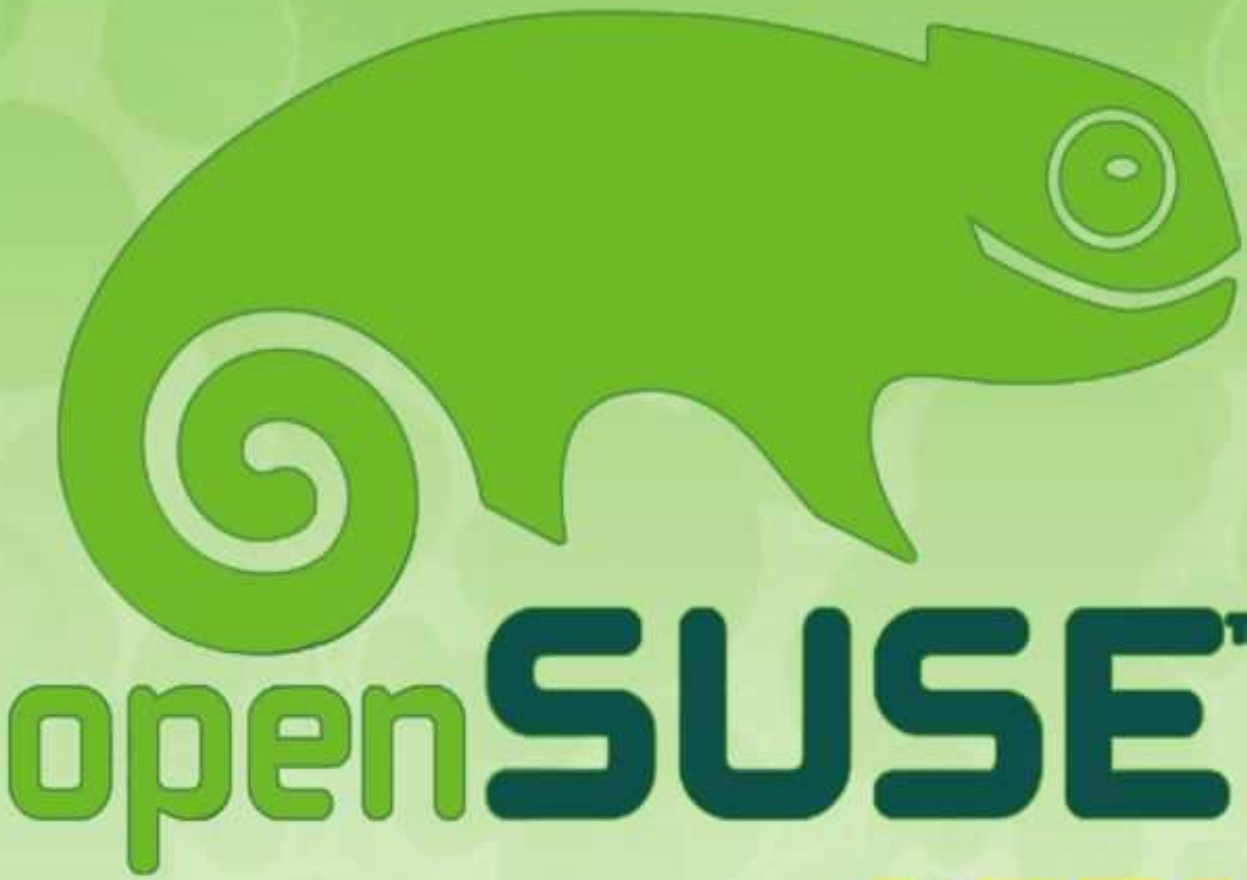
# openSUSE 11.2 con Samba

# Guia Ilustrada



openSUSE™

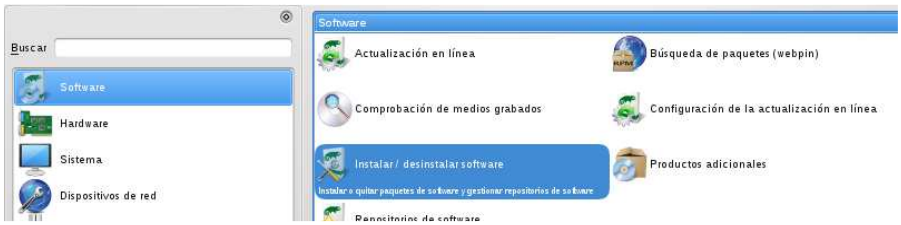

**Eduardo Adolfo Sotomayor G.**

# 1.- OpenSUSE 11.2 participando en un grupo de trabajo mixto.

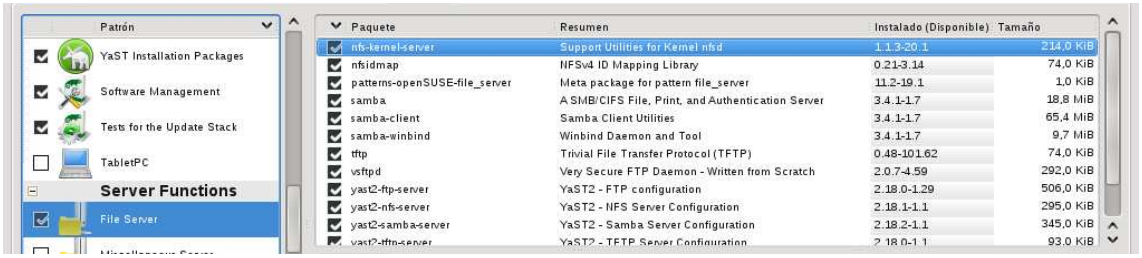
## 1.1 Planteamiento del problema

En este escenario tenemos un grupo de trabajo de unas 10 o 20 maquinas, en este grupo de trabajo tenemos computadoras con openSUSE y Windows XP, era necesario tener un entorno de red estable y que las computadora compartieran archivos entre si fácilmente de forma que los usuarios no tengan ningún inconveniente al momento de necesitar sus archivos en red, recordemos que en este ejemplo los usuarios deben ser coincidentes entre los equipos de la red.

Para instalar samba nos vamos a Yast – Software – Instalar/Desinstalar Software




Luego Seleccionamos Ver – Patrones nos vamos a la sección Server Functions y damos clic en el checkbox File Server.




## 1.2 Configurando la navegación de red.

Luego debemos configurar nuestra navegación por medio del entorno de red, de forma que este sea estable y no nos de errores de acceso para ello agregamos las siguientes opciones a nuestro archivo smb.conf en cual se encuentra en /etc/samba/ usando ya sea kwrite o vi.


Workgroup name = nombre_del_grupo_de_trabajo
Netbios name = nombre_de_la_maquina
Name resolve order = bcast host lmhost wins
Local master = yes

Preferred master = yes
Os level = 65
Server string = “”

## 1.3 Descripción de las opciones

Estas opciones deben ir en la sección [global] del archive smb.conf y se describen con mayor detalle a continuación.

Workgroup name = nombredelgrupodetrabajo

Esto define el grupo de trabajo al que va a pertenecer la maquina.

Netbios name = nombredelamaquina

Esta opción define el nombre de la maquina en el grupo de trabajo.

Name resolve order = bcast host lmhost wins

Esta opción se usa en los programas de Samba para determinar qué servicios de nombres y en qué orden resolver nombres de hosts a direcciones IP. Su principal función es controlar como se realiza la resolución NetBIOS. Esta opción toma una cadena, separada por espacios, de diferentes opciones de resolución, en nuestro ejemplo usaremos difusión como primera opción.

Local master = yes

Esta opción le indica al servidor mantener una lista local de las maquinas de su subred.

Preferred master = yes  (si ya hay uno omitir)

Este parámetro booleano controla si Samba es un examinador principal de listas principal para su grupo de trabajo.

Si se pone a yes, al iniciar, samba forzará una elección y tendrá una ligera ventaja para ganar la elección.

Use esta opción con precaución, porque si hay varios hosts (servidores samba, Windows 95 o NT) que son examinadores de listas preferidos en la misma subred, intentarán continua y periódicamente convertirse en examinador principal local. Esto ocasiona un tráfico de difusión innecesario y reduce las capacidades de las listas.

Os level = 65 (si ya hay uno y desea que este sea secundario poner 33, omitir para las demás estaciones linux)

Este entero controla el nivel en que se anuncia samba a si mismo para la elección de examinador. El de este parámetro determina si nmbd tiene oportunidad de convertirse en examinador principal del Grupo de Trabajo en el área de difusión local.

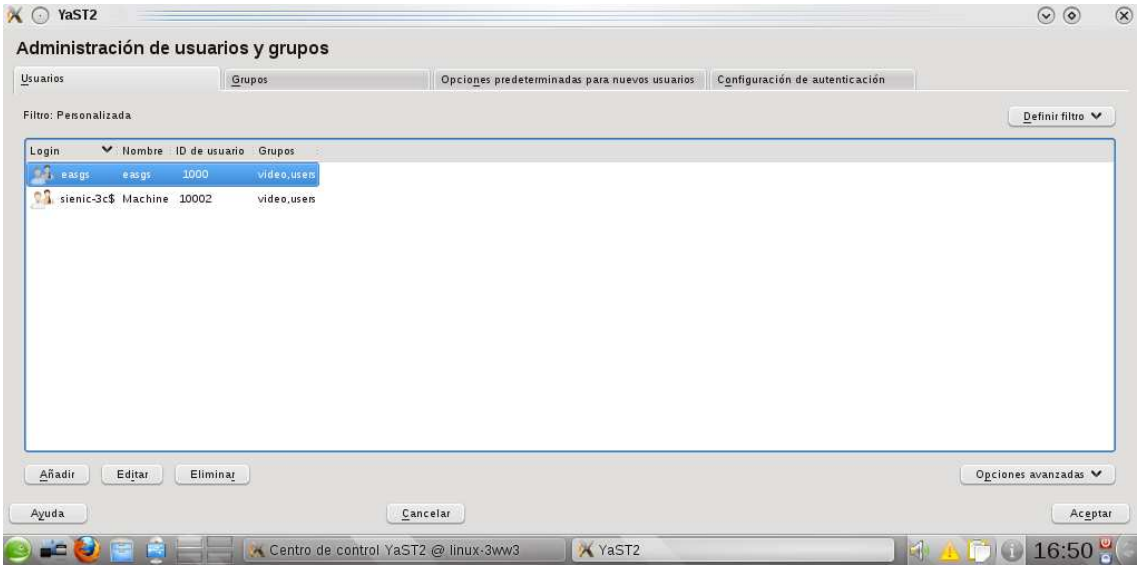
Al poner el valor a 65 se asegura que ganara sobre cualquier otro sistema operativo en la red

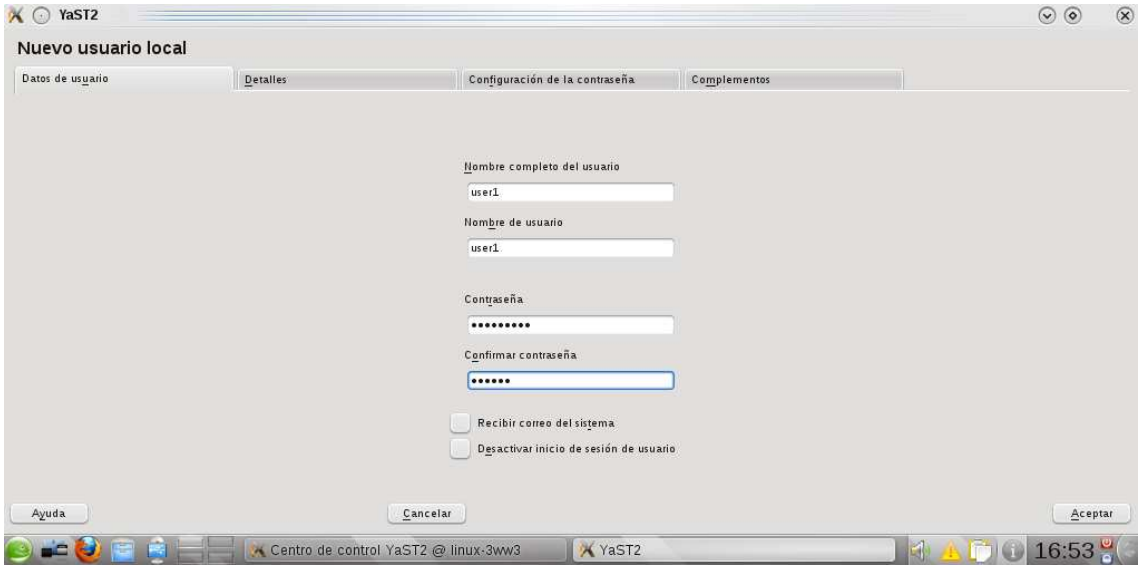
Server string = “”

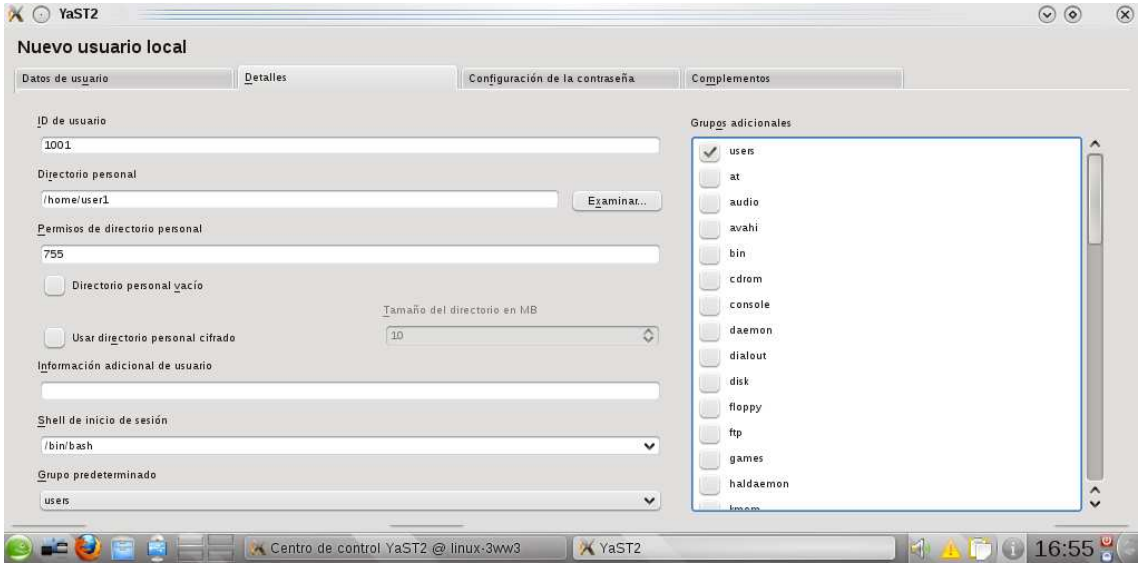
Esto controla qué cadena aparecerá en el cuadro de comentario de la impresora en el gestor de impresión y en la conexión IPC en “net view”. Puede ser cualquier cadena que quiera que vean sus usuarios y es la descripción de su equipo en el entorno de red, si se deja en blanco se usara el nombre de la maquina.

## 1.4 Creando los usuarios en openSUSE 11.2 con Yast

Con esto ya tenemos configurado nuestro grupo de trabajo y la navegación del entorno de red, ahora vamos a compartir un recurso, para esto debemos primero crear los usuarios Linux usando Yast-Gestión de usuarios y grupos-seleccionamos la solapa Usuarios y hacemos clic en añadir, registramos los datos del usuario y luego hacemos clic en la solapa Detalles y agregamos el usuario a los grupos respectivos.




## 1.5 Agregando los usuarios a samba

Después agregar esos usuarios a samba con el comando.

Smbpasswd –a user1
Smbpasswd –a user2

Recordemos usar los nombres que necesitemos.

## 1.6 Compartiendo recursos

Este es el ejemplo de un recurso compartido que va al final del archivo smb.conf

[carpetacompartida]

Path=/home/easgs/sharedfolder
Read list = user1 user2

Write list = user3 user4
Force user = easgs
Guest ok = no
Valid users= user1 user2 user3 user4 easgs

Este es el detalle de las opciones.

Path=/home/easgs/sharedfolder

Es la ruta a la carpeta compartida.

Read list = user1 user2

Los usuarios de esta lista solo tendrán acceso de lectura.

Write list = user3 user4

Los usuarios de esta lista tendrán acceso total

Force user = easgs

Esta opción fuerza que los usuarios que se logean al servicio lo hagan como el usuario easgs por lo tanto todo lo que hagan será con los mismo derechos de este usuario, aun así, los usuarios listados en read list solo tendrán acceso de lectura.

Guest ok = no

Si este parámetro es yes para un servicio, entonces no se requiere clave para conectar con dicho servicio. Los privilegios serán los mismos de guest account.

En este caso no permitiremos eso.

Valid users= user1 user2 user3 user4 easgs

Estos usuarios son los únicos permitidos para usar este recurso.

Para crear sharedfolder primero creamos la carpeta con el usuario que sera propietario y luego ejecutamos el siguiente comando como root, puede usar el nombre de carpeta que mas le convenga.

chmod 775 /sharedfolder

## 1.7 smb.conf final

Al finalizar nuestro archivo smb.conf se vera como el siguiente ejemplo

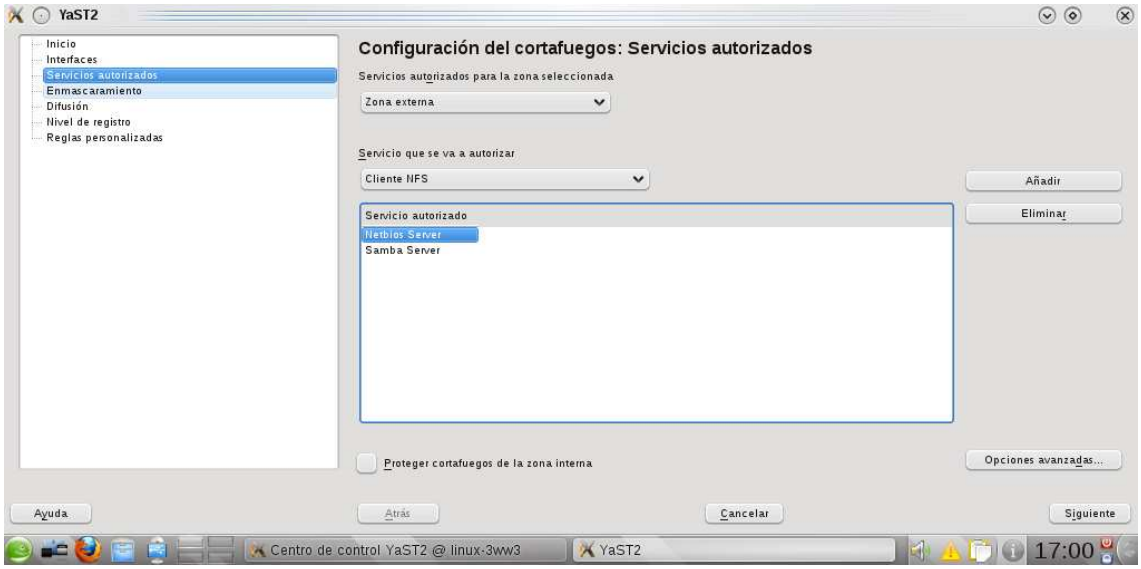
```
[global]
        workgroup = nombredelgrupodetrabajo
        passdb backend = tdbsam
        printing = cups
        printcap name = cups
        printcap cache time = 750
```

```
        cups options = raw
        map to guest = Bad User
        include = /etc/samba/dhcp.conf
        logon path =
        logon home =
        logon drive = P:
        usershare allow guests = No
        netbios name = nombredelamaquina
        resolve name order = bcast host lmhosts win
        local master = yes
        preferred master = yes
        os level = 65
        server string = ""

[homes]
        comment = Home Directories
        valid users = %S, %D%w%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
[users]
        comment = All users
        path = /home
        read only = No
        inherit acls = Yes
        veto files = /aquota.user/groups/shares/
[groups]
        comment = All groups
        path = /home/groups
        read only = No
        inherit acls = Yes
[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No
[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @ntadmin root
        force group = ntadmin
        create mask = 0664
        directory mask = 0775

[sharedfolder]

        Path=/home/easgs/sharedfolder
        Read list = user1 user2
        Write list = user3 user4
        Force user = easgs
        Guest ok = no
        Valid users= user1 user2 user3 user4 easgs
```

Las configuraciones no explicadas en este ejemplo se explican con detalle en los ejemplos mas adelante.

## 1.8 Autorizando los servicios en el Firewall

Para que esto funcione debemos habilitar en el firewall los servicios samba server y Netbios Server a como se muestra a continuación.




Con esto ya tenemos configurado openSUSE para comunicarse con estaciones Windows así como también con otras estaciones con Linux instalado usando samba.

## 1.9 Agregando nuevas estaciones openSUSE 11.2 a la red.

***Nota: Si ya contamos con una maquina en el grupo de trabajo con estas mismas configuraciones, entonces tenemos que modificar las siguientes opciones a como sigue:***

Local master = no
Preferred master = no
Os level = 0

# 2.- openSUSE 11.2 como controlador de Dominio con el tdbsam backend

## 2.1 Planteamiento del problema

Este es un ejemplo de un servidor openSUSE 11.2 configurado como PDC usando samba, en este escenario, era requerido un controlador de dominio para una red de hasta 50 computadoras con Windows XP Professional SP-3 sin necesidad de un BDC por lo que se usara el backend tdbsam, de lo contrario se tendría que usar LDAP, se usara wins para la resolución de nombres, este servidor no funcionara como servidor de impresión por lo que esas opciones no se explican, para evitar redundancia tampoco se explican opciones ya planteadas previamente en el documento, también se necesita el servicio de DHCP para asignar dinámicamente las direcciones IP a las estaciones de trabajo y ofrecer el servidor wins.

¿Porque este escenario?

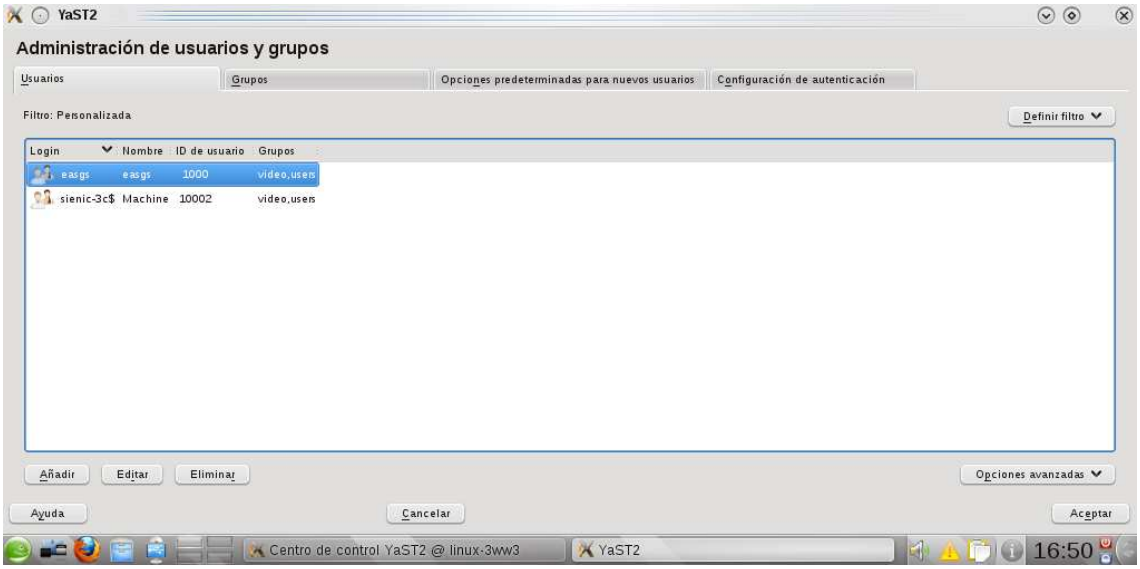
Porque este es el escenario mas común con el que se encuentra un administrador de redes y abarca una gran cantidad de empresas en el ámbito nacional, redes de 10 hasta 50 computadoras, cabe mencionar que el equipo samba dice que el tdbsam se puede usar en redes con hasta 250 usuarios, en cualquier otro escenario LDAP es la recomendación.

## 2.2 ¿Que es un controlador de dominio?

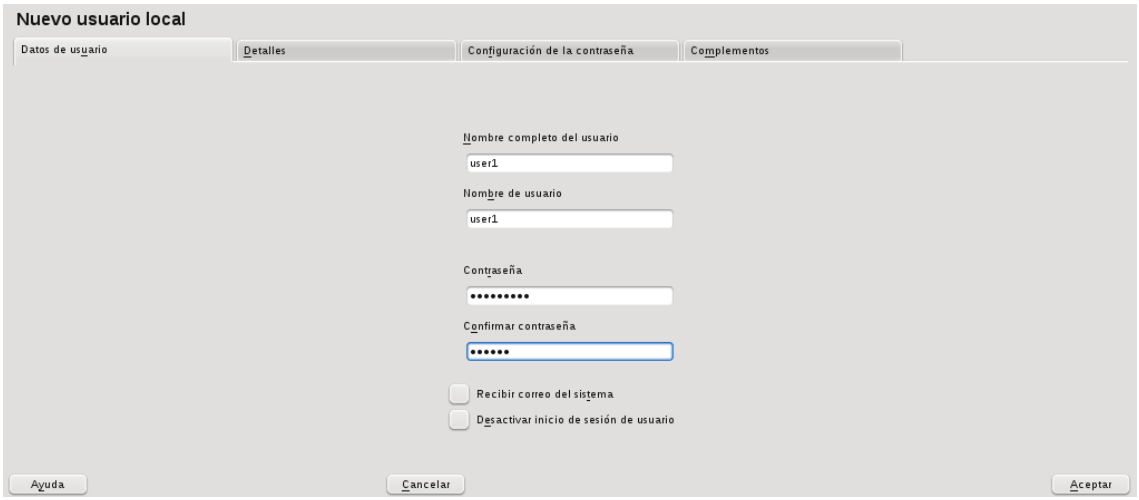
Un Domain Controller o controlador de dominio contiene una base de datos de todos los usuarios y las maquinas que son parte de nuestra red, de esta manera podemos administrar los recursos y políticas de seguridad de manera centralizada y esto nos permite tener un ambiente mas seguro y cómodo para trabajar.

## 2.3 Creando los usuarios

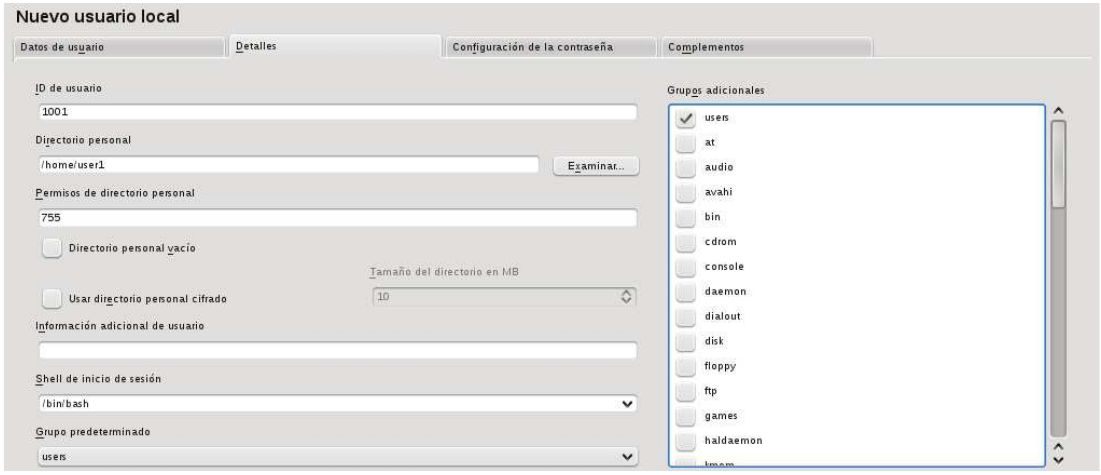
Para comenzar debemos crear primero los usuarios easgs easgs1 easgs2 easgs3 (sustituya con el nombre que mas le convenga) en openSUSE usando Yast – Seguridad y Usuarios - Gestión de usuarios y grupos.




Hacemos clic en añadir y registramos los datos del usuario, luego hacemos clic en detalles




Aquí hacemos al usuario miembro del grupo users haciendo clic en el para seleccionarlo



## 2.4 smb.conf final

Este es el archivo smb.conf completo el cual se encuentra en la ruta /etc/samba y se puede editar usando kwrite o vi, tenemos que editarlo y dejarlo a como el ejemplo.

```
[global]

        workgroup = BLUE
        netbios name = suse-blue
        domain logons = yes
        domain master = yes
        local master = yes
        os level = 65
        preferred master = yes
        security = user
        logon path =
           logon home =
        logon drive = P:
        passdb backend = tdbsam
           usershare allow guests = No
        add machine script = /usr/sbin/useradd  -c Machine -d /var/lib/nobody -s /bin/false %m$
        name resolve order = wins bcast host lmhost
        server string = “”
        printing = cups
        printcap name = cups
        printcap cache time = 750
        cups options = raw
           map to guest = Bad User
        wins support = yes

[homes]

        comment = Home Directories
        valid users = %S, %D%w%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

[printers]

        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No

[print$]

        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @ntadmin root
        force group = ntadmin
        create mask = 0664
        directory mask = 0775

[netlogon]

        comment = network logon service
        path = /var/lib/samba/netlogon
        write list = root

[datos]
        comment = datos varios
        force user = easgs
```

```
guest ok = No
inherit acls = Yes
path = /home/easgs/datos/
valid users = easgs easgs1 easgs2 easgs3
write list = easgs easgs1
read list = easgs2 easgs3
```

Nota: En este ejemplo fueron removidos los recursos compartidos **[homes]** y **[groups]** los cuales se explican con detalle mas adelante.

