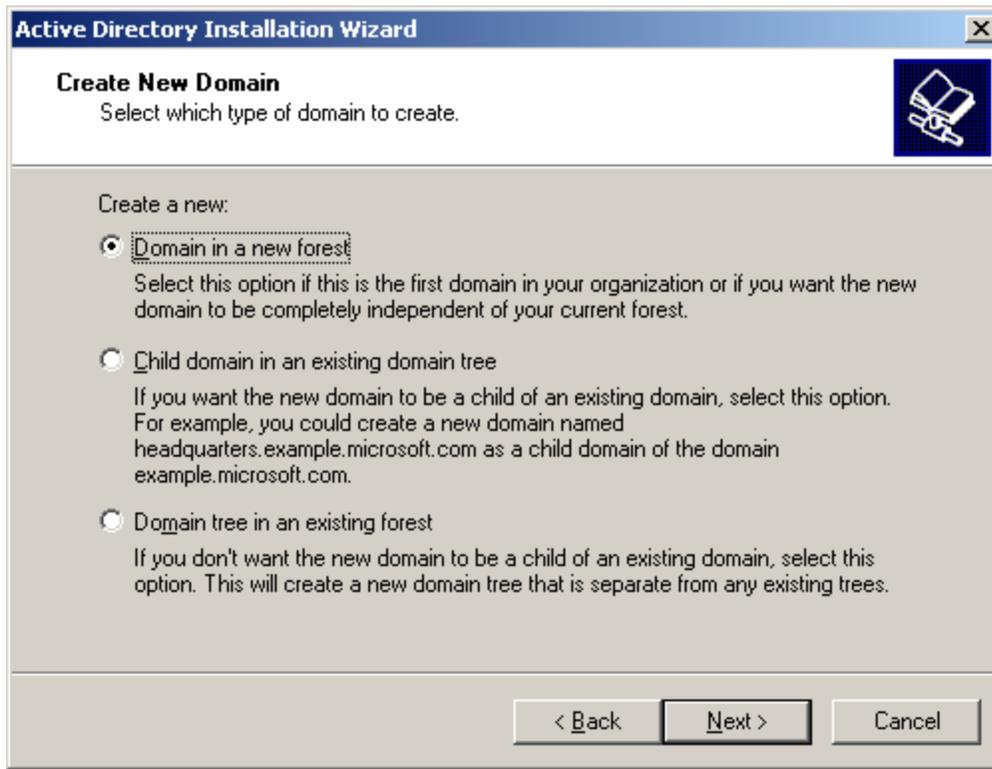


2.- Aparecerá la ventana del asistente para instalación de Active Directory, hacer clic en siguiente para iniciar la instalación.

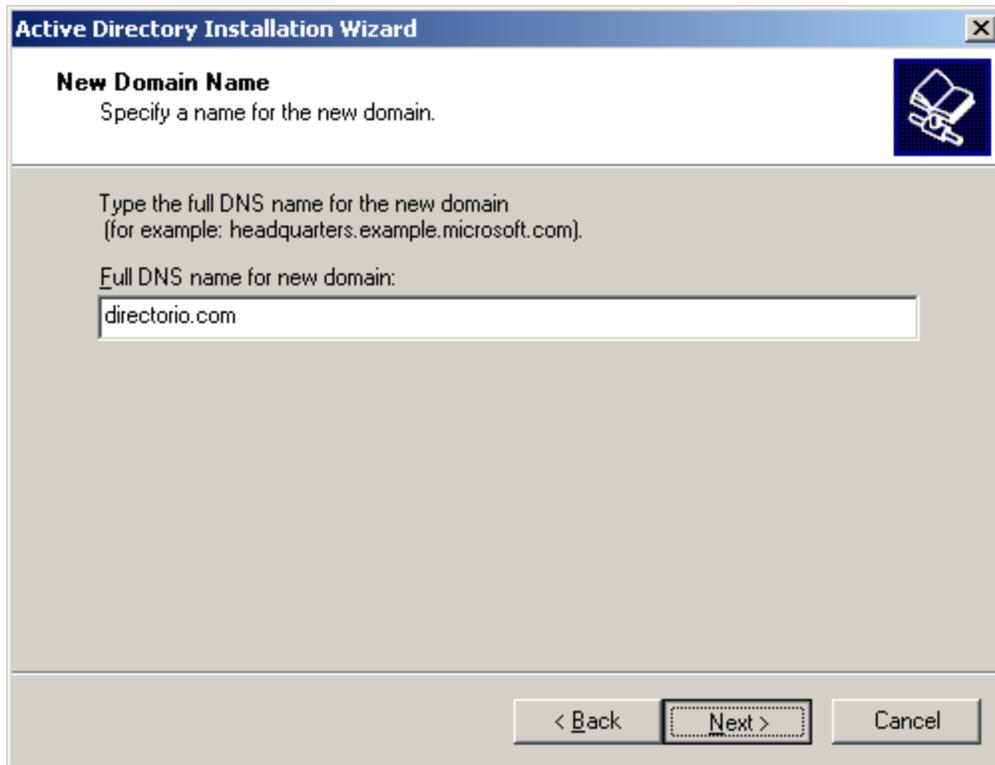
3.- Seleccionar la opción controlador de dominio para un dominio nuevo, hacer clic en siguiente.



4.- Seleccionar la opción dominio en un nuevo bosque y hacer clic en siguiente.



5.- Para nombre de DNS escribir directorio.com y hacer clic en siguiente.

