CONFIGURACION DE SERVIDOR LDAP EN UBUNTU SERVER 8.10

Juan Felipe Rios Ramirez

Julian David Hernandez Valencia

CONFIGURACION DE SERVIDOR LDAP EN UBUNTU SERVER 8.10

Juan Felipe Rios Ramirez
Julian David Hernandez Valencia

En este documento se describe de manera clara la instalación y configuración del servidor LDAP en Ubuntu server 8.10

Tabla de contenidos

1. QUE ES LDAP? 1
    - Conceptos 1
    - ¿Cómo funciona LDAP? 1
    - Arbol de directorio LDAP 1
    - Ventajas de LDAP 3
2. Instalación de Ubuntu Server 8-10 4
    - Descargar e Instalar Ubuntu Server 8-10 4
    - Elegir el Pais 5
    - Seleccionar la distribucion del teclado 6
    - Configurar la red 7
    - Particionado de discos 8
    - Configurar usuarios y contraseñas 11
    - Selección de programas 14
3. Optimización de Ubuntu-Server 8.10 17
    - Deshabilitar el reinicio del sistema con el comano Ctrl + Alt + Supr 17
    - Actualizar y optimizar tras la instalación 17
    - Actualizar la shell 17
    - Desinstalar apparmor 17
    - Optimizar la memoria de intercambio SWAP 17
4. Instalación y configuración del servidor LDAP 19
    - Instalación 19
    - Configuración de LDAP 19
    - Construir el árbol ldap 27
    - Hacer búsquedas 31
    - Iniciar, detener, reiniciar el servidor ldap 32
    - Configurar la red 32
    - Nota adicional 33
5. Bibliografía 34
    - Recursos consultados 34

Capítulo 1. QUE ES LDAP?

Conceptos

LDAP significa Protocolo de Acceso a Directorios Ligeros (siglas en inglés de Lightweight Directory Access Protocol) y es un servicio de directorio, muy similar a los directorios del sistema de ficheros al que estamos acostumbrados, o a la guía de teléfonos que usamos para buscar números de teléfono, o a los servicios de directorios de red como el NIS de SUN (Network Information Service, Servicio de Información de Red), DNS (Domain Name Service), o al árbol que ves en tu jardín. LDAP es una base de datos especializada. Es muy importante recordar que LDAP no es otra base de datos más. LDAP está optimizada para hacer búsquedas (leer datos). Las lecturas en LDAP se realizan de manera mucho más frecuente que las escrituras Toda la información es almacenada en una estructura de árbol. Con LDAPse tiene la libertad de determinar la estructura del árbol.

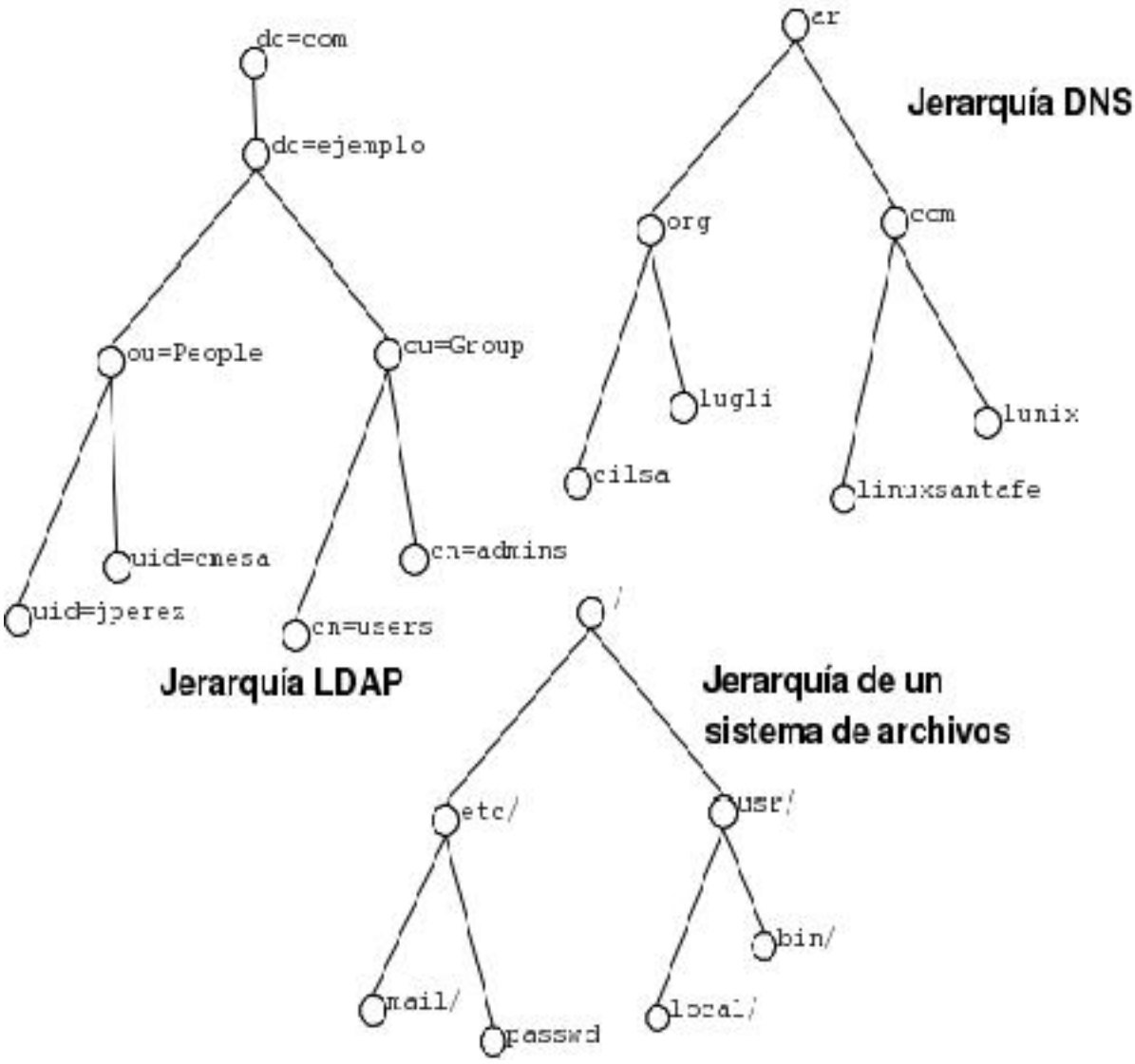
¿Cómo funciona LDAP?

El servicio de directorio LDAP se basa en un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol del directorio LDAP o base de datos troncal. el cliente ldap se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de donde puede el cliente hallar más información (normalmente otro servidor LDAP). No importa con qué servidor LDAP se conecte el cliente: siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que hará referencia en otro servidor LDAP. Es esta una característica importante de un servicio de directorios universal como LDAP

Arbol de directorio LDAP

Un árbol de directorio no es nada más que una manera organizada de proveer contenedores para almacenar diferentes tipos de información. Debe pensarse en el como un sistema para que tus datos lo llenen. Los servidores de directorio LDAP almacenan su información jerárquicamente, no distinto a un sistema de ficheros UNIX. La jeraquía proveé de un método para agrupamiento (y subagrupamiento) lógico de ciertos items juntos. Estos agrupamientos pueden ser útiles en un número de situaciones: • Delegación de autoridad para uno o más grupos de datos a otro servidor o a otro sitio • Replicación de datos • Seguridad y control de acceso • Escalabilidad

Ejemplos de varios tipos de arboles:



Objetos del árbol LDAP.

Los objetos pueden asignarse generalmente a uno de dos tipos posibles: Contenedor: Estos objetos pueden a su vez contener otros objetos. Tales clases de objetos son root (el elemento raíz del árbol de directorios, que no existe realmente), c (país), ou (unidad organizativa) y dc (componente de dominio). Este modelo es comparable con los directorios (carpetas) de un sistema de archivos. Hoja: Estos objetos se encuentran en la parte final de una rama y no incluyen objetos subordinados. Algunos ejemplos serían person, InetOrgPerson o groupofNames. Algunas atributos definidos dentro del árbol LDAP son los siguientes, tomando como base la entrada de datos para personas, que en ldap se define mediante la clase de objetos person, pero también puede definirse mediante atributos en las clases de objetos inetOrgPerson, groupOfNames, y organization. Por ejemplo: el atributo commonName o cn (nombre de pila), se usa para almacenar el nombre de una persona. Puede representarse en en el directorio a una persona llamada René Higuita cn: René Higuita. Cada persona que se introduzca en el directorio se define mediante la colección de atributos que hay en la clase de objetos person. Otros atributos que se usan para definir esta entrada serán: givenName: René surname: Higuita mail: rHiguita@midominio.com (si mi dominio fuese ejemplo.com, quedaria mail: rHiguita@ejemplo.com)

Ventajas de LDAP

La arquitectura cliente-servidor y estructura en forma de árbol que utiliza LDAP para almacenar su información, tiene algunas ventajas muy interesantes, como son: • Evita la duplicación de datos, la estructura de datos obliga a que no exista el mismo dato en dos lugares diferentes del esquema. • Permite la distribución de la administración, al igual que el servicio de DNS, la responsabilidad en la administración de los datos de un árbol se puede separar entre distintos equipos si es necesario. • Acepta niveles de acceso bien detallados, pudiendo definir políticas de seguridad por cada nodo.