## 2.5 Descripción de las opciones

Sección [Globals]

La sección [globals] aparece en todos los ficheros de configuración de Samba, aunque no es obligatoria su definición. Cualquier opción de esta sección se aplicará al resto de recursos, como si los contenidos de la sección se copiasen a todas las demás. Sólo una salvedad: otras secciones pueden contener la misma opción pero con distinto valor; lo último prevalece siempre sobre lo antiguo, así que ese último valor prevalecerá sobre el establecido en la sección [globals].

Workgroup = BLUE

Esta opción establece el nombre de nuestro dominio a BLUE, ponga el que Ud. crea conveniente para su caso.

Netbios name = suse-blue

Este parámetro fija el nombre NetBIOS por el cual es conocido el servidor Samba a suse-blue, ponga el que Ud. crea conveniente para su caso.

.

Domain logons = yes

Configura a Samba para aceptar accesos en el dominio actuando como PDC.

Domain master = yes

Activa la comparación de lista WAN. Este parámetro indica a nmbd que solicite un nombre NetBIOS de dominio especial que lo identifica como examinador principal del dominio para el grupo de trabajo dado. Los examinadores locales del mismo grupo de trabajo dado en subredes-aisladas proporcionan a este nmbd sus listas locales, y solicitan a smbd una copia completa de la lista a la red amplia. Entonces las listas de clientes contactan con sus servidores locales y reciben una lista de la red amplia, en lugar de las listas de las subredes.

En pocas palabras mantiene una lista completa de todas las maquinas del dominio.

Local Master = yes

Le indica al servidor a mantener una lista local de las maquinas de su subred.

Os level = 65

Este entero controla el nivel en que se anuncia samba a si mismo para la elección de examinador. El de este parámetro determina si nmbd tiene oportunidad de convertirse en examinador principal del Grupo de Trabajo en el área de difusión local.

Al poner el valor a 65 se asegura que ganara sobre cualquier otro sistema operativo en la red

Preferred master = yes

Este parámetro booleano controla si Samba es un examinador principal de listas principal para su grupo de trabajo.

Si se pone a yes, al iniciar, samba forzará una elección y tendrá una ligera ventaja para ganar la elección. Es recomendable que este parámetro se use en conjunción con domain master = yes, para que samba pueda garantizar convertirse en un domain master.

Use esta opción con precaución, porque si hay varios hosts (servidores samba, Windows 95 o NT) que son examinadores de listas preferidos en la misma subred, intentarán continua y periódicamente convertirse en examinador principal local. Esto ocasiona un tráfico de difusión innecesario y reduce las capacidades de las listas.

Security = user

La seguridad a nivel de usuario es la configuración predeterminada para Samba. Aún si la directriz security = user no está listada en el archivo smb.conf, es utilizada por Samba. Si el servidor acepta la combinación de nombre de usuario/contraseña del cliente, el cliente puede montar múltiples recursos compartidos sin tener que especificar una contraseña para cada instancia. Samba también puede aceptar solicitudes de nombre de usuario/contraseña basadas en la sesión. El cliente mantiene múltiples contextos de autenticación usando un único UID por cada inicio de sesión.

Logon path =

Este parámetro indica el directorio home donde se guardan los ficheros de perfiles (NTuser.dat para windows NT).

Esta opción toma las sustituciones estándar, permitiendo tener script de conexión para cada usuario o máquina. También especifica el directorio desde el cual se cargan los contenidos de las carpetas “escritorio”, “menú inicio”, “programas” y “entorno de red” y se muestran en sus clientes Windows NT.

El recurso y la ruta deben poderse leer por el usuario para que las preferencias y los directorios sean cargados en los clientes Windows NT. El recurso debe tener permiso de escritura, al menos la primera vez que el usuario se conecta, para que los clientes Windows NT puedan crear el fichero user.dat y otros directorios.

Los directorio y cualquiera de los contenidos, pueden, si se necesita, ponerse como sólo lectura. No es conveniente que el fichero NTuser.dat se haga de sólo lectura,

renómbrelo como NTuser.man para llevar a cabo los efectos deseados ( MANdatory profile).

Los clientes Windows algunas veces pueden mantener conexiones a los recursos [homes], incluso si no hay usuario registrado. Por tanto es vital que la ruta de logon no incluya una referencia a los recursos homes (i.e \\%L\HOMESrofile_path causará problemas). .
Esta opción toma las sustituciones estándar, permitiendo tener script de conexión para cada usuario o máquina.

Tenga en cuenta que esta opción sólo es válida si Samba está configurado como logon server.

Para deshabilitar los perfiles móviles esta opción se deja sin definir, de esta manera se forzara a Windows a crear el perfil en la maquina local que es el caso de nuestro ejemplo, bajo Windows Xp esto se puede verificar en propiedades de la PC, opciones avanzadas, perfiles de usuarios, configuración, en el campo tipo debe de decir local.

Logon home =

Este parámetro especifica la ubicación del directorio home cuando se conectan estaciones Win95/98 a un PDC Samba, en nuestro ejemplo lo dejamos en blanco para deshabilitar los perfiles moviles.

Logon drive = F:

Mapea la carpeta home del usuario a la unidad F: cabe mencionar que puede ser cualquiera siempre y cuando no entre en conflicto con una existente, al dar doble clic sobre el icono de Mi Pc nos aparecerá esta unidad.

Passdb backend = tdbsam

Esta opción permite al administrador elegir qué sistema o backend usa para guardar y recuperar contraseñas. Permite, por ejemplo, usar smbpasswd y tdbsam sin recompilar. Se pueden especificar múltiples backends separados por espacios. Los backends se usan en orden en el que se especifican. Los nuevos usuarios siempre se añaden al primer backend especificado, en nuestro ejemplo se usa tdbsam.

usershare allow guests = No

En nuestro servidor solo el administrador podrá crear recursos compartidos usando el archivo smb.conf por eso dejamos este parámetro con valor “no”.

Add machine script = /usr/sbin/useradd –c Machine –d /var/lib/nobody –s /bin/false %m$

Esta es la ruta completa a un guión que smbd ejecutará cuando agregue una máquina a su dominio usando el método con las contraseñas y claves del administrador.

En este ejemplo se creara la cuenta de la maquina usando el nombre netbios de la misma junto con el carácter $ en el archivo de passwords, también se pondrá el comentario Machine y lo agregara al grupo users que es el predeterminado para opensuse, después que unamos una maquina si revisamos nuestra lista de usuarios Linux y samba tendremos la nueva entrada con el nombre de la maquina con el carácter $ al final.

Name resolve order = wins bcast host lmhost

Esta opción se usa en los programas de Samba para determinar qué servicios de nombres y en qué orden resolver nombres de hosts a direcciones IP. Su principal función es controlar como se realiza la resolución NetBIOS. Esta opción toma una cadena, separada por espacios, de diferentes opciones de resolución.

Las opciones son “lmhosts”, “host”, “wins” y “bcast”. Hacen que los nombres se resuelvan de la siguiente forma:

lmhosts : Busca una dirección IP en el fichero lmhosts de Samba. Si la línea de lmhosts no tiene tipo de nombre adjuntado al nombre NetBIOS (vea lmhosts(5)) entonces vale cualquier tipo para la búsqueda.

host : Hace una resolución de nombre de host a dirección IP usando el sistema de resolución del sistema /etc/hosts , NIS, o búsquedas DNS. Este método de resolución depende del sistema operativo (por ejemplo, en IRIX o Solaris esto puede ser controlado por el fichero /etc/nsswitch.conf). Observe que este método se usa sólo si el tipo de nombre NetBIOS consultado es tipo 0×20 (server) o nombre tipe 0×1c (controladores de dominio). El último caso es solo útil para dominios Active directory y resultan de una consulta para la entrada SRV RR que verifique _ldap._tcp.domain.

wins: Pregunta por un nombre en la dirección IP address indicada en el parámetro wins server. Si no se ha especificado servidor WINS, este método se ignora (no se debería usar wins si no se cuenta con mas de una subred).

bcast : Efectúa una difusión (broadcast) en cada interfaz local conocido listado en el parámetro interfaces = . Este es el método de resolución menos seguro ya que depende de los hosts que están conectados en la red local.

Server String =””

Esto controla qué cadena aparecerá en el cuadro de comentario de la impresora en el gestor de impresión y en la conexión IPC en “net view”. Puede ser cualquier cadena que quiera que vean sus usuarios y es la descripción de su equipo en el entorno de red, en este ejemplo lo dejamos en blanco para que muestre el nombre del servidor.

Map to guest = bad user

Este parámetro sólo es últil cuando el parámetro security tiene un valor distinto a security=share, user, server y domain.

Bad User - Significa que las solicitudes de conexión con una clave incorrecta se rechazan, salvo que el nombre de usuario no exista, en cuyo caso se trata como una conexión de invitado y se aplica en guest account.

Observe que para este parámetro es necesario poner el servicio compartido "invitado" cuando use modos de seguridad (security) distintos a "share". Esto es porque en estos modos el nombre del recurso que se solicita NO se envía al servidor hasta una vez que el servidor ha validado correctamente al cliente y el servidor no puede tomar decisiones en el momento adecuado (conexión al recurso) para recurso "invitados".

Wins support = yes

Este parámetro booleano controla si Samba actúa como servidor WINS. No debería ponerlo como yes salvo que tenga una red multi-sub-red y quiera que un nmbd particular sea su servidor WINS. Tenga en cuanta que NUNCA debería poner esto como true en más de una máquina de su red. .

La sección [homes]

Si existe una sección denominada [homes] incluida en el fichero de configuración, los clientes se podrán conectar a su directorio HOME del servidor.

Comment = Homes directories

Descripción del servicio

Valid users = %S, %D%w%S

Significa que para los usuarios validos se tomaran del valor del servicio actual o el nombre del dominio o grupo de trabajo del usuario actual, nadie más podrá entrar.

Browseable = no

Significa que los usuarios no podrán navegar en el recurso a través del entorno de red pero si podrán ver el recurso homes, cuando se configura a yes en el entorno de red aparecen dos recursos compartidos unos con el nombre del usuario y otro llamado homes.

Read only = no

Por defecto samba siempre configura cualquier directorio como de solo lectura por razones de seguridad, por lo tanto debemos indicarle que queremos ser capaces de escribir en este directorio.

Inherit acls = yes

Este parámetro se puede usar para asegurar que si existen ACL predeterminadas en el directorio padre, estas se asignan cuando se crean subdirectorios. El comportamiento predeterminado es usar el modo especificado cuando se crea un directorio. Al activar

esta opción fija el modo 0777, así garantiza que el las acl predeterminadas del directorio se propagan.

Las ACL son listas que le dicen al sistema operativo u otros dispositivos de red que permisos tiene cada usuario sobre cada objeto en una computadora o dispositivo de red.

Sección [Profiles]

Es una sección especial que define parámetros para perfiles de red de los usuarios.

Path = %H

Es la ruta dada por el nombre del directorio home del usuario obtenido por %u que es el nombre del servicio actual.

Store dos attributes = yes

Esta opción le indica a samba usar el atributo extendido “userDOSATTRIB” para almacenar los permisos ocultos del sistema de archivos DOS “hidden” y “system”.

Create mask = 0600

Cuando se crea un fichero, los permisos necesarios se calculan de acuerdo con la asociación de los modos DOS a los permisos UNIX, y los modelos UNIX resultantes son una AND bit a bit con este parámetro. Este parámetro es una máscara de bits para los modelos UNIX. Cualquier bit no puesto se elimina del conjunto cuando se crea un fichero.

En este caso el propietario tendrá derecho de lectura y escritura y le quitara todos los privilegios a los demás.

Directory mask = 0700

Este parámetro es el modo octal que se usa cuando se convierte el modo DOS al modo UNIX al crear directorios UNIX.

Cuando se crea un directorio, los permisos necesarios se calculan de acuerdo con la traducción de los modos DOS a los permisos UNIX, y el modo UNIX resultante es un AND de los bits correspondientes con este parámetro. Este parámetro puede ser un máscara de bits para los modos UNIX de un directorio. Cualquier bit not puesto aquí se elimina de los modos del directorio cuando se crea.

En este caso el propietario tendrá derechos de lectura escritura y ejecución y les quitara todos los privilegios a los demás.

Sección [netlogon]

Aquí especificamos dónde está el netlogon.

Path= /var/lib/samba/netlogon

Dentro de esta carpeta debemos ubicar los archivos logon script en caso que deseemos usar uno

Write list = root

Esto significa que solo el administrador tiene acceso de lectura a este recurso nadie mas.

## 2.6 Explicación del recurso compartido [datos]

Force user = easgs

Esta opción fuerza que los usuarios que se logean al servicio lo hagan como el usuario easgs por lo tanto todo lo que hagan será con los mismo derechos de este usuario.

path = /home/easgs/datos/

El recurso compartido se encuentra en la carpeta home del usuario easgs.

Guest ok = no

Si este parámetro es yes para un servicio, entonces no se requiere clave para conectar con dicho servicio. Los privilegios serán los mismos de guest account.

En este caso no permitiremos eso.

Valid users = easgs easgs1 easgs2 easgs3

Estos usuarios son los únicos permitidos para usar este recurso, en el caso de que sean muchos usuarios se pueden definir los respectivos grupos por ejemplo valid users= @grupo1 @grupo2.

Write list = easgs easgs1

Estos usuarios son lo únicos permitidos para escribir en este recurso, en el caso de que sean muchos usuarios se pueden definir los respectivos grupos por ejemplo write list = @grupo1 @grupo2.

Read list = easgs2 easgs3

Estos usuarios solo tienen permiso de lectura en este recurso, en el caso de que sean muchos usuarios se pueden definir los respectivos grupos por ejemplo read list = @grupo1 @grupo2.

## 2.7 Creando la carpeta de ejemplo datos

Para crear datos, primero creamos la carpeta con el usuario que será propietario y luego ejecutamos el siguiente comando como root, recuerde usar el nombre de carpeta que mas le convenga.

chmod 775 /datos

## 2.8 Agregar los usuarios a samba.

Para que esto funcione primero debemos crear los usuarios en Linux usando yast (lo cual ya hicimos al inicio de este ejemplo), luego ejecutamos el siguiente comando por cada usuario para agregarlo a samba.

pdbedit –a easgs

## 2.9 Mapeo de los grupos UNIX a grupos Windows.

Cuando unimos una maquina con Windows XP a un controlador de dominio de la gama se servidores Windows server y queremos compartir un recurso tenemos la opción de agregar los grupos domain users u otros para abarcar todos esos usuarios, para tal efecto, en samba ejecutamos los siguiente lo cual es mandatorio al menos para estos tres grupos.

net groupmap add ntgroup=”Domain Admins” unixgroup=root rid=512

net groupmap add ntgroup=”Domain Users” unixgroup=users rid=513

net groupmap add ntgroup=”Domain Guests” unixgroup=nobody rid=514

Esto hará que el grupo detectado por la estación Windows como Domain Users sea en verdad el grupo UNIX users, y tomara todos los usuarios de dicho grupo siempre y cuando existan en el password backend de samba.

## 2.10 Asignación de derechos al grupo Domain Admins.

Esto es necesario para que los miembros de este grupo reciban los privilegios del administrador del dominio, de este modo podemos crear un usuario llamado Administrator y agregarlo a este grupo y con esa cuenta unir las maquinas al dominio y no con la cuenta root, para esto ejecutamos el siguiente comando:

net -S localhost -U root rpc rights grant "suse-blue\Domain Admins" SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege

Donde suse-blue es el nombre del servidor, esto nos pedirá la clave de la cuenta del root de samba.

## 2.11 Revocando los derechos al grupo Domain Admins.

net -S localhost -U root rpc rights revoke "suse-blue\Domain Admins" SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege

## 2.12 Listando los Privilegios asignados a los grupos samba.

Para revisar que privilegios se han asignado a los distintos grupos ejecutamos lo siguiente:

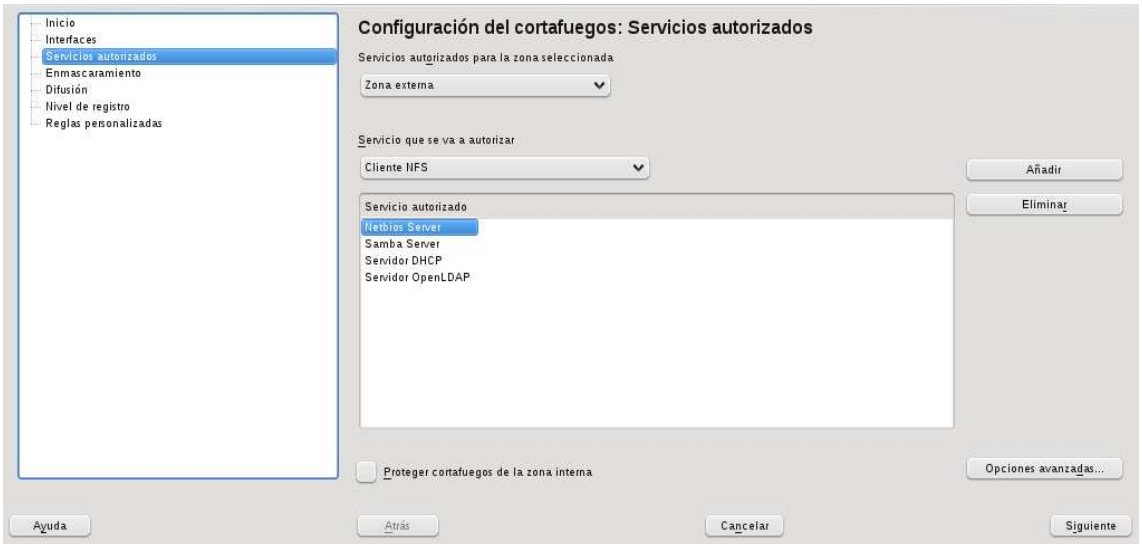
net -S localhost -U% rpc rights list accounts

## 2.13 El FIREWALL

Para que esto funcione debemos habilitar en el firewall los servicios samba server, DHCP y Netbios.

Yast-Seguridad y usuarios-Cortafuegos


Servicios autorizados – servicio que se va a autorizar, seleccionamos los servicios y hacemos clic en añadir.




El uso del servidor DHCP nos ahorra el trabajo de estar configurando manualmente los protocolos TCP/IP en cada maquina, lo único que tendremos que hacer es unir las estaciones con Windows XP a nuestro server a como lo haríamos con cualquier controlador de dominio con Windows server 2003 o 2008, ahora pasemos a configurar el servidor DHCP a la pagina numero 66.

Con esto ya tenemos funcionando nuestro servidor samba como controlador de dominio.

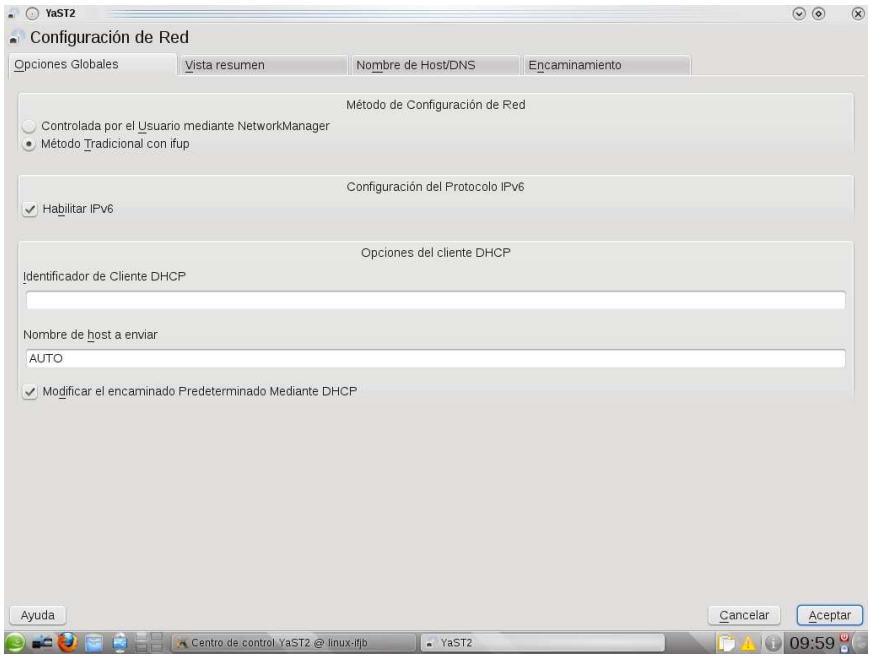
## 3.- OpenSUSE 11.2 como controlador de dominio usando openLDAP como backend.

### 3.1 Planteamiento del problema

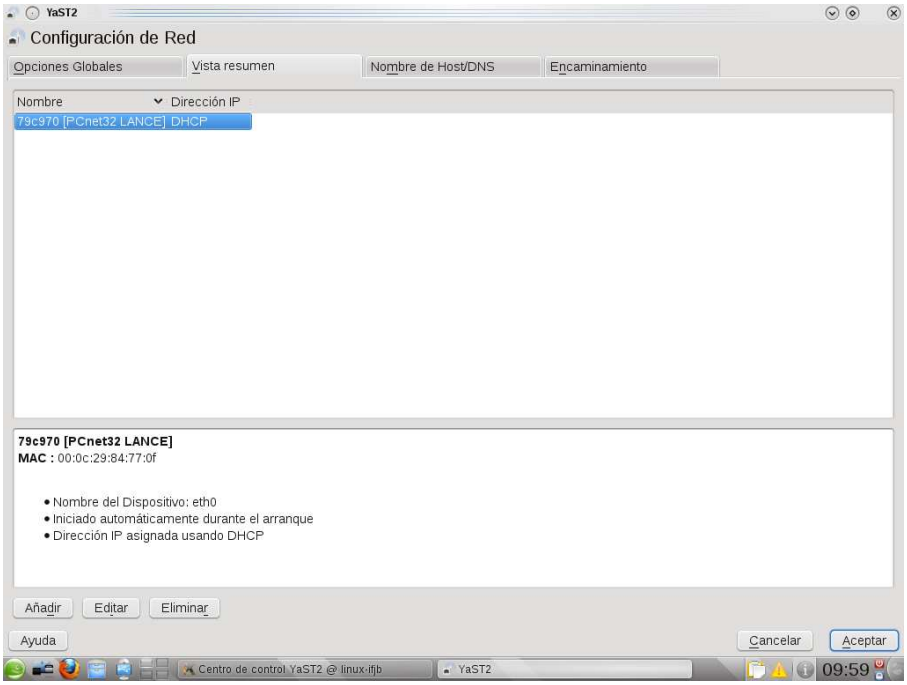
Este es un ejemplo de un servidor openSUSE 11.2 configurado como PDC usando samba, en este escenario, era requerido un controlador de dominio para una red de hasta 200 computadoras con Windows XP Professional SP-3, pero podría crecer mas por lo que se usara el backend ldapsam para poder incluir un BDC en el futuro, se usara wins para la resolución de nombres, este servidor no funcionara como servidor de impresión por lo que esas opciones no se explican, para evitar redundancia tampoco se explican opciones ya planteadas previamente en el documento, también se necesita el servicio de DHCP para asignar dinámicamente las direcciones IP a las estaciones de trabajo y ofrecer el servidor wins.

### 3.2 Configuración de la red

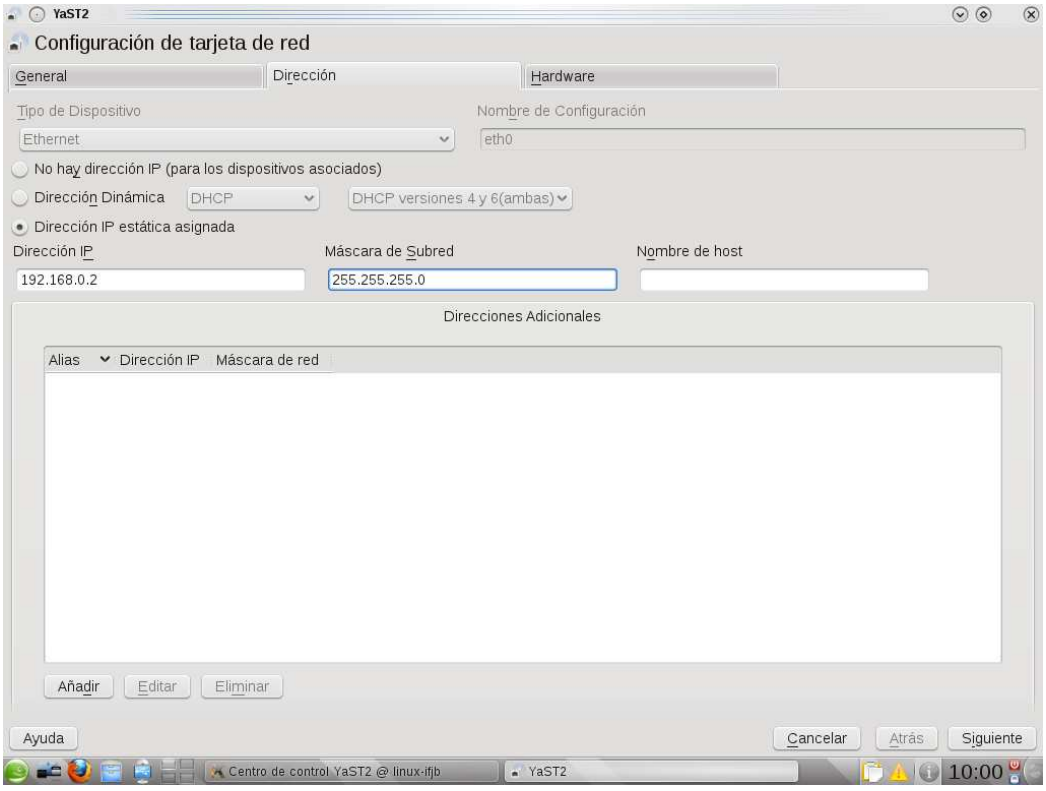
Primero nos vamos a Yast – Dispositivos de red – ajustes de la red, seleccionamos metodo tradicional con ifup, (esto también aplica para los demás escenarios).



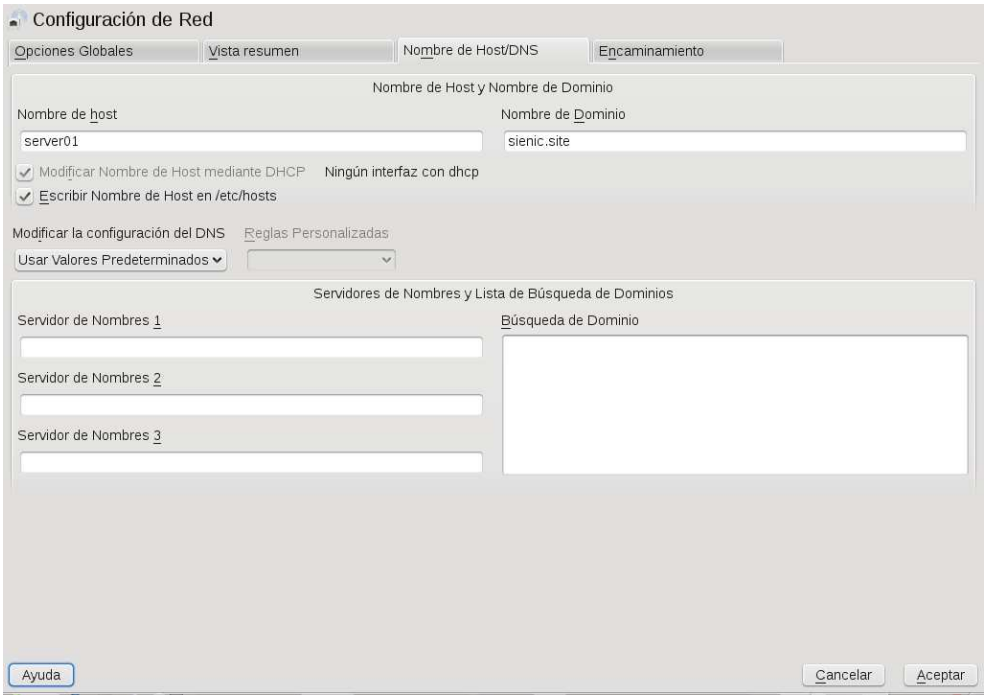

Luego seleccionamos vista resumen, seleccionamos nuestra conexión y hacemos clic en editar a como se muestra en la siguiente figura.