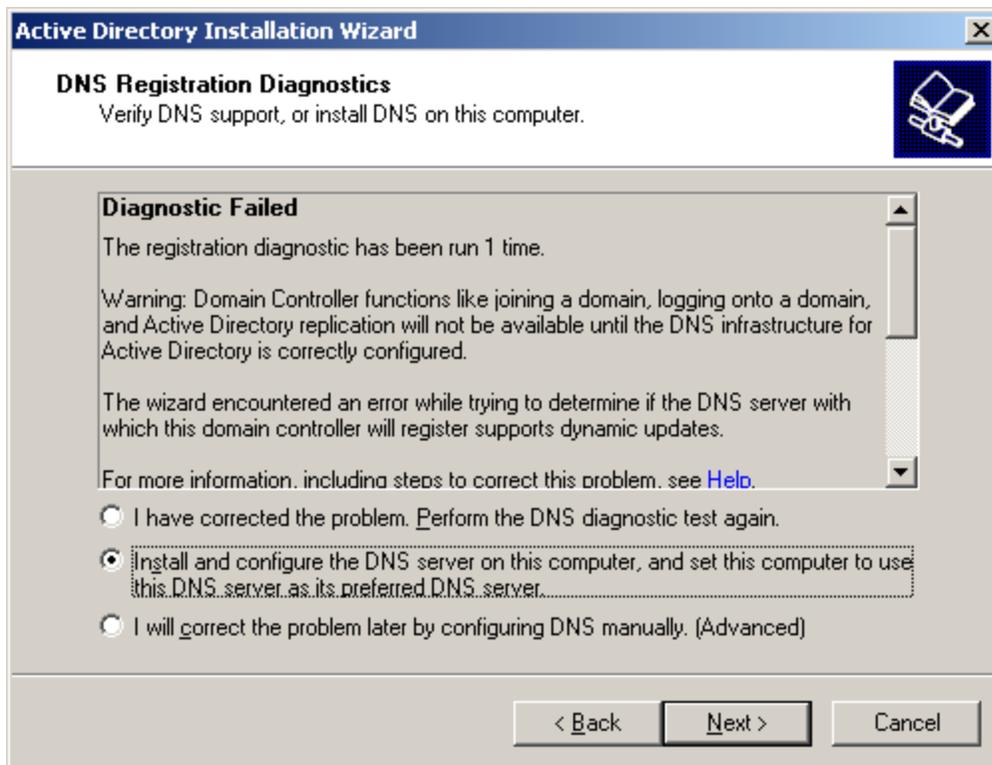


6.- Escribir como nombre de netbios del dominio directorio.

7.- En la ventana de carpetas de la base de datos y del registro dejar las opciones predeterminadas y hacer clic en siguiente.

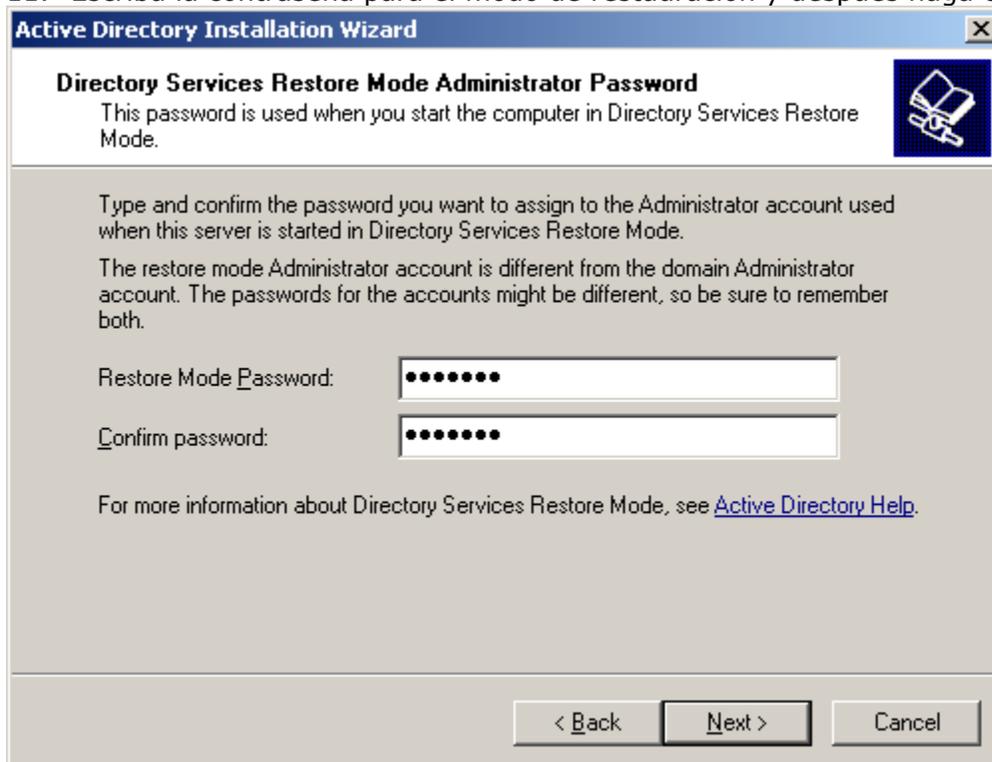
8.- En la ventana de volumen del sistema compartido dejar los valores predeterminados y hacer clic en siguiente.

