

Administración de dominios en Linux

En el mundo Linux no existe un concepto de dominio tan elaborado como en Windows Server. Sin embargo, se consigue un efecto similar al activar un servicio en una máquina Linux (que actuaría como "servidor" de cuentas y grupos) y otro servicio que permite la exportación de directorios a máquinas remotas. En concreto, dichos servicios se denominan LDAP y NFS, respectivamente.

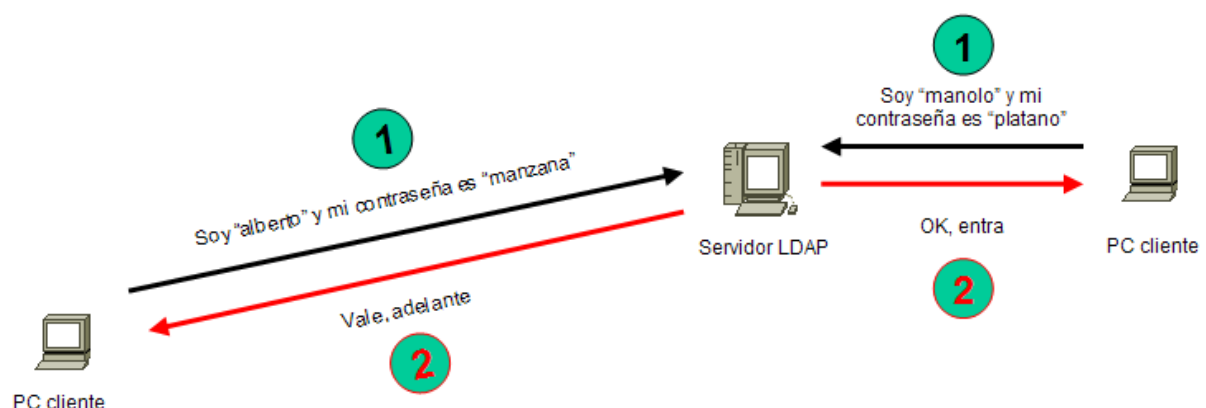
Concepto de dominio

Desde el punto de vista de la administración de sistemas, suele denominarse dominio a un conjunto de equipos interconectados, que comparten información administrativa (usuarios, grupos, contraseñas, etc.) centralizada. Se requiere la disponibilidad de, al menos, un ordenador que almacene físicamente dicha información, y que la comunique al resto cuando sea necesario, mediante un esquema típico de cliente-servidor.

Por ejemplo, cuando un usuario desea iniciar una conexión interactiva en cualquiera de los ordenadores (clientes) del dominio, dicho ordenador deberá validar las credenciales del usuario en el servidor, y obtener de éste todos los datos necesarios para poder crear el contexto inicial de trabajo para el usuario.

En Windows Server, la implementación del concepto de dominio se realiza mediante el denominado Directorio Activo, un servicio de Directorio basado en diferentes estándares como LDAP (Lightweight Directory Access Protocol) y DNS (Domain Name System). En el mundo Unix, los dominios solían implementarse mediante el famoso Network Information System (NIS), del que existían múltiples variantes. Sin embargo, la integración de servicios de Directorio en Unix ha posibilitado la incorporación de esta tecnología, mucho más potente y escalable que NIS en la implementación de dominios.

Usaremos una versión libre del protocolo LDAP para Linux, denominada OpenLDAP



(www.openldap.org), para implementar dominios en Linux.

Servicios de Directorio y LDAP

En el contexto de las redes de ordenadores, se denomina Directorio a una base de datos especializada, que almacena información sobre los recursos u "objetos", presentes en la red (tales como usuarios, grupos, ordenadores, impresoras, etc.) y pone dicha información a disposición de los usuarios de la red. Por este motivo, esta base de datos suele estar optimizada para operaciones de búsqueda, filtrado y lectura, más que para operaciones de inserción o transacciones complejas. Existen diferentes estándares sobre servicios de Directorio, siendo el denominado X.500 el más conocido.

El estándar X.500 define de forma nativa un protocolo de acceso DAP (Directory Access Protocol), que resulta muy complejo (y computacionalmente pesado), porque está definido sobre la pila completa de niveles OSI. Como alternativa a DAP, para acceder a Directorios de tipo X.500, LDAP (Lightweight Directory Access Protocol) ofrece un protocolo "ligero" casi equivalente, pero mucho más sencillo y eficiente, diseñado para operar directamente sobre TCP/IP. Actualmente, la mayoría de servidores de Directorio X.500 incorporan LDAP como uno de sus protocolos de acceso.

LDAP permite el acceso a la información del Directorio mediante un esquema cliente-servidor, donde uno o varios servidores mantienen la misma información de Directorio (actualizada mediante réplicas) y los clientes realizan consultas a cualquiera de ellos. Ante una consulta concreta de un cliente, el servidor contesta con la información solicitada y/o con un "puntero" donde conseguir dicha información (normalmente, el "puntero" es otro servidor de Directorio).

Internamente, el modelo de datos de LDAP define una estructura jerárquica de objetos o entradas en forma de árbol, estos objetos se pueden agrupar en dos grandes tipos:

Contenedores: Pueden a su vez contener otros objetos. Tales clases de objetos son root (el elemento raíz del árbol de directorios, que no existe realmente), ou (unidad organizativa) y dc (componente de dominio). Este modelo es comparable con los directorios (carpetas) de un sistema de ficheros.

Hojas: Se encuentran en la parte final de una rama y no incluyen objetos subordinados. Algunos ejemplos serían person, InetOrgPerson o posixAccount.

Cada objeto o entrada posee un conjunto de atributos. Cada atributo viene identificado mediante un nombre o acrónimo significativo, pertenece a una clase de objetos y puede tener uno o varios valores asociados.

Toda entrada viene identificada unívocamente en la base de datos del Directorio mediante un atributo especial denominado nombre distinguido o **dn** (distinguished name). El resto de atributos de la entrada depende de qué objeto esté describiendo dicha entrada. Por ejemplo, las entradas que describen a usuarios suelen tener, entre otros, atributos como:

- **uid**, nombre por el que se va a identificar en el sistema.
- **uidNumber**, número del usuario en el sistema.

- **gidNumber**, número de su grupo primario.
- **homeDirectory**, directorio de conexión.
- **cn** (common name), para describir su nombre común.
- **sn** (surname), para su apellido.

La definición de los posibles tipos de objetos, así como de sus atributos (incluyendo su nombre, tipo, valor(es) admitido(s) y restricciones), que pueden ser utilizados por el Directorio de un servidor de LDAP, la realiza el propio servidor mediante el denominado esquema del Directorio. Es decir, el esquema contiene las definiciones de los objetos que pueden darse de alta en el Directorio.

El nombre distinguido de cada entrada del Directorio es una cadena de caracteres formada por pares 'atributo=valor' separados por comas, que representa la ruta que lleva desde la posición del objeto en el árbol, hasta la raíz del mismo.

Puesto que un Directorio almacena información sobre los objetos que existen en una cierta organización, cada Directorio posee como raíz (o base, en terminología LDAP), la ubicación de dicha organización, de forma que la base se convierte de forma natural en el sufijo (terminación) de los nombres distinguidos de todas las entradas, que mantiene el Directorio.

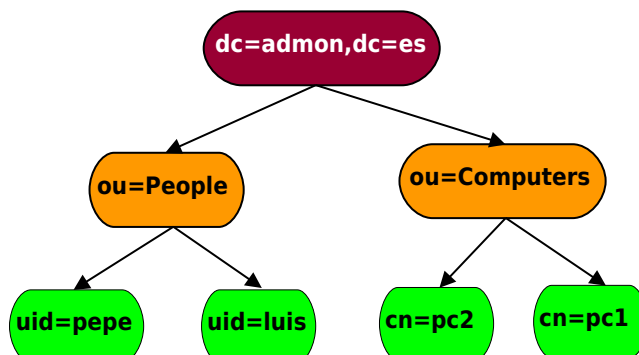
Para denominar la base del Directorio, se sigue el nombrado basado en nombres de dominio de Internet: este nombrado utiliza los dominios DNS para nombrar la raíz de la organización. En este caso, la base del instituto podría ser: "dc=vergel,dc=es" (dc -> domain component o componente de dominio). Este es el nombrado que vamos a utilizar, puesto que permite localizar a los servidores de LDAP utilizando búsquedas DNS.