Capítulo 2. Instalación de Ubuntu Server 8-10

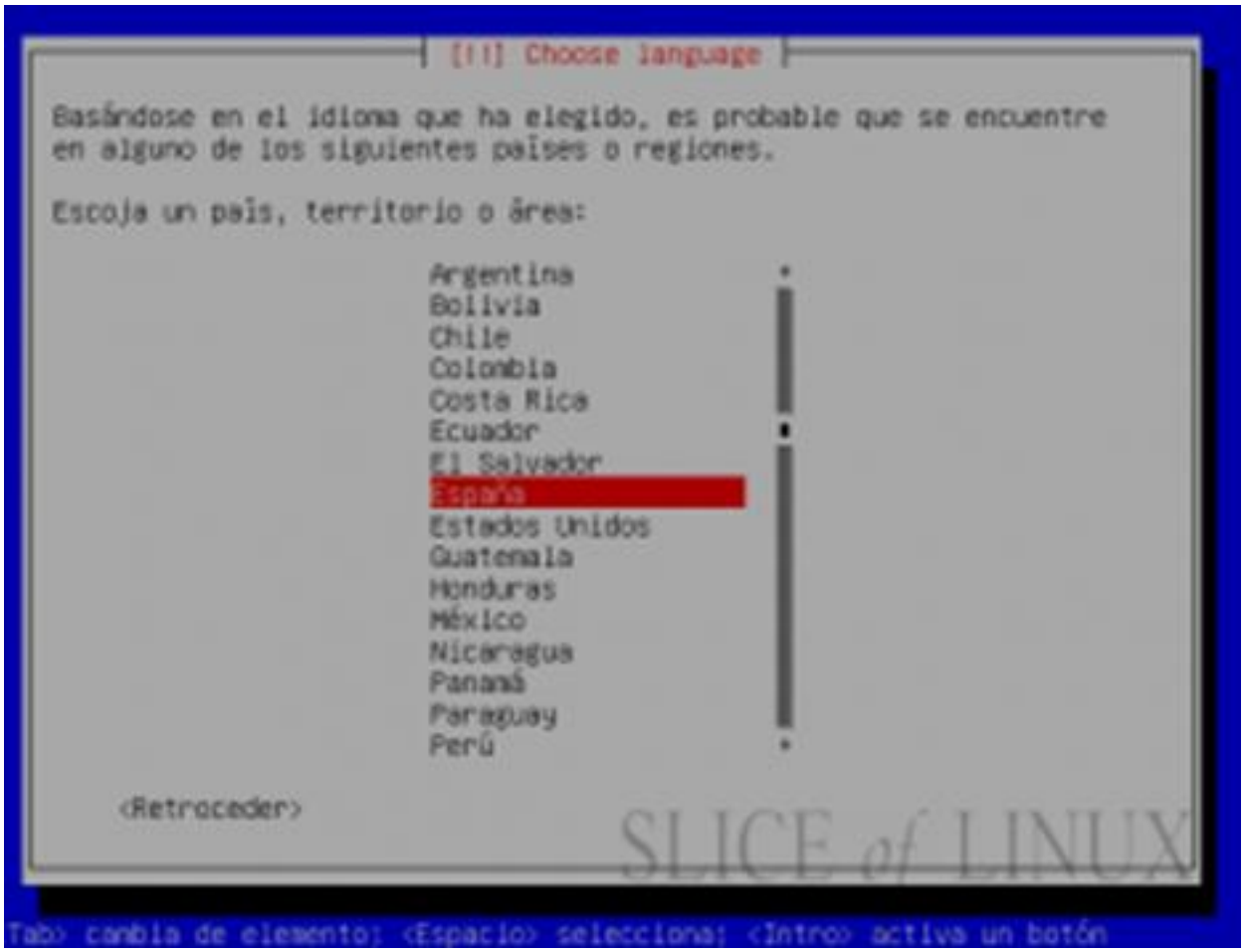
Descargar e Instalar Ubuntu Server 8-10

Si no se tiene disponible el Ubuntu Server 8-10, se puede descargar desde el link http://www.ubuntu.com/getubuntu/download. Una vez que hemos descargado y copiado el Ubuntu Server 8-10 a un cd, podemos comenzar a instalarlo: Insertamos el cd y le damos la opción a nuestro equipo de que inicie desde este, lo primero que aparecerá será la pantalla de selección de idioma, allí ponemos nuestro idioma Español.

Seguido de esto nos aparecerá la pantalla para aceptar la instalación

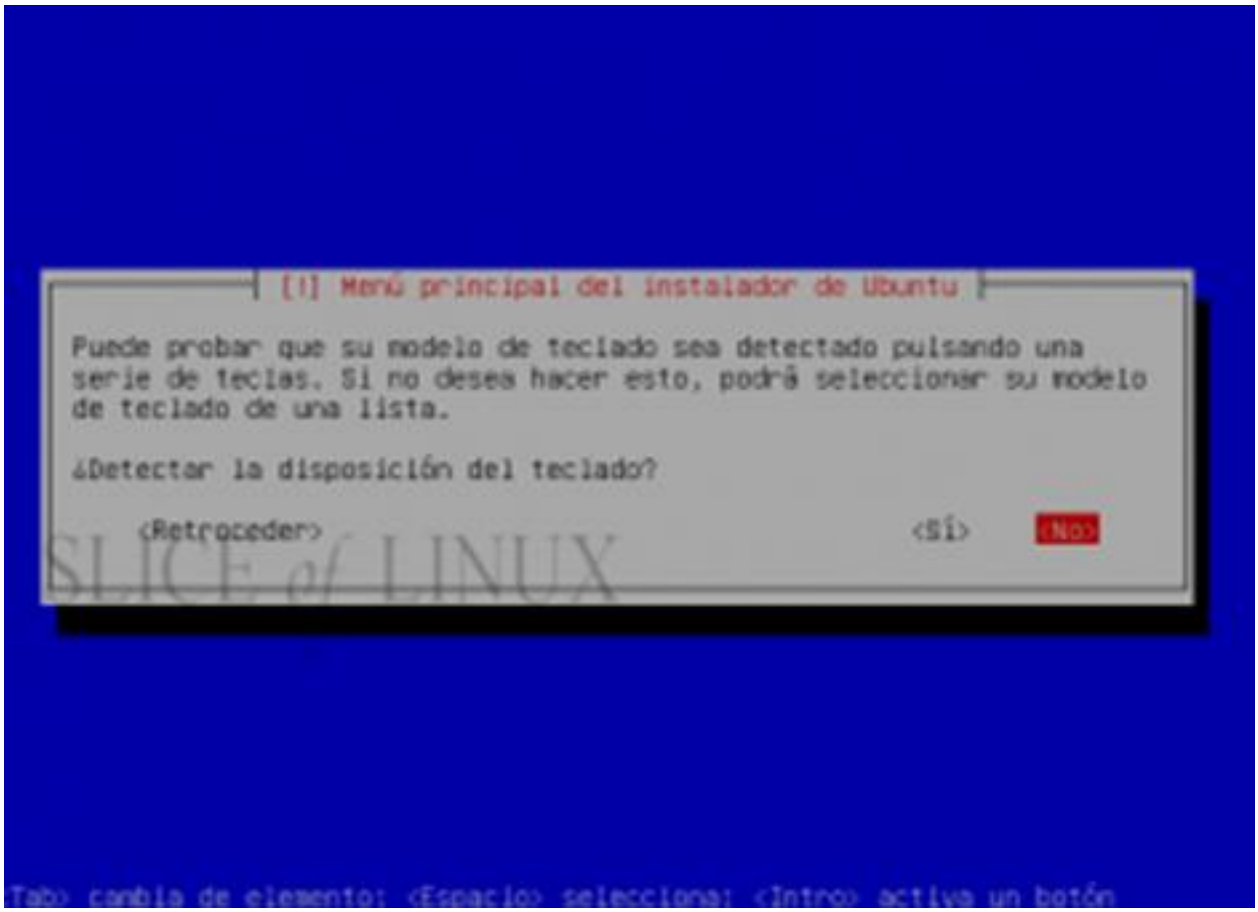
Elegir el Pais

En este punto se debe escoger el país en que nos encontremos. Buscamos para nuestro caso Colombia en la lista mostrada



Seleccionar la distribucion del teclado

Se nos brinda la opción de detectar la configuración del teclado al digitar una serie de teclas, lo cual no es muy recomendable. Ante la presencia de esta opción escogemos NO, y seleccionamos la distribución del teclado más adecuada, que para nuestro caso es Spain



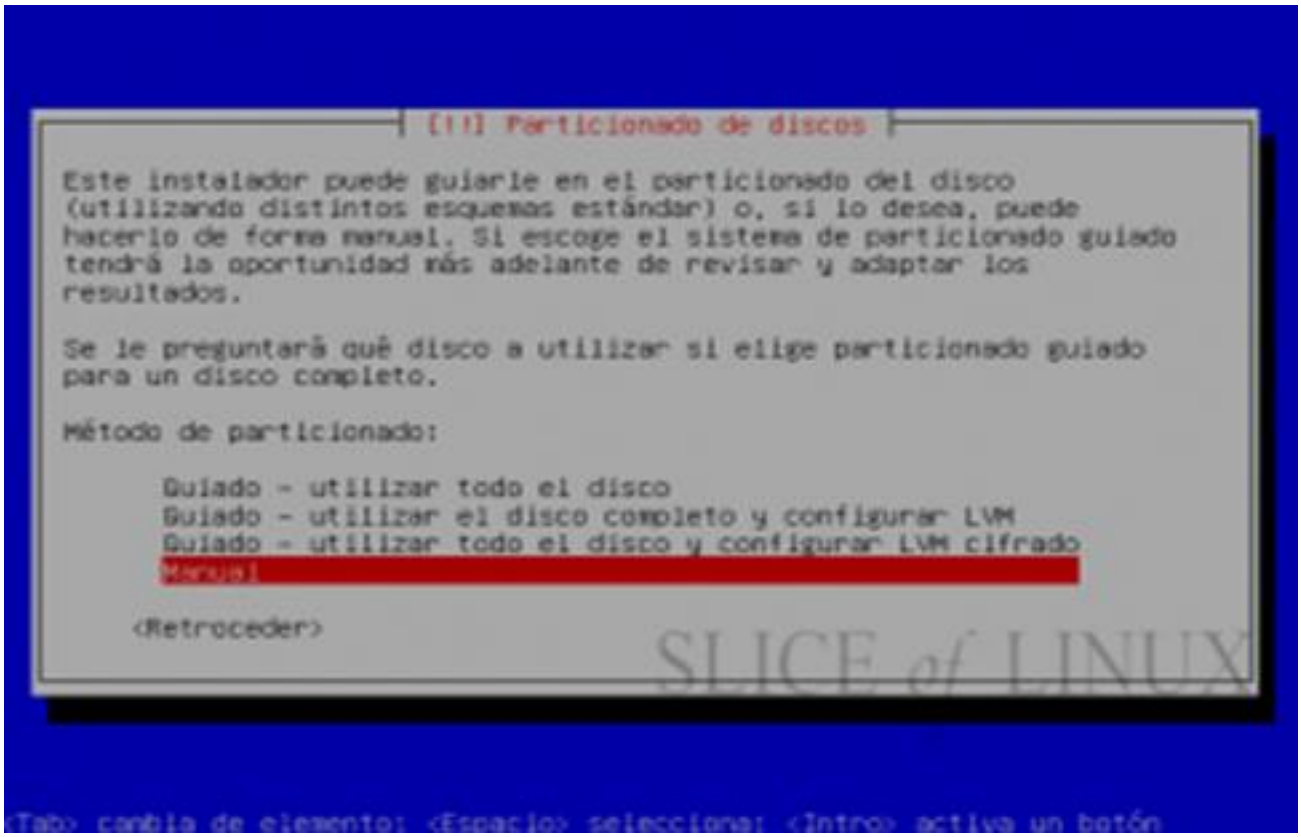
Configurar la red

Se nos solicita que ingresemos el nombre de la máquina, que para nuestro caso sera servidorldap