9.- En la pantalla de diagnosticos de registro de DNS, hacer clic en instalar y configurar el servidor DNS en este equipo, hacer clic en siguiente.



10.- En la ventana permisos dejar la opción predeterminada, permisos compatibles sólo con sistemas operativos de servidor windows 2000 o 2003 y hacer clic en siguiente.

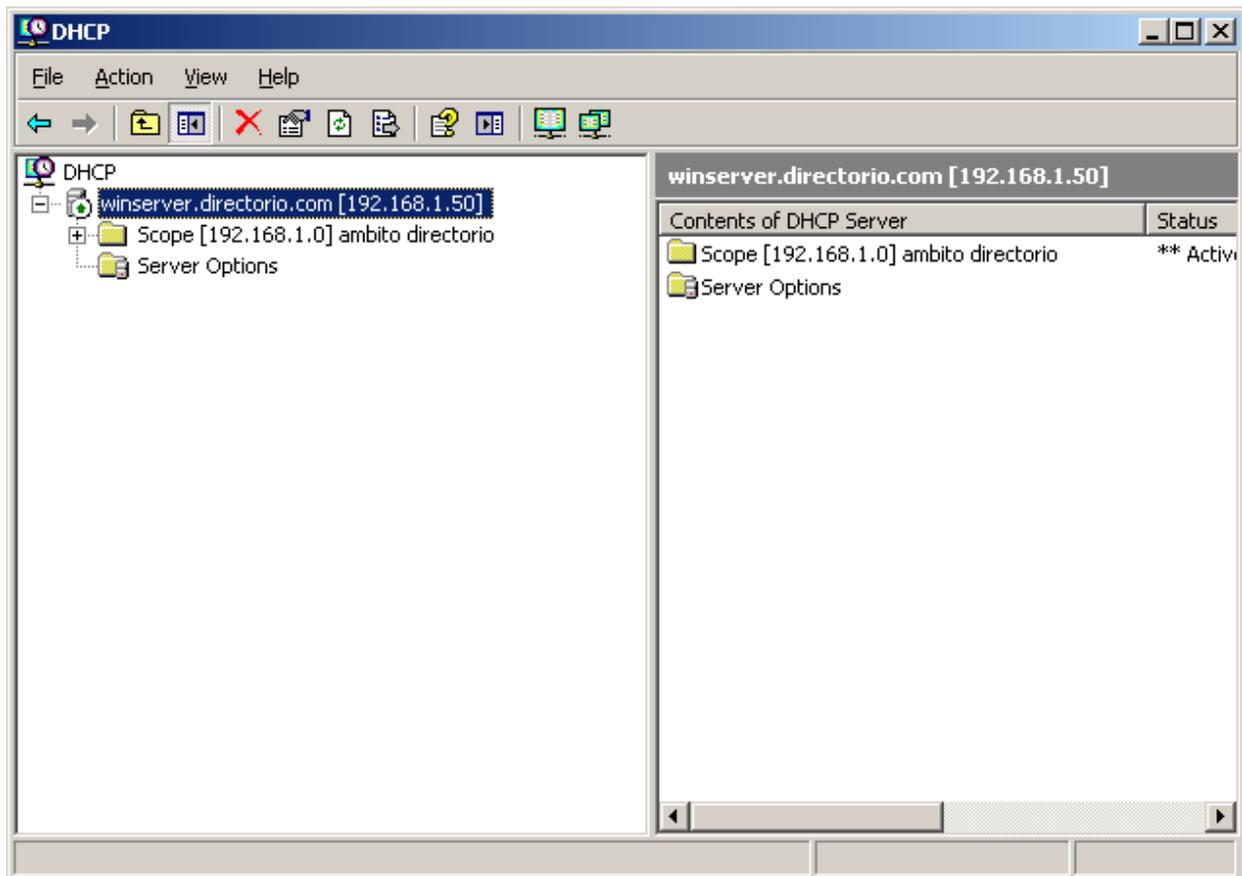
11.- Escriba la contraseña para el modo de restauración y después haga clic en siguiente.



- 12.- Insertar el cd de instalacion de windows 2003 server.
- 13.- Seleccione la interfaz de red adecuada y haga clic en siguiente.
- 14.- Haga clic en protocolo TCP/IP y luego en propiedades.
- 15.- Escriba como direccion ip 192.168.1.2, como mascara de red 255.255.255.0, como puerta de enlace 192.168.1.1 y como DNS preferido 127.0.0.1 y haga clic en finalizar.
- 16.- haga clic en reiniciar ahora.

### **Autorizar el servidor DHCP**

- 1.- hacer clic en inicio, herramientas administrativas y, a continuacion haga clic en DHCP.
- 2.- haga clic en winserver.directorio.com, haga clic con el boton derecho del raton en winserver.directorio.com y despues haga clic en autorizar.