Hacemos clic en la solapa dirección y seleccionamos Dirección IP estática asignada y escribimos 192.168.0.2 y en mascara de subred 255.255.255.0, generalmente la dirección 192.168.0.1 esta reservada para el enrutador, ahora hacemos clic en siguiente

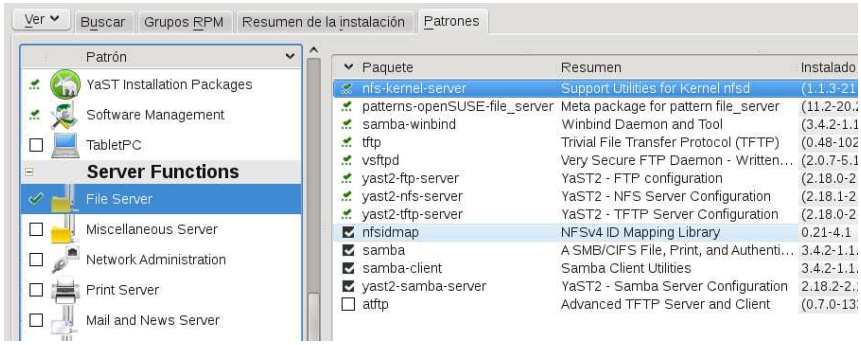


Seleccionamos Nombre de Host/DNS y en nombre de host escribimos el nombre que tendrá nuestro servidor en la red, este nombre debe ser único, en el campo Nombre de dominio escribimos el nombre que tendrá nuestro dominio seguido de .site en este ejemplo el nombre de dominio será el nombre ficticio sienic y hacemos clic en aceptar



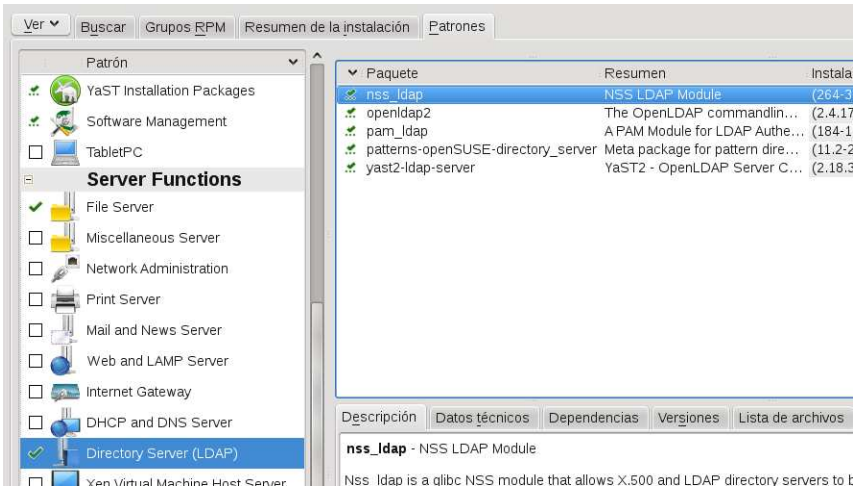

## 3.3 Instalación de samba

Ahora nos vamos a yast – Software – Instalar desinstalar software – hacemos clic en ver y seleccionamos patrones, luego hacemos clic en File Server a como se muestra en la siguiente figura

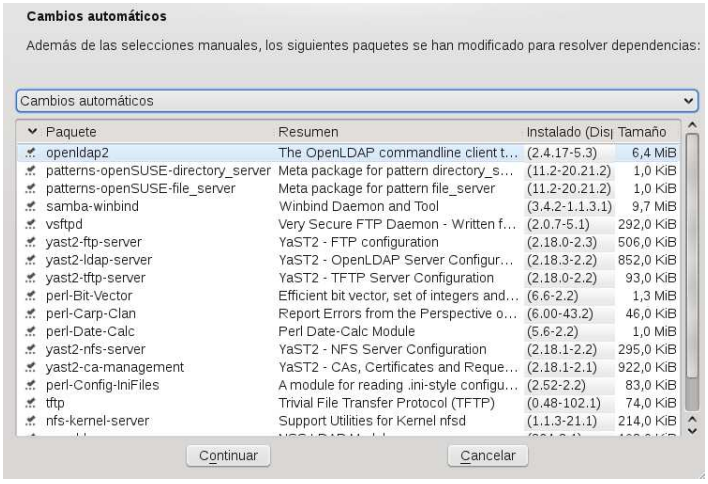


## 3.4 Instalación de openLDAP

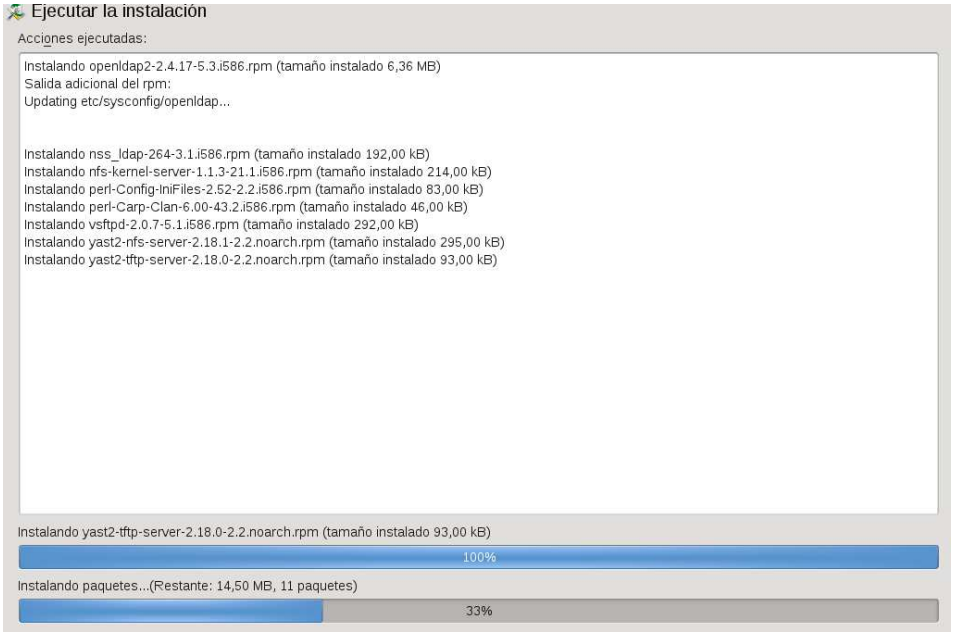
Luego seleccionamos Directory Server (LDAP) y hacemos clic en el check para seleccionar estos servicios y hacemos clic en aceptar




Nos indicara que se instalaran unos paquetes para resolver dependencias, aquí hacemos clic en continuar.



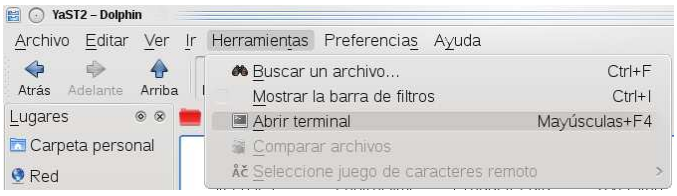

Se mostrara la siguiente pantalla mientras se realiza la instalación.



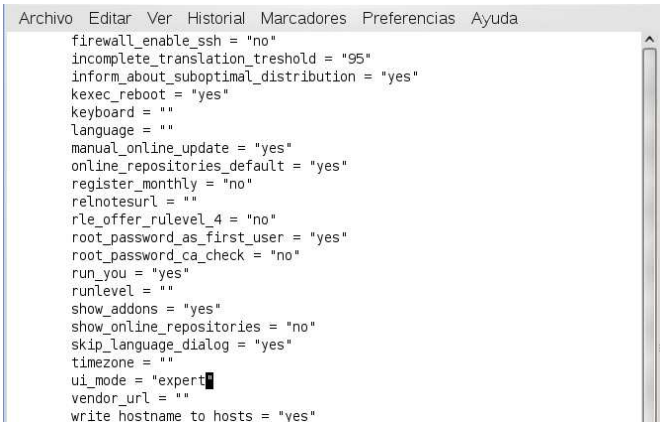

## 3.5 Configuración avanzada de YaST2

Ahora nos vamos a la carpeta /etc/YaST2 y editamos el archivo ProductFeatures


Para editar el archivo podemos usar el kwrite, pero si deseamos usar el vi hacemos clic en herramientas – Abrir terminal y como root ejecutamos *vi ProductFeatures*



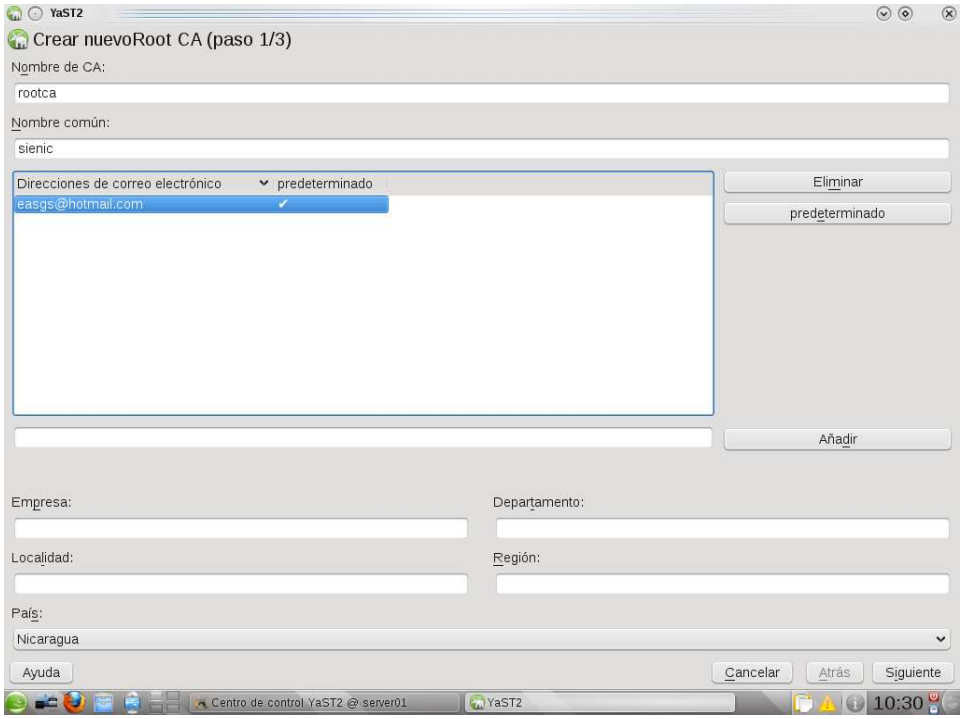

Presionamos la tecla Insert y nos desplazamos a la linea ui_mode y cambiamos el valor a expert a como se muestra en la imagen, luego para guardar presionamos la tecla Esc seguido de :wq y presionamos enter



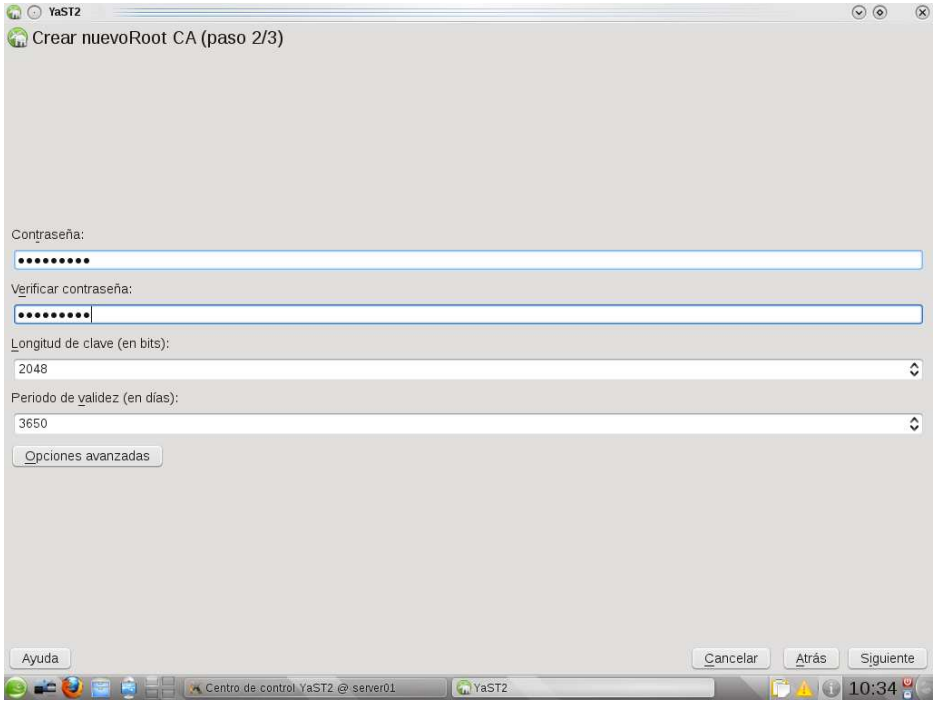

## 3.6 Creación del certificado de servidor común.

Ahora nos vamos a Yast – Seguridad y usuarios y ahora tendremos la opción Gestión de autoridades certificadoras (CA) y la seleccionamos

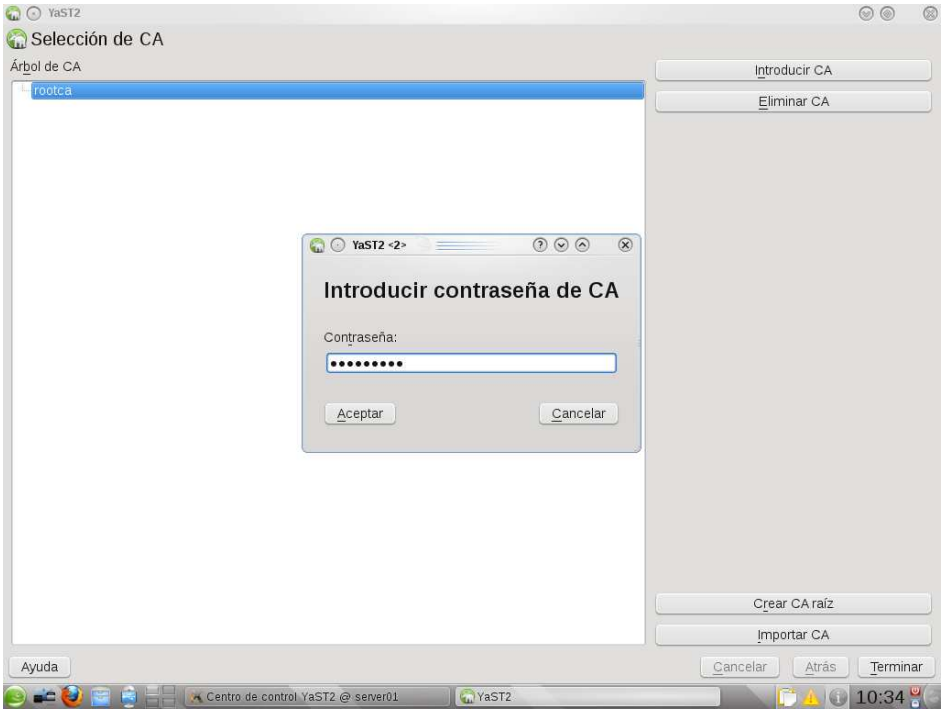

En nombre de ca le ponemos rootca y en nombre común le podemos poner el nombre de la empresa o dominio, agregamos el correo electrónico y seleccionamos el país, los demás campos son opcionales, hacemos clic en siguiente.



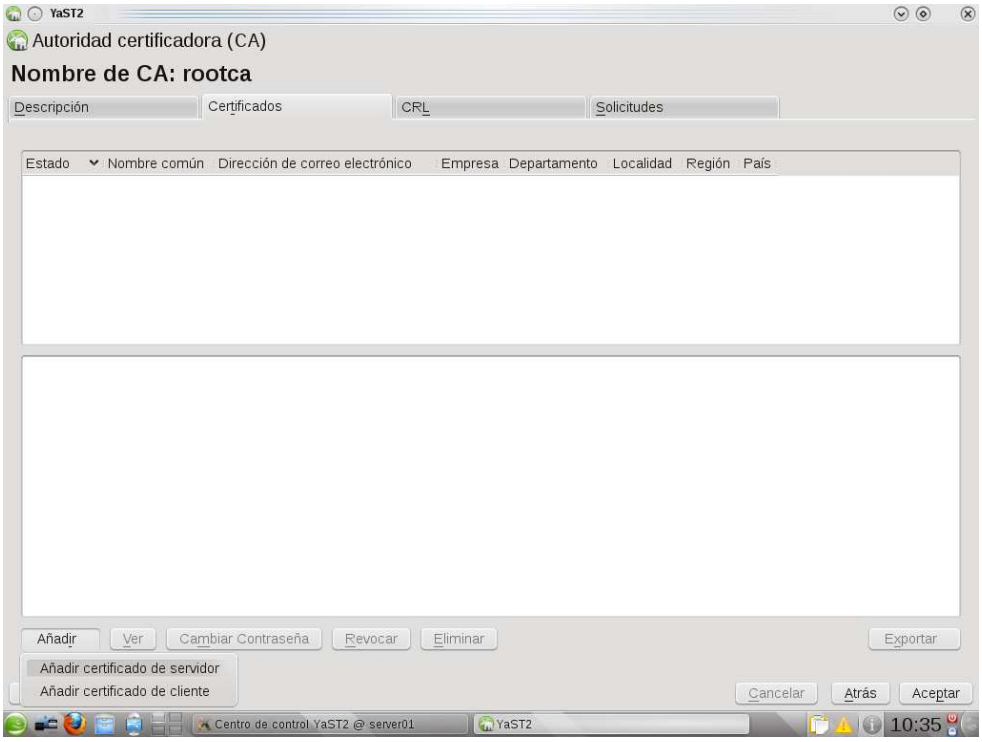

Escribimos y confírmanos la contraseña, en los siguientes campos podemos ver que el periodo de validez de la autoridad será de 10 años, este valor se puede incrementar si fuese necesario.



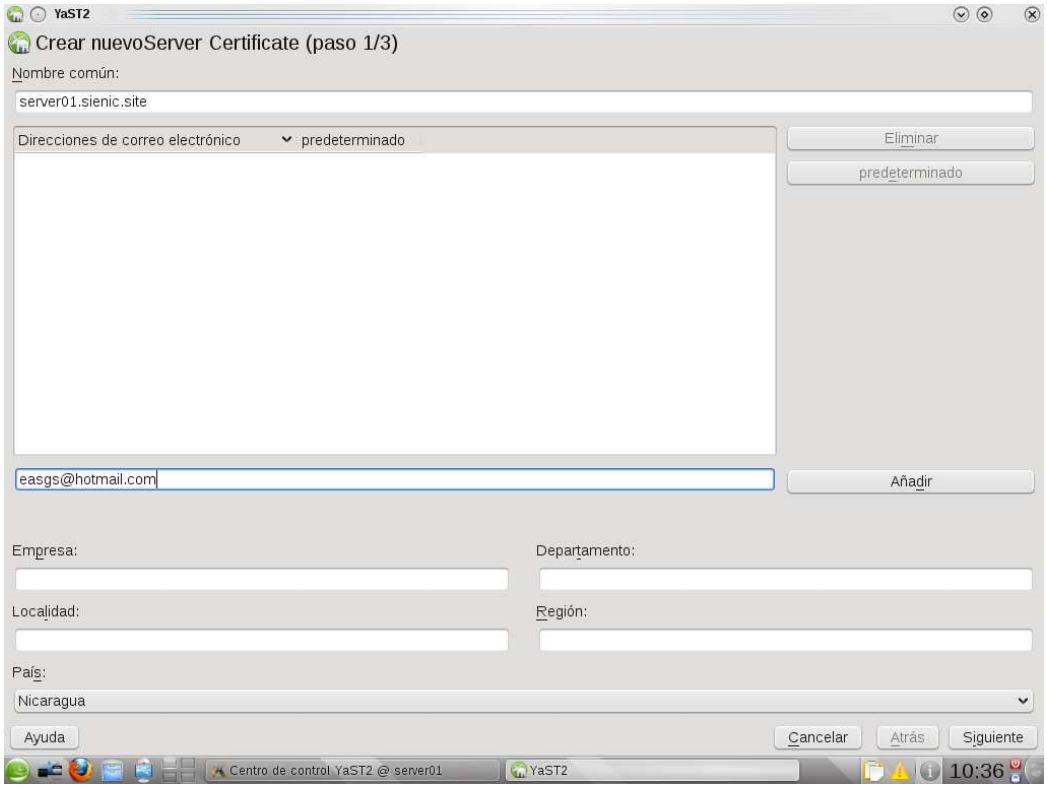

Damos clic en siguiente - crear y luego seleccionamos el CA recién creado y hacemos clic en introducir CA, nos pedirá la clave de acceso.



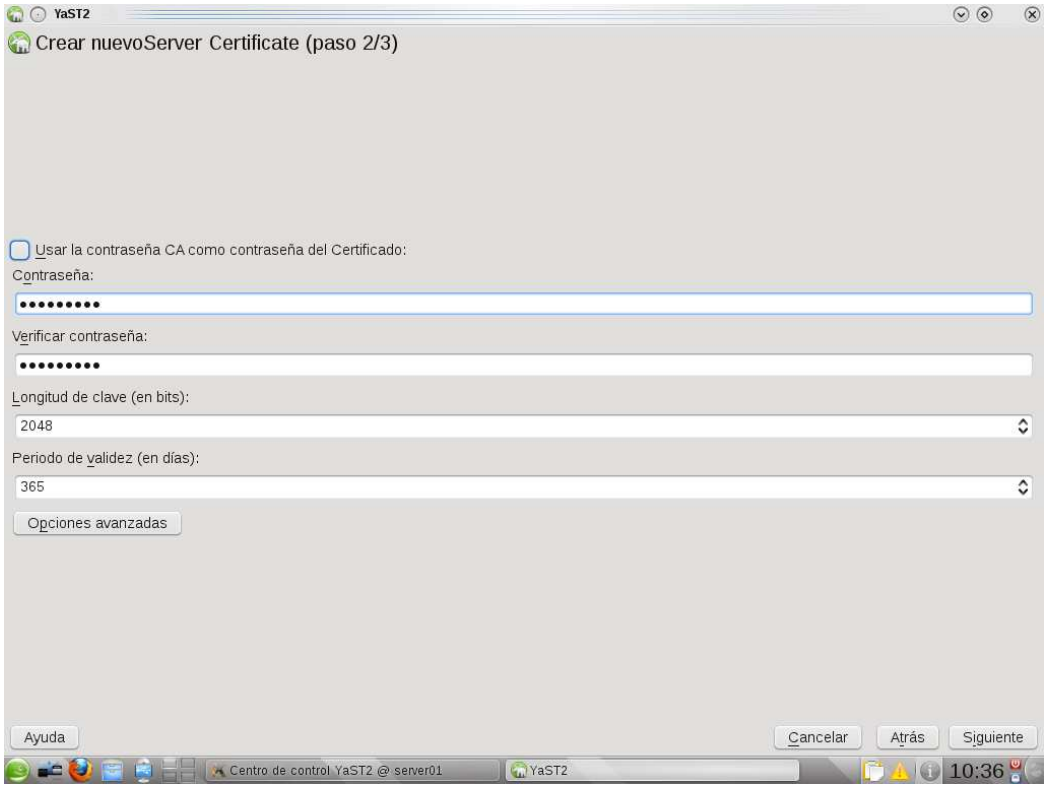

Hacemos clic en certificados – añadir y seleccionamos Añadir certificado de servidor



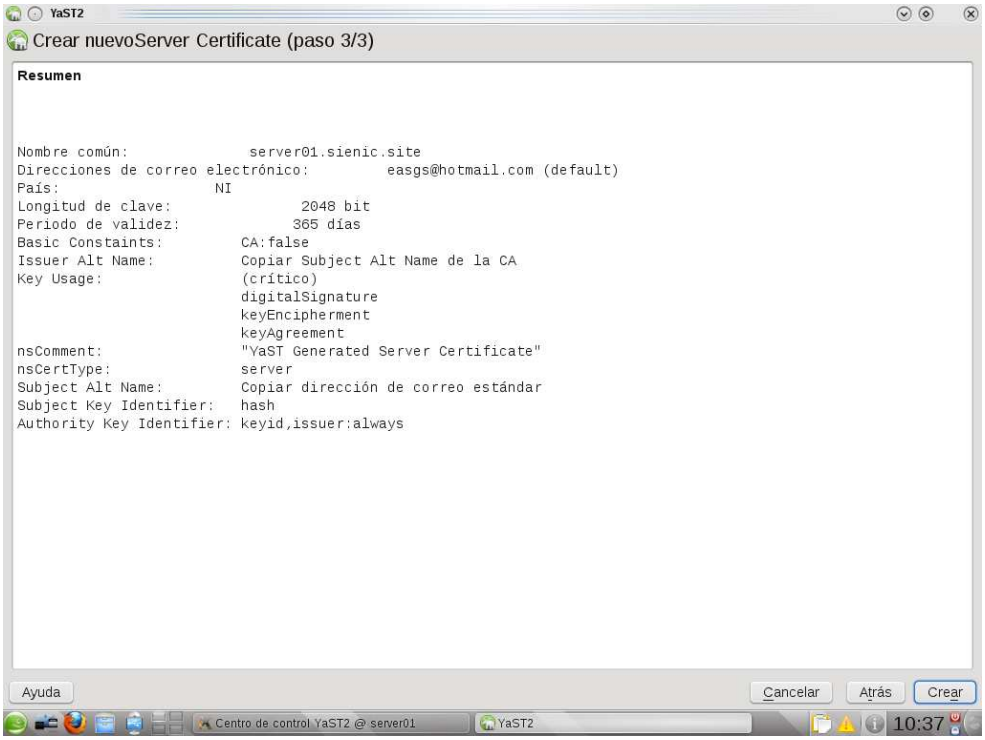

En nombre común debemos poner el nombre completo calificado de dominio de nuestro servidor, para obtener este nombre ejecutamos el comando *hostname - -long*, ponemos el correo electrónico y el país, luego hacemos clic en siguiente.



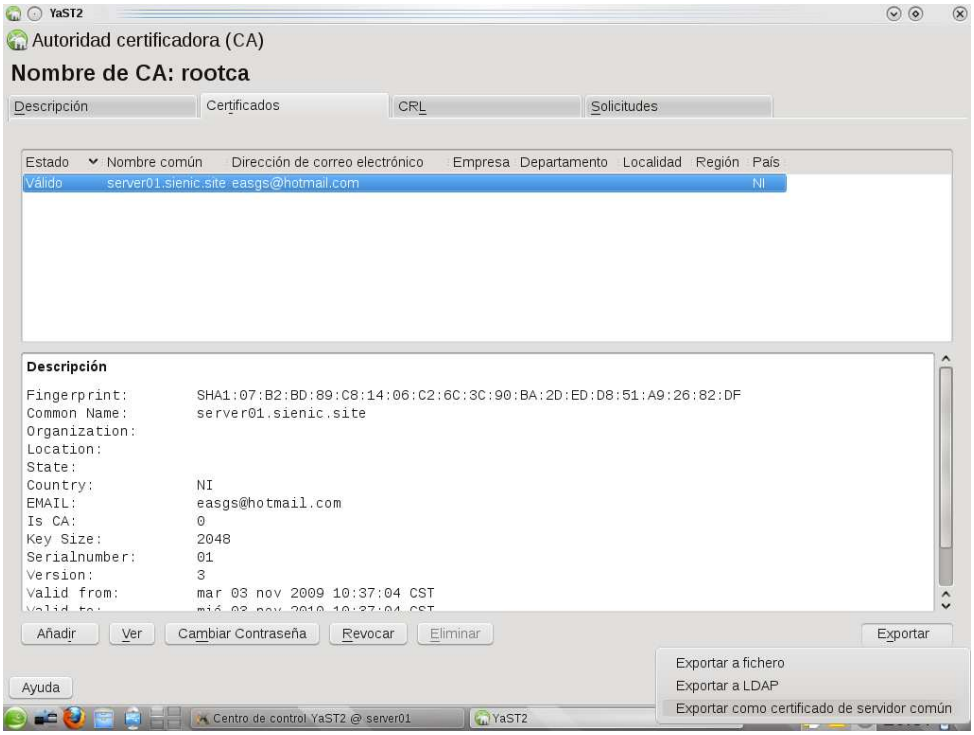

En esta pantalla nos da la opción de usar la misma clave que el CA para este certificado, si optamos por no hacerlo, escribimos una y la confirmamos, para este certificado de servidor el periodo de validez predeterminado es de un año, pero podemos aumentar ese rango.



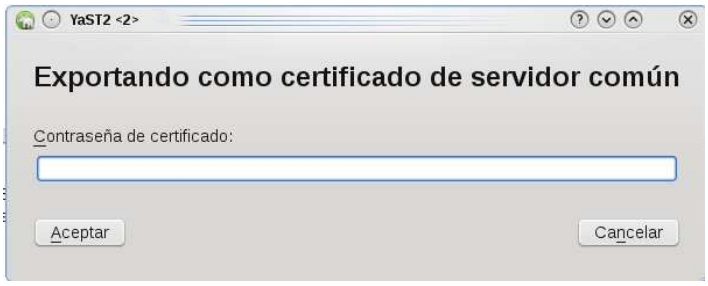
Hacemos clic en siguiente y nos sale esta pantalla, ahora damos clic en crear



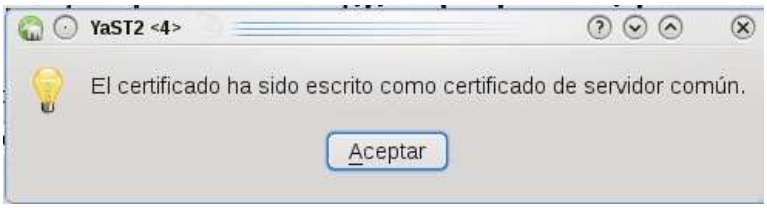

Una vez creado el certificado de servidor procedemos a exportarlo como certificado de servidor común, hacemos clic en exportar y seleccionamos Exportar como certificado de servidor común.



Pedirá la contraseña del certificado de servidor.