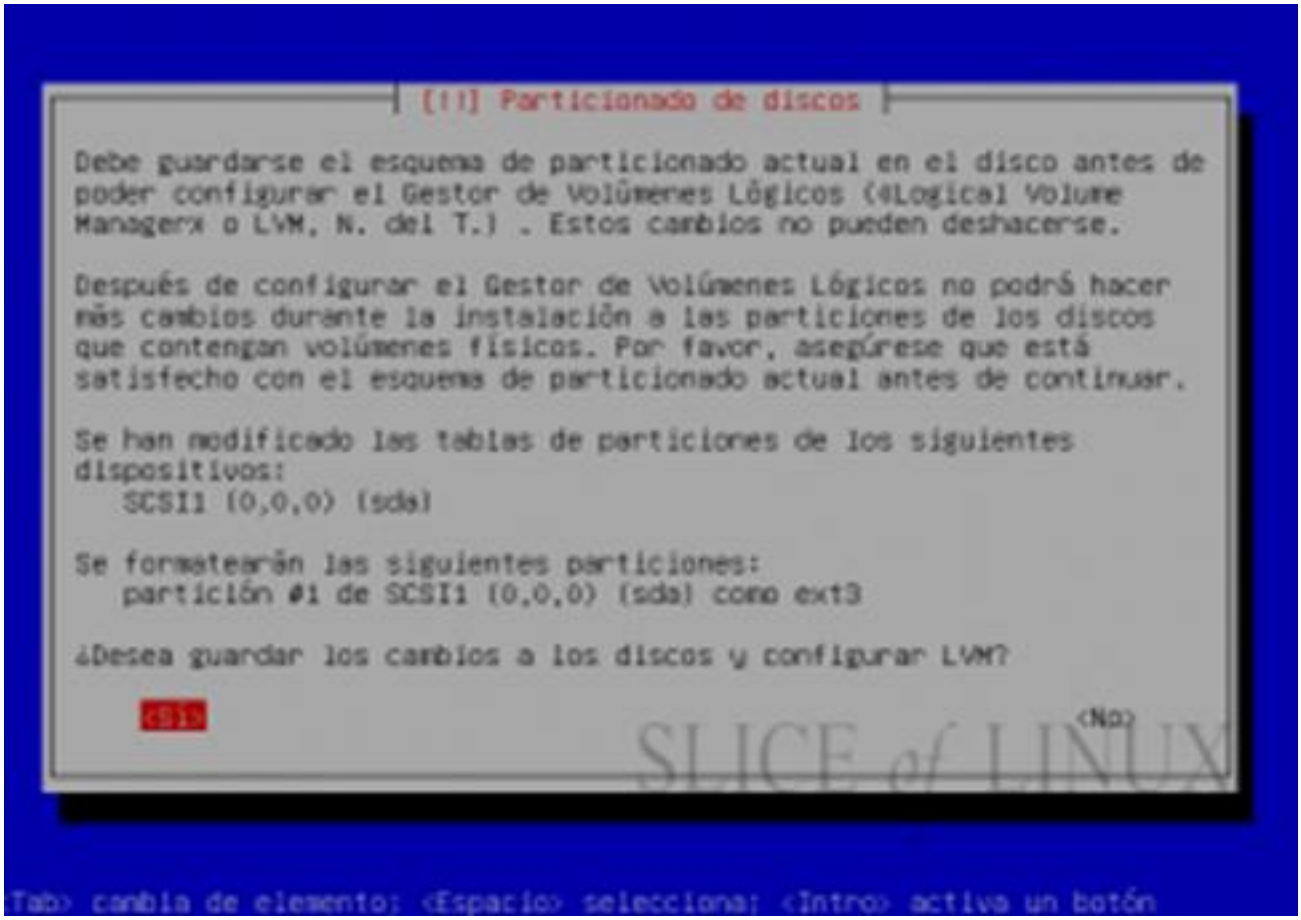
Particionado de discos

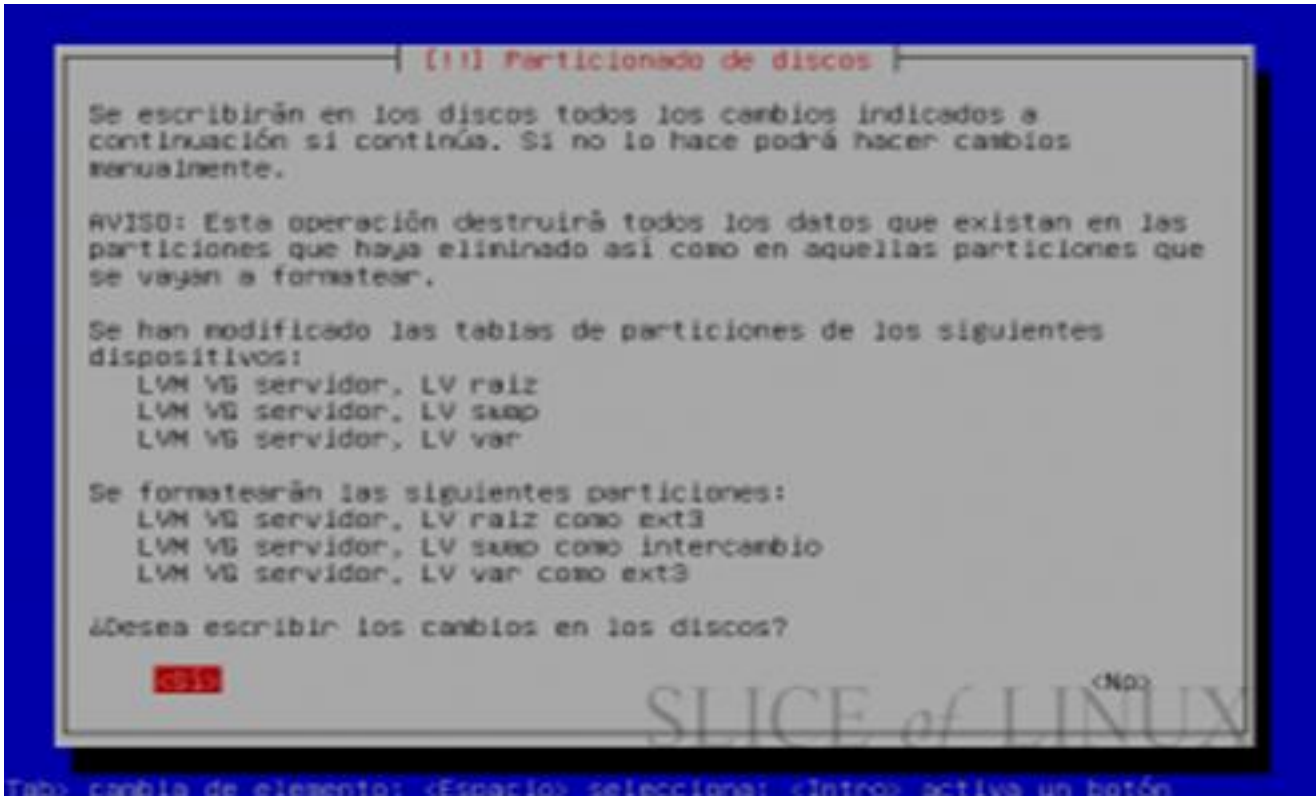
En el menú de particionado de discos se nos ofrecen varias opciones

De acuerdo a las necesidades se puede escoger una de ellas, para este caso en particular, la máquina presenta varias particiones, y debe determinarse el espacio a usar por lo tanto se escoge la opción Manual, que nos permite escoger la partición, definir el tamaño de la misma y otra serie de opciones



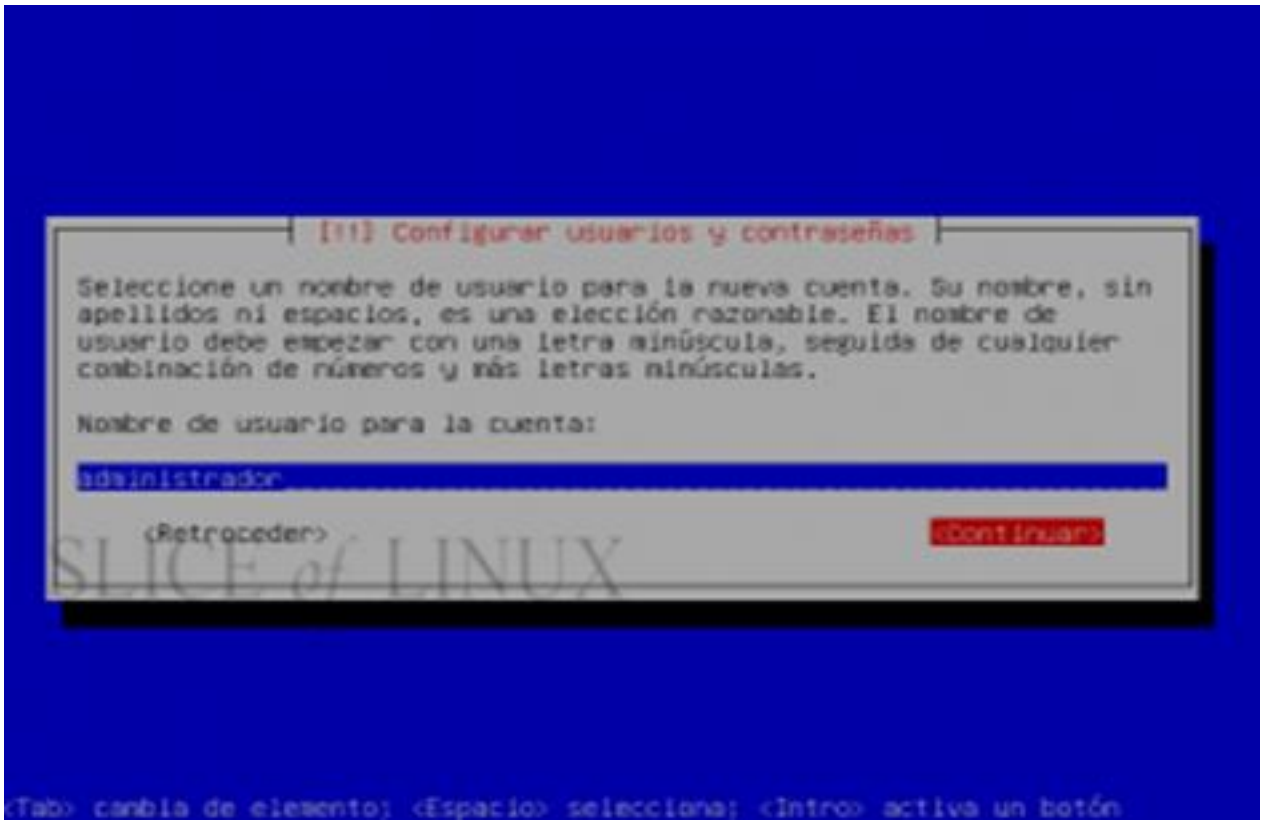
Se procede entonces a escoger la partición a utilizar para el ubuntu server y a confirmar la operación para que los cambios se escriban en el disco


[!!] Particionado de discos
Debe guardarse el esquema de particionado actual en el disco antes de poder configurar el Gestor de Volúmenes Lógicos («Logical Volume Manager» o LVM, N. del T.) . Estos cambios no pueden deshacerse.
Después de configurar el Gestor de Volúmenes Lógicos no podrá hacer más cambios durante la instalación a las particiones de los discos que contengan volúmenes físicos. Por favor, asegúrese que está satisfecho con el esquema de particionado actual antes de continuar.
Se han modificado las tablas de particiones de los siguientes dispositivos:
SCSI1 (0,0,0) (sda)
Se formatearán las siguientes particiones:
partición #1 de SCSI1 (0,0,0) (sda) como ext3
¿Desea guardar los cambios a los discos y configurar LVM?
<Sí>
<No>
SLICE of LINUX
<Tab> cambia de elemento; <Espacio> selecciona; <Intro> activa un botón