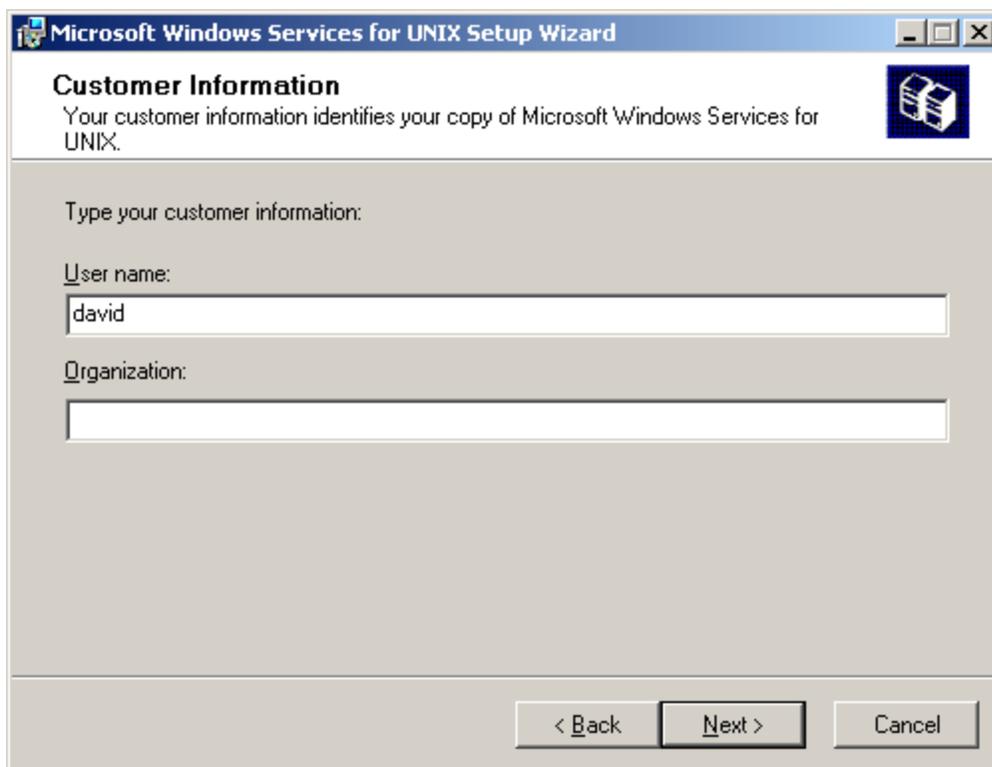
- 3.- Ciera la consola de administracion de DHCP.

### **Instalar los campos necesarios para los usuarios unix**

Al intentar introducir un usuario de un equipo unix en nuestro active directory vemos que ciertos campos necesarios como directorio de home, shell o gid no pueden guardarse puesto que estos atributos no existen en una maquina windows, por lo que su integracion su integracion de forma nativa no tendria sentido.

Para solucionar el problema existente con los campos necesarios para que un usuario de unix pueda se miembro de nuestro dominio tendremos que instalar un paquete que agregue a nuestro active directory los capos necesarios, el paquete necesario se llama SFU35SEL\_EN podemos encontrarlo en el centro de descargas de microsoft <http://www.microsoft.com/DOWNLOADS/Search.aspx?displaylang=es> ahora pasamos a su instalacion.

- 1.- Descomprimimos el archivo.
- 2.- Ejecutamos en archivo setup.exe.
- 3.- Introducimos nuestro nombre de usuario.



Microsoft Windows Services for UNIX Setup Wizard

**Customer Information**  
Your customer information identifies your copy of Microsoft Windows Services for UNIX.

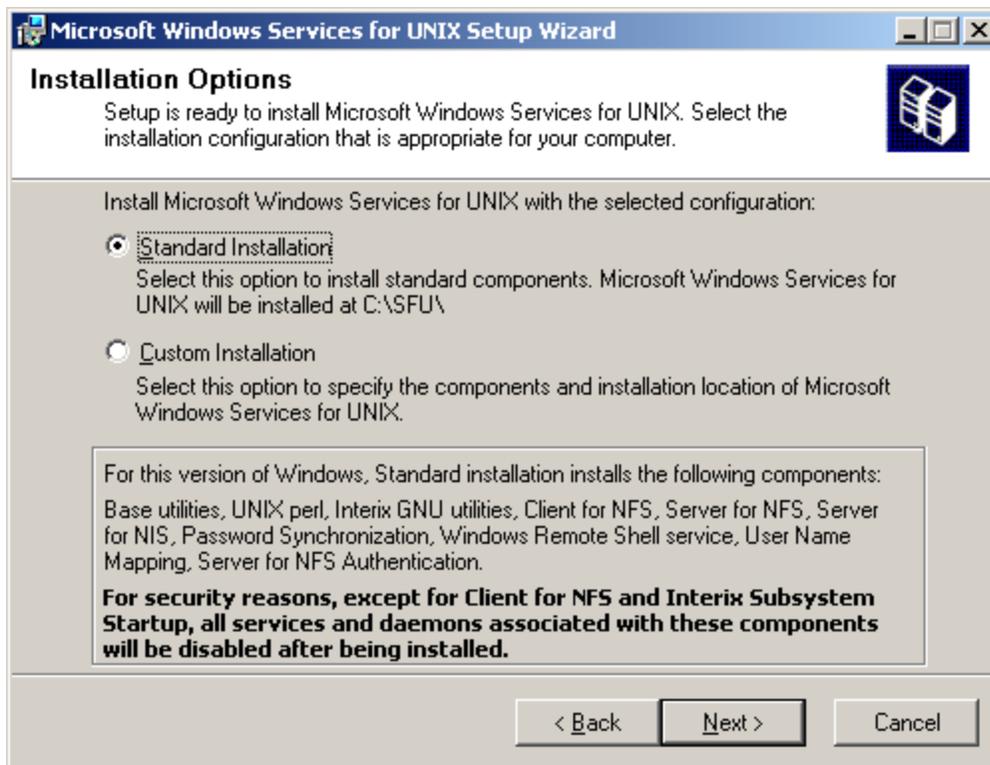
Type your customer information:

User name:  
david

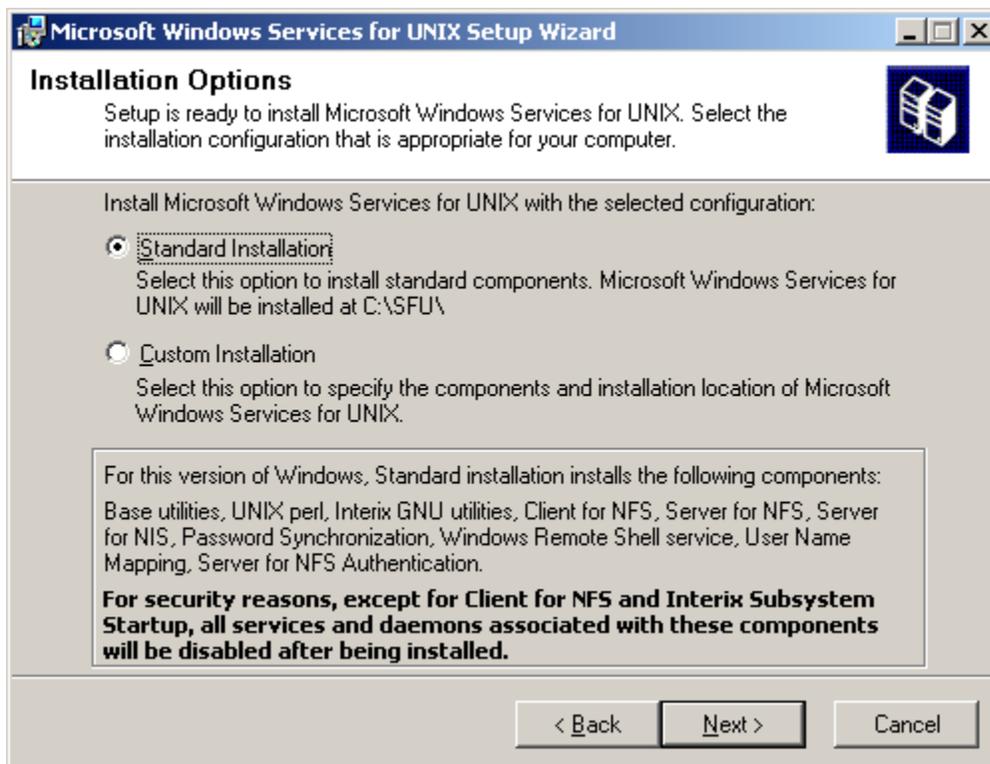
Organization:

< Back   Next >   Cancel

- 4.- Aceptamos los terminos de licencia.
- 5.- En la ventana de opciones de instalacion seleccionamos instalacion estandar



6.- En la ventana de user name mapping seleccionar como nombre de dominio de windows directorio.

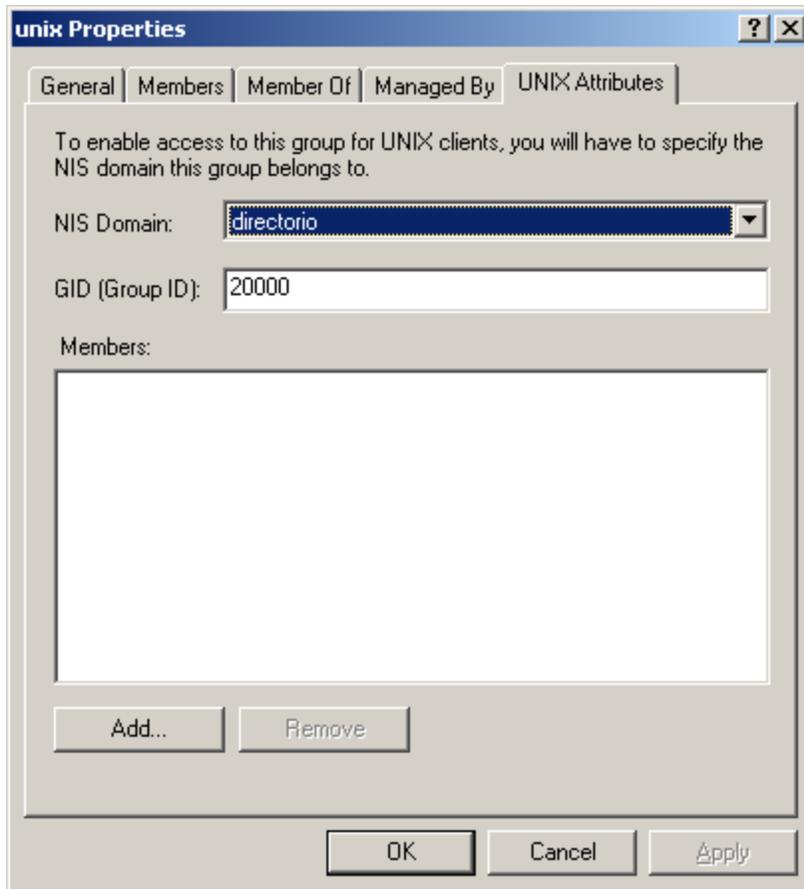


La parte de configuración del servidor a acabado con la instalación de este componente.