A partir de esa base, el árbol se subdivide en los nodos y subnodos que se estime oportuno, para estructurar de forma adecuada los objetos de la organización, los objetos se ubican finalmente como las hojas del árbol. De esta forma, el nombre distinguido de cada entrada describe su posición en el árbol de la organización de forma inequívoca, igual que en un sistema de ficheros típico, en el que la trayectoria absoluta de cada fichero equivale a su posición en la jerarquía de directorios del sistema.

En la estructura de Directorio del dominio "admon.es", se muestra un ejemplo de un Directorio sencillo, dos usuarios y dos equipos, agrupados en dos unidades organizativas.

De acuerdo con dicha figura, la entrada correspondiente al usuario "pepe" tendría como nombre distinguido:

"uid=pepe,ou=People,dc=admon,dc=es".



Al margen de ese identificador único, cada entrada u objeto en el Directorio puede tener, como hemos dicho, un conjunto de atributos tan descriptivo como se desee.

Cada objeto necesita, a parte de su nombre distinguido, su "clase de objeto", que se especifica mediante el atributo `ObjectClass`, un mismo objeto puede pertenecer a diferentes clases simultáneamente, por lo que pueden existir múltiples atributos para un mismo objeto en el Directorio.

El atributo `ObjectClass` determina el resto de atributos de dicho objeto, de acuerdo con la definición establecida en el esquema. Siguiendo con el ejemplo anterior, a continuación se muestra un subconjunto de los atributos del usuario "pepe":

```
dn: uid=pepe,ou=People,dc=admon,dc=es
objectClass: person
cn: José
sn: García
description: Encargado de Nóminas
mail: pepe@admon.es
```

El formato en el que se han mostrado los atributos del objeto se denomina LDIF (LDAP Data Interchange Format), y resulta útil conocerlo porque es el formato que los servidores LDAP (y OpenLDAP entre ellos) utilizan por defecto para insertar y extraer información del Directorio.

Con este formato, en cada línea debe de ir una pareja 'atributo: valor' todos los atributos de un mismo objeto deben de estar en líneas consecutivas. Dentro de un fichero LDIF se pueden definir tantos objetos como necesitemos, para separar los atributos de los distintos objetos sencillamente se deja una línea en blanco.

Puesto que nosotros vamos a utilizar el Directorio con un uso muy específico (centralizar la información administrativa de nuestro dominio para autenticar usuarios de forma global), debemos asegurarnos que en el esquema de nuestro Directorio existen los tipos de objetos (y atributos) adecuados para ello. Afortunadamente, OpenLDAP posee por defecto un esquema suficientemente rico para cubrir este cometido. Por ejemplo, cada usuario puede definirse mediante un objeto de tipo `posixAccount`, que posee los atributos para almacenar su UID, GID, contraseña, etc.

Visión general de la implementación de un dominio Linux con OpenLDAP

La implementación de un dominio Linux utilizando OpenLDAP, es una tarea algo compleja y requiere realizar varios pasos que se resumen a continuación.

Instalar y configurar el servidor OpenLDAP.

El primer paso consiste en elegir uno de los ordenadores de la red, para que actúe como servidor OpenLDAP, e instalar y configurar en dicho ordenador este servicio de red. Finalizado este paso se dispone de un Directorio operativo pero carente de información.

Poblar el Directorio LDAP

Consiste en crear las unidades organizativas y los objetos. Esta información la podemos introducir:

- Directamente usando ficheros ldif.
- Con herramientas gráficas.
- Migrando la información desde otras estructuras de datos.

Es conveniente verificar que el Directorio es accesible desde las herramientas cliente de OpenLDAP.

Configurar la autenticación de los clientes basada en OpenLDAP.

Una vez que se dispone de un Directorio LDAP, en el que reside la información necesaria relativa a usuarios y grupos (UIDs, GIDs, contraseñas, etc.), hay que configurar los clientes Linux, para que utilicen esta información en el proceso de autenticar usuarios.

Instalación del servidor OpenLDAP

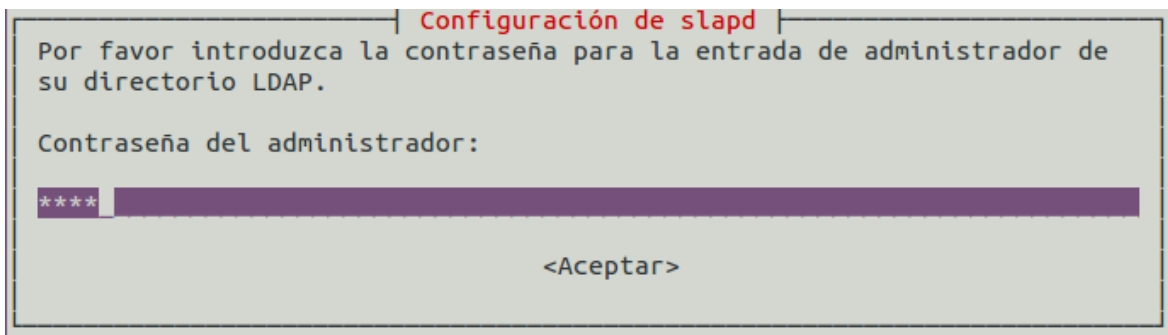
Para simplificar la administración de los usuarios del sistema, es ideal utilizar una base de datos accesible mediante LDAP. Almacenar las cuentas de usuario de forma centralizada en un único repositorio facilitará la creación, modificación y eliminación de cuentas de usuario y grupos de usuarios. Será necesario configurar los PCs de la red para que utilicen el servidor LDAP como servidor de autenticación.

Instalación de OpenLDAP

El servidor OpenLDAP está disponible en el paquete **slapd** por tanto, lo instalaremos utilizando apt-get.

```
apt-get install slapd
```

Solicita la contraseña del administrador (admin) del Directorio LDAP por dos veces:



También instalamos el paquete **ldap-utils**, que contiene utilidades adicionales de administración para el Directorio:

```
apt-get install ldap-utils
```

Una vez instalado, este paquete coloca los ficheros de configuración por defecto bajo el directorio:

```
/etc/ldap
```

En la instalación se debe de haber creado el siguiente directorio, propiedad de "openldap", para albergar la base de datos con la información del Directorio y sus índices:

```
/var/lib/ldap
```

Se instala el servicio o "daemon" de LDAP, denominado slapd.

El servidor LDAP, al igual que todos los servicios en Debian, dispone de un script de arranque y parada en la carpeta /etc/init.d.

```
/etc/init.d/slapd start          # Arrancar el servidor LDAP
```

```
/etc/init.d/slaped restart      # Reiniciar el servidor LDAP
/etc/init.d/slaped stop        # Parar el servidor LDAP
/etc/init.d/slaped status      # Indica si está en funcionamiento
```

Arranque automático del servidor LDAP al iniciar el sistema.

Para un arranque automático del servicio al iniciar el servidor, debemos crear los enlaces simbólicos correspondientes en los directorios `/etc/rcnº.d`.

Comprobar si ya se ha colocado y en qué niveles de arranque:

```
find /etc/ -name "*slaped"
```

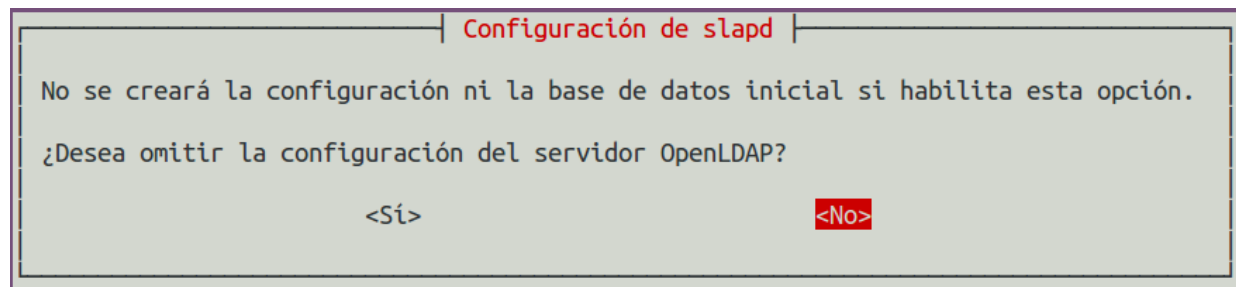
Configuración de slapd

Aunque una configuración mínima se lleva a cabo durante la instalación, es conveniente reconfigurar el servidor para adaptarlo a nuestra empresa, esta tarea la llevamos a cabo con el comando:

```
dpkg-reconfigure slapd
```

Esta instrucción abre una serie de diálogos que nos permiten configurar adecuadamente el servidor.

En este diálogo debemos de seleccionar la opción `<No>`, de lo contrario no haríamos la configuración del servidor.