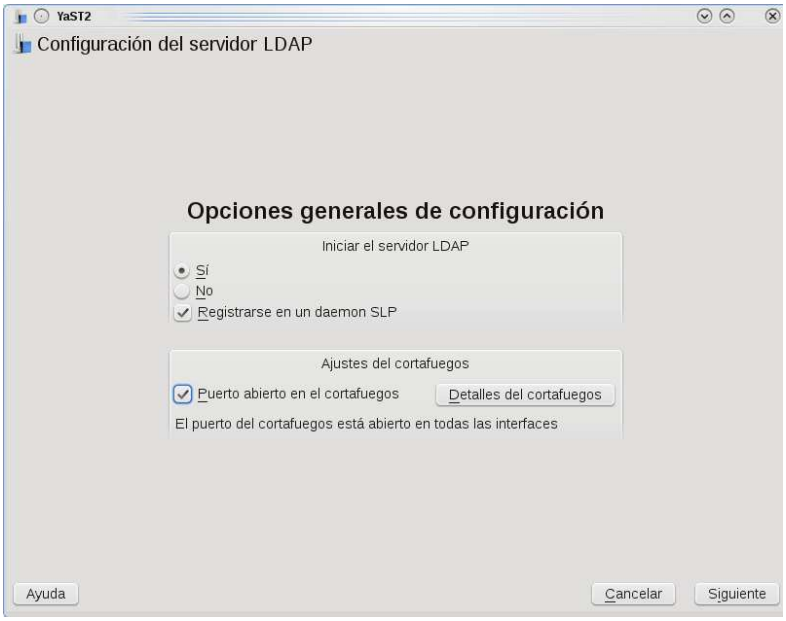

Nos saldrá el siguiente mensaje de que la operación fue un exito



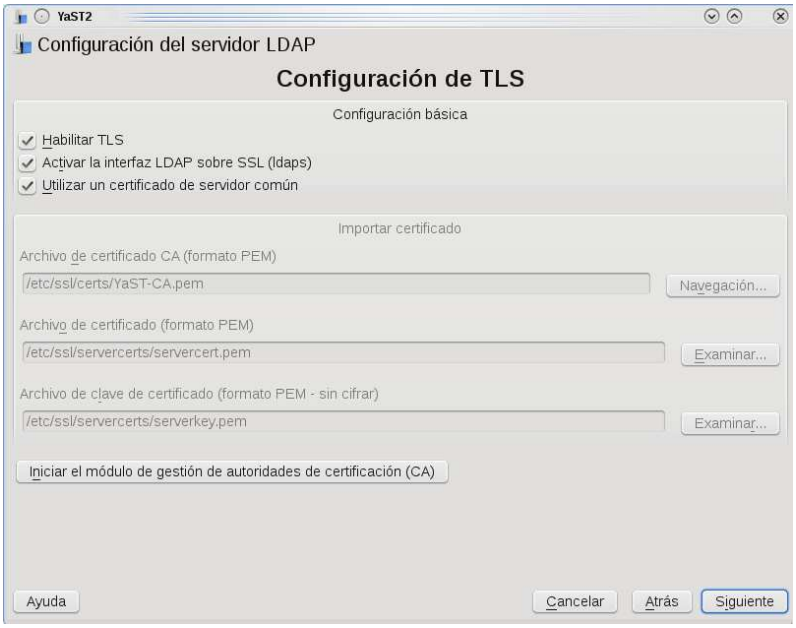

## 3.7 Configuración del servidor LDAP.

Ahora nos vamos a Yast – Servicios de red – Servidor LDAP.

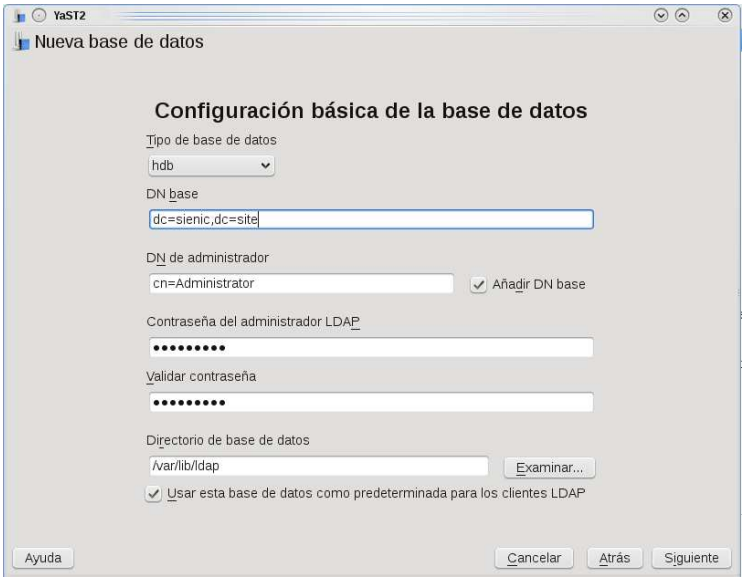

Seleccionamos si en Iniciar el servidor LDAP, hacemos clic en Registrarse en un daemon SLP y abrimos el puerto en el Firewall, luego hacemos clic en siguiente.



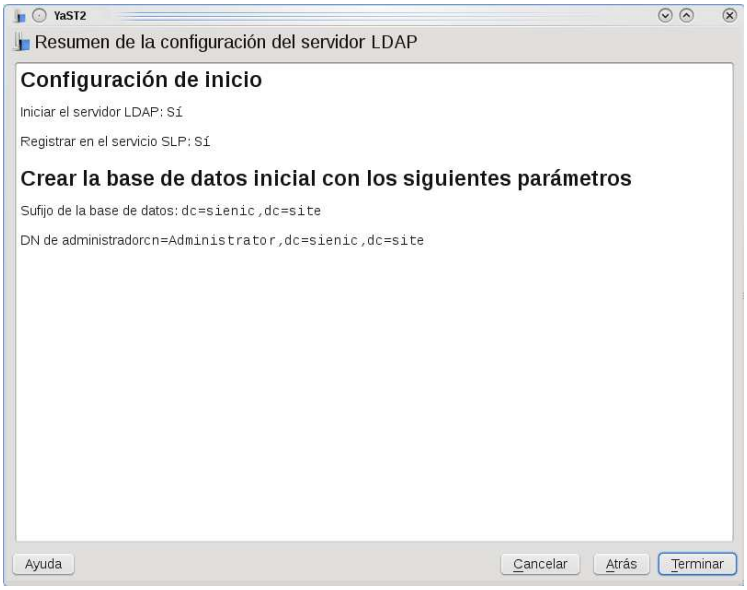

En esta pantalla dejamos los valores a como se muestra en la siguiente imagen y hacemos clic en siguiente.



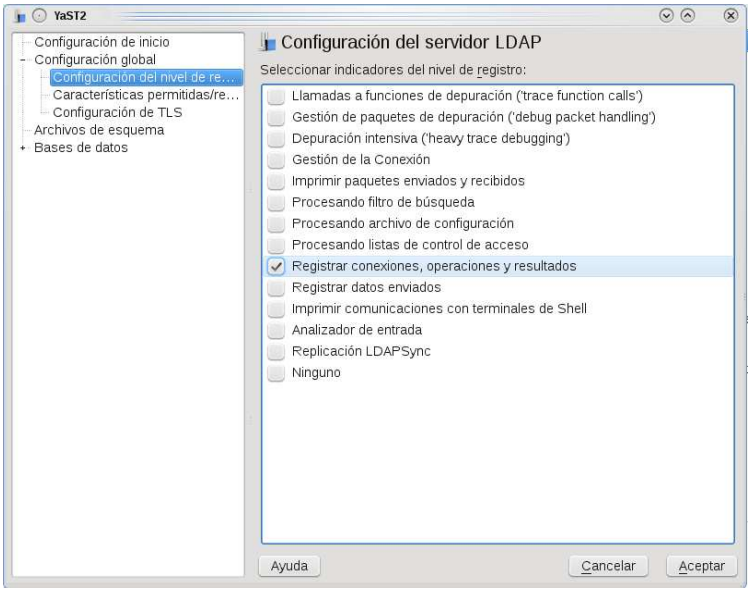

Podemos ver que en DN base tomo los valores que pusimos en Nombre de Dominio cuando configuramos la conexión de red, dejamos los valores a como se muestran en la imagen, tomando en cuenta que podemos cambiar el nombre del DN de administrador y la DN base si así lo deseamos, escribimos una clave y luego hacemos clic en siguiente.



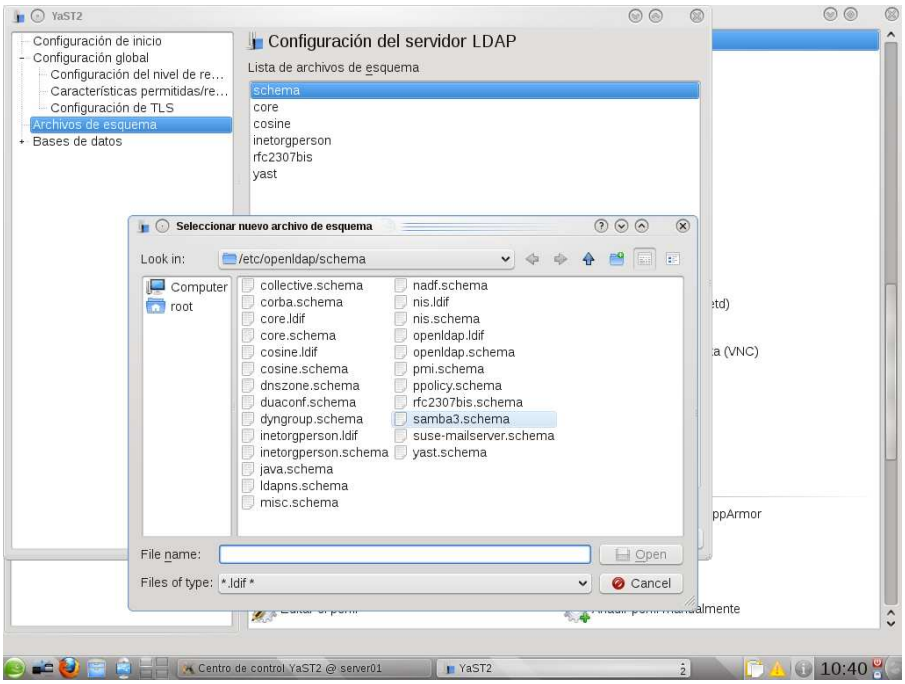

Nos mostrara la siguiente pantalla y hacemos clic en terminar.




Volvemos a abrir el servidor LDAP y seleccionamos configuración global – configuración de registro y seleccionamos Registrar conexiones, operaciones y resultados.



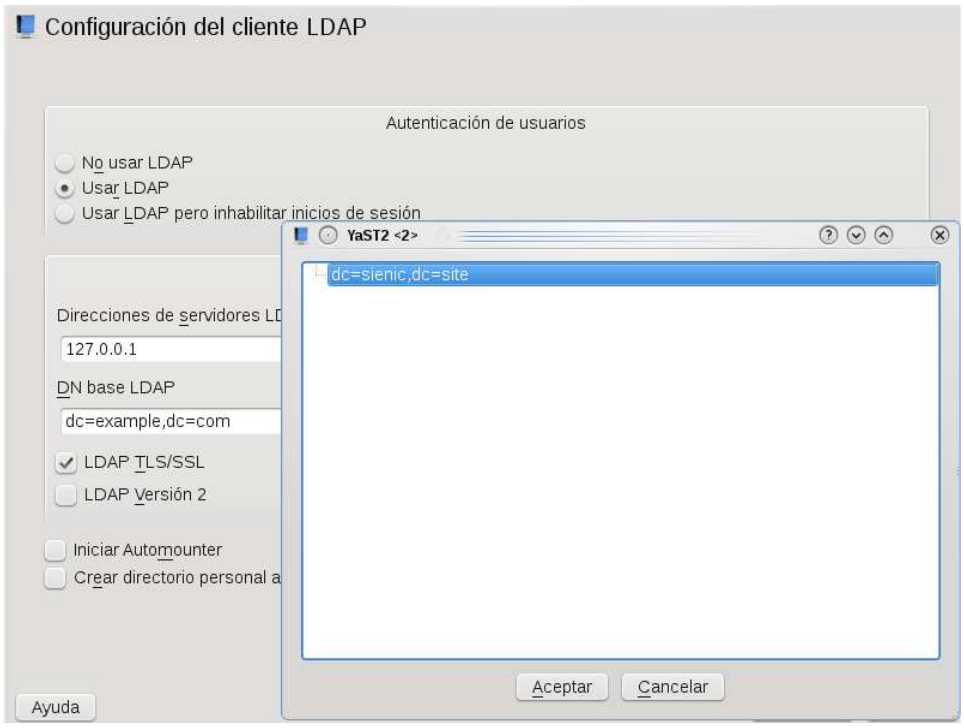

Esto se agrega automáticamente pero aquí lo haremos manual, seleccionamos Archivos de esquema – agregar y seleccionamos samba3.schema y clic en open y luego en aceptar para cerrar la ventana del servidor LDAP




## 3.8 Configuración del cliente LDAP.

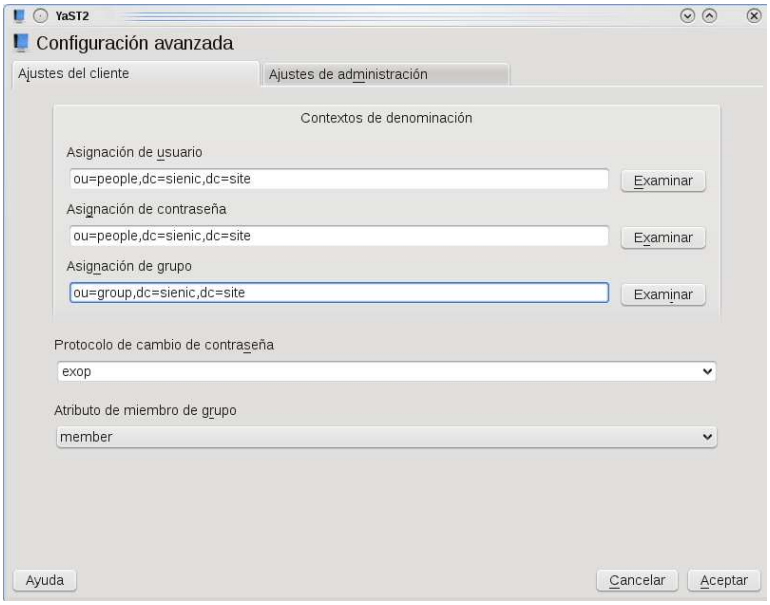
Ahora nos vamos a YAST – Servicios de red - Cliente LDAP


Seleccionamos la opción Usar LDAP y en DN base LDAP damos clic en Obtener DN y seleccionamos el que creamos con anterioridad y damos clic en aceptar.

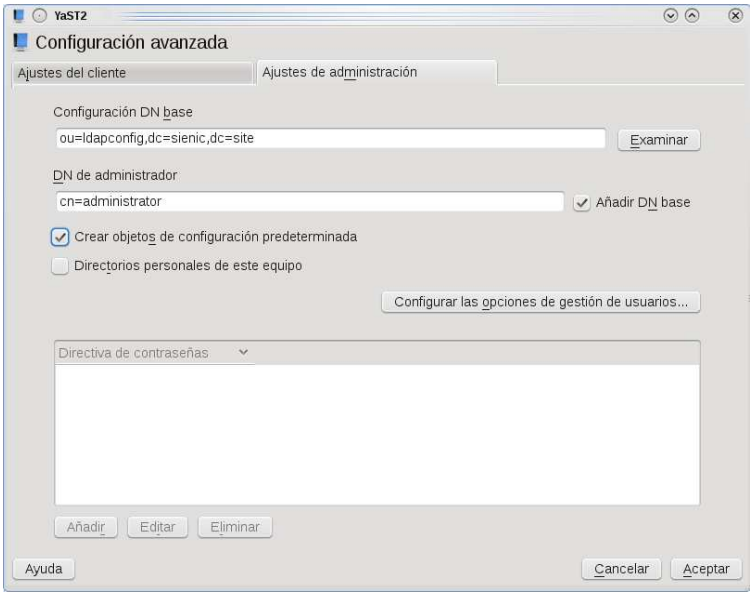



Quedara a como se muestra en la figura a continuación y hacemos clic en configuración avanzada.

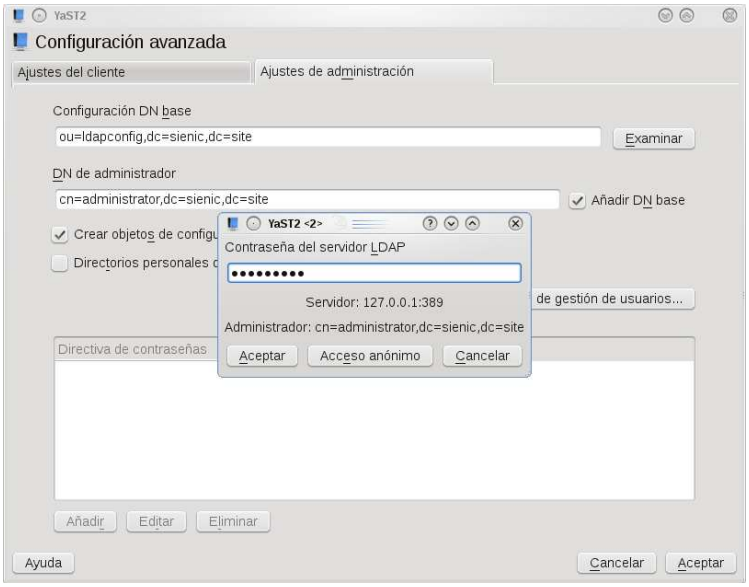

Rellenamos las opciones a como se muestra a continuación



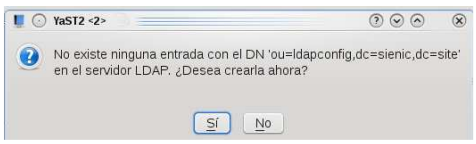

Nos vamos a ajustes de administración y escribimos el DN de administrador, seleccionamos la opción de añadir DN base y la opción crear objetos de configuración predeterminada, ahora hacemos clic en Configurar las opciones de gestión de usuarios.



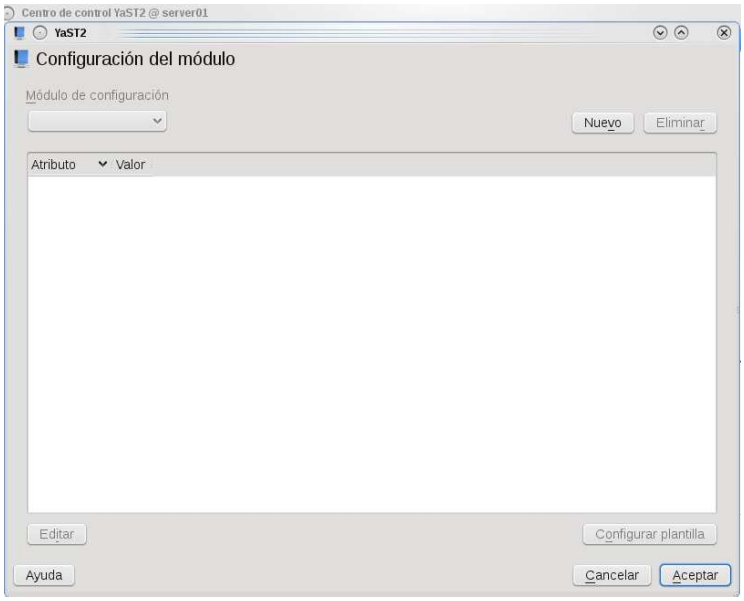

Nos pedirá la clave del administrador LDAP



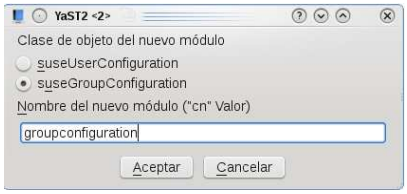

Nos va a aparecer un cuadro de dialogo indicándonos que si deseamos crear la entrada LDAP con el DN indicado, le damos clic en si.



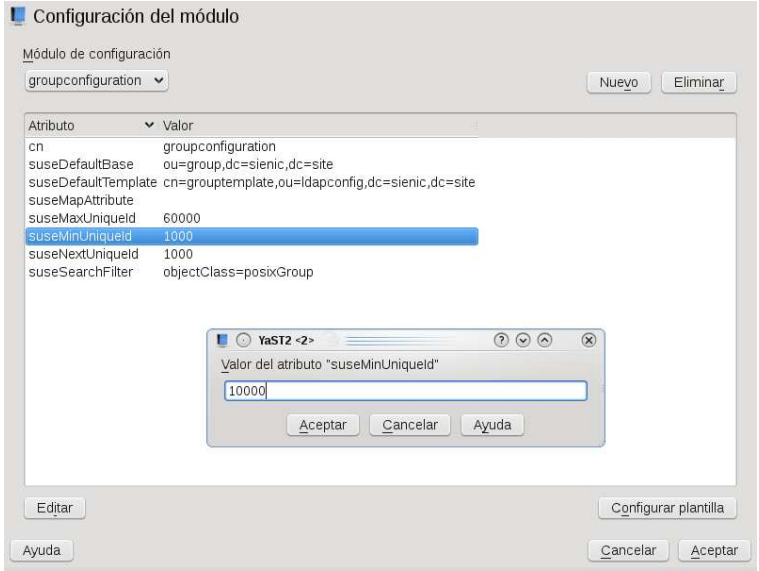

Ahora hacemos clic en nuevo para agregar los módulos de configuración



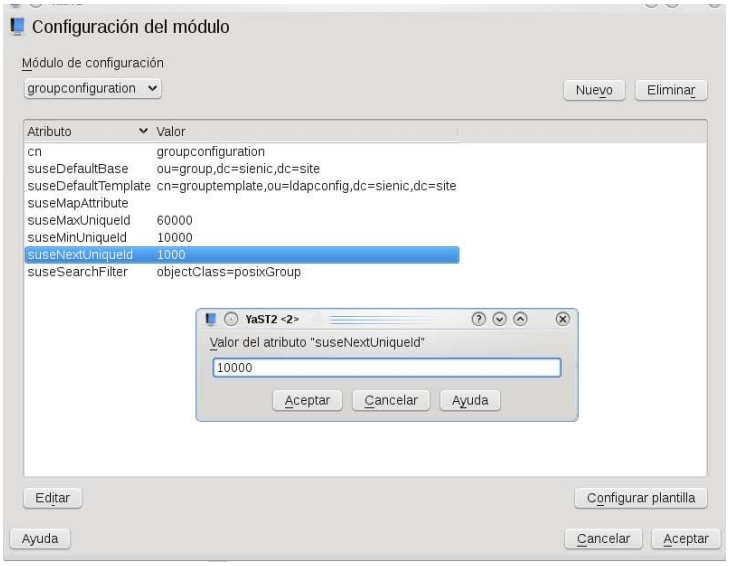

Escribimos groupconfiguration y seleccionamos suseGroupConfiguration y le damos aceptar



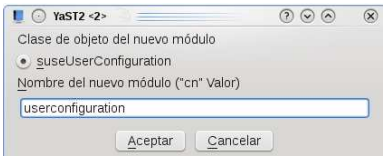

Seleccionamos el suseMinUniqueid, hacemos clic en editar y cambiamos el valor a 10000.



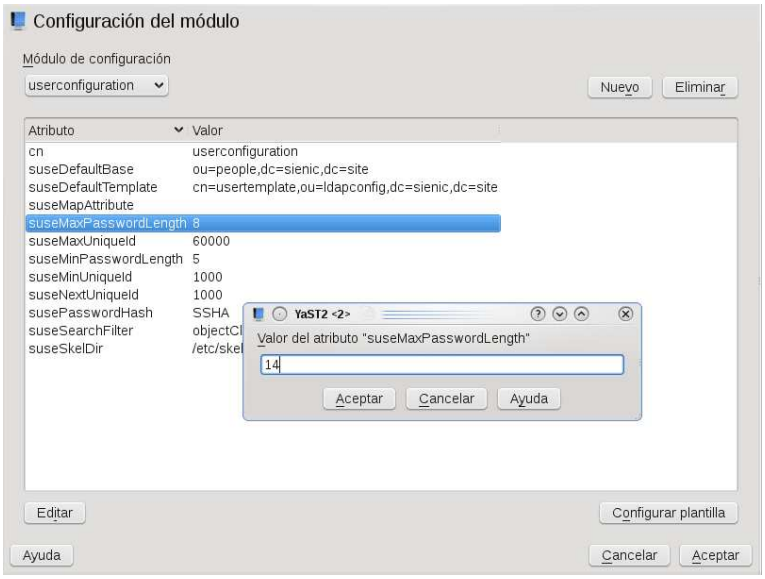
Seleccionamos suseNextUniqueid, seleccionamos editar y modificamos el valor a 10000.



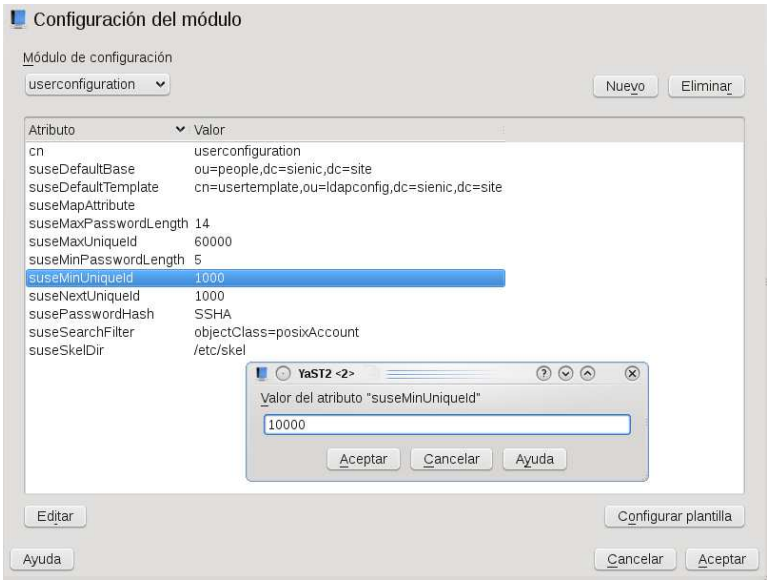

Ahora hacemos clic en nuevo y escribimos userconfiguration luego hacemos clic en aceptar.