### **Creacion de usuarios y grupos**

Para que un usuario pueda guardarse en el Idap de windows con los atributos unix deben rellenarse todos los atributos y puesto que ahora no tenemos ningun grupo de usuarios unix empezaremos por la creacion de un grupo

- 1.- Hacemos clic en inicio, herramientas administrativas, usuarios y maquinas de active directory.
- 2.- Vamos a crear una unidad organizativa para meter dentro todos los grupos asi que boton derecho encima de directorio.com y nuevo, unidad organizativa, como nombre se le a puesto grupos.
- 3.- Dentro de esta unidad organizativa creamos un grupo con el nombre unix con los parametros de configuración por defecto.
- 4.- Si le damos a las propiedades del grupo que acabamos de crear veremos que nos aparece una pestaña llamada atributos unix, en esa pestaña aparecen 2 atributos NIS domain para la que seleccionamos directorio y GID a este le damos como valor 20000.



5.- Una vez creado el grupo unix nos vamos a la unidad organizativa usuarios y creamos un usuario, boton derecho en usuarios, nuevo, usuario. en la ventana que nos aparece debemos configurar dos atributos, nombre al que ponemos prueba y login de usuario para el que hemos puesto prueba, le damos a siguiente y nos aparece una ventana que nos pide las password la introducimos y le damos a finalizar.

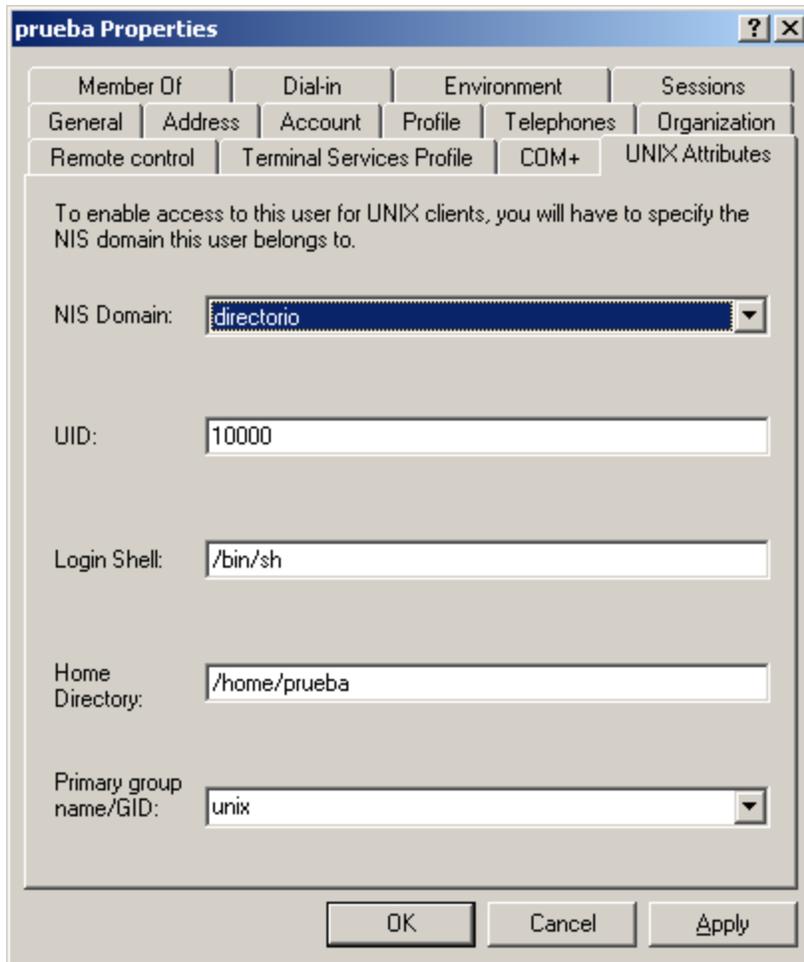
6.- Ahora configuraremos los atributos unix del usuario creado, para ello vamos a las propiedades del usuario y vamos a la pestaña atributos unix, nos pedira dominio para el que introducimos directorio, una vez introducido todos los demas atributos se rellenan solos con los siguientes valores:

UID: 10000

Login shell: /bin/bash

Home directory: /home/prueba

ID de grupo: unix



7.- El siguiente paso es agregar en el grupo al usuario, vamos a las propiedades del grupo unix y en la pestaña atributos unix, hacemos clic en el boton añadir, nos aparecera una ventana en la que seleccionaremos el usuario prueba y haremos clic en el boton añadir, confirmamos y salimos.

Con estos pasos ya tenemos un usuario listo para ser usado por cualquier equipo windows o unix debidamente configurado.

---

## Configuracion del equipo unix

Si hemos seguido todos los pasos anteriores nuestro servidor estara listo para recibir a los clientes, para la configuracion del equipo unix lo primero que haremos sera configurar correctamente la red para ello solo tendremos que utilizar el comando dhclient si el servidor esta funcionando correctamente respondera a nuestra peticion y nos dara todos los datos necesarios incluso para hacernos miembros del dominio, en la imagen vemos la salida de el comando dhclient

```

debiandios:/# dhclient
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:1a:4d:f7:9d:cd
Sending on LPF/eth0/00:1a:4d:f7:9d:cd
Sending on Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4
DHCPOFFER from 192.168.1.2
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.1.2
bound to 192.168.1.100 -- renewal in 316394 seconds.
debiandios:/# clear

debiandios:/#

debiandios:/mnt/home/david/Desktop/venosa# ls
common-account  common-auth  common-password  common-session  ldap.conf  ldap.conf  ldap.conf~  libnss-ldap
debiandios:/mnt/home/david/Desktop/venosa# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1a:4d:f7:9d:cd
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::21a:4dff:fe77:9dcd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10499  errors:0  dropped:0  overruns:0  frame:0
          TX packets:6391  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14740761 (14.0 MiB)  TX bytes:575937 (562.4 KiB)
          Interrupt:22

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0  errors:0  dropped:0  overruns:0  frame:0
          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:0
          RX bytes:560 (560.0 B)  TX bytes:560 (560.0 B)

debiandios:/mnt/home/david/Desktop/venosa#

```

El siguiente paso sera instalar los paquetes necesarios, libpam-ldap, libnss-ldap, libpam-krb5, krb5-user ..