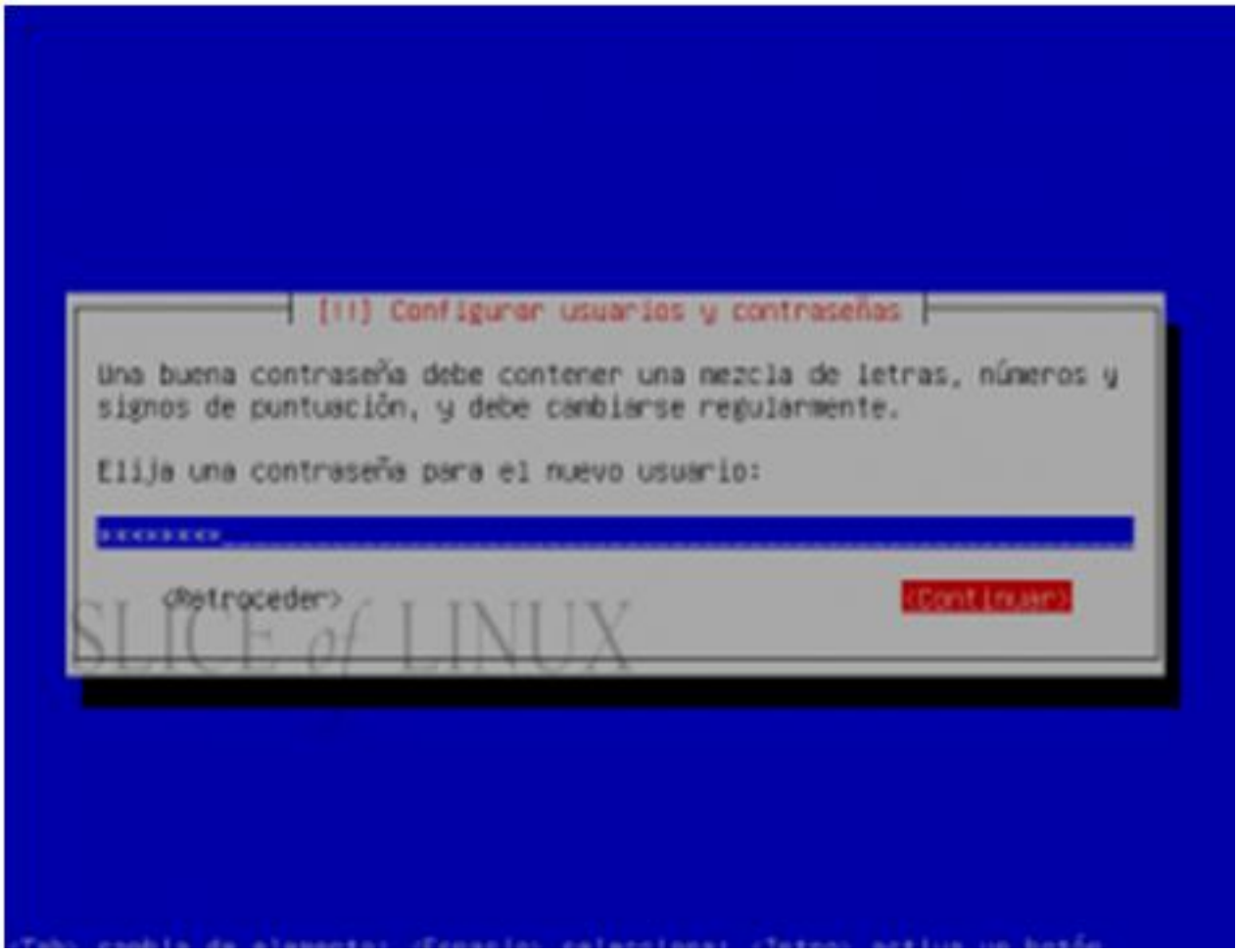


Configurar usuarios y contraseñas

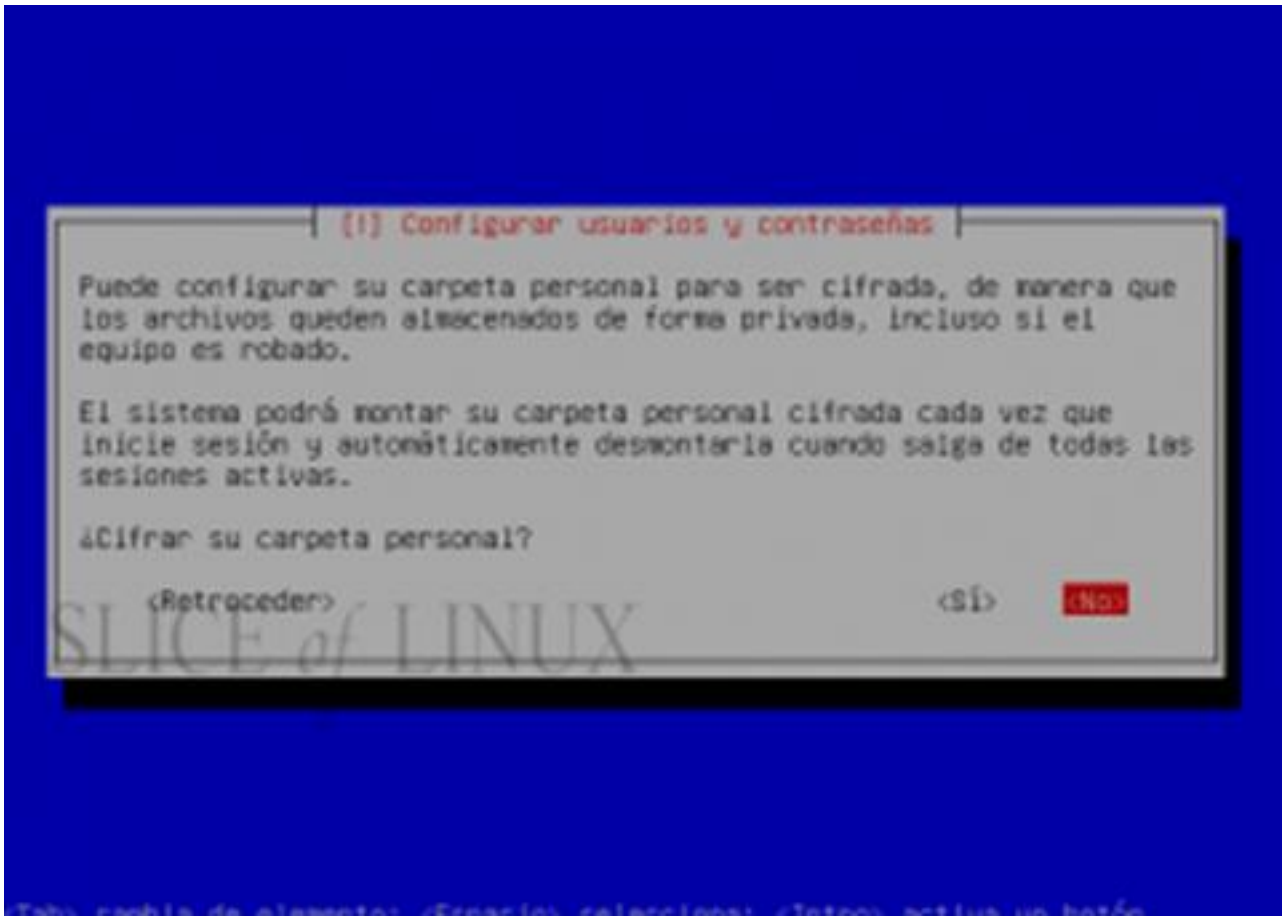
En esta etapa procedemos a ingresar el nombre de usuario para una nueva cuenta dentro del sistema, para este caso es servidorldap



Procedemos a digitar la contraseña del servidor

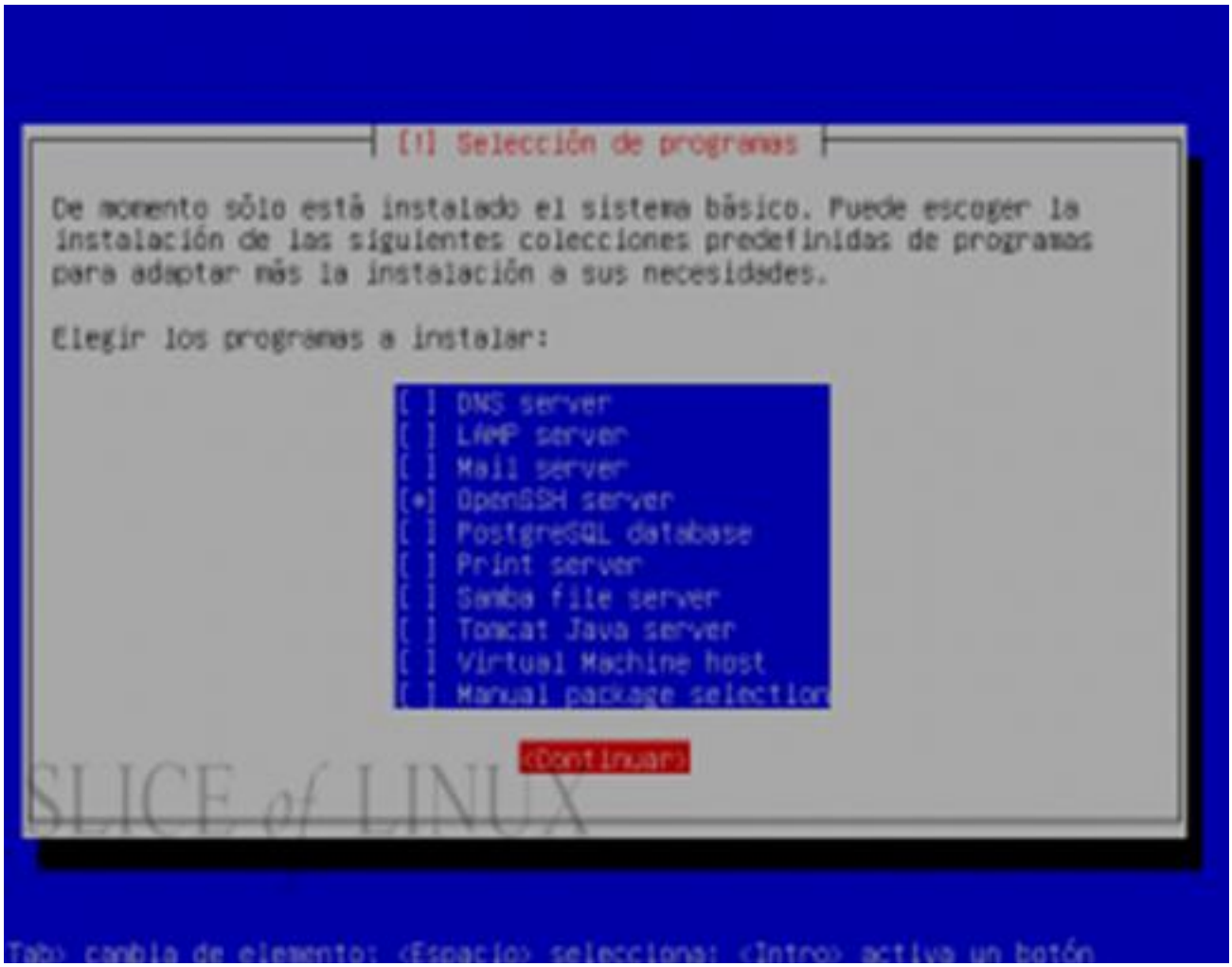


Ante la pregunta de cifrar su carpeta personal, escogemos no, al menos para el objetivo de este tutorial, esa opción no es necesaria. Vale la pena mecionar que esa opción es útil en el caso de que alguien nos robe nuestro equipo