Ahora escribimos el nombre del dominio, que va a ser la base o raíz del Directorio, para nuestra práctica usamos **vergel.es**.

Configuración de slapd

El nombre de dominio DNS se utiliza para construir el DN base del directorio LDAP. Por ejemplo, si introduce «mi.dominio.org» el directorio se creará con un DN base de «dc=mi, dc=dominio, dc=org».

Introduzca su nombre de dominio DNS:

<Aceptar>

A continuación nos solicita el nombre de la organización, podemos utilizar el mismo.

Configuración de slapd

Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

<Aceptar>

Nos solicita la contraseña del administrador del Directorio de LDAP por dos veces, en nuestro caso ponemos **tierra**.

Configuración de slapd

Por favor introduzca la contraseña para la entrada de administrador de su directorio LDAP.

Contraseña del administrador:

<Aceptar>

Aquí seleccionamos el motor de base de datos para el Directorio, dejamos la opción recomendada **HDB**.

Configuración de slapd

Se recomienda el motor HDB. Los motores HDB y BDB utilizan formatos de almacenamiento semejantes, pero HDB permite realizar cambios de nombre de subárboles («subtree renames»). Ambos tienen las mismas opciones de configuración.

En cualquier caso, debe revisar la configuración de la base de datos. Vea en «/usr/share/doc/slapd/README.DB_CONFIG.gz» para más detalles.

Motor de base de datos a utilizar:

BDB

HDB

<Aceptar>

Responderemos <Sí>, para que cuando desintalemos slapd, también se borre la base de datos. En nuestro ejemplo no habría ningún problema en responder <No>.

Configuración de slapd

¿Desea que se borre la base de datos cuando se purgue el paquete slapd?

<Sí>

<No>

Como no tenemos bases de datos antiguas podemos seleccionar <No>. En nuestro caso también podemos responder <Sí>. En futuras reinstalaciones, responderemos afirmativamente si deseamos comenzar con una base de datos limpia.

Configuración de slapd

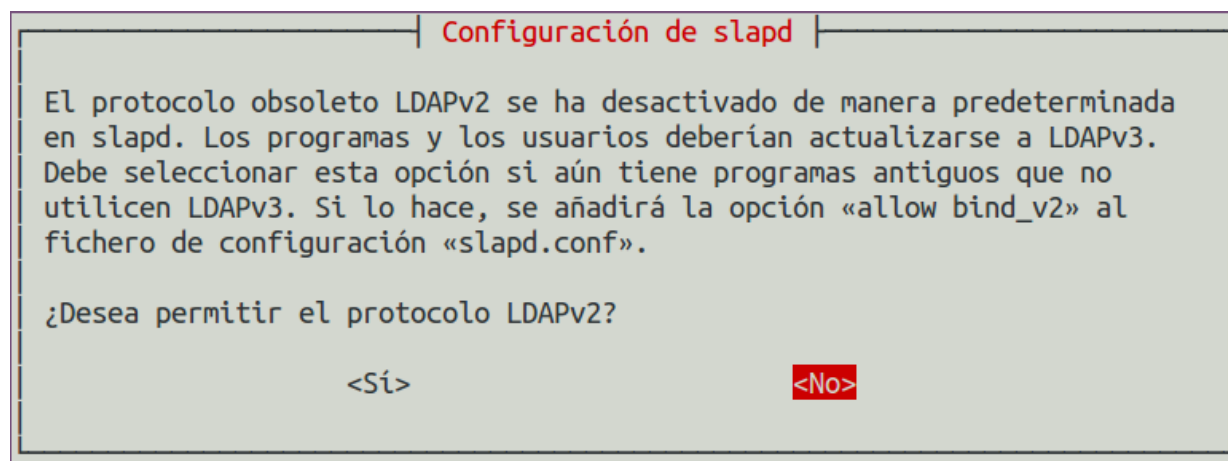
Existen ficheros en «/var/lib/ldap» que probablemente interrumpen el proceso de configuración. Si activa esta opción, se moverá los ficheros de las bases de datos antiguas antes de crear una nueva base de datos.

¿Desea mover la base de datos antigua?

<Sí>

<No>

Finalmente no activamos la antigua versión del protocolo LDAP.



Con el siguiente comando podemos ver los objetos que ya hay creados en nuestro Directorio, que deben de ser la raíz o base y el administrador.

```
ldapsearch -xLLL -b "dc=vergel,dc=es"
```

Debemos de observar el nombre que se le da por defecto al administrador, ya que nos será necesario para futuros comandos.

1. Instalar el servidor LDAP y realizar la configuración básica explicada hasta el momento.

Poblar el Directorio LDAP

Comando Idapadd

El comando Idapadd (incluido en el paquete ldap-utils), se usa para añadir información al Directorio, esta información debe de estar en formato LDIF, algunas opciones de este comando son:

-x

Opción para usar autenticación simple, en lugar de la usada por defecto en LDAP, que se llama SASL, algo más compleja.

-D "usuario"

Aquí indicamos el "dn" del usuario que tiene permiso para realizar la operación de inserción en el Directorio.

-W

Solicitará la contraseña del usuario, en lugar de tener que escribirla en la línea de comandos.

-f fichero.ldif

La información que se quiere añadir al Directorio se encuentra en el fichero, que debe de tener formato LDIF.

Crear Unidades Organizativas

Ahora creamos dos unidades organizativas, una de ellas para albergar los grupos y otra para los usuarios. Usamos un fichero LDIF, para almacenar las definiciones, llamándolo por ejemplo UniOrg.ldif.

```
# Creación unidad organizativa "usuarios"
dn: ou=usuarios,dc=vergel,dc=es
ou: usuarios
objectClass: top
objectClass: organizationalUnit

# Creación unidad organizativa "grupos"
dn: ou=grupos,dc=vergel,dc=es
ou: grupos
objectClass: top
objectClass: organizationalUnit
```

Para añadir esta configuración al Directorio, usaremos ldapadd autenticándonos como el usuario administrador del Directorio LDAP.

```
ldapadd -x -D "cn=admin,dc=vergel,dc=es" -W -f UniOrg.ldif
```

Comprobar buscando la unidad organizativa "usuarios".

Para realizar búsquedas dentro del Directorio usamos la utilidad ldapsearch, que tiene el siguiente formato básico:

```
ldapsearch -xLLL -b "PuntoInicio" QuéBusco
-x
```

Para que use el método de autenticación simple en lugar de SASL.

```
-b
```

Base a partir de donde buscará el objeto.

```
-LLL
```

Es común usar estas tres letras mayúsculas, con ello obtenemos la salida en formato LDIF, de una forma más compacta, sin comentarios y sin el nombre de la versión.

Como siempre para más información en el man.

Por ejemplo, para buscar la información relativa a la unidad organizativa "usuarios" escribiremos:

```
ldapsearch -x -b "dc=vergel,dc=es" ou=usuarios
```

2. Añadir al directorio las dos unidades organizativas y comprobarlo realizando las búsquedas correspondientes.

Creación de usuarios y grupos

La creación de usuarios y grupos en LDAP sigue el mismo procedimiento que en los apartados anteriores: Crear el fichero en formato LDIF con la información adecuada y luego, introducir dicha información en la base de datos con el comando `ldapadd`.

Es importante tener en cuenta que los identificadores de usuarios y grupos deben de ser únicos, nosotros hemos comenzado a numerarlos a partir de 5000, es responsabilidad del administrador asignar rangos de identificadores para determinados tipos de usuarios y grupos.

Creación del fichero `nuevoGrupo.ldif`:

```
# Creación del grupo "frutales"
dn: cn=frutales,ou=grupos,dc=vergel,dc=es
objectClass: posixGroup
objectClass: top
cn: frutales
gidNumber: 5000
```

Añadir la información al Directorio:

```
ldapadd -x -D "cn=admin,dc=vergel,dc=es" -W -f nuevoGrupo.ldif
```

3. Una vez dado de alta en el Directorio, comprobar que está, realizando una búsqueda.

Ahora añadimos un usuario dentro de la unidad organizativa usuarios, que va a pertenecer al grupo anterior. De tal forma que se pueda autenticar desde cualquier equipo perteneciente al dominio.

Creación del fichero `nuevoUsuario.ldif`:

```
# Creación del usuario manzano
dn: uid=manzano,ou=usuarios,dc=vergel,dc=es
uid: manzano
cn: manzano rojo
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: manzano
loginShell: /bin/bash
uidNumber: 5000
gidNumber: 5000
homeDirectory: /home/movil/manzano
gecos: Mi fruta es rica y digestiva
host: *
```

En este ejemplo, todos los usuarios con perfil móvil tendrán su directorio de conexión dentro de **/home/movil**, para que de esta forma sea más cómodo ponerlos disponibles en la red a través de NFS.