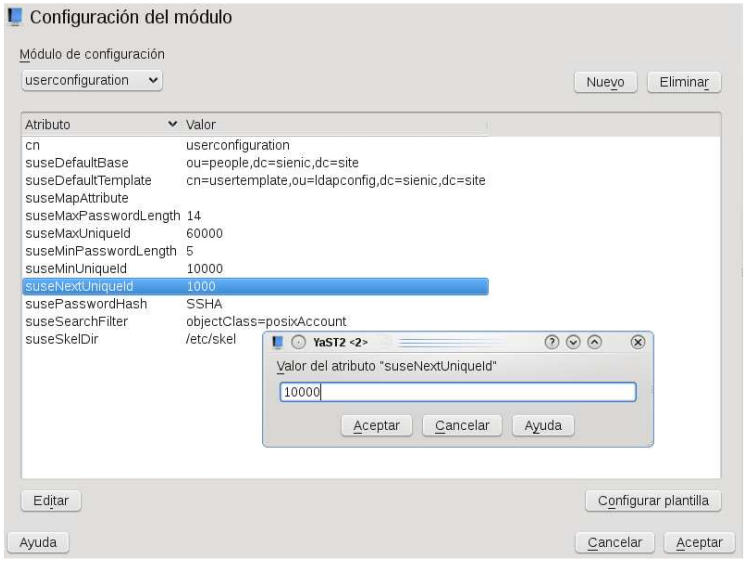

Hacemos clic en suseMaxPasswordLength y cambiamos el valor a 14




Seleccionamos suseMinUniqueid y cambiamos el valor a 10000

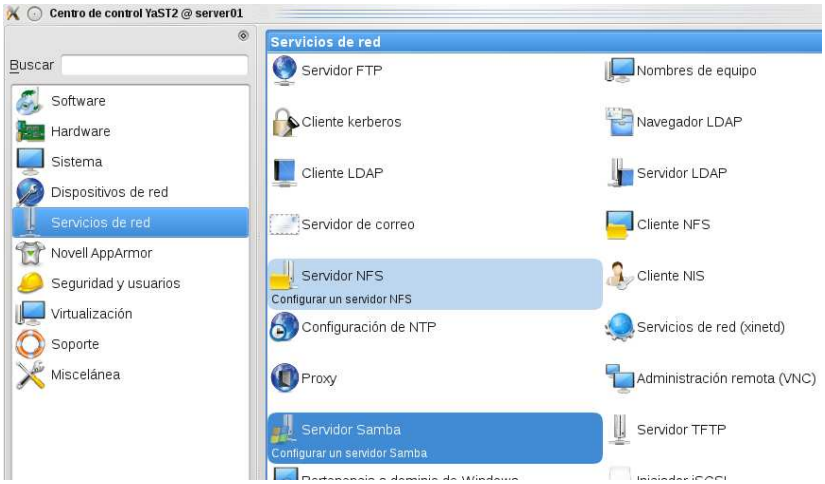



Seleccionamos suseNextUniqueid y cambiamos el valor a 10000

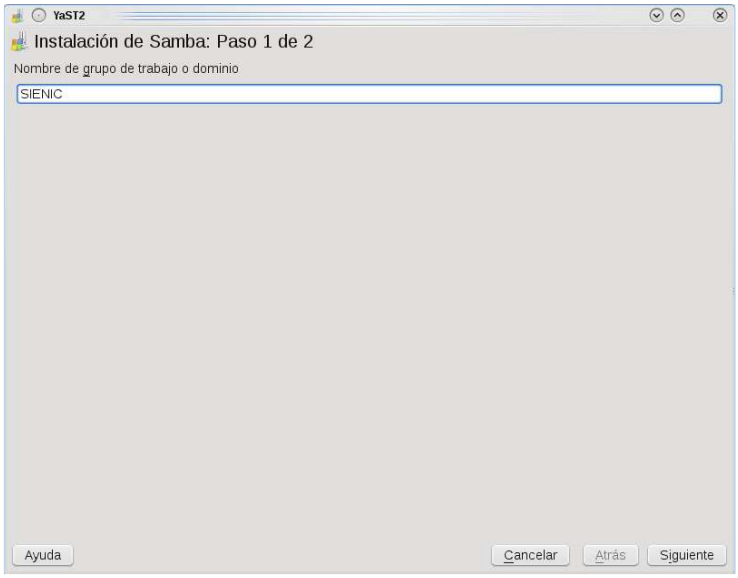



## 3.9 Configuración del servidor Samba.

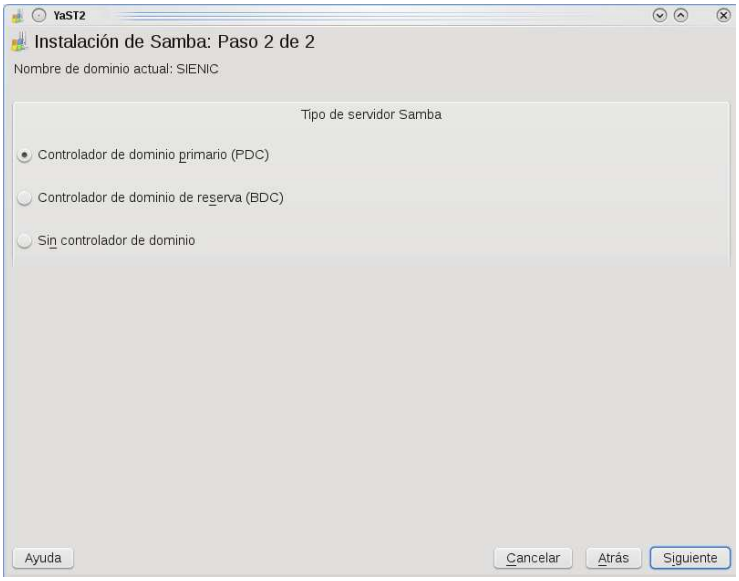
Ahora vamos a configurar el servidor samba para eso nos vamos a Yast – servicios de red – Servidor samba



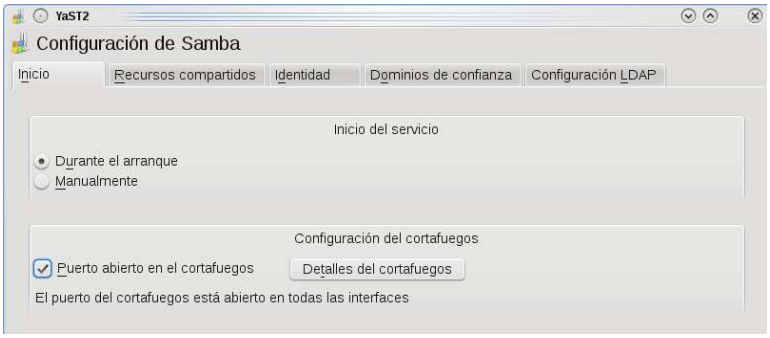

En esta pantalla escribimos el nombre que tendrá nuestro dominio, en este ejemplo es SIENIC, pongan el que acomode sus necesidades, hacemos clic en siguiente.



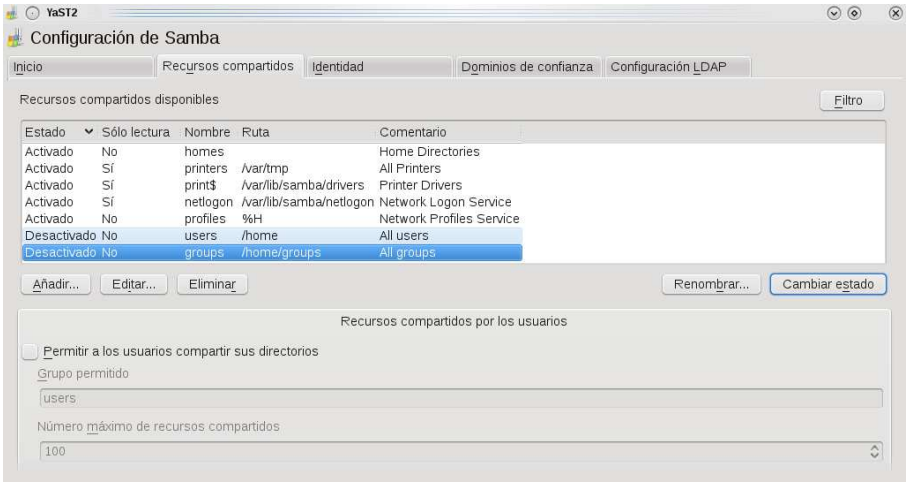

Seleccionamos la opción controlador de dominio primario (PDC) y hacemos clic en siguiente.



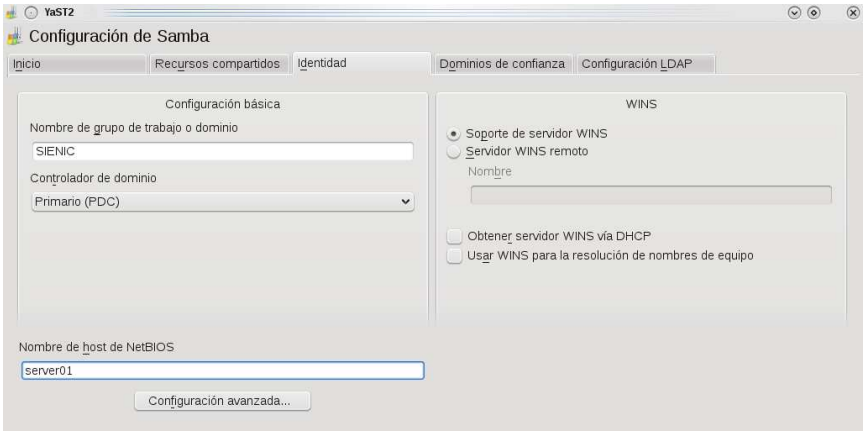

En la siguiente pantalla seleccionamos Durante el arranque para que el servidor samba se inicie de manera automática cada vez que reiniciemos el servidor, también seleccionamos Puerto abierto en el cortafuegos.



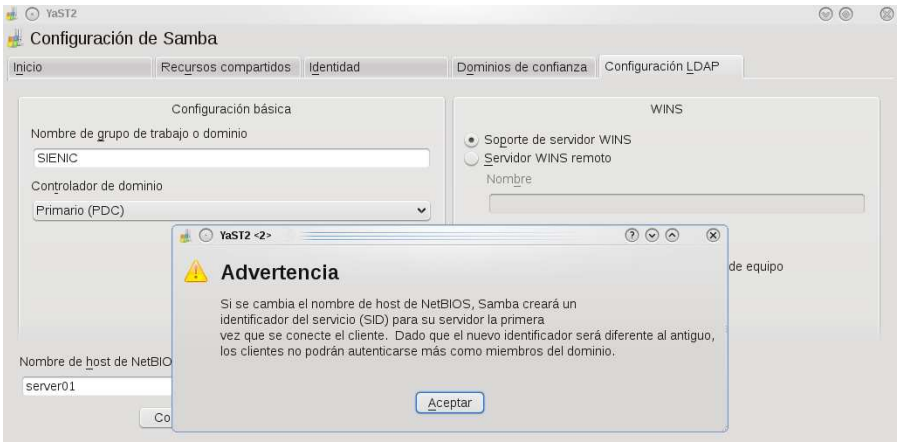

Ahora nos vamos a la solapa recursos compartidos y desactivamos los recursos compartidos users y groups, estos se explicaran con mas detalle mas adelante.



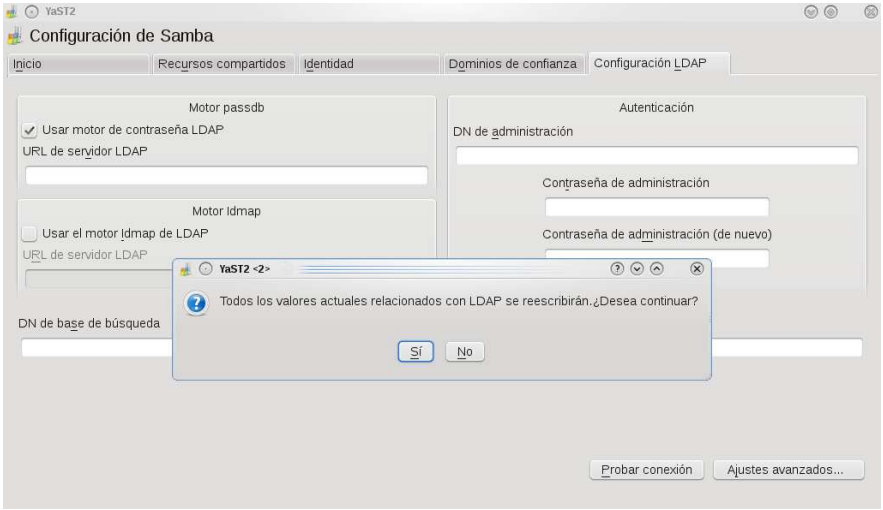

En la solapa identidad escribimos el nombre de host de NETBIOS de nuestro servidor el cual se obtiene ejecutando el comando *hostname*.



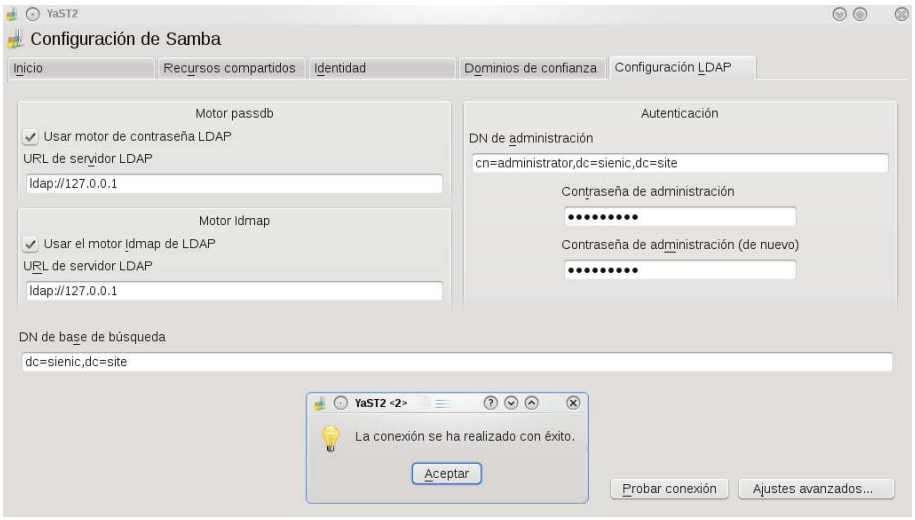

Hacemos clic en la solapa configuración LDAP y nos aparecerá un mensaje como el de la imagen, solo damos clic en aceptar.



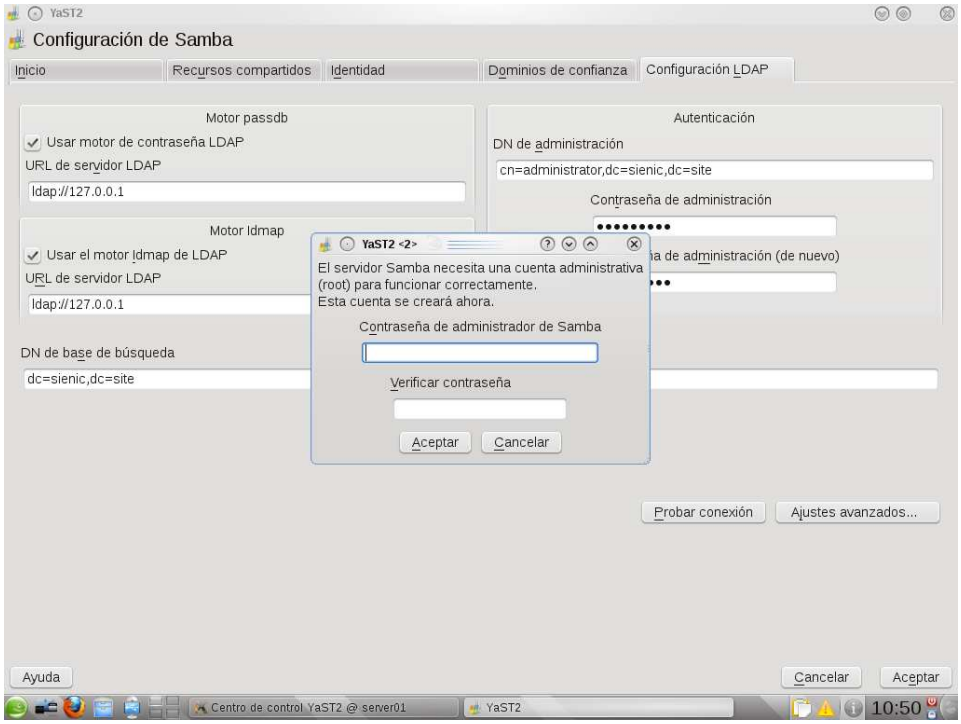
Hacemos clic en Usar motor de contraseña LDAP y nos va a aparecer un mensaje como el que se muestra a continuación solo damos clic en si.




En autenticación escribimos la contraseña del administrador LDAP la confirmamos y hacemos clic en probar conexión.



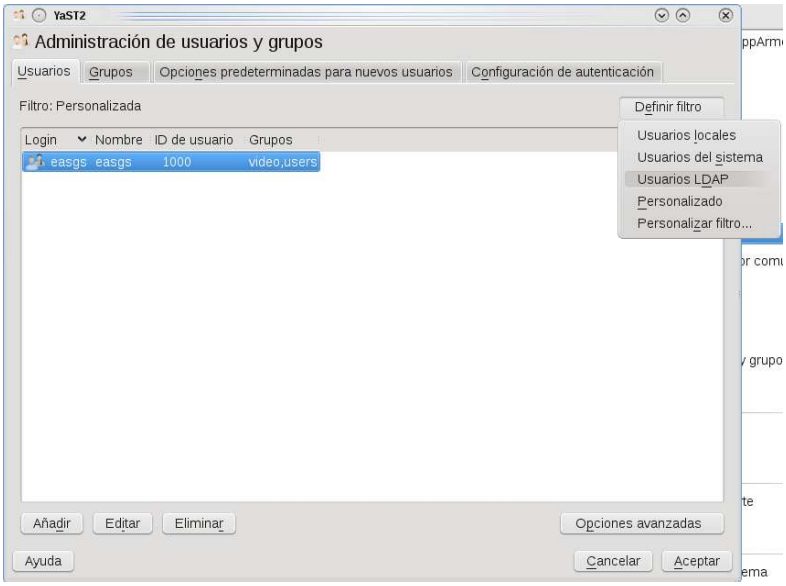

Al hacer clic en aceptar nos pedirá que ingresemos la clave del administrador de samba.



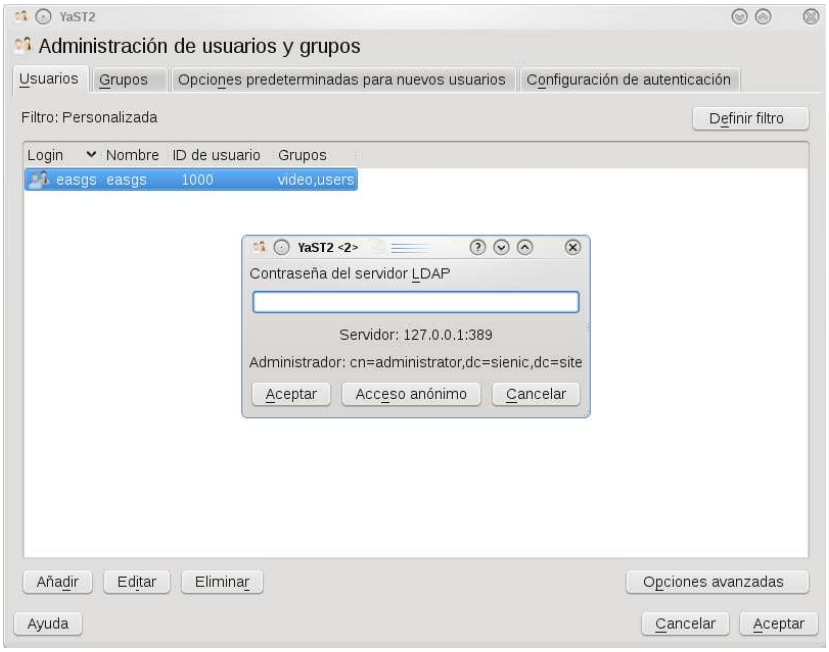

## 3.10 Creación de los usuarios y grupos LDAP.

Ahora nos vamos a yast – Seguridad y usuarios – Gestión de usuarios y grupos.

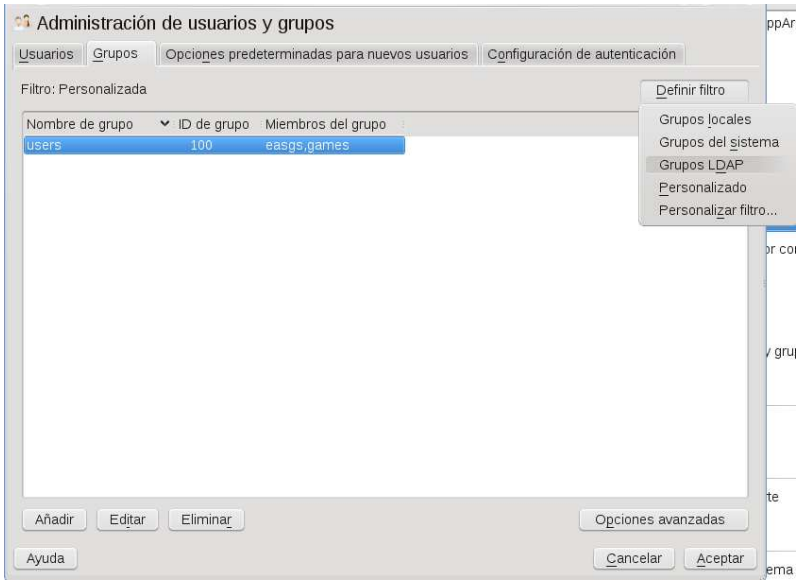

Hacemos clic en Definir filtro y seleccionamos Usuarios LDAP.



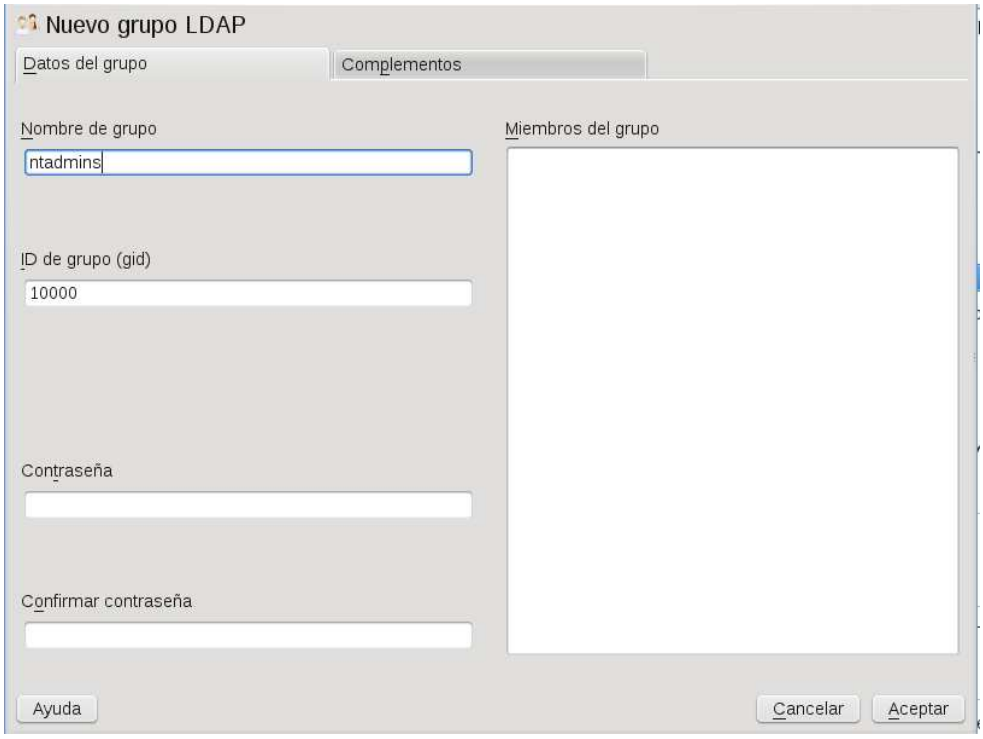

Nos pedirá la contraseña del administrador LDAP.



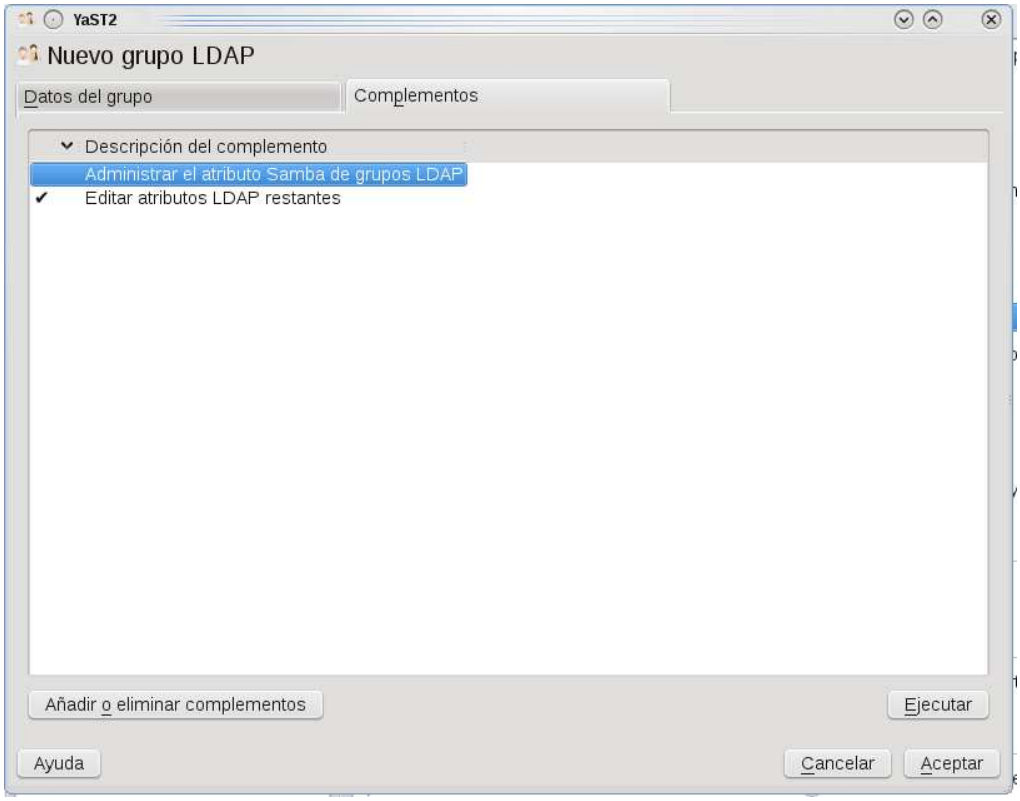

Hacemos clic en grupos y hacemos clic en Definir filtro, luego seleccionamos grupos LDAP y hacemos clic en añadir.



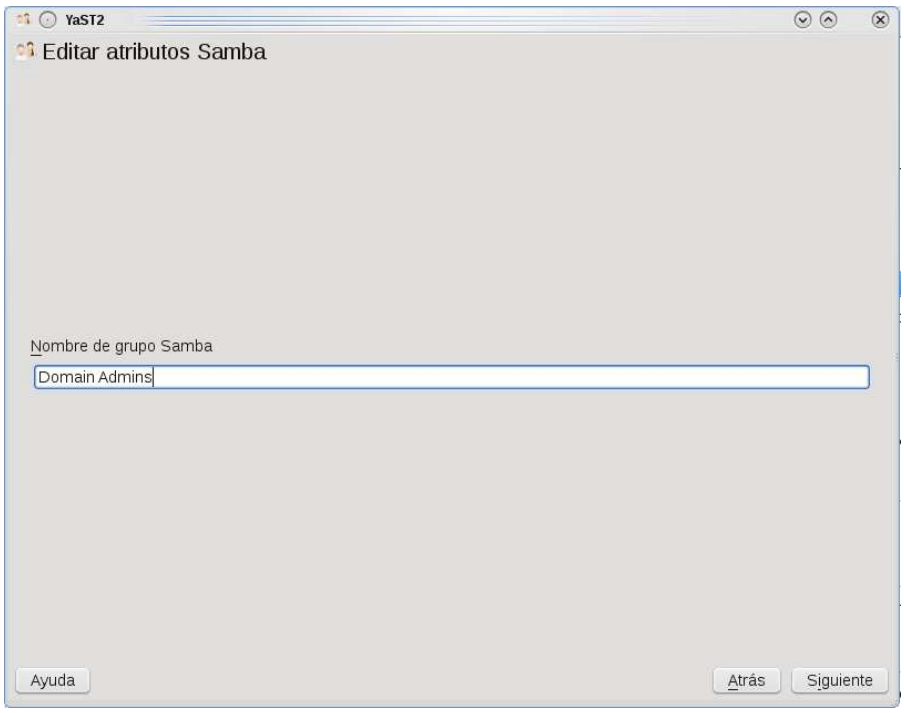

Agregaremos el grupo LDAP que será nuestro grupo Domain Users, rellenamos los campos a como se muestra en la figura.



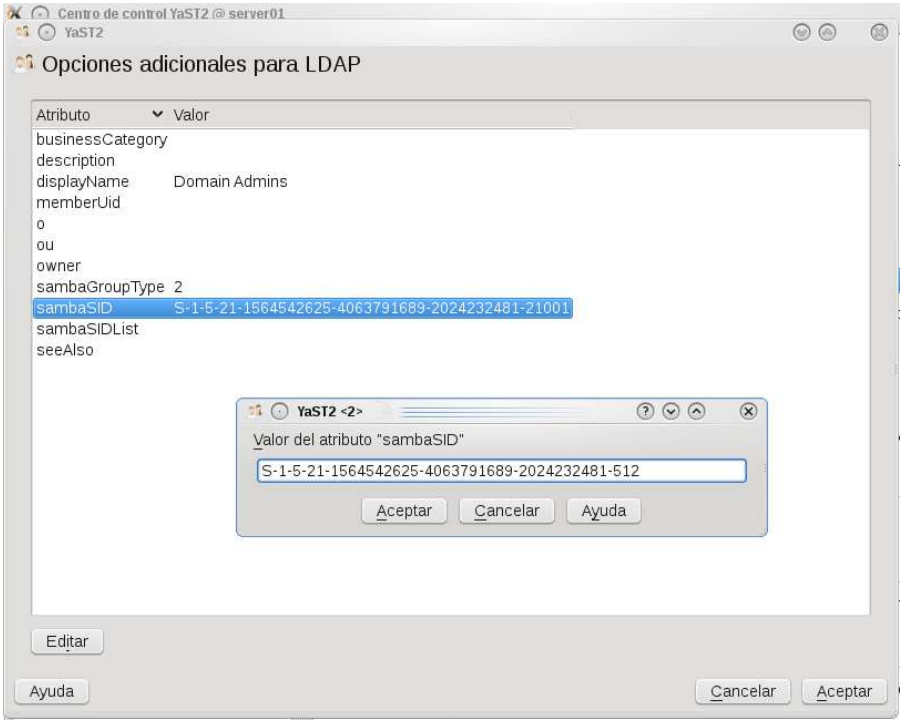

Nos vamos a complementos y seleccionamos Administrar el atributo samba de grupos LDAP y damos clic en ejecutar



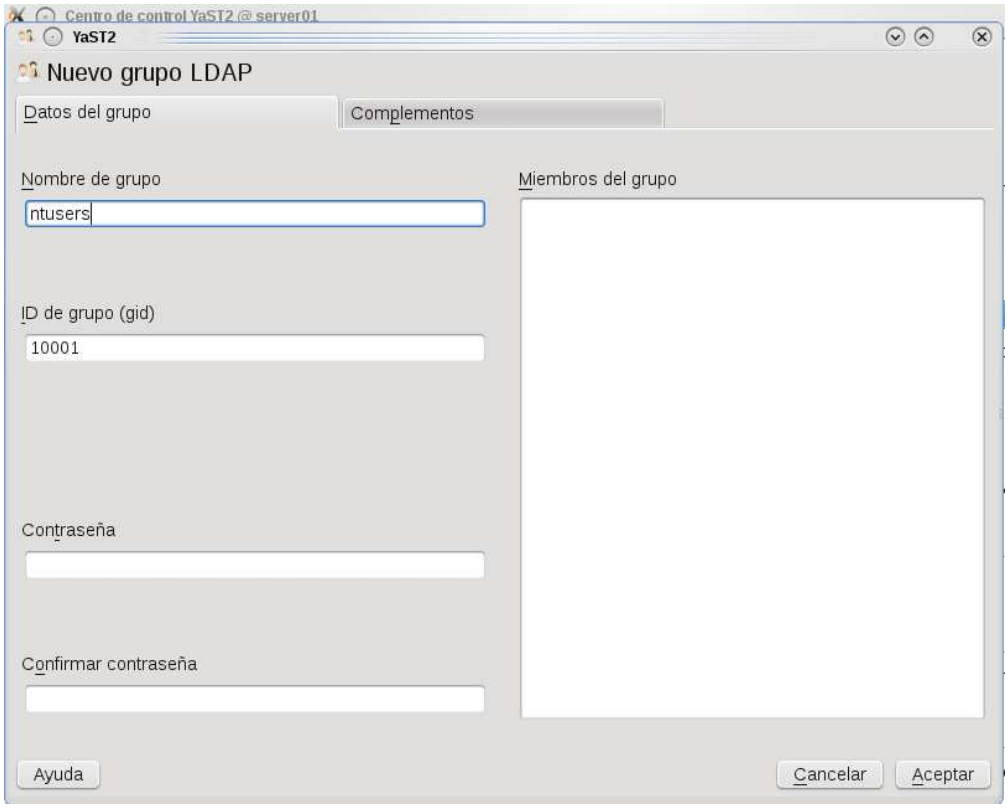

Escribimos Domain Admins y hacemos clic en siguiente.