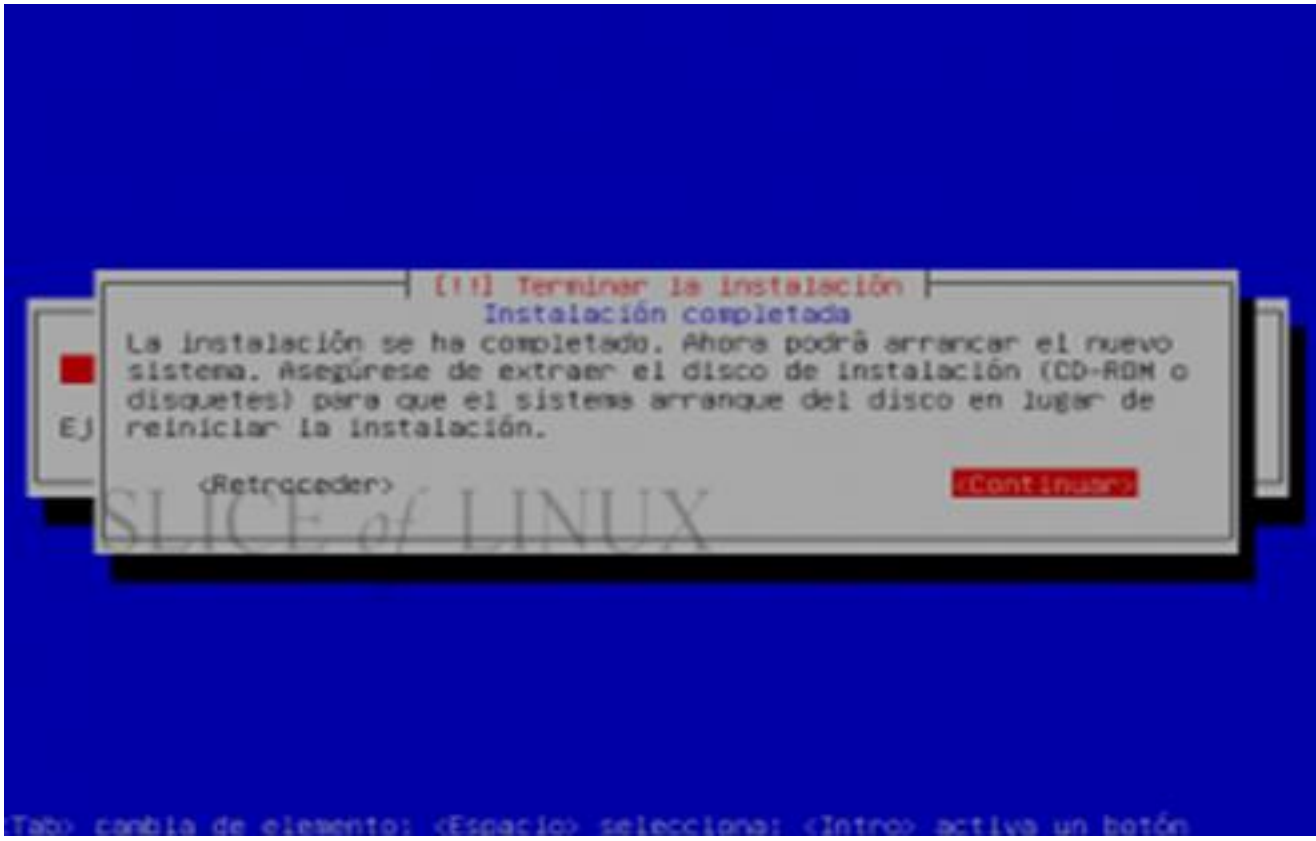
Selección de programas

Se nos muestran una serie de programas que podríamos instalar, para esta práctica no se escoge ningun programa



En esta instancia nos pregunta configuraciones de red las cuales se asignaran posteriormente.

El sistema comienza a instalarse en el disco, al finalizar este proceso se muestra la siguiente imagen y seguimos las recomendaciones que allí se dan, pulsamos "continuar" y el sistema se reiniciará y estaremos listos para usar nuestro Ubuntu-Server 8.10


[!!] Terminar la instalación
Instalación completada
La instalación se ha completado. Ahora podrá arrancar el nuevo sistema. Asegúrese de extraer el disco de instalación (CD-ROM o disquetes) para que el sistema arranque del disco en lugar de reiniciar la instalación.
<Retroceder>
<Continuar>
<Tab> cambia de elemento; <Espacio> selecciona; <Intro> activa un botón

Capítulo 3. Optimización de Ubuntu-Server 8.10

Deshabilitar el reinicio del sistema con el comano Ctrl + Alt + Supr

Es muy conveniente desactivar esta opción para que cualquier curioso no pueda reiniciar nuestro servidor con un comando tan sencillo (Ctrl+Alt+Supr).

Para evitar esto se hace lo siguiente:

1 - Ejecutamos el comando "sudo nano /etc/event.d/control-alt-delete" y se comenta la segunda línea que allí aparece.

2 - Luego reiniciamos el sistema para que los cambios sean aplicados y al ingresar de nuevo probamos el comando y así nos daremos cuenta de que esa opción ya no funciona.

Actualizar y optimizar tras la instalación

Antes de iniciar la actualización debemos verificar que los repositorios repositorios universe y multiverse están activados, para mirar esto vamos al archivo sources.list de la siguiente forma:

"sudo nano /etc/apt/sources.list" una vez estemos allí, comprobamos que estos repositorios, 8 líneas en total, no aparecen comentados.

Ahora sí podremos utilizar el comando "sudo apt-get update" para actualizar nuestro sistema

Luego tecleamos el comando "sudo apt-get upgrade" y así podremos actualizar todos los paquetes actualmentes instalados .

Actualizar la shell

Para actualizar la shell usamos el comando "sudo ln -sf /bin/bash /bin/sh"

Desinstalar apparmor

1 - Se ejecuta el comando "sudo /etc/init.d/apparmor stop"

2 - Se ejecuta "sudo update-rc.d -f apparmor remove"

3 - Se ejecuta "sudo apt-get remove apparmor apparmor-utils", por último se reinicia el sistema para que los cambios surjan efecto

Optimizar la memoria de intercambio SWAP

Para ello digitamos:

sudo cat /proc/sys/vm/swappiness, que nos muestra el valor de la swap

Si se nos muestra un valor muy alto, como por ejemplo, por encima de 20, podemos modificarlo digitando lo siguiente:

sudo nano /etc/sysctl.conf en el archivo que allí nos aparece añadimos en la última línea lo siguiente: "vm.swappiness=10".

Para este ejemplo utilizamos un valor de 10, que es óptimo

Capítulo 4. Instalación y configuración del servidor LDAP

Instalación

Lo primero que hay que hacer es instalar el demonio slapd del servidor OPENLDAP e instalar ldap-utils, un paquete que contiene utilidades de administración de LDAP.

La instalación se hace con el comando:

sudo apt-get install slapd ldap-utils

Sólo bastará con digitar la contraseña de administración y el paquete se instalará correctamente

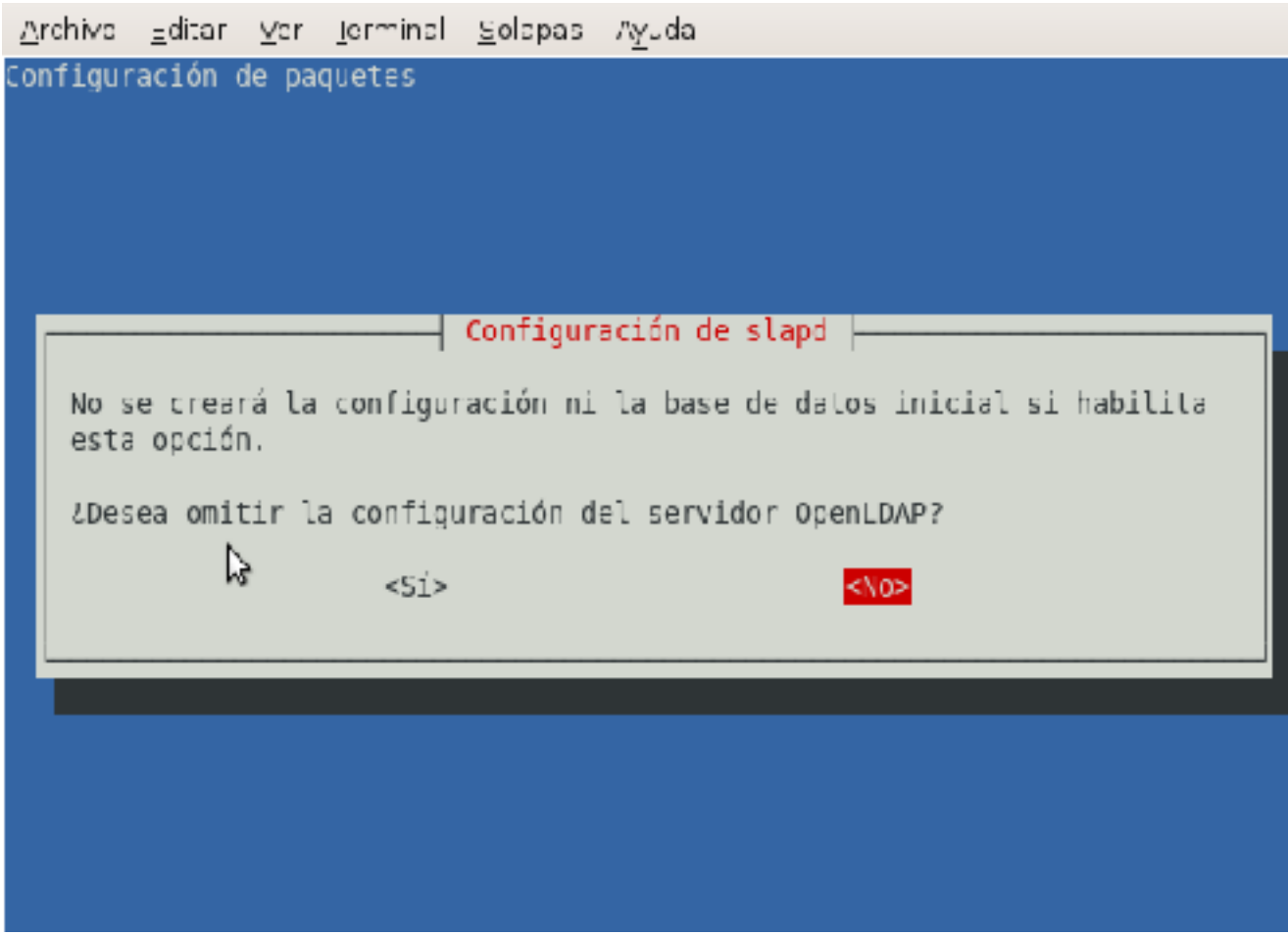
Configuración de LDAP

Desde las ultimas versiones de ldap el archivo de configuración que habitualmente estaba ubicado en /etc/openlap/ldap.conf, no se incluye, por el contrario la configuración es automática durante la instalación del ldap-utils, además para que el servidor trabaje sobre protocolo seguro anteriormente era necesario configurar SSL (SSL permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes.), pero en las nuevas versiones no es necesario ya que el paquete trae incluido dicha opción, sin embargo es recomendable reconfigurar el servidor para adecuarlo aún más a lo que deseamos, esto se lleva a cabo con la siguiente instrucción:

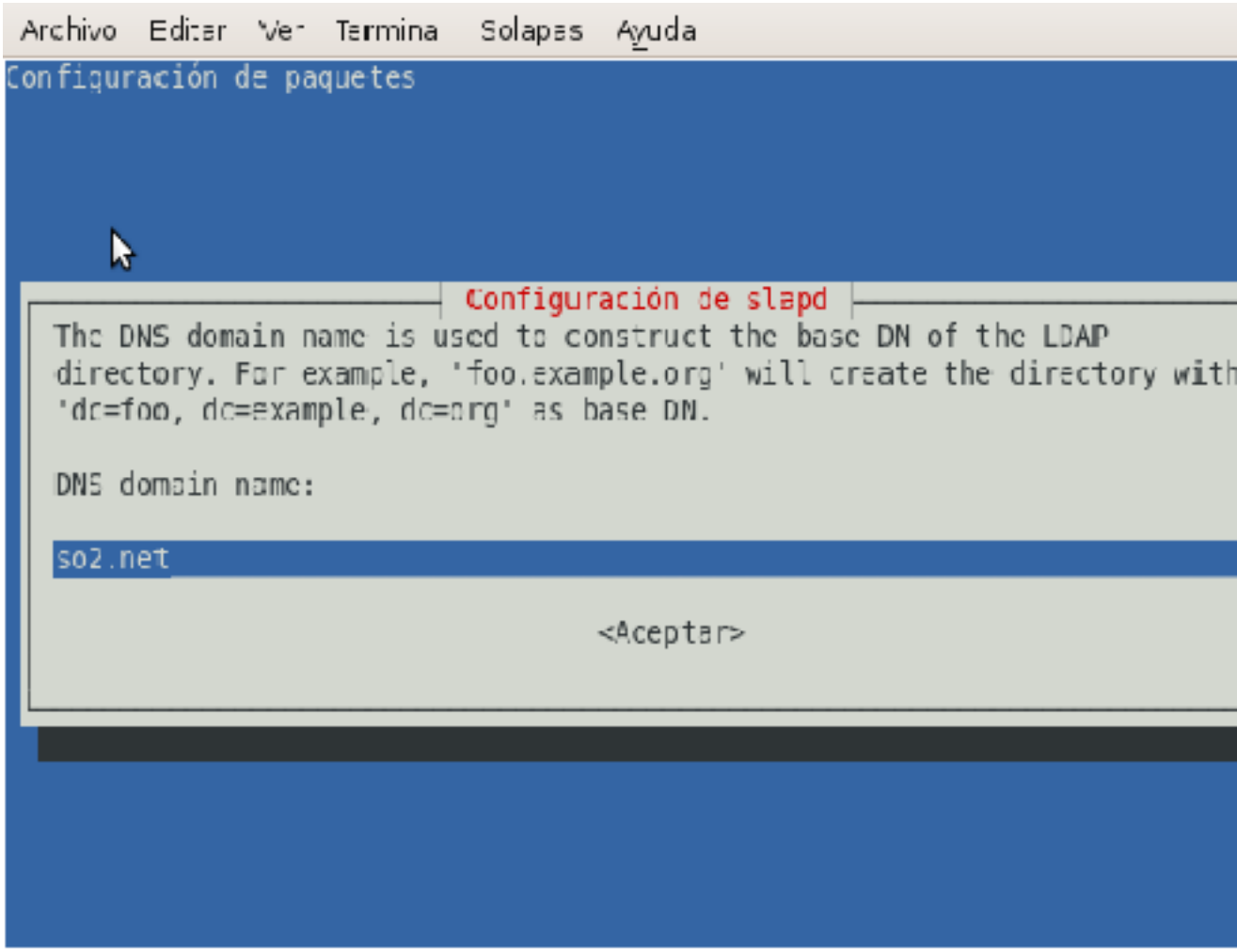
sudo dpkg-reconfigure slapd

Una vez digitamos esta instrucción se abren una serie de opciones para configurar adecuadamente el servidor.

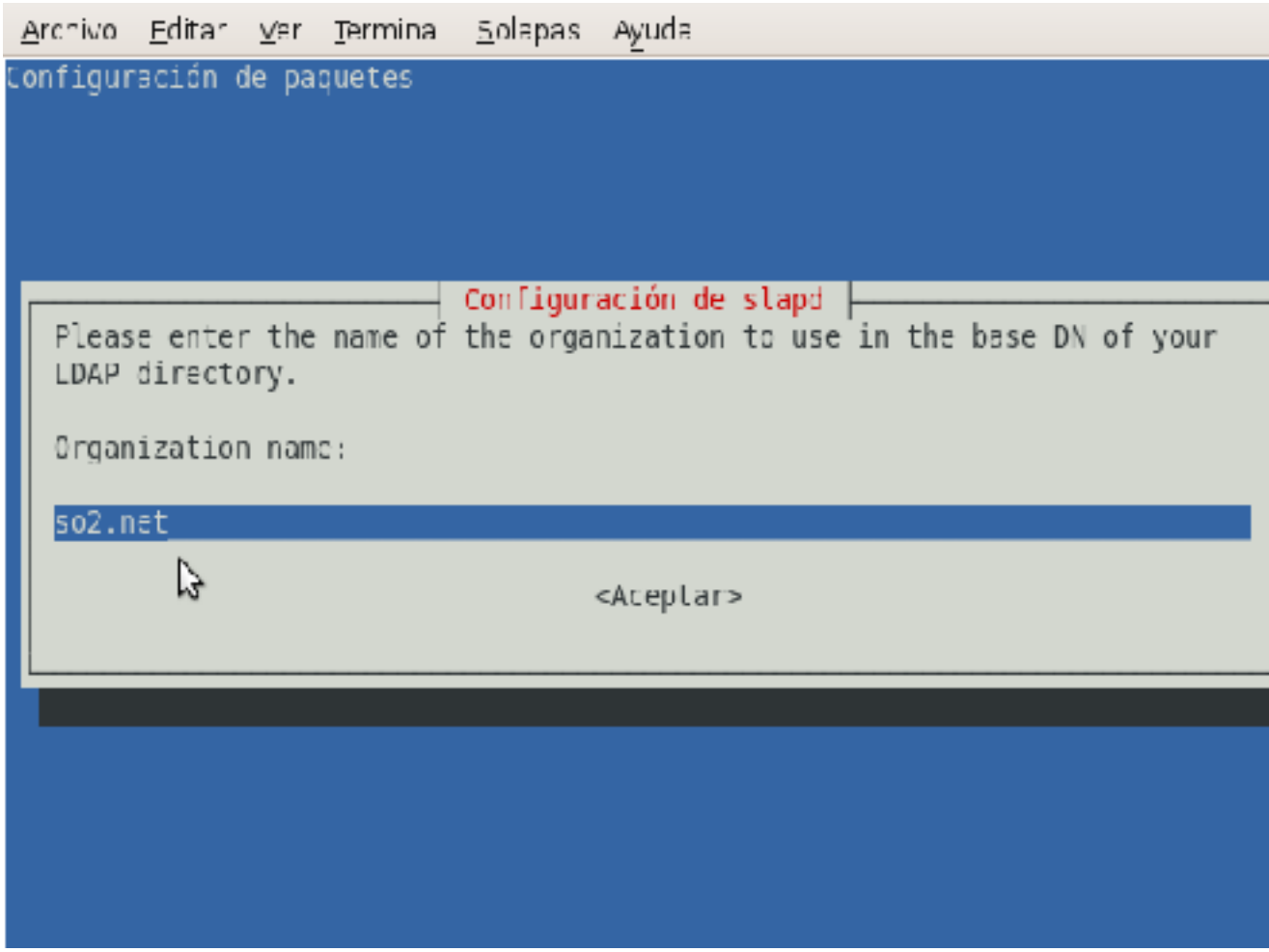
En este cuadro de diálogo debemos escoger la opción de lo contrario no podríamos modificar las opciones de configuración del servidor



En este cuadro de diálogo digitamos el dominio de nuestro servidor que para esta practica es so2.net



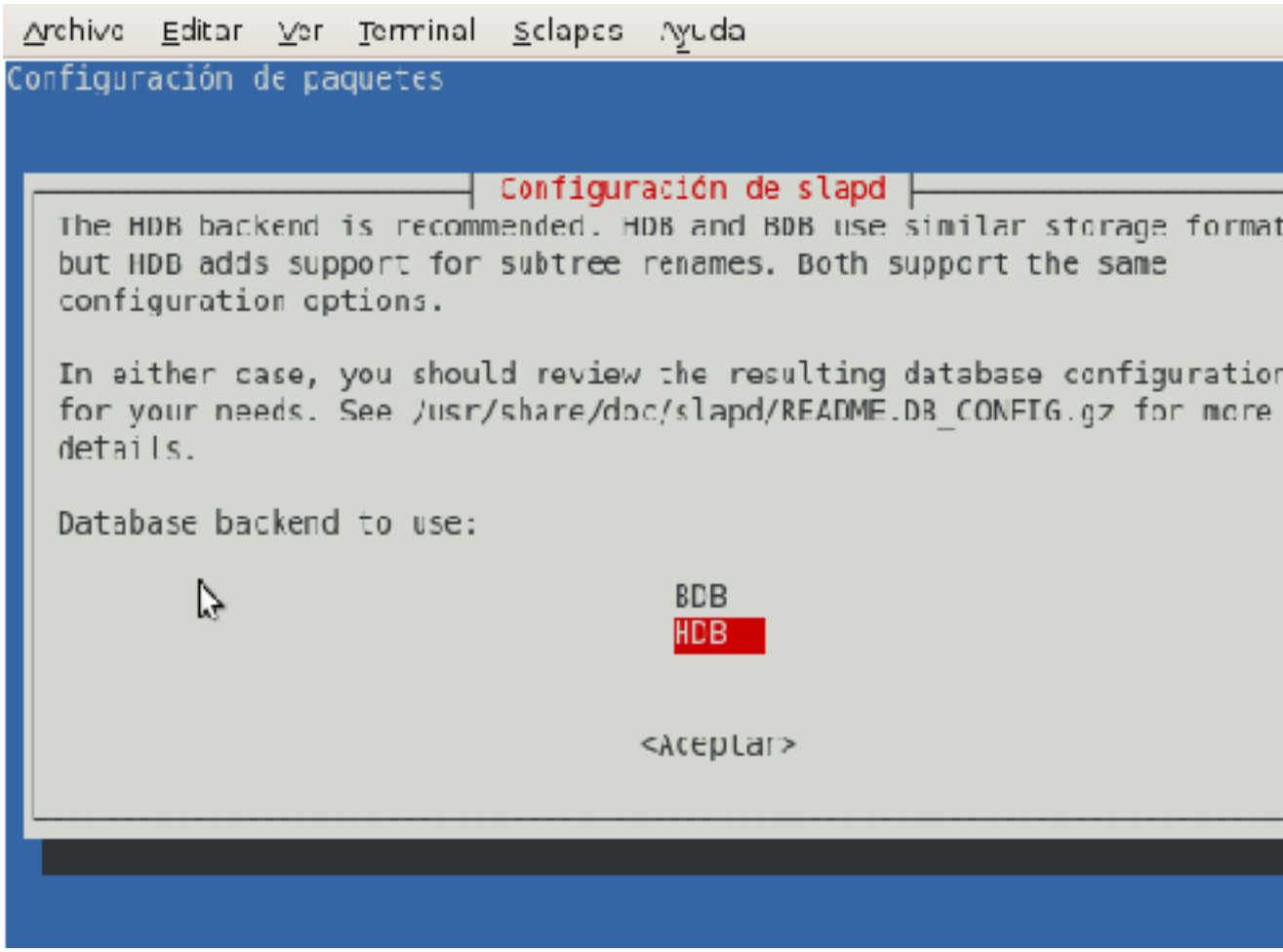
Ahora se nos pide el nombre de la organización que para este caso es igualmente so2.net



