Unidad 4

LDAP

Administración de sistemas operativos

Índice

Introducción

Aunque ya vimos en unidades anteriores que los usuarios en Linux se almacenan en ficheros y que para acceder a este sistema es necesario estar registrado en dicho fichero, estop no es del todo eficiente. Si nos encontramos en un ámbito pequeño, su gestión no es complicadas, pero cuando se acumula un número alto de usuarios, cualquier tarea de administración puede resultar muy tediosa.

Para esto existe el sistema centralizado de administración de cuentas de usuario de Linux, con una base de datos enlazada a este y donde se almacena la información de manera similar a lo que Microsoft ofrece con el directorio activo.

En este aspecto lo más usado es el protocolo ligero de acceso a directorio o LDAP y el que vamos a explicar en esta unidad.

Al finalizar esta unidad

- Sabremos identificar la función, los elementos y las estructuras lógicas del servicio de directorio.
- Conoceremos las características y el funcionamiento de LDAP como mecanismo de acreditación centralizada de los usuarios en una red
- Seremos capaces de instalar el servicio de directorio en el servidor correspondiente.
- Podremos gestionar usuarios y grupos del directorio.
- Conoceremos como añadir usuarios y grupos, así como eliminarlos y modificarlos.
- Seremos capaces de usar herramientas gráficas y comandos para la administración del servicio de directorio.
- Podremos integrar LDAP con ostros sistemas, comprobando la conectividad de la red en un escenario heterogéneo.

4.1. El servicio de directorio como infraestructura

El servicio de directorio es una de las principales partes de un sistema ya que permite que tanto a aplicaciones como personas puedan acceder a los recursos y objetos alojados en dicho sistema. En este caso, el directorio en sí lo entendemos como una única unidad y no como un conjunto de partes independientes. Cuando tenemos distintas aplicaciones que usan muchos tipos de datos distintos podemos sufrir de inconsistencias.

Para solucionar dichas inconsistencias es el servicio de directorio común. Dicho directorio proporciona las funcionalidades que las aplicaciones nos reclaman.

Ahora sí, la definición de servicio de directorio podría decirse como una aplicación o un conjunto de distintas aplicaciones que nos ayudan a organizar y almacenar los datos que tenemos sobre usuarios y recursos de la red, permitiendo que los usuarios encargados de la administración gestionen los correctos accesos de los usuarios a los recursos de la red.

Lo más común en este momento es que se establezca la arquitectura cliente-servidor, pero es verdad que hay ocasiones en las que un servidor a su vez puede actuar como cliente de otro servidor por falta de información.

En este momento, la solución que más se usa es el protocolo ligero de acceso a directorio, o LDAP, que funciona de menar muy similar al AD de Microsoft.

4.1.1. Gestión centralizada de usuarios

Cuando queremos disponer de un control eficiente sobre usuarios y tener una política de contraseñas homogénea a la organización, es casi imprescindible contar con un servicio centralizado de autenticación.

Las implementaciones de LDAP más conocidas realmente son el AD de Windows y *OpenLDAP* de Linux.

OpenLDAP nos va a permitir crear un servicio centralizado de autenticación en nuestra estructura para así poder cumplir con los siguientes requisitos:

- Autenticación contra solo un punto de la red que está centralizado.
- Conexiones cifradas con TLS.
- Solo se podrán conectar a los servidores los usuarios que tengan certificados digitales creados por distintas organizaciones aceptados en las estaciones.
- La política de contraseñas será homogénea y robusta.
- Cuando se definan los usuarios se indicarán mediante campos a que máquinas tendrán acceso. Además, las ACL o *Access Control List* nos permitirán que se controlen los accesos y los permisos de los accesos.
- La primera vez que un usuario se autentique sus credenciales quedarán almacenadas de manera temporal para evitar desconexiones frente a caídas temporales.

4.2. Funcionamiento del protocolo ligero de acceso a directorio

LDAP o *Lightweight Directory Access Protocol* consiste en un protocolo que funciona como una aplicación con la que se pueden llevar a cabo consultas acerca de un servicio de directorio para realizar búsquedas de información.