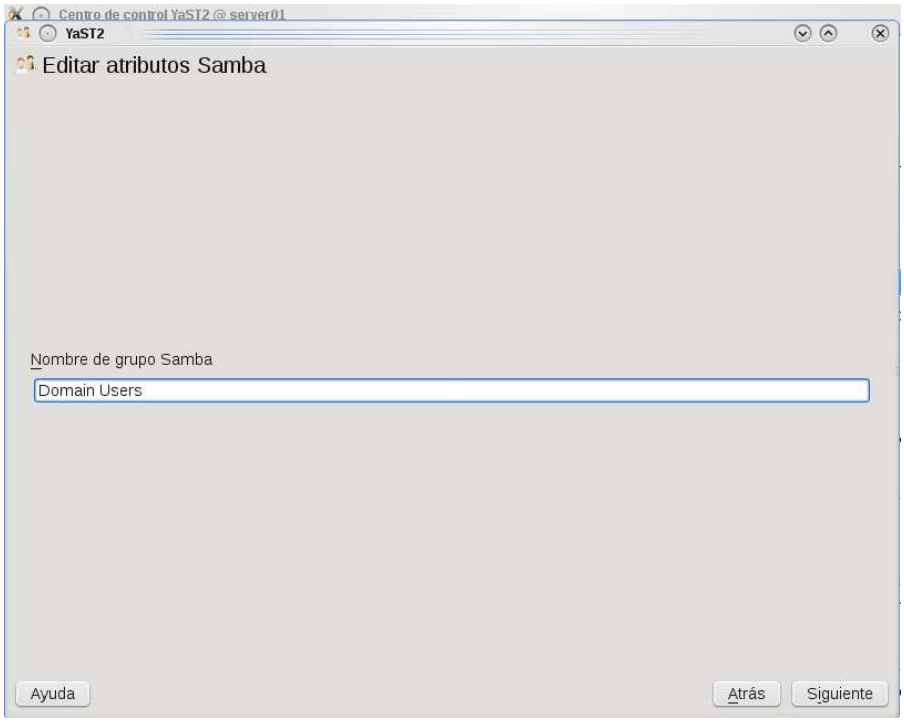
Ahora seleccionamos Editar atributos LDAP restantes y modificamos el sambaSID y editamos el RID que son los últimos cinco dígitos para que tenga el valor 512.



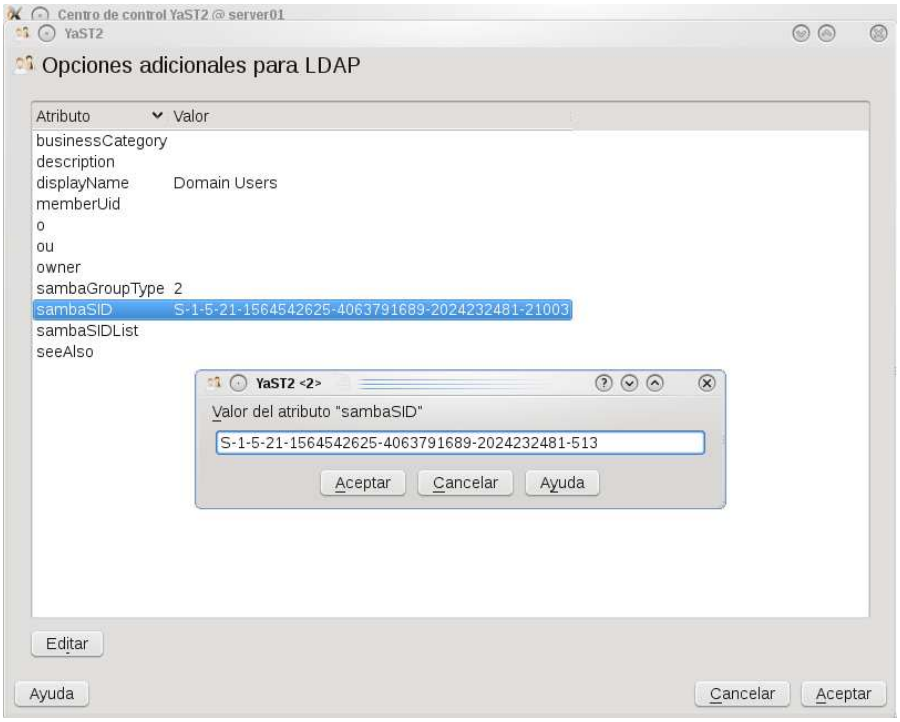

Ahora vamos a crear el grupo UNIX que será nuestro grupo Domain Users, escribimos los datos a como se muestra en las figuras siguientes.



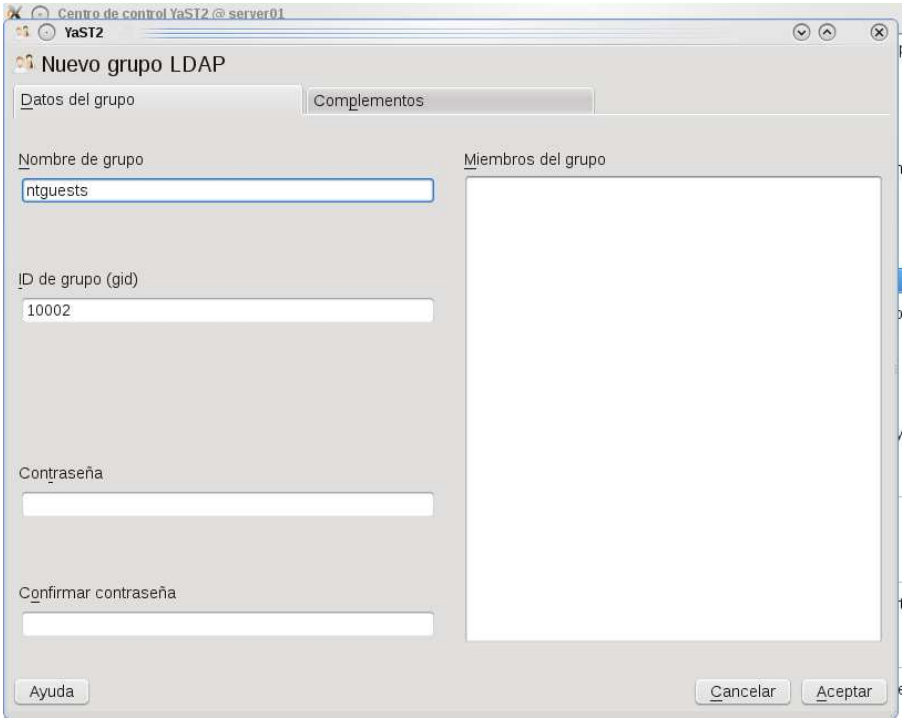

Nos vamos a complementos y seleccionamos el complemento Administrar el atributo samba de grupos LDAP y le ponemos Domain Users

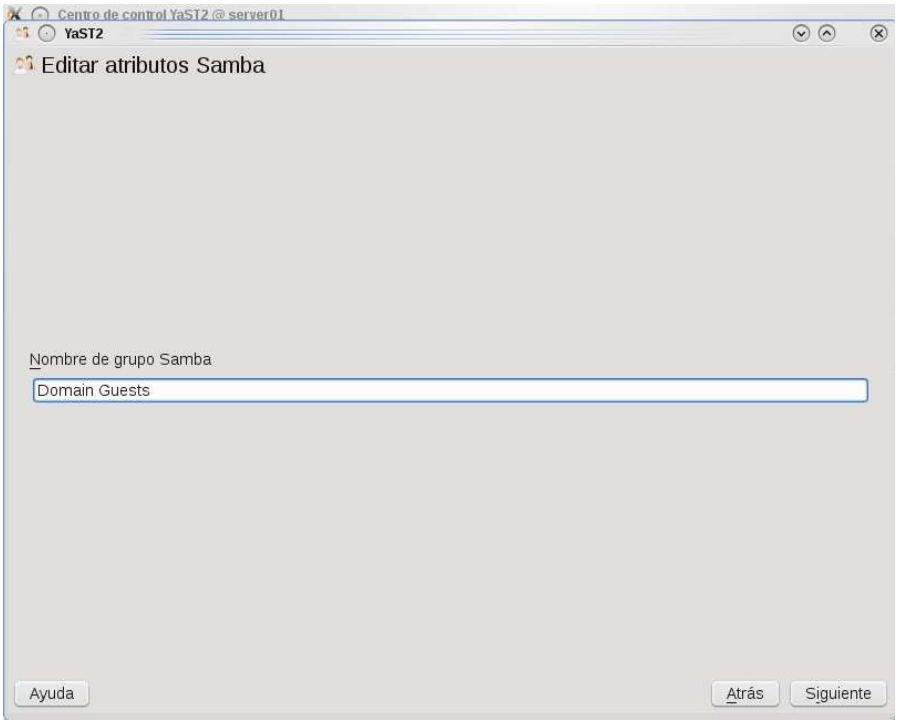


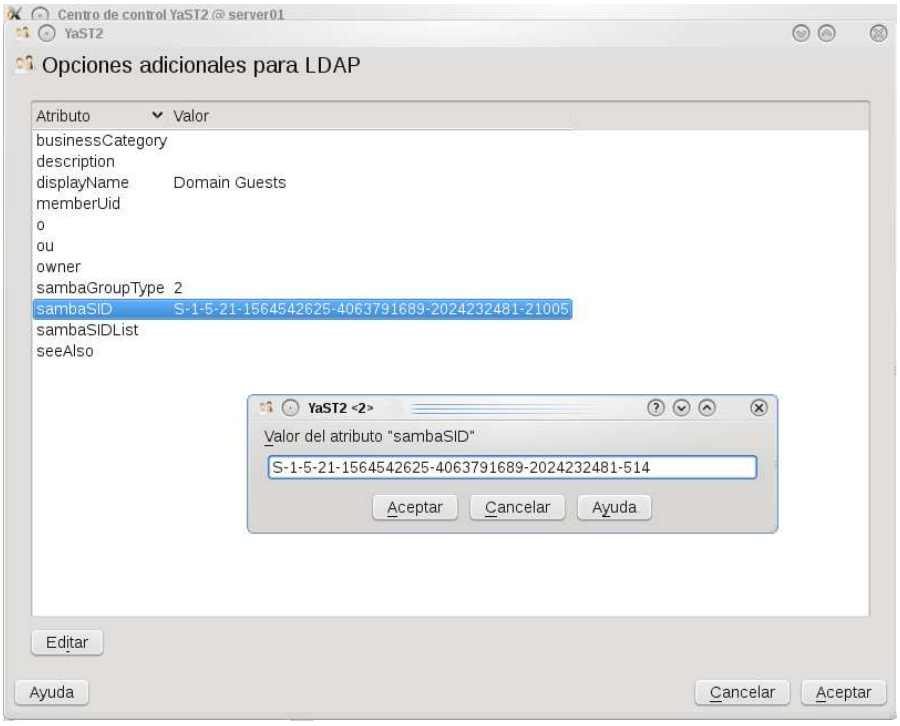

Seleccionamos Editar atributos LDAP restantes y cambiamos el sambaSID modificando el RID que son los últimos cinco dígitos a 513.



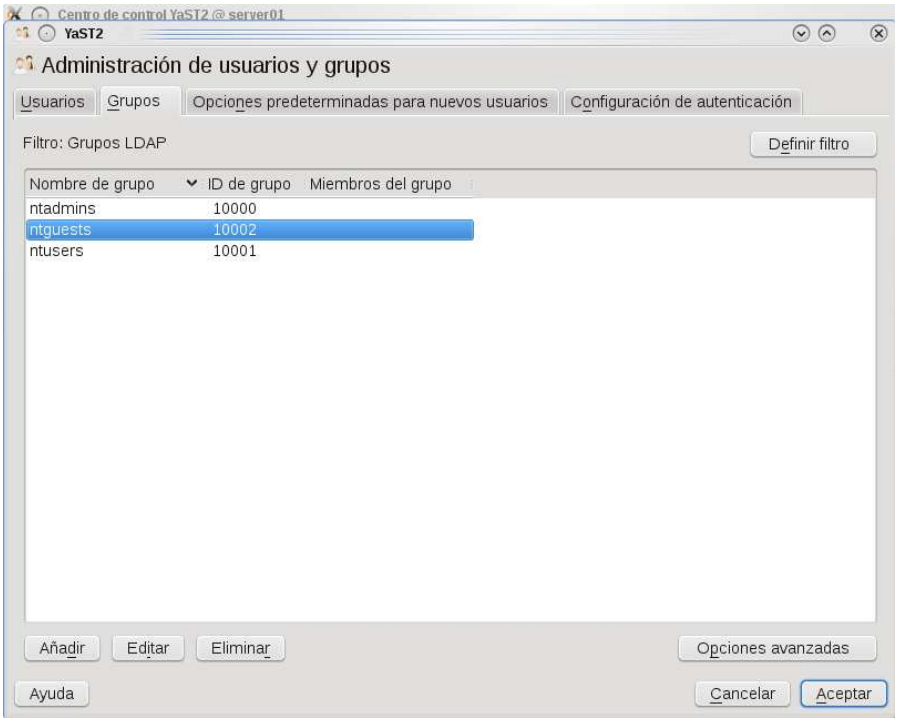

Ahora vamos a crear el grupo UNIX que será nuestro grupo Domain Guests.



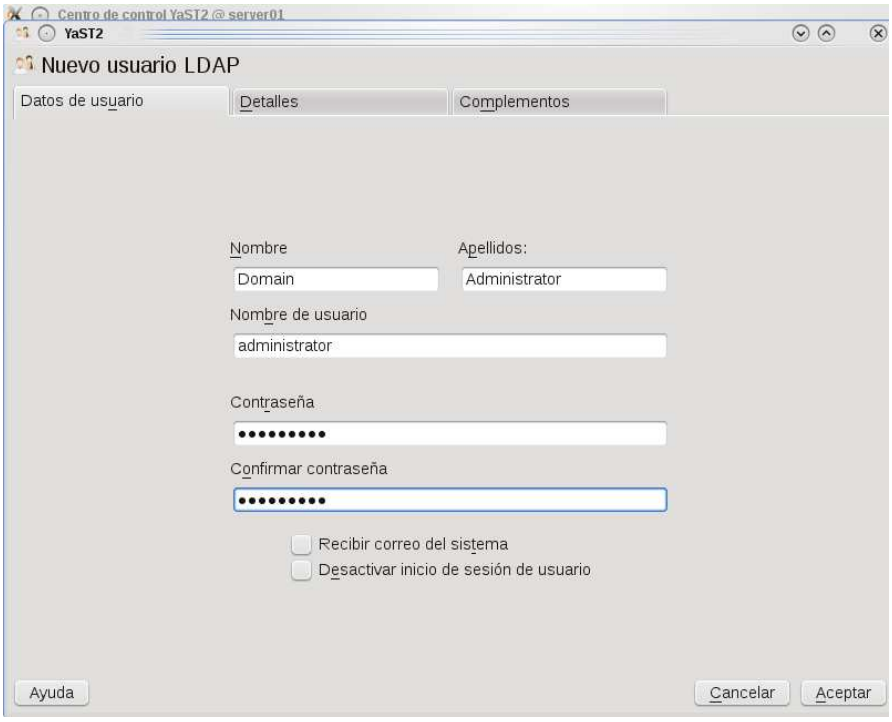


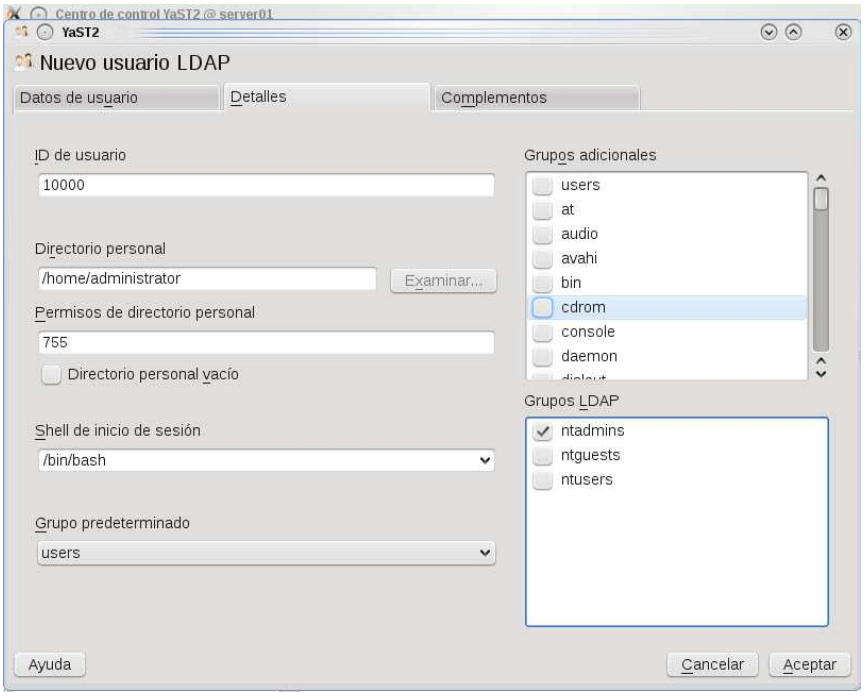

Cuando terminemos tendremos tres grupos ntadmins, ntusers y ntguest que serán nuestros grupos Domain Admins, Domain Users y Domain Guests respectivamente.




Ahora vamos a proceder a crear nuestra cuenta administrador Yast – Seguridad y usuarios – gestión de usuarios y grupos – usuarios – Filtro – usuarios LDAP – Añadir y rellenamos los datos a como se muestra.

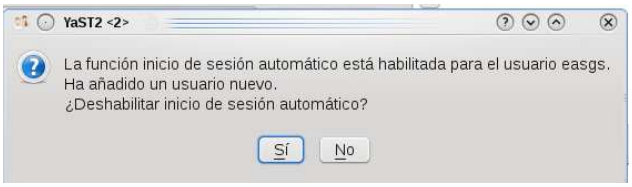



Lo hacemos miembro del grupo LDAP ntadmins.



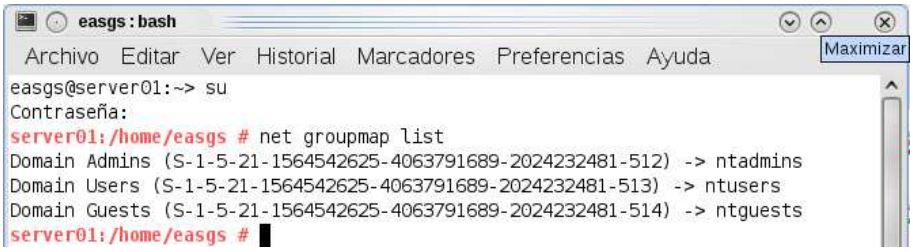

Para crear un usuario normal el procedimiento es el mismo con la excepción que lo haremos miembro del los grupos users de la sección Grupos adicionales y del grupo ntusers de la sección Grupos LDAP.

Damos clic en aceptar y nos saldrá un cuadro de dialogo preguntándonos si deseamos deshabilitar el inicio de sesión automática y le damos que si.




## 3.11 Listando el mapeo de grupos samba.

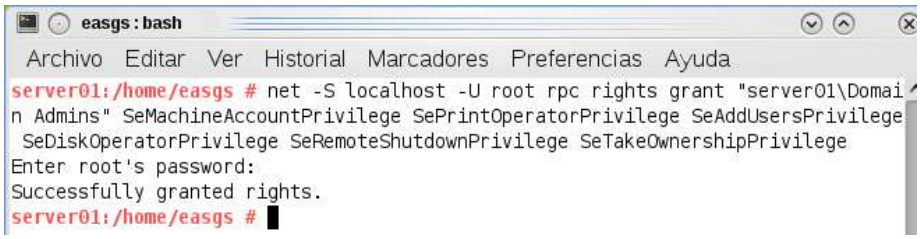
Ahora si ejecutamos el comando net groupmap list, podremos ver que ya están mapeados a los grupos Windows,



## 3.12 Asignando privilegios al grupo Domain Admins.

Lo que sigue es asignarle los privilegios correspondientes al grupo Domain Admins para ello ejecutamos el siguiente comando, nos pedirá la clave del root Samba:

net -S localhost -U root rpc rights grant "server01\Domain Admins" SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege SeTakeOwnershipPrivilege SeAddUsersPrivilege SeBackupPrivilege




Ahora todos los miembros del grupo ntadmins serán capaces de agregar maquinas al dominio así como otras funciones conocidas del administrador de un dominio Windows 200x Server, esto nos va a permitir usar la cuenta llamada Administrator en lugar de la cuenta root.

## 3.13 Listando privilegios asignados a los grupos samba.

Ahora si ejecutamos el comando net –S localhost –U% rpc rights list accounts veremos los privilegios asignados.

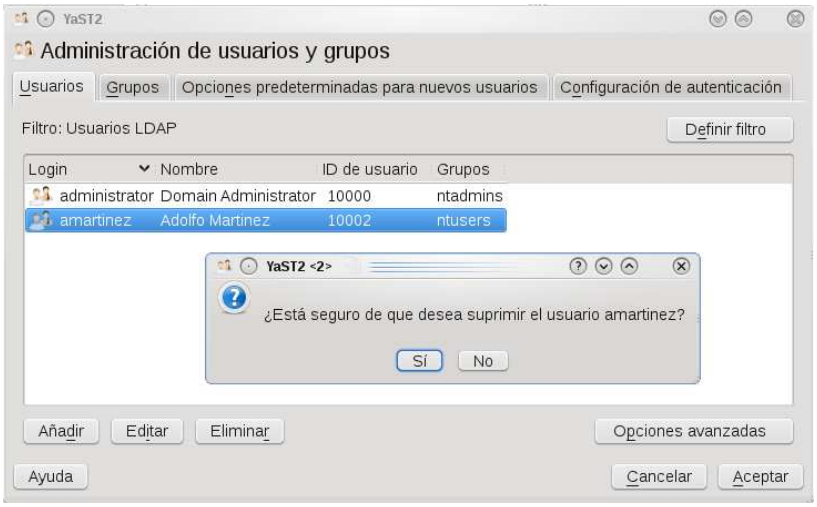
## 3.14 Revocando privilegios al grupo Domain Admins.

Para revocar esos privilegios ejecutamos el comando:

net -S localhost -U root rpc rights revoke "server01\Domain Admins" SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege SeTakeOwnershipPrivilege SeAddUsersPrivilege SeBackupPrivilege

## 3.15 Eliminando usuarios LDAP.

Para eliminar un usuario LDAP procedemos a Yast – Seguridad y usuarios – gestión de usuarios y grupos – usuarios – Filtro – usuarios LDAP – seleccionamos el usuario a eliminar y hacemos clic en el botón eliminar y confirmamos que si cuando pregunte que si estamos seguros.



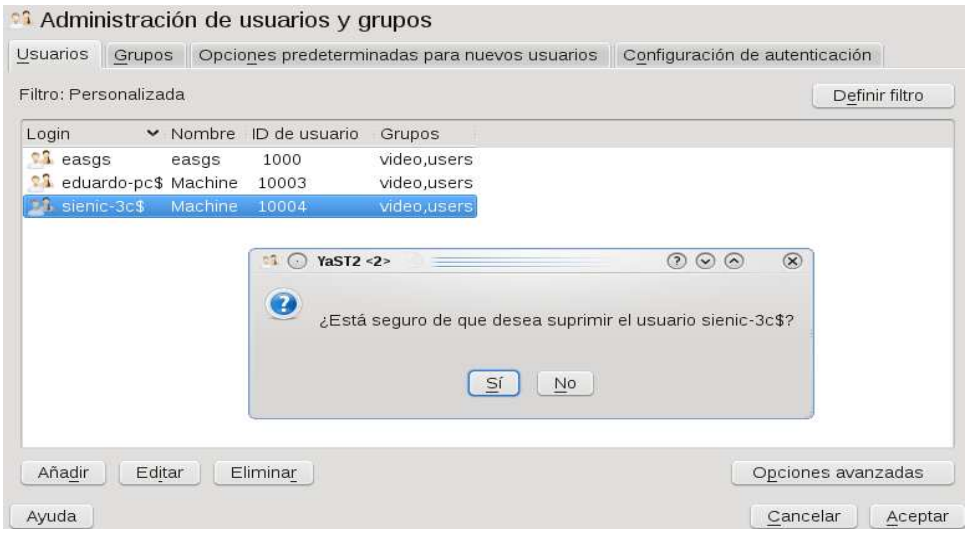

## 3.16 Eliminando cuentas de maquinas.

Para eliminar cuentas de maquinas que ya no existan en la red o que han sido renombradas procedemos a ejecutar el siguiente comando

ldapdelete -x -D "cn=administrator,dc=sienic,dc=site" -W "uid=SIENIC-3C$,ou=Machines,dc=sienic,dc=site"

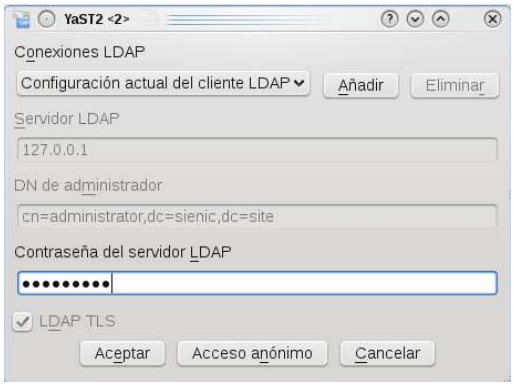
Nos pedirá la clave de la cuenta administrator LDAP.

Luego nos vamos a Yast – Seguridad y usuarios – gestión de usuarios y grupos – usuarios, seleccionamos la cuenta de la maquina que queremos eliminar y hacemos clic en eliminar y luego confirmamos la acción.

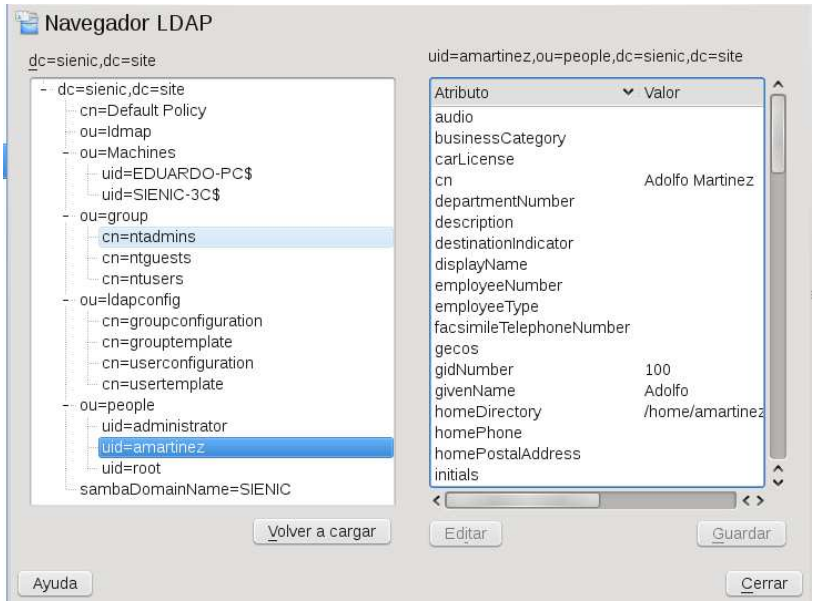



## 3.17 Navegador LDAP

Esta herramienta nos permite navegar por las distintas entradas del árbol LDAP, permitiéndonos modificar algunas de sus propiedades, para usar esta herramienta tenemos que introducir la clave del administrador LDAP.