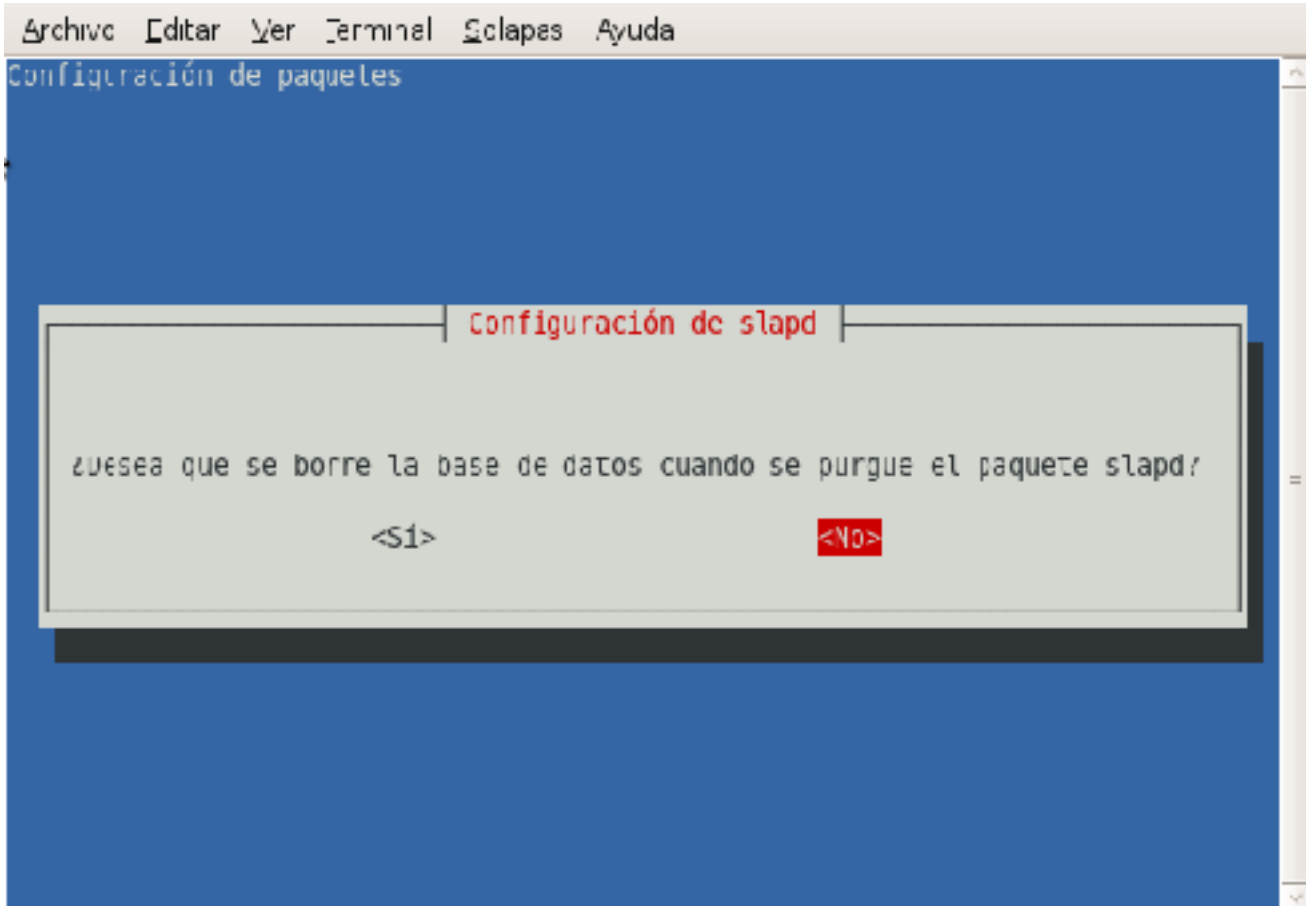
En esta instancia se nos pide escoger escoger el tipo de base de datos backbend (dorsal o base de datos de segundo plano)

Si se lee la explicación que da el cuadro de diálogo se observa que se recomienda utilizar la base de datos HDB y no la BDB, y también la justificación de porque escoger dicha opción

Para esta practica se escoge HDB

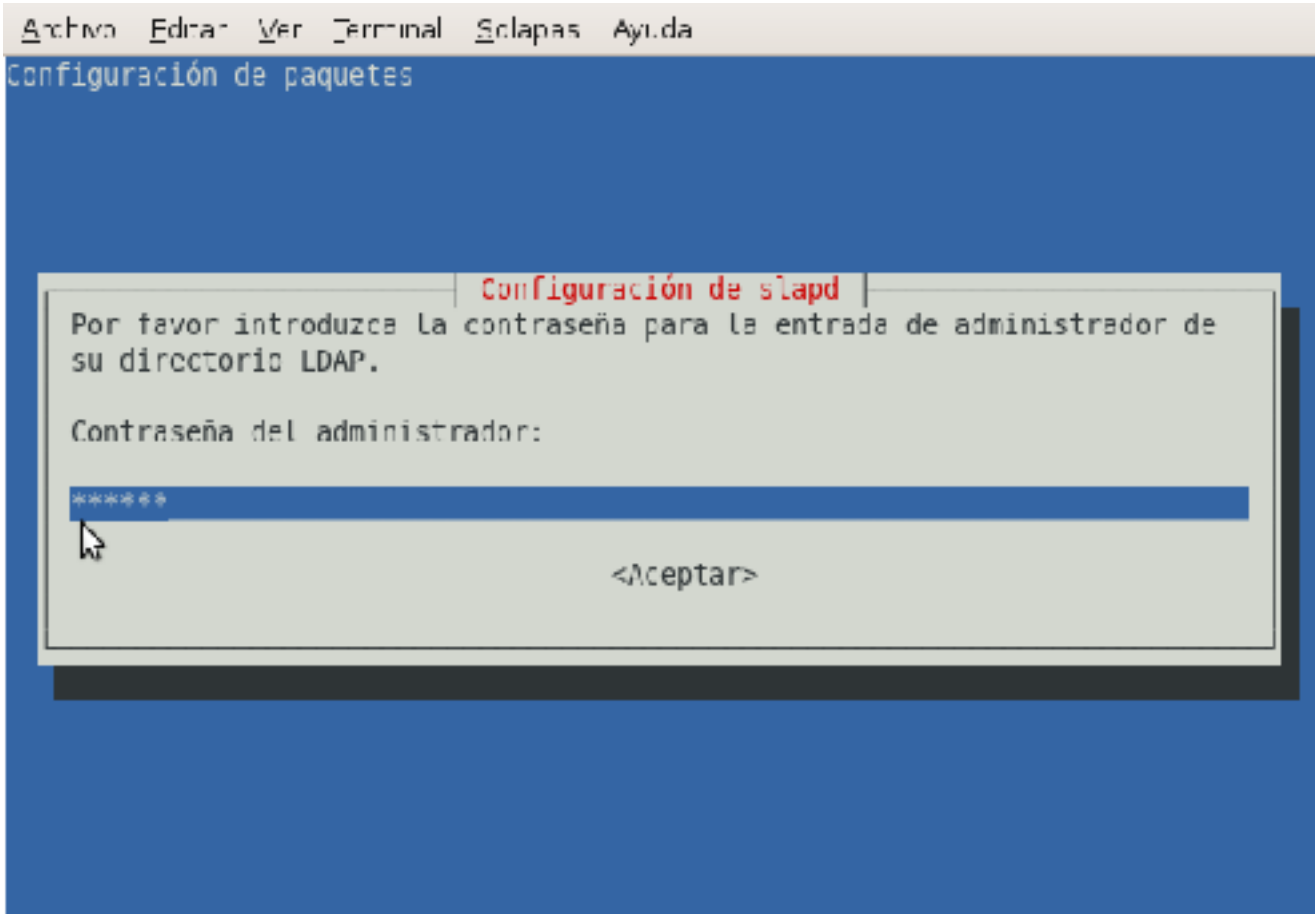


Ante la pregunta de si desea que se borre la base de datos cuando se purgue el paquete slapd, para esta práctica se escoge que no

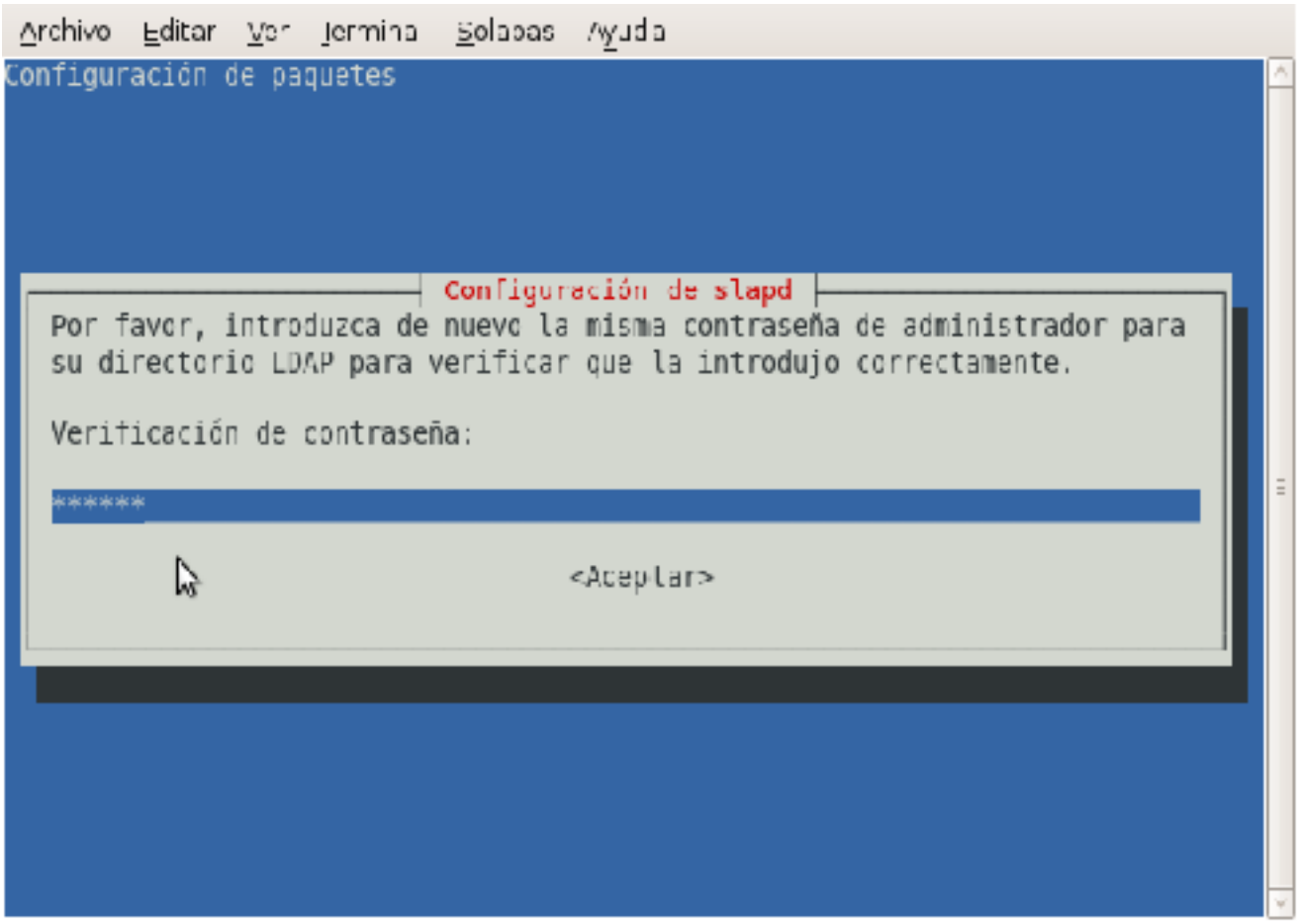


En este nuevo cuadro de diálogo se escoge la opción NO

Digitamos la contraseña del administrador (root)