Añadir al Directorio:

```
ldapadd -x -D "cn=admin,dc=vergel,dc=es" -W -f nuevoUsuario.ldif
```

4. Después de añadirlo, buscar la información relativa al usuario dentro del Directorio, para confirmar que se ha dado de alta.


Comprobaciones

slapcat

Este comando, que requiere permisos de administrador, genera una salida en formato LDIF de todo el contenido del Directorio LDAP.

```
-l fichero.ldif
```

Si le añadimos esta opción, obtenemos una copia del Directorio en un fichero con formato LDIF.

5. Comprueba el estado del Directorio con slapcat.
6. Añadir dos usuarios más al grupo frutales (usa la plantilla anterior), atención al uidNumber.
7. Añade un grupo llamado "aromaticas" a la unidad organizativa grupos, atención al gidNumber.
8. Añade tres usuarios (tomillo, romero, mejorana, oregano, salvia, ...), uno de ellos con tu nombre, a la unidad organizativa usuarios y que pertenezcan al grupo "aromaticas".
9. Muestra información sobre una unidad organizativa.
10. Busca información sobre el grupo "aromaticas".
-  11. Consulta la información de un usuario cualquiera y del que tiene tu nombre.

Otras utilidades

El administrador del Directorio LDAP puede **cambiar la contraseña**, tanto de los usuarios como de él mismo con el siguiente comando:

```
ldappasswd -x -D "dn administrador" -W -s nueva_contraseña
           "dn a quien se le cambia"
```

Esta utilidad también nos sirve para generar una contraseña encriptada, que podemos usar en los ficheros LDIF. Por ejemplo:

```
slappasswd -h {MD5}
```

Dentro del fichero LDIF usaremos exactamente lo que nos devuelve el comando.

Igualmente se pueden **eliminar objetos** del Directorio, con el comando `ldapdelete`, cuyo formato es:

```
ldapdelete -x -D "dn administrador" -W "dn objeto a eliminar"
```

El administrador también puede **modificar objetos**, con la herramienta `ldapmodify`. El método más fácil consiste en crear un fichero LDIF, donde se indican las modificaciones y añadirlo al servidor LDAP.

Por ejemplo, para cambiar el nombre común 'cn' del usuario manzano, añadirle el atributo 'description' y quitarle el atributo 'gecos', creamos un fichero LDIF como el siguiente:

```
# Modificando el usuario manzano.

dn: uid=manzano,ou=usuarios,dc=vergel,dc=es
changetype: modify
replace: cn
cn: manzano
-
add: description
description: Arbol de hoja caduca
-
delete: gecos
-
```

Y a continuación como administradores ejecutamos el comando:

```
ldapmodify -x -D 'cn=admin,dc=vergel,dc=es' -W -f modificar.ldif
```

Más información sobre estos comandos en las páginas del manual (man).

Configuración de un cliente LDAP

Arquitectura de autenticación y validación de nombres en Linux: PAM y NSS

Existen dos servicios que intervienen en este proceso.

NSS (Name Service Switch, Conmutador de servicio de nombres). Permite a las aplicaciones y comandos obtener información administrativa (usuarios, grupos, caducidad de las contraseñas, fortaleza de las mismas,...) sin tener que conocer que método se usa para almacenar dicha información. NSS se encarga de recoger la información administrativa de los distintos medios.

PAM (Pluggable Authentication Module, Módulo de Autenticación intercambiable) Posibilita configurar en un sistema Linux varios sistemas de autenticación.

Software necesario en el cliente de LDAP

Dos paquetes son necesarios para implementar esta arquitectura:

libpam-ldap

libnss-ldap

nscd (Name Service Cache Daemon) Opcional

Utilizando el comando de instalación:

```
apt-get install libpam-ldap
```

Se instalarán los paquetes:

auth-client-config

ldap-auth-client

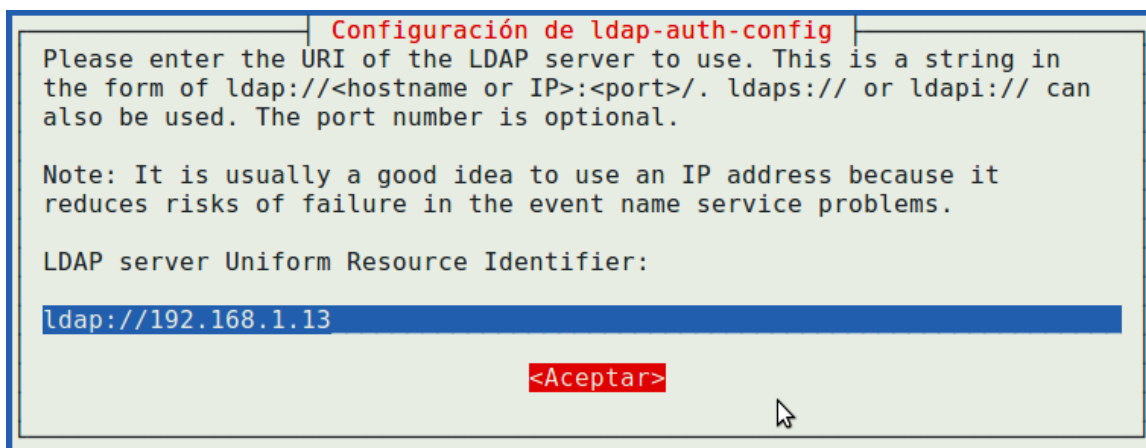
ldap-auth-config

libnss-ldap

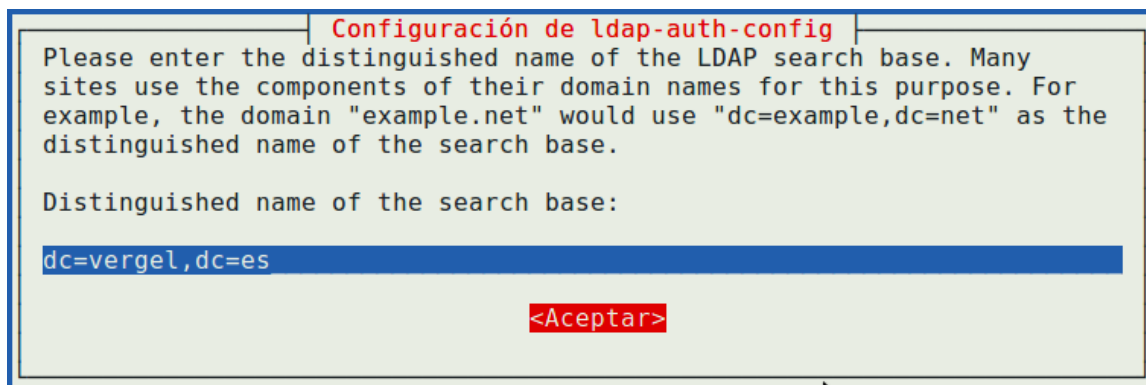
libpam-ldap

Una vez terminada la instalación, muestra unas ventanas de texto para la configuración básica de LDAP en el cliente.

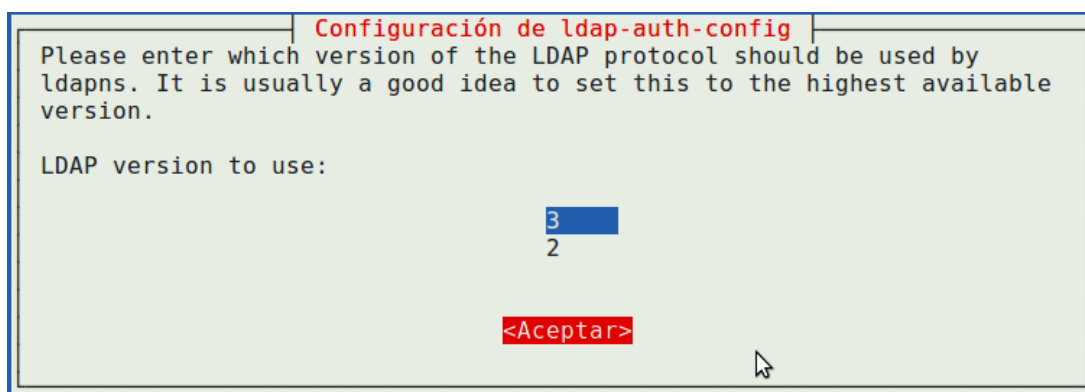
En la primera ventana anotamos la IP del servidor LDAP utilizando el prefijo **ldap://**.