En la siguiente imagen podemos ver como nos muestra la información el Navegador LDAP

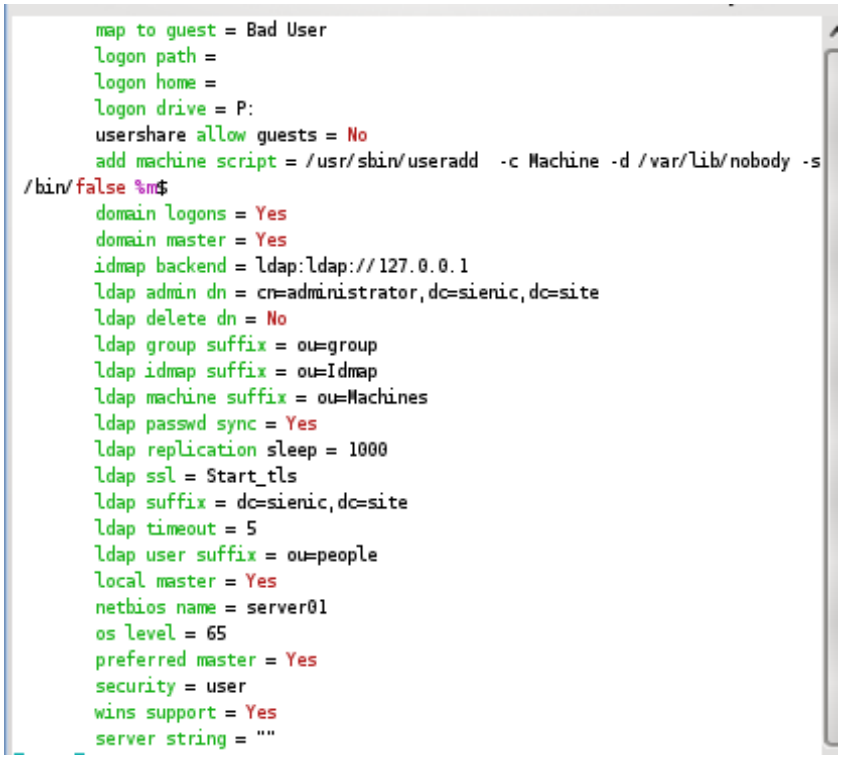



## 3.18 Realizando ajustes en el archivo smb.conf

Aun hay unos cuantos ajustes que debemos hacer en nuestro smb.conf que se encuentra en la ruta /etc/samba, las opciones deben quedar a como sigue en la sección [global].

Logon path =
Logon home =
Usershare allow guest = no
Server string = ””

También podemos agregar la opción browseable = no a las secciones [profiles] y [netlogon], los recursos [users] y [groups] estarán deshabilitados por yast, esto impedirá que los usuarios vean estos recursos cuando entren al servidor por medio del entorno de red.



```
        map to guest = Bad User
        logon path =
        logon home =
        logon drive = P:
        usershare allow guests = No
        add machine script = /usr/sbin/useradd  -c Machine -d /var/lib/nobody -s
/bin/false %m$
        domain logons = Yes
        domain master = Yes
        idmap backend = ldap:ldap://127.0.0.1
        ldap admin dn = cn=administrator,dc=sienic,dc=site
        ldap delete dn = No
        ldap group suffix = ou=group
        ldap idmap suffix = ou=Idmap
        ldap machine suffix = ou=Machines
        ldap passwd sync = Yes
        ldap replication sleep = 1000
        ldap ssl = Start_tls
        ldap suffix = dc=sienic,dc=site
        ldap timeout = 5
        ldap user suffix = ou=people
        local master = Yes
        netbios name = server01
        os level = 65
        preferred master = Yes
        security = user
        wins support = Yes
        server string = ""
```

## 3.19 Comando smbpasswd -w

Cabe mencionar que no es necesario ejecutar el comando smbpasswd -w secret (donde secret es la nueva clave de administrador LDAP) ya que esta clave ya esta registrada en el archivo secrets.tdb, esto solo será necesario si cambiamos la clave de administrador LDAP, para ver el contenido de este archivo ejecutamos el comando *tdbdump secrets.tdb* de esta forma podemos verificar si la clave ya esta registrada..

## 3.20 smb final

Al finalizar nuestro archivo smb.conf se vera así:

```
# smb.conf is the main Samba configuration file. You find a full commented
# version at /usr/share/doc/packages/samba/examples/smb.conf.SUSE if the
# samba-doc package is installed.
# Date: 2009-10-27
[global]
        workgroup = SIENIC
        passdb backend = ldapsam:ldap://127.0.0.1
        printing = cups
        printcap name = cups
        printcap cache time = 750
        cups options = raw
        map to guest = Bad User
        logon path =
        logon home =
        logon drive = P:
        usershare allow guests = No
        add machine script = /usr/sbin/useradd  -c Machine -d /var/lib/nobody -s /bin/false %m$
        domain logons = Yes
        domain master = Yes
        idmap backend = ldap:ldap://127.0.0.1
        ldap admin dn = cn=administrator,dc=sienic,dc=site
        ldap delete dn = No
        ldap group suffix = ou=group
        ldap idmap suffix = ou=Idmap
        ldap machine suffix = ou=Machines
```

```
        ldap passwd sync = Yes
        ldap replication sleep = 1000
        ldap ssl = Start_tls
        ldap suffix = dc=sienic,dc=site
        ldap timeout = 5
        ldap user suffix = ou=people
        local master = Yes
        netbios name = server01
        os level = 65
        preferred master = Yes
        security = user
        wins support = Yes
        server string = ""
[homes]
        comment = Home Directories
        valid users = %S, %D%w%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
        browseable = no

## Share disabled by YaST
# [users]
#       comment = All users
#       path = /home
#       read only = No
#       inherit acls = Yes
#       veto files = /aquota.user/groups/shares/

## Share disabled by YaST
# [groups]
#       comment = All groups
#       path = /home/groups
#       read only = No
#       inherit acls = Yes
[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No
[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @ntadmin root
        force group = ntadmin
        create mask = 0664
        directory mask = 0775

[netlogon]
        comment = Network Logon Service
        path = /var/lib/samba/netlogon
        write list = root
        browseable = no
```

### 3.21 Descripción de las opciones

A continuación se explican algunas de las opciones, las demás ya han sido expuestas en los ejemplos anteriores.

idmap backend = ldap:ldap://127.0.0.1

El propósito de este parámetro es permitir que idmap NO use el fichero idmap tdb local para obtener las asociaciones de SID a UID / GID mappings, para obtenerlos en su lugar de una base ldap común. De esta forma todos los miembros del dominio tendrán los mismos UID y GID asociados a SID. Para evitar el riesgo de inconsistencia de UID / GID entre sistemas UNIX / Linux que comparten información bajo protocolos distintos de SMB/CIFS (ie: NFS).

ldap admin dn = cn=administrator,dc=sienic,dc=site

Este parámetro define el nombre "Distinguished Name" (DN) que usa samba para contactar con el servidor ldap cuando solicita información de las cuentas. El parámetro *`ldap admin dn`* se usa conjuntamente con la contraseña de administración almacenada en el fichero `private/secrets.tdb`.

ldap delete dn = No

Este parámetro especifica si una operación de borrado en la base de datos ldapsam elimina toda la entrada o sólo los atributos específicos de Samba.

ldap group suffix = ou=group

Este parámetro especifica el sufijo que se usa para los grupos que se añaden al directorio LDAP. Si el parámetro no está definido se usa el valor de *`ldap suffix`*.

ldap idmap suffix = ou=Idmap

Este parámetro especifica el sufijo que se usa cuando se almacenan asociaciones idmap. Si el parámetro no está definido se usa el valor de *`ldap suffix`*.

ldap machine suffix = ou=Machines

Especifica en qué parte del árbol LDAP se agregan las máquinas.

ldap passwd sync = Yes

Esta opción se usa para definir si Samba sincroniza o no la contraseña LDAP con las contraseñas NT y LM para las cuentas normales (no para las estaciones de trabajo, servidores o dominios de confianza) cunado se efectúa un cambio de contraseña mediante SAMBA.

*`ldap passwd sync`* se puede configurar con tres posibles valores:

- *`Yes`* = Intenta actualizar las contraseñas LDAP, NT y LM y actualizar pwdLastSet.
- *`No`* = Actualiza las contraseñas NT y LM y actualiza pwdLastSet.

- *Only* = Sólo actualiza la contraseña LDAP y deja que el servidor LDAP haga el resto.

ldap replication sleep = 1000

Cuando se le solicita a Samba que escriba en una réplica LDAP de sólo lectura, no redirecciona para dialogar con el servidor principal de lectura y escritura. Entonces este servidor replica los cambios al servidor local, sin embargo esta réplica puede tardar algunos segundos, especialmente sobre enlaces lentos. La actividad de algunos clientes, particularmente las uniones al dominio, pueden confundirse por el éxito que no cambia inmediatamente los datos del back-end' de LDAP.

Esta opción simplemente hace que Samba espere un poco para permitir al servidor LDAP actualizarse. Si tiene una red con una latencia particularmente alta, le puede interesar ver el tiempo de la réplica LDAP con un sniffer, e incrementar el valor según los resultados. Tenga cuidado porque no se comprueba que los datos se hayan replicado.

El valor se especifica en milisegundos.

ldap ssl = Start_tls

Esta opción se usa para definir si Samba usa SSL o no cuando se conecta al servidor ldap. Esto no tiene relación con el soporte previo SSL de Samba que se activa especificando -- with-ssl durante la configuración con el script configure.

The ldap ssl puede tomar alguno de los valores:

Off = Nunca usa SSL cuando consulta el directorio.

Start_tls = Usa la operación extendida LDAPv3 StartTLS (RFC2830) para comunicar con el servidor ldap.

On = Usa SSL en el puerto ldaps cuando contacta con ldap server. Sólo está disponible cuando se ha especificado la opción de compatibilidad previa --with-ldapsam para la configuración de Samba.

ldap suffix = dc=sienic,dc=site

Este parámetro especifica donde se añaden las cuentas de usuario y de máquina en el árbol. Se puede modificar mediante ldap user suffix y ldap machine suffix. También se puede usar como la base dn para todas las búsquedas ldap.

ldap timeout = 5

Este parámetro define el tiempo en segundos que samba debe usar como tiempo de respuesta máximo para operaciones LDAP.

Predeterminado: *ldap timeout = 15*

ldap user suffix = ou=people

Este parámetro especifica donde se añaden las cuentas de usuario en el árbol. Si no se especifica este parámetro se usa el valor de *ldap suffix*.

## 3.22 Los recursos compartidos [users] y [groups]

El recurso [users] se usa para compartir el directorio /home a todos los usuarios, este recursos muestra todos los subdirectorios bajo /home en el servidor de la red a todos aquellos usuarios que puedan introducir un nombre de usuario y una clave validas y podrán ver este recurso introduciendo el nombre del servidor seguido de /users

Los usuarios podrán ver los directorios de los demás y tendrán acceso de lectura y escritura a su propio directorio.

El recurso [groups] es accesible para todos los usuarios, se debe crear el directorio Group especificado en el parámetro path. Este debe ser creado como root bajo el directorio /home.

Este recurso es de solo lectura y es útil para compartir cualquier tipo de archivo que deba ser visto por cualquier usuario autenticado en la red, si deseamos que sea de escritura debemos cambiar los permisos con el comando chmod 777.

En esta guía en todos los ejemplos estos recursos han sido deshabilitados por motivos de seguridad, para ver un ejemplo de carpeta compartida en este escenario pase a la página Numero 81.

## 3.23 Políticas de contraseñas

Con samba se pueden agregar políticas de contraseña, esto nos sirve para mejorar la seguridad de nuestra red, en algunas empresas esto es requerido mas aun cuando existe un departamento de auditoria interna que monitorea regularmente el cumplimiento de estándares básicos de seguridad informática.

Las políticas aplicables son:

min password length

Define el tamaño mínimo que debe tener una contraseña

password history

Define la cantidad de contraseñas almacenadas, esto evita que una contraseña se vuelva a definir dentro del rango especificado.

user must logon to change password

Define que el usuario debe hacer logon para poder cambiar su contraseña.

maximum password age

Establece el tiempo máximo que puede usarse una contraseña su valor se especifica en segundos.

minimum password age

Establece el tiempo mínimo antes de permitir un cambio de contraseña, su valor se especifica en segundos.

lockout duration

Define el tiempo que durara el bloqueo de una cuenta, su valor se especifica en minutos.

reset count minutes

Regresa a cero el contador de claves erróneas introducidas después del tiempo minutos indicados, su valor se especifica en minutos.

bad lockout attempt

Numero de intentos con clave errónea antes que la cuenta se bloquee.

Otras politicas son:  disconnect time y refuse machine password change

## 3.24 Flags que se pueden asignar a un usuario

D  La cuenta esta Deshabilitada.
H  Requiere del directorio home.
I  Una cuenta de confianza entre dominios.
L  La cuenta se ha autobloqueado.
M  Una cuenta deMNS (Microsoft network service)
N  No requiere contraseña.
S  Una cuenta de confianza de servidor.
T  Entrada de contraseña temporalmente duplicada.
U  Una cuenta de usuario.
W  Una cuenta de estación de trabajo o maquina.
X  La clave no expira.

Para ver las flags que tiene un usuario se ejecuta el comando pdbedit –Lv amartinez y nos aparecerá algo como lo que se muestra en la siguiente figura, reemplazando amartinez por el nombre de usuario adecuado.


Para aplicar las siguientes políticas de contraseña:

Tamaño mínimo de una clave = 5

Historial de claves = 4

Antigüedad máxima para una clave = 60 días (86400 segundos en un día * 60 días)

Antigüedad minima para cambiar una clave = 7 días (86400 segundos en un día * 7)

Intentos permitidos con clave errónea = 4

Duración de bloqueo = 60 minutos.

Ejecutamos los siguientes comandos:

pdbedit -P "min password length" -C 5

pdbedit -P "password history" -C 4

pdbedit -P "maximum password age" -C 5184000

pdbedit -P "minimum password age" -C 604800

pdbedit -P "bad lockout attempt" -C 4

pdbedit -P "lockout duration" -C 60

Cuando se bloquea una cuenta por intentos de clave fallidos ejecutamos los siguiente para desbloquear la cuenta, para borrar el bad password count ejecutamos

pdbedit -z usuario

Para desbloquear el usuario y resetear las flags al valor predeterminado ejecutamos.

pdbedit -r -c=[] usuario

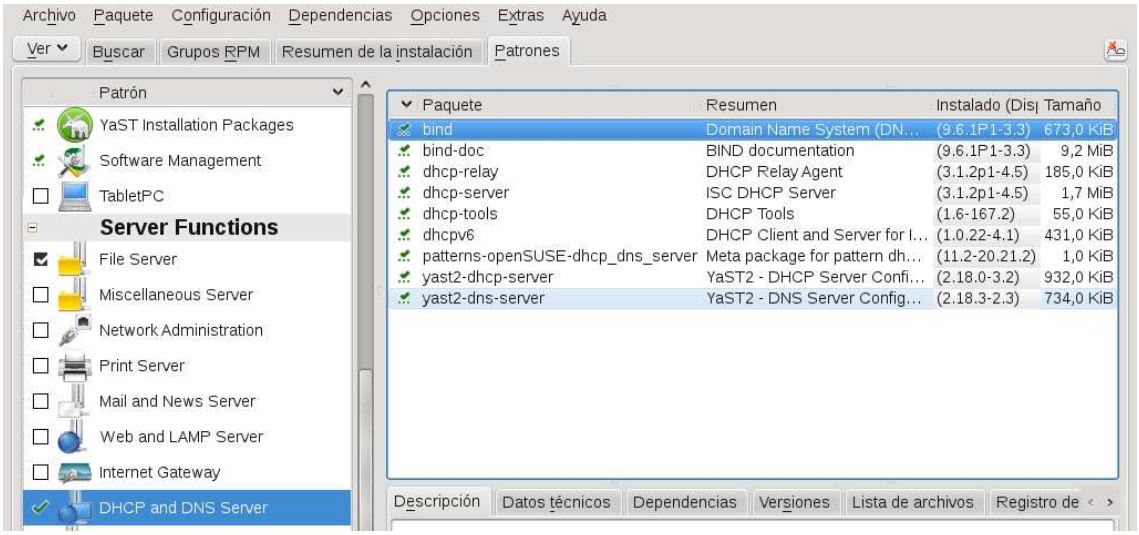
### 3.25 El Firewall

Debemos autorizar los servicios de Samba Server, Netbios Server y LDAP Server en el firewall, si aun no están autorizados.

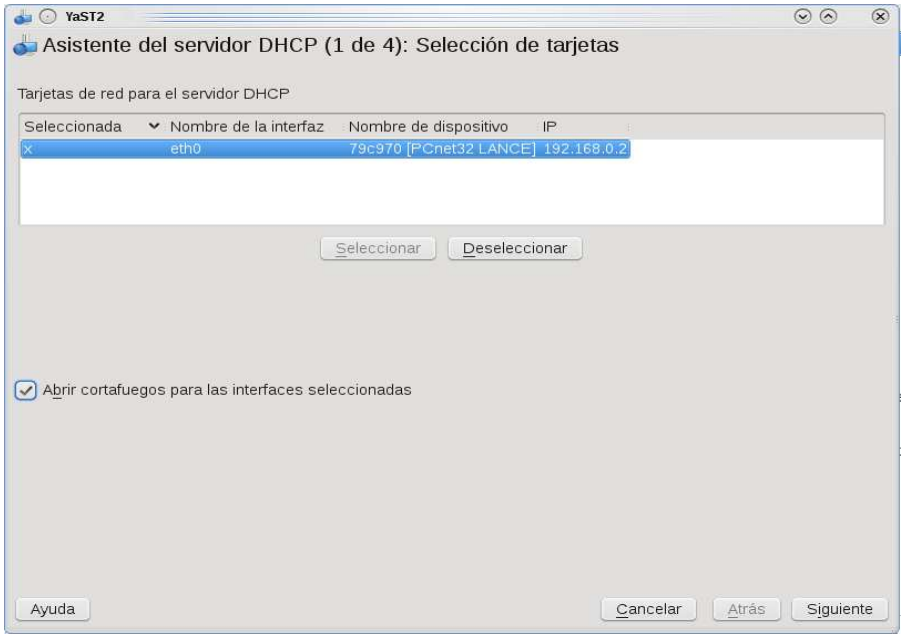
# 4.- Configuración del servidor DHCP.

## 4.1 Instalación del servidor DHCP

Ahora procederemos a configurar el servidor DHCP para que este asigne de manera automática las direcciones IP a las maquinas de nuestra red y no tengamos que preocuparnos por eso, procedemos a instalar el servidor DHCP a como se muestra en la imagen.

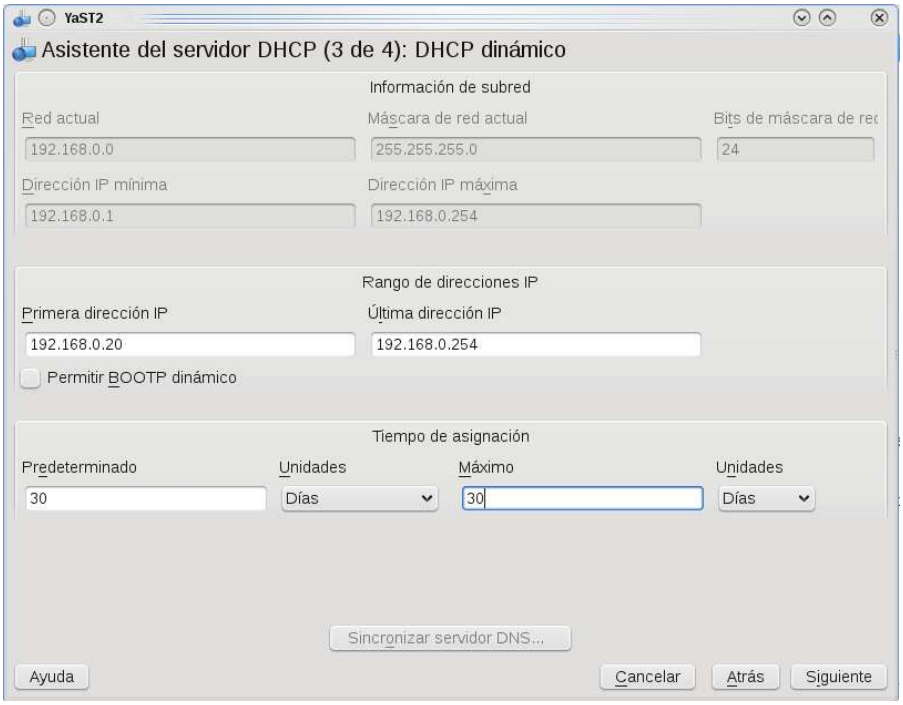



Nos vamos a Servicios de red y seleccionamos servidor DHCP, seleccionamos nuestra interfaz de red y abrir cortafuegos para las interfaces seleccionadas, hacemos clic en siguiente.




En nombre de dominio escribimos sienic.site, sustituyendo sienic por el nombre de su dominio, en servidor WINS ponemos la dirección de este servidor ya que funcionara como tal, en tiempo de asignación predeterminada seleccionemos 30 días, este plazo será el tiempo en el que una PC de nuestra red tendrá asignada una dirección de red, hacemos clic en siguiente.


En esta pantalla vamos a definir nuestro ámbito DHCP, será el rango de direcciones ip disponibles para ser asignada a maquinas en la red, en tiempo de asignación dejamos como predeterminado 30 días y en Máximo 30 días, hacemos clic en siguiente




Aquí vamos a definir que el servidor DHCP se iniciara de manera automática cada vez que reiniciemos el servidor, hacemos clic en terminar.


## 4.2 Liberando direcciones IP

En algunos casos nuestro servidor se puede quedar sin direcciones IP, esto por alguna actualización de la flota de PC de la red o porque muchas laptops han entrado y salido de la red, para liberar direcciones ip que estén asignadas a maquinas que ya no se encuentren en la red nos vamos a /val/lib/dhcp/db/ y editamos el archivo dhcpd.leases su contenido es parecido a este:

```
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.1.2p1

lease 192.168.0.31 {
  starts 2 2009/11/03 19:24:49;
  ends 4 2009/12/03 19:24:49;
  tstp 4 2009/12/03 19:24:49;
  cltt 2 2009/11/03 19:24:49;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:9a:5e:82;
  uid "\001\000\014)\232^\202";
  client-hostname "EDUARDO-PC";
}
lease 192.168.0.30 {
  starts 3 2009/11/04 22:41:58;
  ends 5 2009/12/04 22:41:58;
  cltt 3 2009/11/04 22:41:58;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:49:da:79;
  uid "\001\000\014)I\332y";
  client-hostname "sienic-3c";
}
```

Para liberar la dirección asignada a la maquina sienic-3c simplemente borramos la entrada desde donde dice lease 192.168.0.30 hasta donde cierra el corchete que es la parte que hemos puesto en negrilla por motivos ilustrativos.

## 4.3 Renovando direcciones IP en las estaciones de trabajo.

Para renovar las direcciones IP en las estaciones de trabajo Windows ejecutamos

Ipconfig /release
Ipconfig /renew

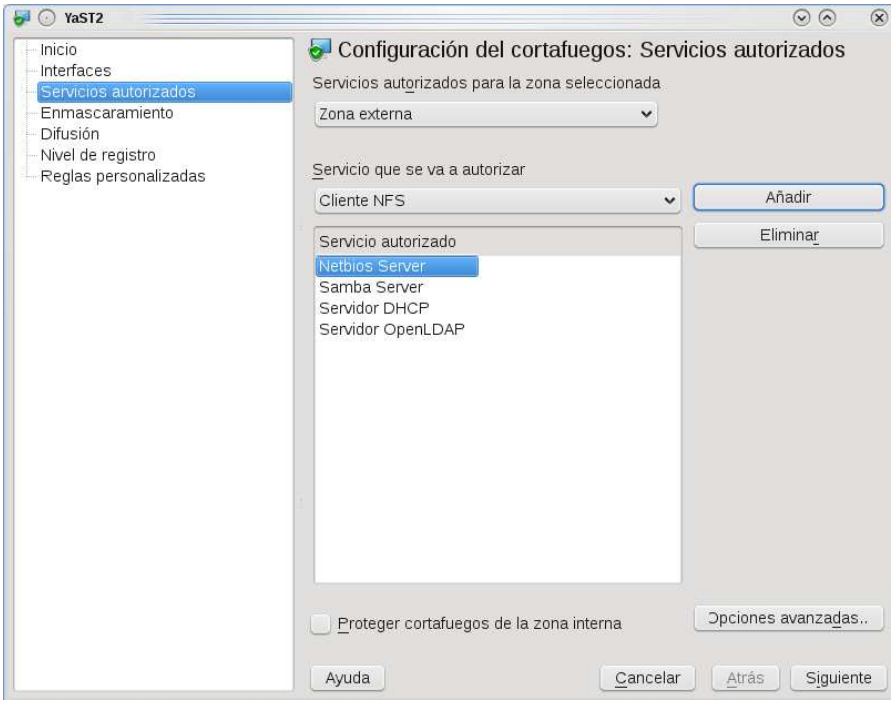
En las estaciones linux

dhclient –r  para liberar la dirección

dhclient  para renovar la dirección

## 4.4 EL FIREWALL

Al finalizar de configurar openSUSE como PDC con LDAP, WINS y DHCP debemos revisar que los todos los servicios necesarios estén autorizados, tal a como se muestra en la siguiente grafica.




# 4.- Como limpiar la cache de Wins

## 4.1 Limpiando la cache de Wins

Algunas veces es necesario que después de algunos cambios en la red sean limpiadas del archivo wins.dat algunas entradas erróneas y antiguas que nos pueden estar causando problemas, también a veces cuando hemos cambiado el nombre a varias maquinas estas entradas pueden permanecer en el archivo antes mencionado, es por eso que en algunas ocasiones es necesario limpiar la cache de wins en nuestro servidor openSUSE, para lograr esto hacemos lo siguiente:

1) Localicemos el archivo /var/lib/samba/wins.dat y lo borramos.

2) Ejecutemos el siguiente comando: rcnmb restart

Si las viejas entradas vuelven a aparecer entonces borramos /var/lib/samba/wins.dat y /var/lib/samba/wins.tdb, detenemos el servicio por completo y lo volvemos a arrancar.

En caso de ser necesario se puede hacer que un cliente Windows se vuelva a registrar con el comando: nbtstat -RR

# 6.- Variables de entorno usadas por samba.

## 6.1 Explicación de las variables de entorno usadas por samba.

Muchas de las variables que se pueden establecer en el archivo de configuración de samba pueden tomar otros valores, por ejemplo la opcion “path = /tmp/%u” es interpretada como “path = tmp/easgs” si el nombre del usuario conectado es easgs.

Estas sustituciones se explican a continuación.

U%

Nombre de usuario de la sesión (el nombre de usuario que el cliente quería, no necesariamente el que obtuvo)

%G

Nombre del grupo primario de %U

%h

El nombre de hostname de internet en el que samba se esta ejecutando

%m

El nombre netbios de la maquina.

%L

El nombre netbios del servidor.

%M

El nombre de Internet de la maquina cliente.

%R

El nivel de protocolo seleccionado después de la negociación del mismo. Este puede ser CORE, COREPLUS, LANMAN1, LANMAN2 o NT1.

%d

El id del proceso del actual proceso del servidor.

%a

La arquitectura de la maquina remota, actualmente las reconocidas son samba (samba), el sistema de archivos de linux CIFS (CIFSFS), OS/2 (OS2), Windows para grupos de trabajo (WfWg), Windows 9x/ME (win95), Windows NT (WinNT), Windows 2000 (Win2K), Windows XP (WinXP), Windows XP 64 bit (WinXP64), Windows 2003

incluyendo 2003R2 (Win2K3) y Windows Vista (Vista) cualquier otro sera conocido como UNKNOWN.

%I

La dirección IP de la maquina cliente.

%i

La dirección IP local a la cual el cliente esta conectado.

%T

Fecha y Hora actuales

%D

El nombre del dominio o grupo de trabajo del usuario actual.

%w

El separador winbind
%$ (envvar)

El valor de la variable de entorno envar.

Los siguientes sustitutos aplican únicamente a algunas opciones de configuración (solamente aquellas en donde la conexión ya a sido establecida)

%$

El nombre del servicio actual, si hay uno.

%P

El directorio raíz del servicio actual, si hay uno.

%u

El nombre de usuario del servicio actual, si hay uno.

%g

El nombre del grupo primario de %u.

%H

El directorio home del usuario dado por %u.

%N

El nombre del su NIS home directory server. Este se obtiene de la entrada NIS auto.map. Si no a compilado samba con la opción –with-automount, este valor será el mismo de %L.

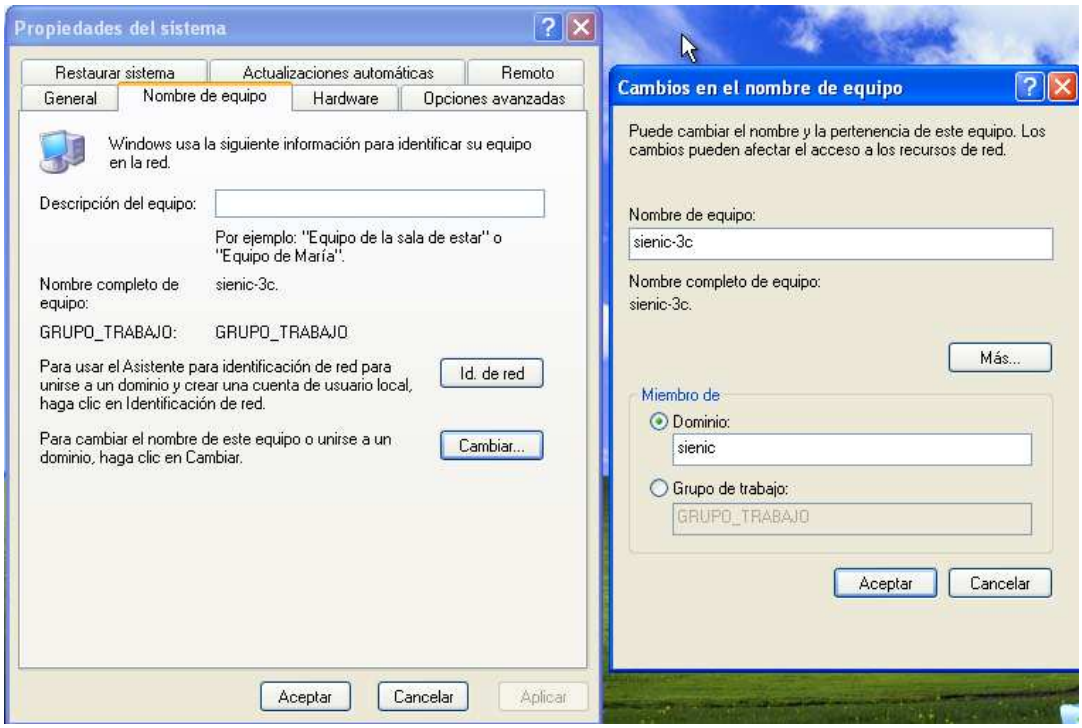
%p

La ruta al directorio home del servicio, obtenido de su entrada NIS auto.map. La entrada NIS auto.map se dividirá como %N:%p.