Confirmamos la contraseña



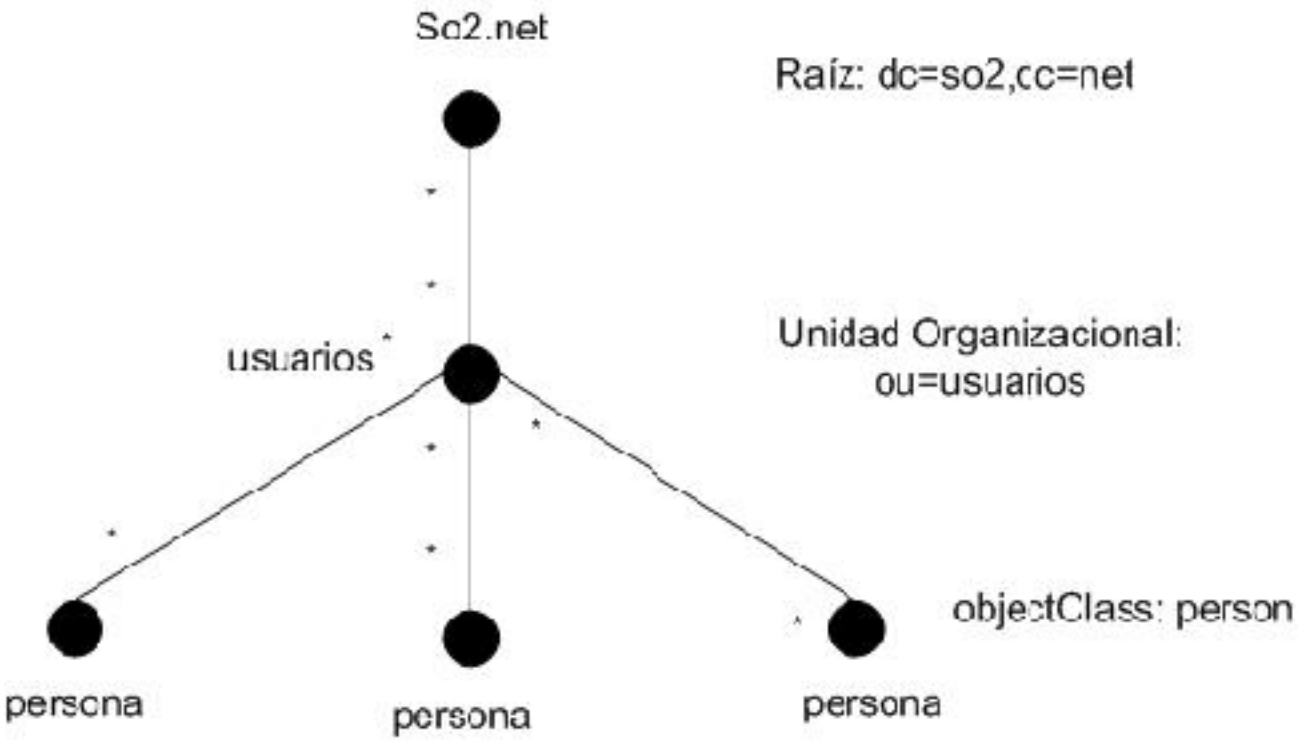
Con esto hemos terminado de configurar ldap

Construir el árbol ldap

Tras haber configurado el servidor ldap procedemos a construir el árbol ldap.

La estructura y los datos del árbol ldap, se almacenan en un fichero con formato .ldif.

El árbol para esta practica es la siguiente:



Abrimos un editor bien sea con vi o con nano, y comenzamos a construir el fichero .ldif:

sudo nano so2.net.ldif

Comenzamos a llenar el árbol digitando primero la raíz (dc=so2,dc=net), la unidad organizacional (ou=usuarios), y los objetos persona (objectClass=person)

#Se define la raíz del árbol

dn: dc=so2,dc=net

dc=so2,dc=net

objectClass: top

objectClass: organization

#Se define la unidad organizacional para el árbol

dn: ou=usuarios,dc=so2,dc=net

objectClass: organizationalUnit

ou: usuarios

#Se define el conjunto de usuarios

dn: uid=raMontoya,ou=usuarios,dc=so2,dc=net

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

objectClass: person

uid: raMontoya

sn: Montoya

givenName: Ramiro

cn: Ramiro Montoya

displayName: Ramiro Montoya

uidNumber: 1001

gidNumber: 1001

userPassword: {CRYPT}mb/RUPYgkZ11o

gecos: Ramiro Montoya

loginShell: /bin/bash

homeDirectory: /home/ichiro

mail: raMontoya@so2.net

#Aca se agregara a un nuevo usuario: Vanessa Pineda

dn: uid=vPineda,ou=usuarios,dc=so2,dc=net

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

objectClass: person

uid: vPineda

sn: Pineda

givenName: Vanessa

cn: Vanessa Pineda

displayName: Vanessa Pineda

uidNumber: 1003

gidNumber: 1003

userPassword: {CRYPT}mbq1AsI5f3xq.

gecos: Vanessa Pineda

loginShell: /bin/bash

homeDirectory: /home/ichiro

mail: vPineda@so2.net

#Aca se agregara a un nuevo usuario: Jhonatan Vallejo

dn: uid=jVallejo,ou=usuarios,dc=so2,dc=net

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

objectClass: person

uid: jVallejo

sn: Vallejo

givenName: Jhonatan

cn: Jhonatan Vallejo

displayName: Jhonatan Vallejo

uidNumber: 1004

gidNumber: 1004

userPassword: {CRYPT}mbASdzsfH3VF2

gecos: Jhonatan Vallejo

loginShell: /bin/bash

homeDirectory: /home/ichiro

mail: jVallejo@so2.net

Tras digitar esto en el archivo lo almacenamos con el nombre de so2.net.ldif, o con el nombre que se desee

Ahora ejecutamos la orden:

ldapadd -x -D cn=admin,dc=so2,dc=net -W -f so2.net.ldif

esto lo hacemos con el fin de agregar el fichero al directorio LDAP

Si quisieramos agregar nuevas usuarios simplemente creamos el fichero .ldif y lo agregamos, como por ejemplo, creemos al usuario Ana Corredor

sudo nano darioSalgado.ldif

estando en el archivo comenzamos a ingresar su información

dn: uid=aCorredor,ou=usuarios,dc=so2,dc=net

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

objectClass: person

uid: aCorredor

sn: Corredor

givenName: Ana

cn: Ana Corredor

displayName: Ana Corredor

uidNumber: 1005

gidNumber: 1005

userPassword: {CRYPT}mb7XvLQ6bmXmQ

gecos: Ana Corredor

loginShell: /bin/bash

homeDirectory: /home/ichiro

mail: aCorredor@so2.net

Guardamos el archivo con el nombre que queramos pero siempre con extensión .ldif, por ejemplo anaCorredor.ldif

Ahora ejecutamos la orden:

ldapadd -x -D cn=admin,dc=so2,dc=net -W -f anaCorredor

esto lo hacemos con el fin de agregar esta nueva entrada al directorio LDAP

Lo anterior lo podemos hacer con la cantidad de usuarios que deseemos

Hacer búsquedas

Teniendo ya la información de nuestro árbol en el directorio ldap, podemos hacer búsquedas, estas se hacen con el comando ldapsearch, por ejemplo

Para mostrar la información de todos los usuarios: ldapsearch -xLLL -b "dc=so2,dc=net", esto muestra la información del árbol, todos los usuarios, con todos sus datos

Para buscar el mail, el common name cn, surname, de un usuario específico. Si el usuario fuese Ana Corredor. Se digita: ldapsearch -xLLL -b "dc=so2,dc=net" uid=aCorredor mail cn sn

Para buscar el givenName, el uidNumber, el gidNumber, de un usuario específico. Si el usuario fuese Jhonatan Vallejo. Se digita: ldapsearch -xLLL -b "dc=so2,dc=net" uid=jVallejo givenName uidNumber gidNumber

De esta manera podemos hacer cualquier tipo de búsqueda en nuestro directorio ldap, de acuerdo a la estructura que hayamos definido

ldap-utils ofrece una serie de herramientas para modificar, agregar, consultar, entre otras acciones en el directorio ldap:

ldapadd: ldapadd abre una conexión a un servidor LDAP, enlaza y añade entradas.

ldapcompare: ldapcompare abre una conexión a un servidor LDAP, enlaza y hace una comparación usando los parámetros especificados.

ldapdelete: ldapdelete abre una conexión a un servidor LDAP, enlaza y borra una o mas entradas.

ldapmodify: ldapmodify abre una conexión a un servidor LDAP, enlaza y modifica entradas.

ldapmodrdn: ldapmodrdn abre una conexión a un servidor LDAP, enlaza y modifica el RDN de las entradas.

ldappasswd: ldappasswd es una herramienta para establecer la contraseña de un usuario LDAP.

ldapsearch: ldapsearch abre una conexión a un servidor LDAP, enlaza y hace una búsqueda usando los parámetros especificados.

ldapwhoami: ldapwhoami abre una conexión a un servidor LDAP, enlaza y realiza una operación whoami.

Iniciar, detener, reiniciar el servidor ldap

Muchas veces necesitaremos detener, reniciar y iniciar el servidor para que ciertos cambios surjan efecto, los comandos para realizarlo son los siguientes

Reiniciar el servidor: sudo /etc/init.d/slapd restart

Detener el servidor: sudo /etc/init.d/slapd stop

Iniciar el servirod sudo /etc/init.d/slapd start

Configurar la red

En esta práctica usaremos una dirección específica para nuestro equipo, el gateway, y el servidor dns, es por esto que para que el equipo funcione de manera óptima debemos configurar las direcciones ip y de red manualmente, para ello hacemos lo siguiente:

1 - Digitamos sudo etc/network/interfaces, estando allí escribimos las direcciones que se nos solicitan de acuerdo a lo que estemos configurando

2 - Digitamos sudo etc/resolve.conf, e igual que en el paso anterior digitamos la dirección ip que se nos solicita en el archivo

3 - Digitamos sudo etc/hosts, y modificamos de acuerdo a nuestras necesidades el contenido de dicho archivo

4 - Por último reniciamos el servidor para que los cambios surjan efecto: sudo /etc/init.d/slapd restart

Nota adicional

En el campo de userPassword de los ficheros .ldif como los que se hicieron un poco más arriba en este documento, es recomendable tener la contraseña del usuario encriptada, para lograr esto se puede hacer lo siguiente:

Para lograr esto se usa el siguiente comando: sudo slappasswd -C 'mb', habiendo hecho esto,se nos pide la contraseña, despues la confirmacion de esta, y esta herrramienta nos mostrará por pantalla la contraseña encriptada. Es fundamental copiar toda la cadena de texto que allí aparece, ejemplo de una contrase encriptada: {CRYPT}mbt2zRlEwEN3s

Capítulo 5. Bibliografía

Recursos consultados

Pinheiro Malere,Luiz Ernesto. LDAP-Linux-Como (en línea). Disponible en http://es.tldp.org/COMO-INSFLUG/COMOs/LDAP-Linux-Como/LDAP-Linux-Como.html#toc2. Consultado 12 de Abril de 2009.

BLFS , Equipo de Desarrollo. OpenLDAP-2.1.22. Introducción a OpenLDAP (en línea). Disponible en http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/blfs-es/blfs-es-5.0/server/openldap.html. Consultado 21 de Abril de 2009.

Donnelly, Michael. Diseñando un árbol de Directorio LDAP (en línea). Disponible en http://ldapman.org/articles/arbol_diseno.htm#que. Consultado 8 de Abril de 2009.

Ghaffar, Atif. Introducción a LDAP sobre Linux (en línea).Disponible en http://www.linuxfocus.org/Castellano/July2000/article159.shtml#lfindex0. Consultado 2 de Abril de 2009.

Ubuntu Documentation. OpenLDAP Server (en línea). Disponible en https://help.ubuntu.com/8.10/serverguide/C/openldap-server.html. Consultado 2 de Abril de 2009.

Las capturas de la instalación del ubuntu server 8.10 fueron tomadas de:

Ver: http://sliceoflinux.wordpress.com/2009/05/08/instalar-ubuntu-810-server-paso-a-paso