## Configuración de ficheros

en este paso indicare las partes importates de cada fichero o las que han necesitado modificación

### - /etc/ldap/ldap.conf

Este fichero indica donde esta el servidor ldap

```

BASE    dc=directorio,dc=com
URI     ldap://davi-portati.directorio.com/

```

despues de configurar este fichero podemos comprobar que tenemos acceso al servidor ldap con el siguiente comando

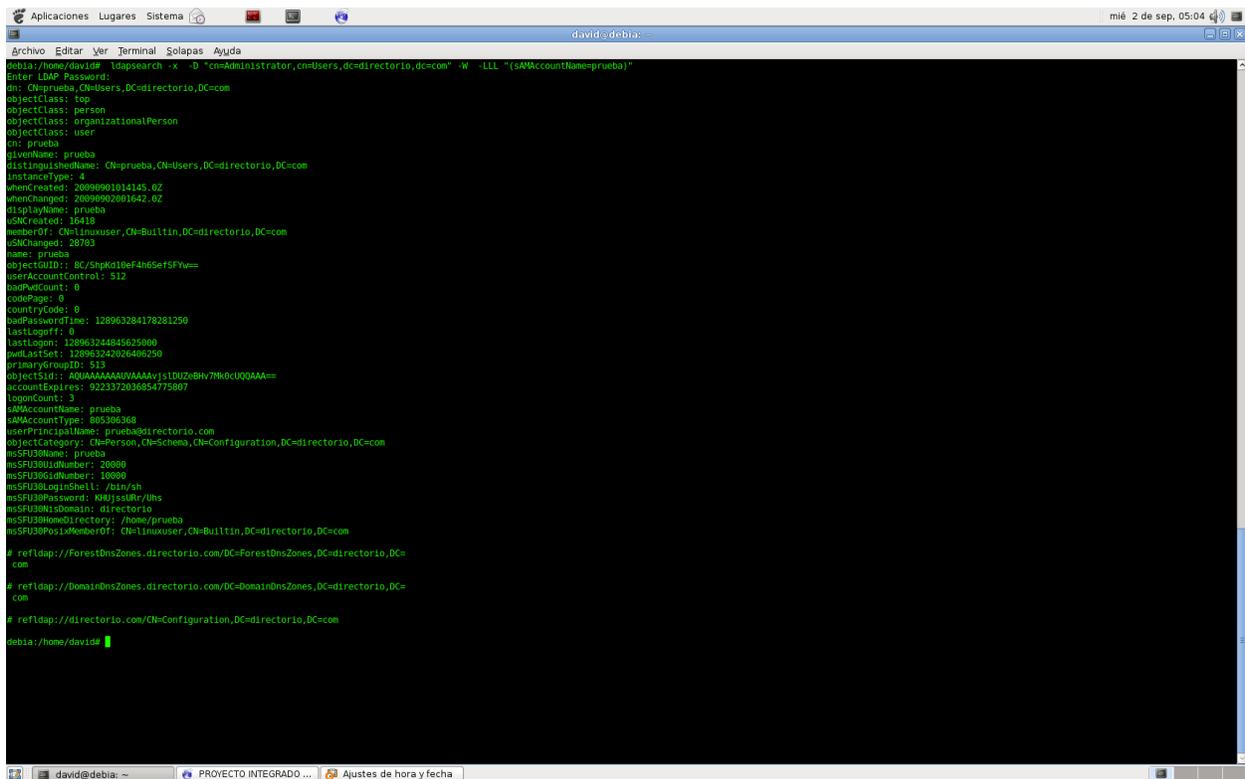
```

ldapsearch -x -D "cn=Administrator,cn=Users,dc=directorio,dc=com" -W -LLL
"(sAMAccountName=prueba)"

```

nos pedira la pass del usuario que emos introducido "-D "cn=Administrator,cn=..."