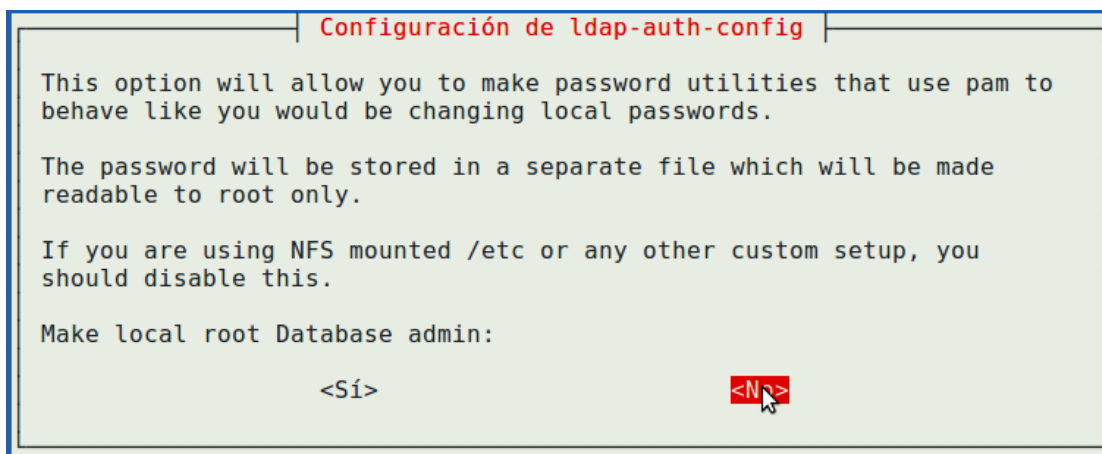
En la segunda se especifica el DN (nombre distinguido) de la base del Directorio.



A continuación seleccionamos la versión **3**.



Luego nos pregunta si deseamos que las contraseñas se almacenen en un fichero aparte. Respondemos que No.



También respondemos que el cliente No necesita autenticarse para acceder a la base de datos, ya que únicamente va a leerla.



Finalmente informa sobre los sistemas de cifrado y pregunta por el que se debe de seguir cuando se cambien contraseñas.

Esto último sólo ocurre si realizamos la reconfiguración, como se indica a continuación.



Toda la configuración del cliente se almacena en el fichero /etc/ldap.conf, siendo este usado tanto por PAM como por NSS.

Para hacer cambios en esta configuración se ejecuta el comando:

```
dpkg-reconfigure ldap-auth-config
```

Configuración del servicio NSS

En el fichero `/etc/nsswitch.conf` se especifica el orden de búsqueda de información, en nuestro caso queremos autenticar a los usuarios de forma que se use la información local y la disponible en el Directorio LDAP, por lo que tendremos que añadir la palabra **ldap** al final de las líneas que comienzan por `"passwd:", "group:"` y `"shadow:"`.

```
vim /etc/nsswitch.conf
```

Buscamos las siguientes 3 líneas:

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

Y las editamos para que queden así:

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

De esta forma primero buscará en los ficheros locales (`/etc/passwd`, `/etc/group` y `/etc/shadow`), y si el usuario no se encuentra buscará a continuación en el Directorio LDAP.

Para probar que NSS está funcionando correctamente, y accede a la información contenida en el Directorio del servidor, ejecutamos los siguientes comandos:

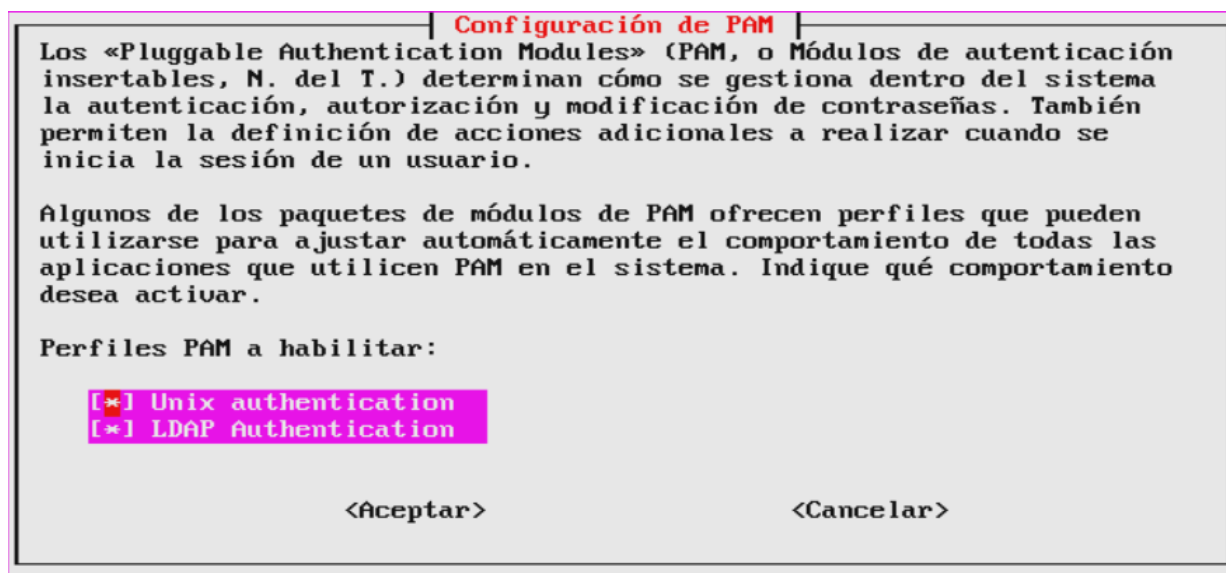
```
getent group
getent passwd
```

Si tenemos el servidor LDAP funcionando, en la respuesta debe de incluir a los grupos y usuarios creados en el Directorio LDAP.

Configuración de PAM

Sus ficheros de configuración se encuentran en `"/etc/pam.d/"`. realizamos una configuración básica ejecutando el comando:

```
pam-auth-update
```



Atención: si muestra más métodos, marcar solo los dos primeros (barra espaciadora marca y desmarca).


Para que LDAP sea totalmente operativo, faltaría reiniciar el equipo cliente.

Es conveniente comprobar que PAM está funcionando correctamente, para lo que instalaremos el paquete

```
apt-get install libpam-dotfile
```

Y a continuación ejecutamos la herramienta contenida en este paquete, que se llama **pamtest**, requiere dos parámetros: el servicio que se quiere testear (passwd, login, ssh, ...) y para qué usuario. En nuestro caso nos interesa sobre todo, que los usuarios puedan hacer login, por lo que ejecutaremos:

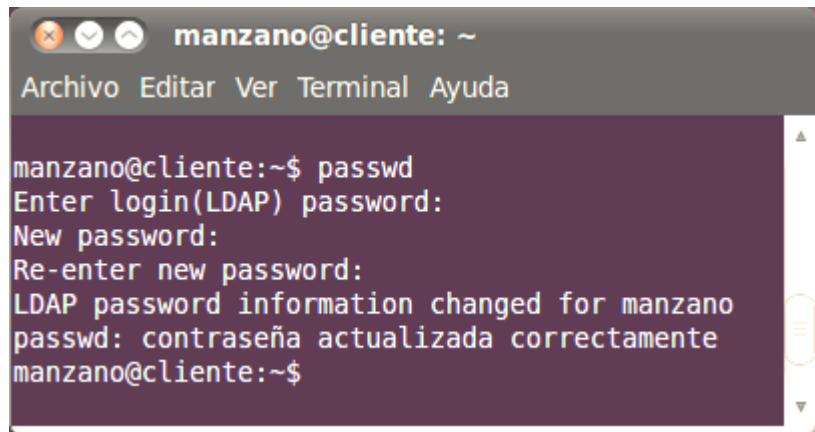
```
pamtest login usuario
```

12. Probar con un usuario local, otro del Directorio LDAP y otro que no exista. 

La configuración realizada por pam-auth-update es válida para la mayoría de los casos, pero se puede personalizar en los ficheros de configuración.

Por defecto, un usuario LDAP conectado desde un cliente no puede cambiar su contraseña con el comando passwd, para permitirlo editamos el fichero **/etc/pam.d/common-password** y modificamos la línea donde aparece "pam_ldap.so" y de ella eliminamos la opción "use_authok".

Un usuario del Directorio se cambia su passwd.