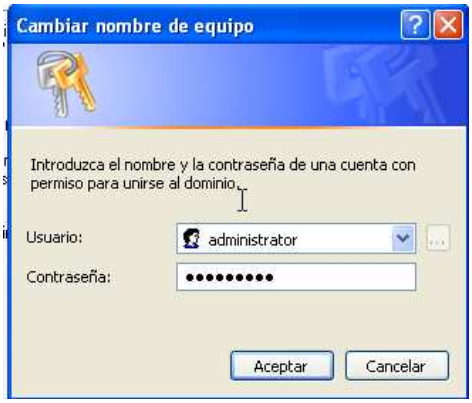
# 7.- Uniendo las estaciones de trabajo a nuestro Dominio.

## 7.1 Windows xp

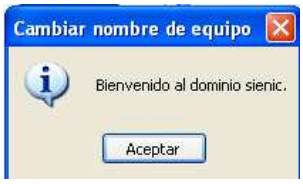
Nos vamos a Inicio – Mi PC – hacemos clic con el botón secundario – propiedades – Nombre de equipo y hacemos clic en Cambiar, en Miembro de, seleccionamos Dominio y escribimos el nombre de nuestro dominio, luego hacemos clic en aceptar.



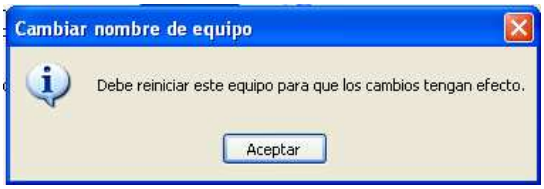

Nos pedirá la clave de administrador y la clave.




Nos aparecerá el mensaje de bienvenida al dominio



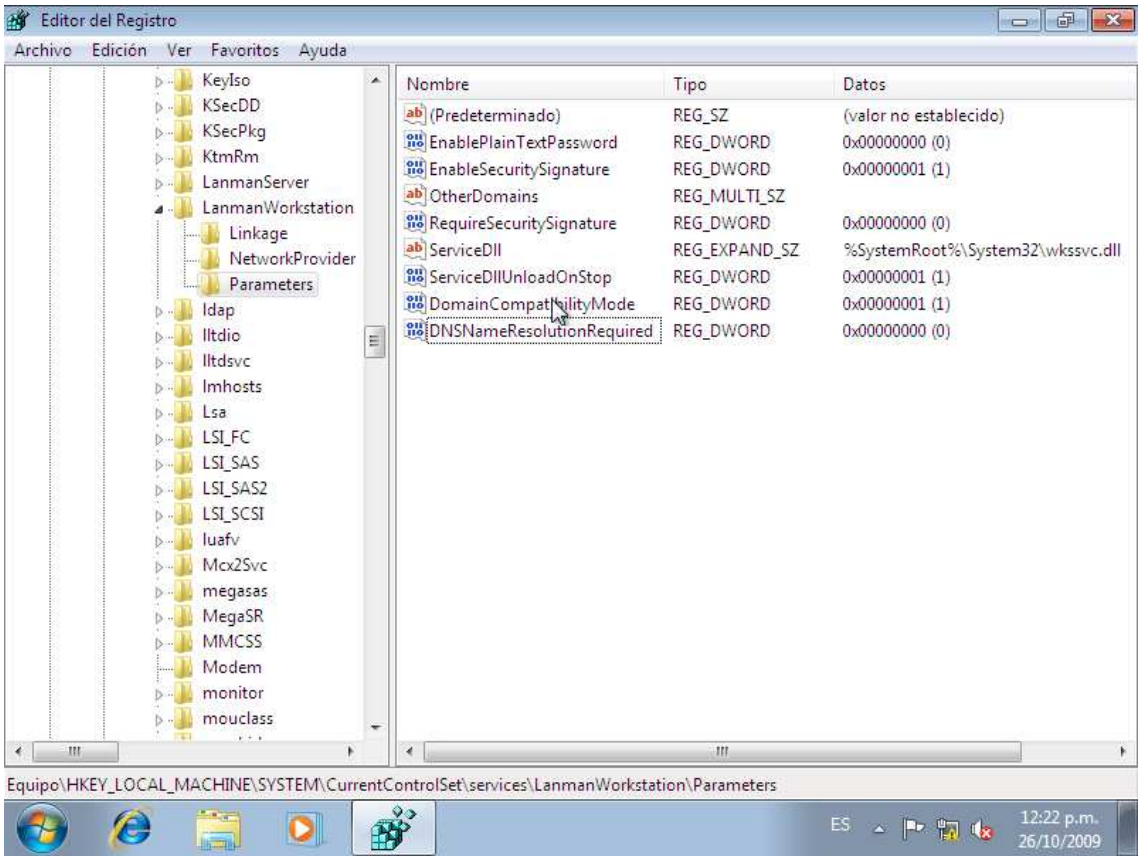

Debemos reiniciar la pc para aplicar los cambios.



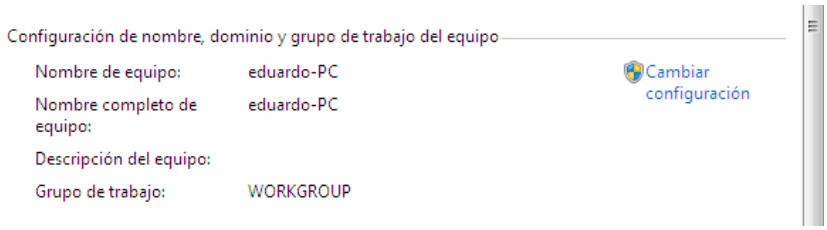

Una vez reiniciada la maquina nos aparecerá el dominio en la lista.

## 7.2 Windows 7

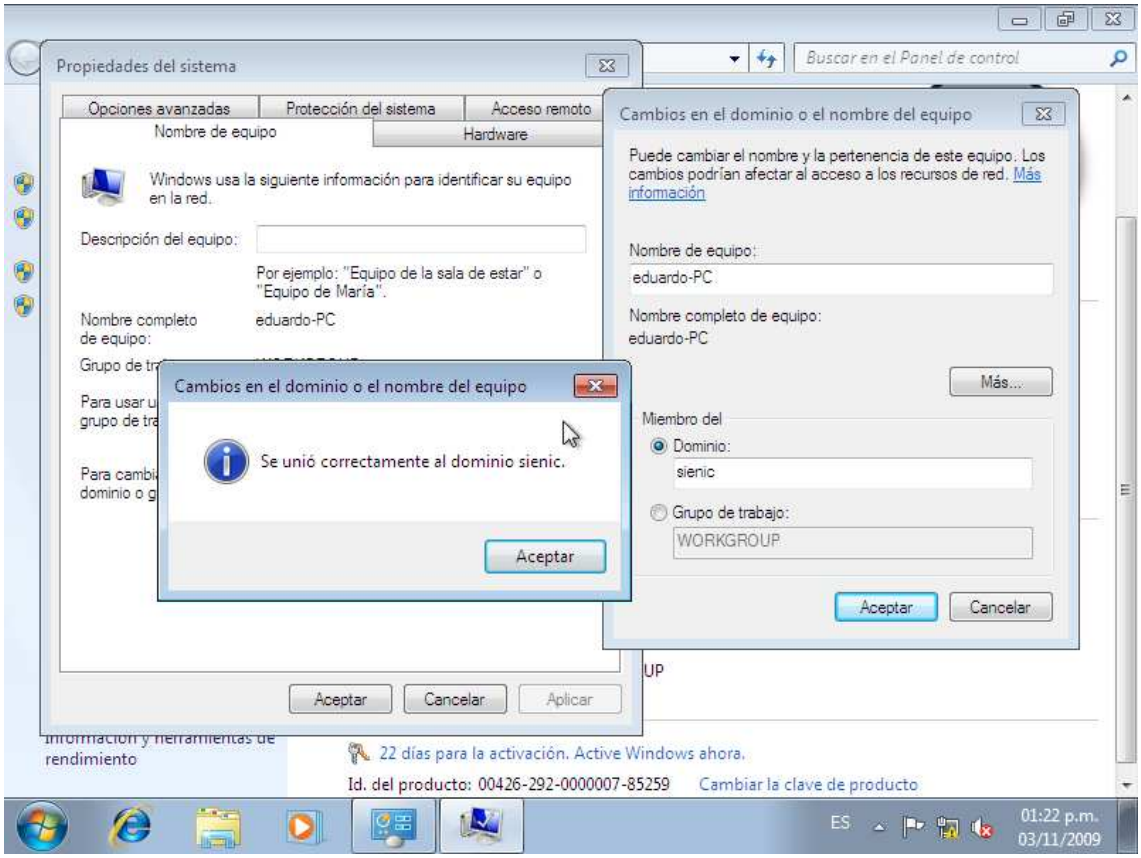
Para unir Windows 7 nos vamos a regedit y agregamos las ultimas dos entradas que se muestran en la siguiente imagen que son DomainCompatibilityMode con valor 1 y DNSNameResolutionRequired con valor 0.



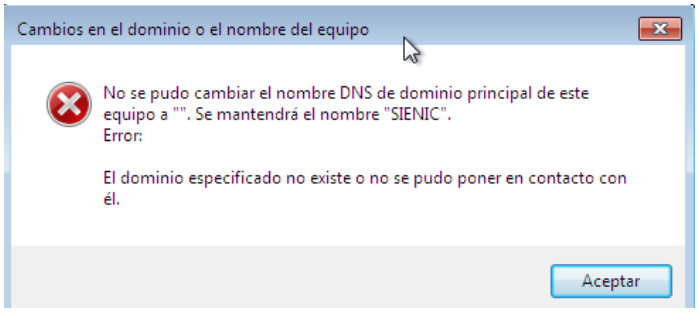

Inicio – Computadora – clic con el botón secundario del Mouse – propiedades y damos clic a Cambiar configuración.



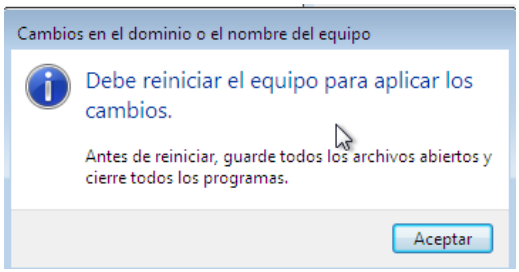
El resto del proceso es igual que el de Windows xp.




Con la única diferencia que nos va a aparecer el siguiente mensaje de error, damos clic en aceptar




Debemos reiniciar el equipo para que se apliquen los cambios



## 7.3 Windows Vista

Para unir Windows Vista a un dominio samba procedemos a como sigue

- Presionamos la tecla Windows + R y ejecutamos `secpol.msc`.
- Security Settings -> Local Policies -> Security Options.
- Seleccionamos Network Manager: LAN Manager authentication level.
- Lo cambiamos a  LM and NTLM – use NTLMv2 if negotiated.

El resto del procedimiento es igual que el de Windows 7 a excepción de los cambios en el registro que no son necesarios.

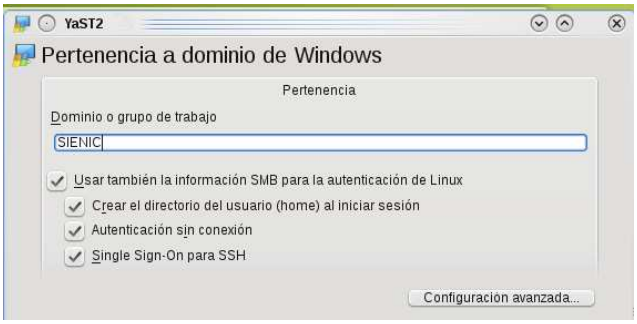
***Nota: Ninguna de las versiones "Home" de los sistemas operativos Windows son capaces de unirse a un Dominio***

## 7.4 OpenSUSE 11.2

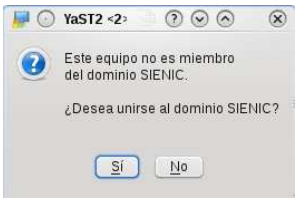
Para unir openSUSE 11.2 a nuestro dominio procedemos a como sigue.

Yast – Seguridad y Usuarios – Firewall y autorizamos los servicios samba Server y samba client.

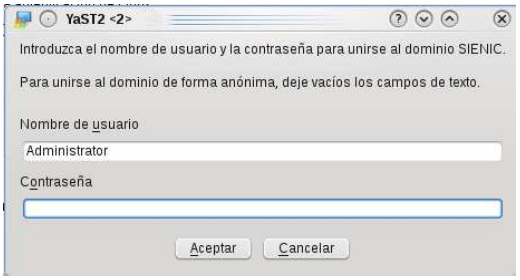

Luego nos vamos a Yast – Servicios de red – Pertenencia a dominio de Windows  y en Dominio o grupo de trabajo escribimos el nombre de nuestro dominio, también seleccionamos las otras cuatro opciones, el resto lo dejamos a como esta y le damos aceptar.



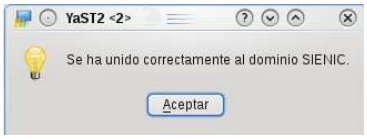
Cuando nos salga el mensaje que se muestra a continuación le damos que si



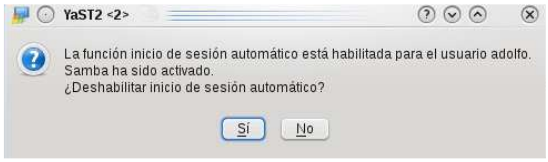

Nos pedirá la contraseña del usuario con privilegios para agregar maquinas al dominio.




En el siguiente mensaje le damos aceptar

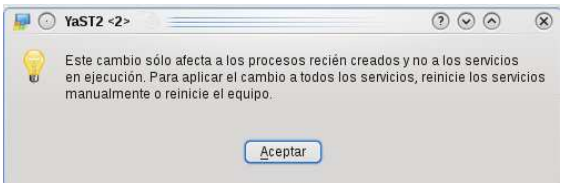



Y procedemos a darle que si deshabilite el inicio de sesión automático




Nos indicara que va a instalar el paquete samba-winbind, le damos clic en instalar


En el siguiente mensaje le damos aceptar y reiniciamos la maquina




Ahora en la ventana de inicio de sesión tendremos la opción de Dominio en donde podemos escoger iniciar sesión con un usuario local o un usuario del dominio, en nuestro ejemplo SIENIC así que lo seleccionamos he introducimos la clave.


Nos indicara que va a crear el directorio home para dicho usuario le damos clic en aceptar y listo.


### 7.4.1 smb.conf final

Al final el archivo smb.conf de la estación se vera como el siguiente, tomando en cuenta que este ejemplo también se han deshabilitado los recursos compartidos [users] y [groups]

```
[global]
        workgroup = SIENIC
        passdb backend = tdbsam
        printing = cups
        printcap name = cups
        printcap cache time = 750
        cups options = raw
        map to guest = Bad User
        include = /etc/samba/dhcp.conf
        logon path = \\%L\profiles\.msprofile
        logon home = \\%L\%U\.9xprofile
        logon drive = P:
        usershare allow guests = No
        idmap gid = 10000-20000
        idmap uid = 10000-20000
        security = domain
        template shell = /bin/bash
        winbind offline logon = yes
        wins support = No
[homes]
        comment = Home Directories
        valid users = %S, %D%w%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

## Share disabled by YaST
# [users]
#       comment = All users
#       path = /home
#       read only = No
#       inherit acls = Yes
#       veto files = /aquota.user/groups/shares/

## Share disabled by YaST
# [groups]
#       comment = All groups
#       path = /home/groups
#       read only = No
#       inherit acls = Yes
[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No
[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @ntadmin root
        force group = ntadmin
        create mask = 0664
        directory mask = 0775
```

### 7.4.2 Compartiendo recursos en nuestra estación de trabajo openSUSE 11.2

Para compartir recursos en nuestra estación de trabajo openSUSE que es parte de nuestro dominio creamos una carpeta por ejemplo llamada prueba, a como podemos ver, dentro de nuestra carpeta home se a creado otra llamada SIENIC que representa al dominio y dentro de la cual se almacenaran las carpetas de los usuarios, en la del usuario actual crearemos la carpeta en cuestión y ejecutamos los siguientes comandos como root.

chgrp “SIENIC\domain users” /home/SIENIC/amartinez/prueba
chmod 2775 /home/SIENIC/amartinez/prueba

**El comando chgrp solo es necesario cuando el usuario creador de la carpeta no pertenece al grupo requerido, aquí se muestra como ejemplo.**

Y creamos el recurso compartido en nuestro archivo smb.conf de la siguiente manera.

```
[datos]
        comment = datos prueba
        inherit acls = Yes
        path = /home/SIENIC/amartinez/prueba
        read only = No
        valid users = @"SIENIC\domain users"
        write list = @"SIENIC\domain users"
        force create mode = 0660
        force directory mode = 0770
```

Y si los usuarios que se van a conectar no pertenecen al grupo SIENIC\domain users, agregamos la opción.

force group = SIENIC\domain users

En este caso @ representa que es un grupo y abrimos comillas por la presencia de espacios, SIENIC que es el nombre de nuestro dominio el carácter \ esta definido en la opción samba *winbind separator* y es el valor predeterminado, domain users es el nombre del grupo ya mapeado en samba y cerramos comillas.

***Nota: En el caso de tratarse de un servidor y no un cliente de dominio, este recurso compartido quedaría similar al siguiente:***

Creamos la carpeta y ejecutamos lo siguiente:

chgrp ntusers /home/amartinez/prueba
chmod 2775 /home/amartinez/prueba

```
[datos]
        comment = datos prueba
        inherit acls = Yes
        path = /home/amartinez/prueba
        read only = No
        valid users = @ntusers
        write list = @ntusers
        force create mode = 0660
        force directory mode = 0770
```

Y si los usuarios que se van a conectar no pertenecen al grupo ntusers, agregamos la opción.

force group = ntusers

Esto se expone para mostrar la diferencia entre compartir recursos como cliente de Dominio y hacerlo como controlador de dominio.

### 7.4.3 Montando los recursos compartidos de la red.

Ya hemos visto como compartir recursos como estación de trabajo, pero ¿que hay si queremos acceder a recursos compartidos en el servidor?, para esto debemos montar el recurso compartido como si fuera parte de la estructura local de archivos, hasta este punto si ejecutamos el comando ls –l en nuestra carperta home veremos privilegios como los siguientes

```
drwxr-xr-x 2 SIENIC\amartinez SIENIC\domain users  4096 nov  6 14:15 Documentos
```

amartinez es uno de los usuarios de Dominio, no un usuario local.

Ahora procederemos a agregar las siguientes opciones en nuestro archivo smb.conf

winbind enum users = yes

winbind enum groups = yes

Luego nos vamos a Yast-Sistema-Servicios de Sistema (Niveles de ejecución) y detenemos el servicio **nscd**, ahora reiniciamos la estación de trabajo

Lo que sigue es crear la carpeta en la que vamos a montar los recursos compartidos que se encuentran en el servidor

Para ello ejecutamos lo siguiente en la carpeta home del usuario actual y que va a usar los datos.

mkdir datosremotos

Y el siguiente comando como root

chmod 2775

Ahora procederemos a montar el recurso compartido en la carpeta recién creada de esta manera usaremos los datos que están en el servidor como si fueran parte de la estructura local de archivos, pero antes debemos verificar que todo este bien, ejecutamos los siguientes comandos:

wbinfo –g

Nos va a dar una lista como la siguiente:

SIENIC\domain admins
SIENIC\domain guests
SIENIC\domain users

Ahora ejecutamos

wbinfo –u

Nos va a dar una lista como la que sigue:

SIENIC\root
SIENIC\administrator
SIENIC\amartinez
SIENIC\esotomayor
SIENIC\contador

Procedemos a ejecutar

getent passwd

Al final de esta lista nos tienen que salir los usuarios del dominio tal a como se muestra a continuación.

```
SIENIC\root:*:10004:10000:root:/home/SIENIC/root:/bin/bash
SIENIC\administrator:*:10002:10000::/home/SIENIC/administrator:/bin/bash
SIENIC\amartinez:*:10000:10000::/home/SIENIC/amartinez:/bin/bash
SIENIC\esotomayor:*:10001:10000::/home/SIENIC/esotomayor:/bin/bash
SIENIC\contador:*:10003:10000::/home/SIENIC/contador:/bin/bash
```

Luego procedemos a ejecutar

getent group

Nos va a salir algo como lo que sigue:

```
SIENIC\domain admins:x:10010:SIENIC\administrator
SIENIC\domain guests:x:10011:
SIENIC\domain users:x:10000:SIENIC\amartinez,SIENIC\contador,SIENIC\esotomayor
```

Ahora vamos a ejecutar el comando que va a montar el recurso compartido en la carpeta que hemos creado:

mount -t cifs -o username=amartinez,UID=10000,GID=10000 //192.168.0.2/archivos1 /home/SIENIC/amartinez/datosremotos

Nos va a pedir la clave del usuario de dominio, username=amartinez indica el nombre del usuario de dominio, UID=1000 indica el identificador del usuario que será propietario del recurso, en nuestro caso el usuario actual que es amartinez, este numero se obtiene al ejecutar el comando getent passwd, GID=10000 indica el identificador del grupo al cual pertenece el usuario propietario, este numero también se obtiene ejecutando el comando getent passwd, si queremos ver el nombre del grupo y no solo el GID ejecutamos el comando getent group, //192.168.0.2/archivos1 indica la ruta al recurso de red, /home/SIENIC/amartinez/datosremotos indica el punto de montaje, también podemos agregar la opcion ***nobrl***, esto para evitar un problema al tratar de guardar archivos de openoffice y Staroffice.

Ahora si ejecutamos el comando ls –l veremos lo siguiente

```
drwxrwsr-x 4 SIENIC\amartinez SIENIC\domain users     0 nov 19 13:28 datosremotos
```

Este método monta el recurso solo por el tiempo que dure la sesión pero hay métodos para montar los recursos de forma permanente los cuales se pueden encontrar en el sitio:

http://opensuse.swerdna.org/susesambacifs.html

Al finalizar de compartir carpetas y accesar a recursos externos nuestro archivo smb.conf se vera como el siguiente:

```
[global]
        workgroup = SIENIC
        passdb backend = tdbsam
        printing = cups
        printcap name = cups
        printcap cache time = 750
        cups options = raw
        map to guest = Bad User
        include = /etc/samba/dhcp.conf
        logon path = \\%L\profiles\.msprofile
        logon home = \\%L\%U\.9xprofile
        logon drive = P:
```

```
        usershare allow guests = No
        idmap gid = 10000-20000
        idmap uid = 10000-20000
        security = domain
        template shell = /bin/bash
        winbind offline logon = yes
        wins support = No
        winbind enum groups = Yes
        winbind enum users = Yes
[homes]
        comment = Home Directories
        valid users = %S, %D%w%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

## Share disabled by YaST
# [users]
#       comment = All users
#       path = /home
#       read only = No
#       inherit acls = Yes
#       veto files = /aquota.user/groups/shares/

## Share disabled by YaST
# [groups]
#       comment = All groups
#       path = /home/groups
#       read only = No
#       inherit acls = Yes
[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No
[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @ntadmin root
        force group = ntadmin
        create mask = 0664
        directory mask = 0775

[datos]
        comment = datos prueba
        inherit acls = Yes
        path = /home/SIENIC/amartinez/prueba
        read only = No
        valid users = @"SIENIC\domain users"
        write list = @"SIENIC\domain users"
        force create mode = 0660
        force directory mode = 0770
        force group = "SIENIC\domain users"
```

# 8.- Servicios involucrados

Para poder diagnosticar problemas el primer paso es conocer cuales son los servicios involucrados en cada escenario planteado con anterioridad.

### 8.1 openSUSE en un grupo de trabajo

Para un equipo openSUSE 11.2 participando en un grupo de trabajo deben estar habilitados los servicios **nmb** y **smb**.

### 8.2 openSUSE como controlador de Dominio con el backend tdbsam.

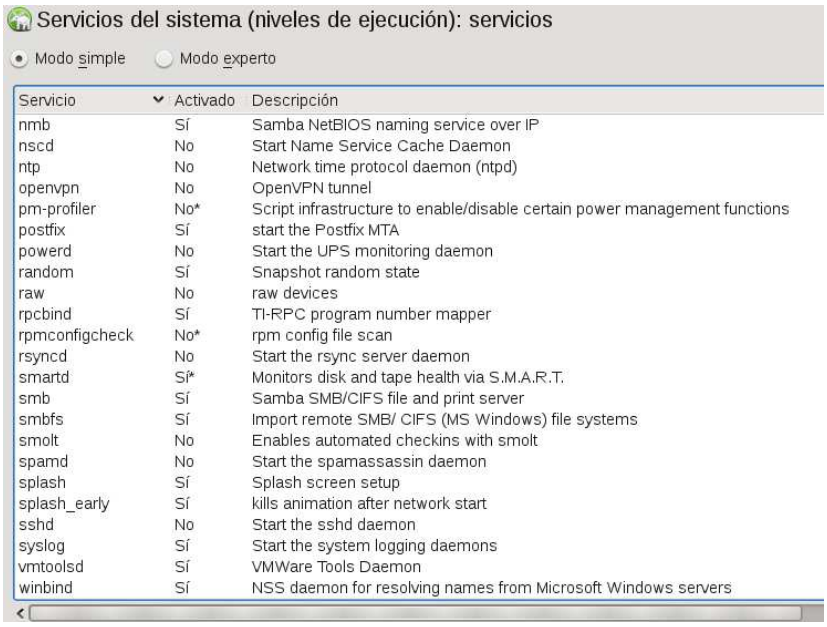
Para un servidor openSUSE 11.2 configurado como controlador de dominio primario usando el backend tdbsam, deben estar funcionando los servicios **nmb** y **smb**, recordemos que si también este servidor presta el servicio de servidor DHCP debe estar arriba el servicio **dhcpd**

### 8.3 openSUSE como controlador de Dominio con el backend ldapsam.

Para un servidor openSUSE 11.2 configurado como controlador de dominio primario usando el backend ldapsam, deben estar funcionando los servicios **nmb, smb y ldap**, también deberá estar funcionando el servicio **dhcpd** si el servidor presta servicios DHCP.

### 8.4 openSUSE como miembro de Dominio

Para un equipo openSUSE 11.2 que es miembro de un Dominio Samba, debe estar funcionando el servicio **winbind**, si deseamos compartir recursos con otros equipos también deben estar funcionando los servicios **smb** y **nmb**, si deseamos montar recursos compartidos en  la red en nuestra estación de trabajo openSUSE 11.2, debe estar arriba el servicio **smfs** y debemos bajar el servicio **nscd.**




| Servicio | Activado | Descripción |
|---|---|---|
| nmb | Sí | Samba NetBIOS naming service over IP |
| nscd | No | Start Name Service Cache Daemon |
| ntp | No | Network time protocol daemon (ntpd) |
| openvpn | No | OpenVPN tunnel |
| pm-profiler | No* | Script infrastructure to enable/disable certain power management functions |
| postfix | Sí | start the Postfix MTA |
| powerd | No | Start the UPS monitoring daemon |
| random | Sí | Snapshot random state |
| raw | No | raw devices |
| rpcbind | Sí | TI-RPC program number mapper |
| rpmconfigcheck | No* | rpm config file scan |
| rsyncd | No | Start the rsync server daemon |
| smartd | Sí* | Monitors disk and tape health via S.M.A.R.T. |
| smb | Sí | Samba SMB/CIFS file and print server |
| smbfs | Sí | Import remote SMB/ CIFS (MS Windows) file systems |
| smolt | No | Enables automated checkins with smolt |
| spamd | No | Start the spamassassin daemon |
| splash | Sí | Splash screen setup |
| splash_early | Sí | kills animation after network start |
| sshd | No | Start the sshd daemon |
| syslog | Sí | Start the system logging daemons |
| vmtoolsd | Sí | VMWare Tools Daemon |
| winbind | Sí | NSS daemon for resolving names from Microsoft Windows servers |

# 9.- Créditos

## 9.1 Créditos

Este manual no hubiera sido posible sin la información contenida en los siguientes sitios, ni la ayuda brindada por los autores y participantes:

http://www.arrakis.es/~pfabrega/samba.html

http://opensuse.swerdna.org/index.html

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/

http://www.novell.com/documentation/opensuse111/

http://www.urbana.fm/~antocm/ldap-samba-howto-v4.html

http://forums.opensuse.org

http://wiki.samba.org/index.php/Windows7

La portada gracias a:

Psyfurius
http://www.linuxboricua.com/
Puerto Rico

Para comentarios y preguntas contactar al autor:

Eduardo Adolfo Sotomayor G.
adolfo2007@starlinux.net
http://easgs.wordpress.com