obtendremos una salida con toda la informacion relacionada con el usuario prueba.



```
Archivo Editar Ver Terminal Solapas Ayuda
debia:/home/david$ ldapsearch -x -D "cn=Administrator,cn=users,dc=directorio,dc=com" -w "LLL" "(sAMAccountName=prueba)"
Enter LDAP Password:
dn: cn=prueba,cn=users,dc=directorio,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: prueba
givenName: prueba
displayShellName: cn=prueba,cn=users,dc=directorio,dc=com
instanceType: 4
whenCreated: 20090901014145.0Z
whenChanged: 20090902010442.0Z
displayName: prueba
uSNCreated: 16418
memberOf: cn=linuxuser,cn=BuiltIn,DC=directorio,DC=com
uSNCreated: 20763
name: prueba
objectGUID:: BC/5hpK10eF4h6SeFSFV==
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 128963284178281250
lastLogoff: 0
lastLogon: 128963244845625000
pwdLastSet: 128963242026406250
primaryGroupID: 513
objectSID:: A00AAAAA00VAAAyJ1DUZvBHv7MkUQ0AAA=
accountExpires: 9223372036854775807
logonCount: 3
sAMAccountName: prueba
sAMAccountType: 805306360
userPrincipalName: prueba@directorio.com
msFSUPName: prueba
msFSUOUIDNumber: 20000
msFSUGuidNumber: 10000
msFSUlogInShell: /bin/sh
msFSUPassword: MjJ5MjRlRjU5
msFSUNisDomain: directorio
msFSUHomeDirectory: /home/prueba
msFSUPosixMemberOf: cn=linuxuser,cn=BuiltIn,DC=directorio,DC=com
# refidap://ForestDnsZones.directorio.com/DC=ForestDnsZones,DC=directorio,DC=com
# refidap://DomainDnsZones.directorio.com/DC=DomainDnsZones,DC=directorio,DC=com
# refidap://directorio.com/CN=Configuration,DC=directorio,DC=com
debia:/home/david$
```

## - /etc/krb5.conf

```
[libdefaults]
    default_realm = DIRECTORIO.COM

[realms]
    DIRECTORIO.COM = {
        kdc = davi-portati.directorio.com
        admin_server = davi-portati.directorio.com
    }

[domain_realm]
    .directorio.com = DIRECTORIO.COM
    directorio.com = DIRECTORIO.COM
```

## -/etc/nsswich.conf

este fichero indica donde deben buscarse los atributos o campos de los usuarios, le añadimos ldap para que tamb busque nuestros usuarios dentro de el servidor ldap

```
passwd:      compat ldap
group:       compat ldap
shadow:     compat ldap
```

### **- /etc/libnss-ldap.conf y /etc/pam\_ldap.conf**

estos dos archivos deben quedar exactamente iguales asi que lo mas adecuado sera configurar uno y que el otro sea un enlace al primero

```
base dc=directorio,dc=com
uri ldap://davi-portati.directorio.com/
ldap_version 3
binddn cn=root,cn=Users,dc=directorio,dc=com
bindpw abc.123
rootbinddn cn=root,cn=Users,dc=directorio,dc=com
nss_map_objectclass posixAccount user
nss_map_objectclass shadowAccount user
nss_map_objectclass posixGroup group
nss_map_attribute uid sAMAccountName
nss_map_attribute uidNumber msSFU30UidNumber
nss_map_attribute gidNumber msSFU30GidNumber
nss_map_attribute loginShell msSFU30LoginShell
nss_map_attribute gecos name
nss_map_attribute uniqueMember msSFU30PosixMember
nss_map_attribute userPassword msSFU30Password
nss_map_attribute homeDirectory msSFU30HomeDirectory
```

### **- /etc/pam.d/common-account**

```
account    sufficient    pam_krb5.so
account    required      pam_unix.so
```

### **- /etc/pam.d/common-auth**

```
auth [success=done default=ignore] pam_unix.so likeauth nullok_secure try_first_pass
auth [authinfo unavail=ignore success=1 default=2] pam_krb5.so ccache=/tmp/
krb5cc_%u use_first_pass
```

### **- /etc/pam.d/common-auth**

```
ssword    sufficient    pam_krb5.sopassword    required    pam_unix.so
```

### **- /etc/pam.d/common-session**

```
session    required      pam_unix.so
```

### **Crear la carpeta del usuario**

Crearemos una carpeta para el usuario alojado en el servidor ldap y le cambiaremos el propietario indicando su uid y gid que solo existen en el servidor ldap

```
mkdir /home/prueba  
chown 20000:10000 /home/prueba
```

en el comando chown el 20000 es el uid del usuario y el 10000 es el gid del grupo

y con estos cambios ya podremos iniciar una sesión de un usuario alojado en el servidor ldap

-----

## **Configuración del equipo windows**

La configuración del equipo windows es más sencilla que la anterior, empezaremos al igual que en el caso anterior con la configuración de la red, la pondremos en modo dhcp o automática para que nuestro servidor le de una ip que este libre.

El siguiente paso será introducir un registro en el dns del servidor con los datos del equipo windows para ello nos vamos a la pestaña de administración de servicio dns del servidor y en la zona de búsqueda directa le damos botón derecho new host(A) e introducimos los datos necesarios, nos pedirá el nombre del equipo en este caso sobremesa, una dirección ip en este caso la dirección ip asignada a sido la 192.168.1.101 y marcaremos la casilla que indica si queremos que nos cree el registro de la zona inversa automáticamente.

Lo siguiente será introducir el equipo en el dominio directorio.com, para ello hacemos clic con el botón derecho en mipc y en propiedades, nos vamos a la pestaña nombre del equipo pulsamos el botón cambiar nos aparecerá una ventana en la que abajo nos saldrá la opción de cambiar de un grupo de trabajo a un dominio clicamos y en el recuadro introducimos el nombre de nuestro dominio directorio.com y pulsamos aceptar, al hacer esto aparecerá una ventana en la que nos pedirá un nombre y un usuario, el usuario debe ser un usuario del dominio con permisos de administración, introducimos el nombre del usuario en nuestro caso administrator y su contraseña, después de esto solo necesitaremos reiniciar para poder iniciar sesión como miembro del dominio.