A terminal window titled 'manzano@cliente: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Terminal', and 'Ayuda'. The terminal output shows the command 'passwd' being executed, followed by prompts for the current password, a new password, and a confirmation of the new password. The output indicates that the LDAP password information was successfully changed for the user 'manzano'.

```
manzano@cliente:~$ passwd
Enter login(LDAP) password:
New password:
Re-enter new password:
LDAP password information changed for manzano
passwd: contraseña actualizada correctamente
manzano@cliente:~$
```

13. Desde un terminal virtual, en el cliente, conéctate con un usuario creado en LDAP:

¿En qué directorio inicia sesión?

¿Puede escribir en alguna parte de la estructura de directorios?

14. Probar el cambio de contraseña del usuario LDAP.

15. Parar el servicio LDAP en el servidor.

Verificar si se puede conectar un usuario local.

Intentar conectarse como un usuario de LDAP.

Gestión de los directorios de conexión para habilitar perfiles móviles

En el servidor:

Dar de alta los grupos y usuarios de forma local, con las mismas características que los del Directorio:

- Crear el directorio /home/movil, para que contenga todos los directorios de conexión de los usuarios móviles.
- Crear los grupos y usuarios en el servidor, lo que nos facilita poder conectarnos también desde el servidor sin que este sea cliente LDAP, y además así se crea automáticamente su directorio de conexión.

```
groupadd -g 5000 frutales
useradd -d /home/movil/manzano -m -u 5000 -g frutales
        -s /bin/bash manzano
```

- Con el comando passwd le asignamos la misma contraseña a los usuarios de forma local.

Si no necesitamos crearlos localmente: crear su directorio de conexión, copiar en él de forma recursiva el contenido de /etc/skel y también de forma recursiva cambiar de propietario y grupo el directorio de conexión, usando el nº de usuario y grupo.

Poner a disposición del dominio los directorios HOME de los usuarios móviles:

- Exportar el directorio /home/movil a toda la red usando NFS, para lo cual editamos el fichero /etc/exports y le añadimos una línea similar a:

```
/home/movil 192.168.208.0/24(rw)
```

- Una vez guardado el fichero, para que se haga efectivo el cambio:

```
exportfs -ra
```

- Y comprobamos que se está exportando con:

```
showmount -e
```

En el cliente:


Para tener disponible el directorio de conexión de forma automática, cada vez que se arranque el sistema:

- Instalar el cliente de NFS (`apt-get install nfs-common`).
- Crear el punto de montaje `/home/movil`.
- Añadir al fichero `/etc/fstab` la línea correspondiente para que monte el directorio `/home/movil`, que se encuentra en el servidor, en el punto de montaje que hemos creado.

Con esto hemos completado la creación de nuestro dominio en Linux, para la gestión de usuarios con perfiles móviles.

Por lo tanto, los usuarios del Directorio LDAP se pueden conectar desde cualquier equipo cliente, y trabajar en sus directorios HOME.

15. Efectuar la conexión a un usuario del Directorio desde el equipo cliente, y realizar algún cambio, como la creación de un fichero.
16. Conectar al mismo usuario desde el servidor de forma local, y comprobar el cambio realizado desde el cliente.
17. Conectarse todos al mismo servidor (se elige el de un compañero), deberemos:
 - Reconfigurar NSS, para indicar la IP del nuevo servidor.
 - En `/etc/fstab`, montar el directorio `/home/movil` del servidor seleccionado.

 **Con el final del comando mount y donde se vea el prompt con la máquina y el nombre del usuario.**

Una vez terminado este ejercicio, volver a conectaros a vuestro servidor.

Gestión gráfica de usuarios y grupos

Para acceder al Directorio LDAP y poder crear y modificar objetos de una forma cómoda, es necesario disponer de un explorador de Directorios LDAP (LDAP browser). Existen muchos exploradores LDAP, entre los libres encontramos:

gq: GQ LDAP client.

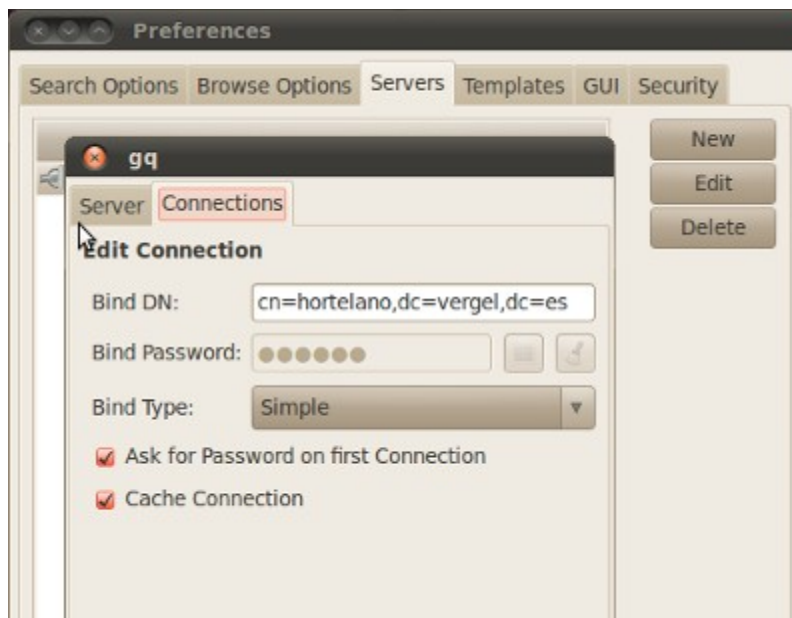
Se instala con `apt-get install gq`

Para ejecutarlo debemos pulsar `alt + F2` y escribir `gq`.

La primera vez que lo usamos tenemos que configurar el servidor, para ello accedemos a través del menú:

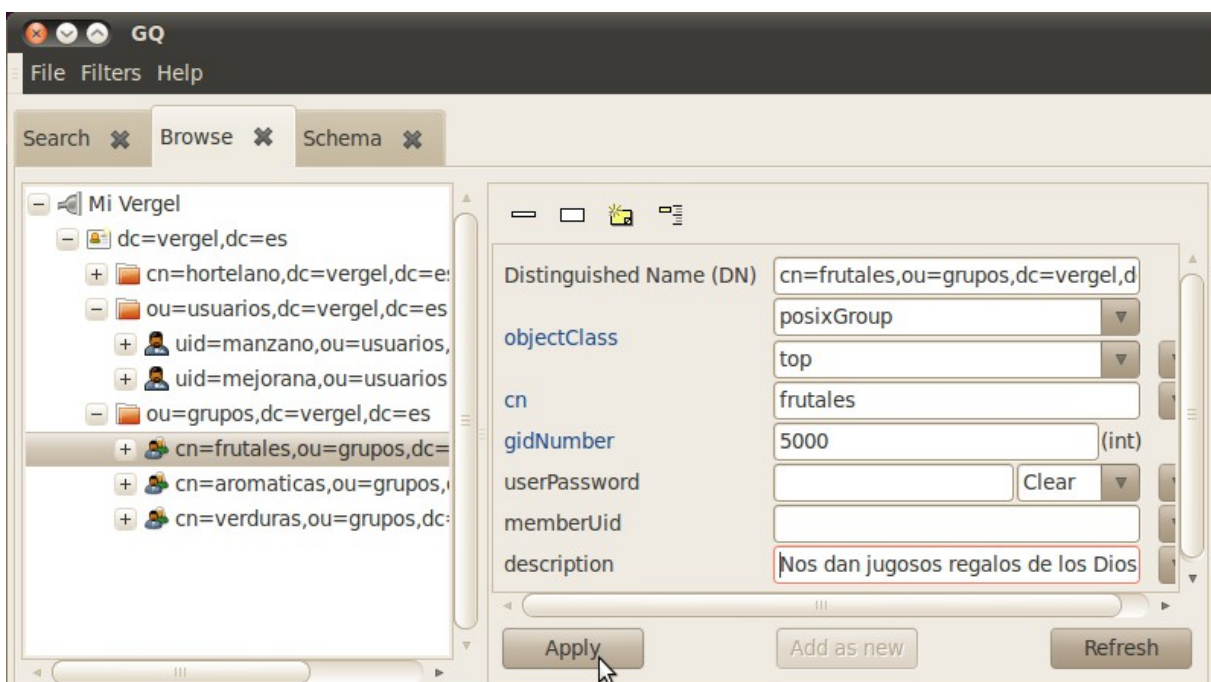
Menú File -> Preferences -> Servers -> Nuevo

E indicamos los datos de nuestro servidor LDAP, tanto en la pestaña Server como Connections.



NOTA: es importante reiniciar `gq` tras cualquier configuración...

Aquí tenemos una visión general del Directorio, justo en el momento de confirmar una modificación en el grupo frutales.



JXplorer: Un explorador de LDAP basado en java, requiere tener instalada la máquina virtual java de Sun.

phpLDAPadmin: Es una aplicación web escrita en PHP, para su funcionamiento es necesario que esté instalado el servidor web Apache, pero como es una dependencia, si no lo está se instalará automáticamente. Lo instalamos en el servidor con el comando habitual:

```
apt-get install phpldapadmin
```

Para comprobar que se ha instalado correctamente, abrimos un navegador web y en la barra de direcciones escribimos:

<http://localhost/phpldapadmin>

O si lo queremos probar desde otro equipo de la LAN:

http://IP_del_Servidor/phpldapadmin

Nos debería aparecer la pantalla principal de phpLDAPadmin.

Es conveniente, aunque no imprescindible, ajustar el fichero de configuración de la aplicación, este se encuentra en `/usr/share/phpldapadmin/config/config.php`. Como siempre hacer una copia antes de iniciar las modificaciones.

Más allá de la línea 250 nos encontramos con la sección que nos interesa.

(Tener en cuenta que en la captura se han eliminado los comentarios)

Concretamente podemos modificar:

- El nombre "name" del servidor LDAP (en la captura línea 267).
- La base o raíz del Directorio (línea en la captura 271).
- El usuario administrador por defecto (línea 275).
- La IP del servidor LDAP (línea 269).

Este último cambio es imprescindible, si se pretende hacer administración remota de LDAP.


```

257 /*****
258 /* Define your LDAP servers in this section */
259 /*****
260
261 $servers = new Datastore();
262
263 /* $servers->NewServer('ldap_pla') must be called before each new LDAP server
264    declaration. */
265 $servers->newServer('ldap_pla');
266
267 $servers->setValue('server','name','Gestión Usuarios');
268
269 $servers->setValue('server','host','192.168.1.13');
270
271 $servers->setValue('server','base',array('dc=vergel,dc=es'));
272
273 $servers->setValue('login','auth_type','session');
274
275 $servers->setValue('login','bind_id','cn=hortelano,dc=vergel,dc=es');
276 # $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
277

```

Una vez iniciado phpLDAPadmin, pulsamos en "conectar", para identificarnos como administradores:

Si hemos realizado correctamente los cambios anteriores, el "Login:" ya aparecerá escrito.

Para realizar administración remota, escribiremos en el navegador:

`http://IP_Servidor/phpldapadmin`

La creación de usuarios y grupos en el entorno web de phpLDAPadmin, aunque es bastante amigable “tiene su aquel”, por lo que se van a mostrar los pasos para la creación de nuevos grupos y usuarios.

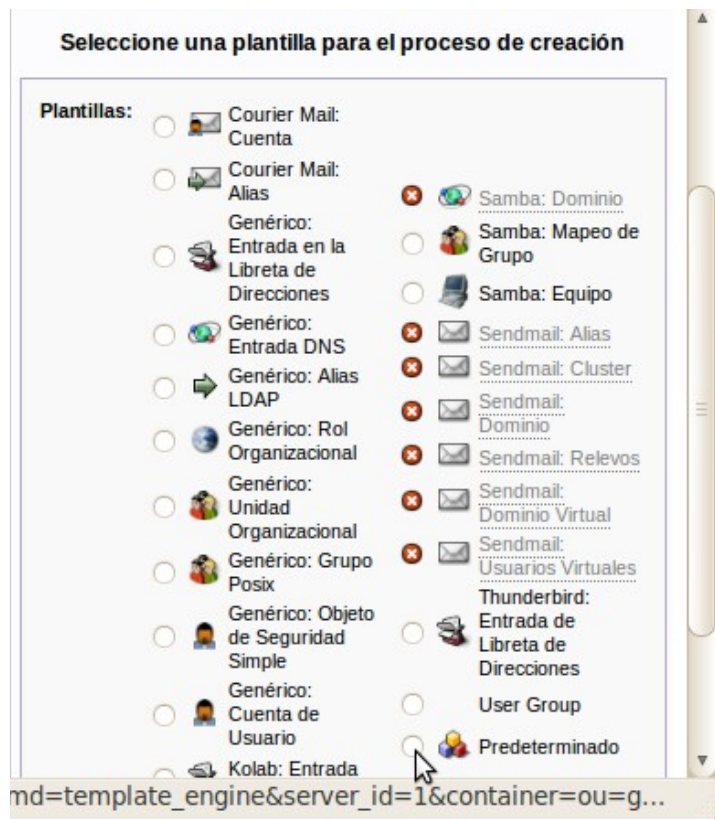
Creación de grupos

Recordar que los UID y GID deben de ser únicos para cada usuario y grupo en todo el Directorio LDAP, y no deben de coincidir con los identificadores de usuarios o grupos locales.

Seleccionar la opción **Crear nuevo objeto** dentro de ou=grupos.



Escogemos la plantilla "Predeterminado", ya que nos da más flexibilidad a la hora de definir el nuevo objeto.



En la lista de clases de objetos seleccionamos **posixGroup** y pulsamos en "Proceder".

En el campo RDN (Relative Distinguished Name), marcamos **cn**.

Y rellenaremos los campos:

- cn: nombre del grupo.
- gidNumber: identificador numérico del grupo (único).
- descripción: por si se necesita poner alguna observación.
- memberUid: los usuarios que tendrán este como su grupo secundario.
- Contraseña: la dejamos en vacía.

Una vez cumplimentado, pulsamos en **Crear objeto**.

Atributo	Nuevo valor	Omitir
cn=verduras,ou=grupos,dc=vergel,dc=es		
cn	verduras	<input type="checkbox"/>
description	Ricas en vitaminas y minerales	<input type="checkbox"/>
gidNumber	5002	<input type="checkbox"/>
objectClass	posixGroup	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>

Nos muestra el resumen y si todo está correcto, pulsamos en **Cometer** para que se cree la nueva entrada.

Podemos comprobar que se ha creado en el esquema del Directorio, parte izquierda.

Creación de usuarios

Seleccionar **Crear nuevo objeto** dentro de ou=usuarios.

Seleccionar la opción **Predeterminado**.

Paso 1 de 2: Contenedor y ObjectClass(es)

Contenedor: ou=usuarios,dc=vergel,dc=es

Clases de objeto:

- organizationalRole
- organizationalUnit
- person
- pilotDSA
- pilotOrganization
- pilotPerson
- pkiCA
- pkiUser
- posixAccount
- posixGroup
- qualityLabelledData
- referral
- residentialPerson
- RFC822localPart
- room

Nota: Debe escoger al menos una clase de objeto estructural

Proceder >>

En la lista que aparecen las clases de objeto, seleccionar account y posixAccount (mantener pulsada la tecla Ctrl mientras se selecciona).

En el campo RDN seleccione el valor userid.

Se deben de rellenar, además de los campos obligatorios, loginShell el userPassword.

Paso 2 de 2: Especifique atributos y valores

RDN: userid (userid)

Atributos requeridos:

- cn: mejorana
- gidNumber: 5001
- homeDirectory: /home/movil/mejorana
- uidNumber: 5005
- userid: mejorana

Atributos opcionales:

- description:

y

Finalmente confirmamos el alta, en la traducción "**Cometer**".



phpLDAPAdmin (1.2.0.5) -

Servidor: Gestion Usuarios Contenedor: ou=usuarios,dc=vergel,dc=es

¿Desea crear esta entrada?

Atributo	Nuevo valor	Omitir
userid=mejorana,ou=usuarios,dc=vergel,dc=es		
cn	mejorana	<input type="checkbox"/>
gecos	Gusto por las zonas humedas	<input type="checkbox"/>
gidNumber	5001	<input type="checkbox"/>
homeDirectory	/home/movil/mejorana	<input type="checkbox"/>
host	*	<input type="checkbox"/>
loginShell	/bin/bash	<input type="checkbox"/>
objectClass	account posixAccount	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
uidNumber	5005	<input type="checkbox"/>
userid	mejorana	<input type="checkbox"/>

Cometer Cancelar

Terminado

18. Dar de alta un grupo y un usuario.
19. Examinar las posibilidades de esta herramienta gráfica.
20. Entrar a administrar el Directorio de un compañero.

Por otra parte, se puede utilizar el paquete **migrationtools** para migrar información de usuarios y grupos locales (/etc/passwd, /etc/group, /etc/shadow) a LDAP.

Migración de información existente en el servidor

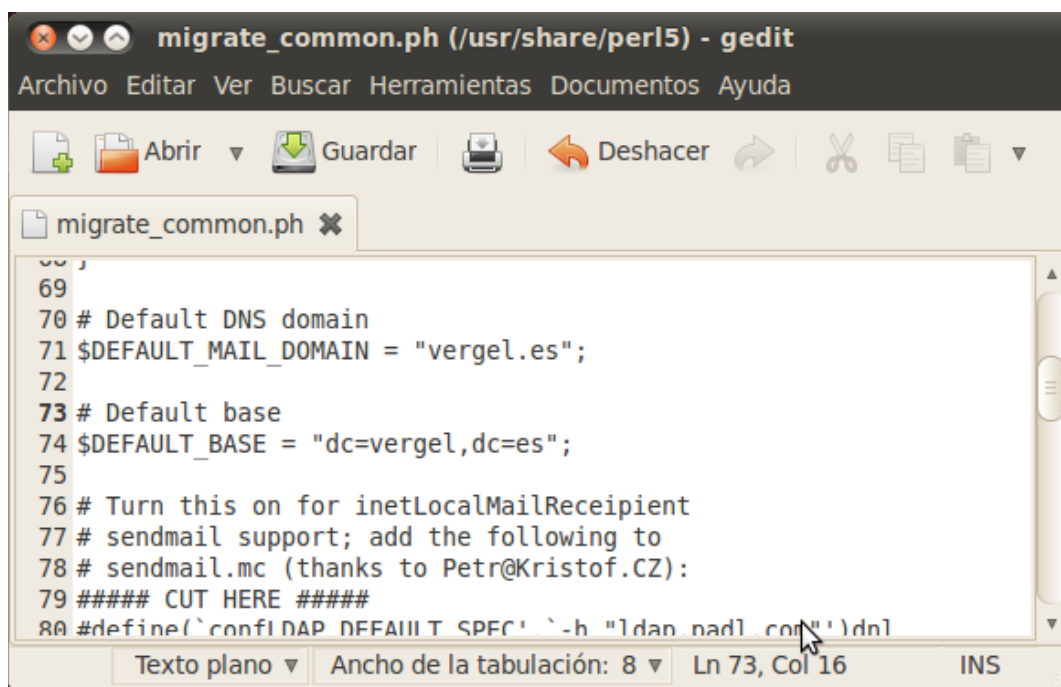
Se puede añadir al Directorio toda la información presente en el ordenador, que está haciendo de servidor. Esto incluye todos los recursos dados de alta en sus ficheros de configuración, tales como cuentas de usuarios, grupos, ordenadores, etc., así como diferentes "contenedores" o "unidades organizativas" (OrganizationalUnits) que distribuyen los objetos de forma racional.

OpenLDAP incorpora un conjunto de herramientas, que pueden utilizarse para realizar esta migración de forma automática.

Instalación de las herramientas de migración:

```
apt-get install migrationtools
```

Una vez instaladas debemos de indicar cuál es la base de nuestro dominio, esto se hace en el fichero `"/usr/share/perl5/migrate_common.ph"`, modificaremos las líneas que en la captura aparecen con el nº 71 y 74.



Una vez modificadas, tenemos diferentes opciones para incorporar la información del sistema al Directorio. Entre ellas, la más recomendable es realizar la migración por partes, añadiendo primero la "base" (es decir, las entradas correspondientes a la organización y sus unidades organizativas por defecto) y posteriormente migrando los usuarios, grupos, hosts, etc., que se ubicarán dentro de dichas unidades.

En el fichero anterior también podemos personalizar el nombre de las unidades organizativas (ou).



```
53     $NAMINGCONTEXT{'rpc'}           = "cn=rpcs";
54     $NAMINGCONTEXT{'services'}      = "cn=services";
55 } else {
56     $NAMINGCONTEXT{'aliases'}       = "ou=Aliases";
57     $NAMINGCONTEXT{'fstab'}         = "ou=Mounts";
58     $NAMINGCONTEXT{'passwd'}        = "ou=usuarios";
59     $NAMINGCONTEXT{'netgroup_byuser'} = "nisMapName=netgroup.byuser";
60     $NAMINGCONTEXT{'netgroup_byhost'} = "nisMapName=netgroup.byhost";
61     $NAMINGCONTEXT{'group'}         = "ou=grupos";
62     $NAMINGCONTEXT{'netgroup'}      = "ou=Netgroup";
63     $NAMINGCONTEXT{'hosts'}         = "ou=Hosts";
64     $NAMINGCONTEXT{'networks'}      = "ou=Networks";
65     $NAMINGCONTEXT{'protocols'}     = "ou=Protocols";
66     $NAMINGCONTEXT{'rpc'}           = "ou=Rpc";
67     $NAMINGCONTEXT{'services'}      = "ou=Services";
68 }
69
```

Para el proceso de migración, existen scripts de Perl en el directorio `/usr/share/migrationtools/`, que podemos utilizar de la siguiente forma (en todo el proceso, el servicio ldap debe estar ejecutándose):

Migración de la base

Si ya tenemos creada la base de nuestro dominio y sus unidades organizativas, saltamos este punto.

Se exportan primero sus objetos a un fichero, en formato LDIF, y luego se insertan en el Directorio mediante la orden `ldapadd`.

Trabajando como administrador y con el directorio activo `"/usr/share/migrationtools/"`.

```
./migrate_base.pl > /tmp/base.ldif
```

```
(NO) ldapadd -x -c -D "cn=admin,dc=vergel,dc=es" -W  
-f /tmp/base.ldif
```


Recordar que con las opciones:

- D Estamos acreditándonos, para la operación, como el usuario "administrador del Directorio".
- W Le decimos a la orden que nos pida la contraseña de dicho usuario de forma interactiva.
- c Consigue que ldapadd siga insertando registros, a pesar de que se produzcan errores en alguna inserción.

1. Instalar las migrationtools.
2. Configurar en el fichero migrate_common.ph.
3. Generar el fichero base.ldif y observar su contenido (no lo añadimos al Directorio de LDAP).

Migración de los grupos:

Para realizar la migración de los usuarios existentes en el servidor de forma local, podemos proceder de dos formas:

Una es:

- Primero realizando la migración de todo el contenido del fichero /etc/group
`./migrate_group.pl /etc/group /tmp/grupos.ldif`
- Y a continuación eliminamos del fichero grupos.ldif los grupos especiales, y dejamos sólo los grupos de los usuarios que van a pertenecer al Directorio LDAP.
- Tras la modificación, añadimos esos grupos al Directorio:
`ldapadd -x -c -D "cn=admin,dc=vergel,dc=es" -W
-f /tmp/grupos.ldif`

Otra forma, quizás más cómoda es:

- Primero realizar una copia del fichero /etc/group.
- En la copia se dejan sólo los usuarios que queremos migrar.
- Se realiza la migración.
- Y finalmente se añaden al Directorio.

4. Crear de forma local en el servidor de LDAP, el grupo verduras

(lechuga, acelga, espinaca, escarola), cuidar que tenga el GID que le corresponda.

5. Migrar sólo el grupo verduras.

Migración de los usuarios:

Para la migración de los usuarios podemos proceder al igual que para la de los grupos:

-Migrar y posteriormente en el fichero ldif eliminar los usuarios que no deseamos que pertenezcan al directorio.

O hacer una copia del fichero /etc/passwd y en la copia dejar solo los que queremos que pertenezcan el Directorio.


Tener en cuenta, que en general no se recomienda exportar la cuenta de "root" mediante LDAP, por cuestiones de seguridad.

El script para realizar la migración es:

```
./migrate_passwd.pl /etc/passwd /tmp/usuarios.ldif
```

Y como siempre para añadir los registros al Directorio:

```
ldapadd -x -c -D "cn=admin,dc=vergel,dc=es" -W  
-f /tmp/usuarios.ldif
```

6. Crear la usuaria lechuga en el servidor de forma local, teniendo en cuenta que su directorio de conexión debe de ser /home/movil/lechuga y asignándole el UID que le corresponda. Ponerle contraseña "lechuga".
7. Extraer en un fichero llamado "lechuga" la línea correspondiente a la usuaria lechuga.
8. Generar el fichero usuarios.ldif a partir del fichero "lechuga".
9. Migrarla al Directorio de LDAP.
10. Comprobar con ldapsearch y con phpLDAPAdmin que se han dado de alta.
11. Captura de phpLDAPAdmin, con los usuarios y grupos desplegados. 

Como hemos comprobado, la migración es útil si creamos los grupos y los usuarios de forma local en el servidor, y después los añadimos al Directorio LDAP.

Eliminar LDAP del servidor

```
/etc/init.d/slaped stop  
apt-get remove slapd  
dpkg --purge slapd  
rm -Rf /var/lib/ldap  
rm -Rf /var/lib/slaped
```