Se define servicio de directorio como aquella aplicación o conjunto de aplicaciones, similar a una base de datos, donde se recoge y gestiona la información acerca de los usuarios y los recursos de una red de ordenadores. También puede actuar como servidor de autenticación, ofreciendo el servicio de contraseña única. Por otro lado, permite utilizar el servicio de directorio como repositorio en el cual conservar la información: configuración, control de accesos, etc. Se trata de una parte relevante del sistema, ya que se facilita un acceso un informe a los usuarios, recursos y otros objetos, ofreciendo una perspectiva global de la red.

La utilidad más importante de un directorio LDAP es la de servidor de autenticación para el acceso a los diferentes servicios de un sistema informático o a una aplicación web. En caso de que se tenga un servidor LDAP y esté configurado para que todos los servicios se verifiquen en él, será suficiente con establecer las cuentas de usuario y grupos en el servidor LDAP para que los usuarios puedan utilizar el sistema y sus servicios desde cualquier punto de la red. Por ello, es un sistema adecuado para reunir la administración de usuarios en un único punto o lugar.

Por último, hay que tener en cuenta que si el servicio de directorio es centralizado habrá un único servidor para todo el servicio de directorio, el cual responderá a todas las consultas de los clientes. Sin embargo, si el sistema está distribuido, serán diferentes servidores los que ofrezcan servicio de directorio

El directorio guarda y gestiona la información mediante estructuras de datos llamadas entradas. A continuación, se muestra la estructura de LDAP:

Estructura de LDAP	
Clases	Se establece cuál es el tipo de objeto que se va a definir, los atributos que va a contener según el tipo de objeto, etc.
Objeto	Son instancias que se crean desde una clase o de varias según los atributos dirigidos a un objeto. Un directorio dispondrá de objetos distintos.
Atributos	Son los campos relacionados con el objeto creado y con sus rasgos o características fijas. En cada atributo existe un valor informativo, como el nombre de usuario, apellidos, etc.

Como se muestra en la siguiente tabla, los atributos en LDAP disponen de una abreviatura:

Atributos de LDAP	
Atributo	**Significado**
Cn	Common-name o nombre
Sn	Surname o apellido
Uid	Userid o nombre de usuario
Mail	E-mail o correo electrónico
Ou	Organizacional unit o unidad organizativa
Des-cription	Description o descripción de un objeto

Ventajas

- Rápido y sencillo en las lecturas y escrituras.
- Se puede replicar el servidor de manera económica y sencilla
- Tiene un modelo de nombres globales que establece que todas las entradas son únicas.
- Puede albergar diferentes directorios
- Se determinan medidas de seguridad mediante SSL
- La mayor parte de las aplicaciones tienen un soporte para LDAP.

Inconvenientes

- Es poco intuitivo y complejo de utilizar, pero hay diferentes instrumentos que facilitan su empleo.

4.3. Seguridad en el protocolo ligero de acceso a directorio

4.3.1. Política de contraseñas

Nos referimos a política o directiva de contraseñas como el conjunto de reglas que se deben aplicar en todas las contraseñas de una organización para poder gestionar estas más fácilmente al mismo tiempo que administrar una mayor seguridad en los directorios con LDAP implantado. Los principales objetivos que tiene este conjunto de reglas son:

- Garantizar el cambio de la contraseña por parte de los usuarios de manera periódica.
- Obligar a los usuarios a que las contraseñas cumplan unos requisitos mínimos de complejidad.
- Obligar a los usuarios a no usar contraseñas antiguas.

4.3.2. Autorización basada en equipos

Host-Based Access Control es el principal nombre de la autorización basada en *host* que nos permite decidir que usuarios pueden o no iniciar sesión en un *host* en específico cuando tenemos LDAP como servidor de autenticación también.

Para esto bastará con la agregación de un nuevo atributo al registro de cada usuario de LDAP donde se incluirán los nombres de los *hosts* en los que sí que puedan iniciar sesión. Como cada cliente comprobará este campo, verá si aparece el nombre de su equipo y en función de esto permitirá o no el acceso a la máquina.

En el fichero */etc/pam.conf* tenemos una directiva que se llama *pam_check_host_attr* que solo se usa en caso de que queramos informar a los usuarios sin acceso de que no pueden entrar con un mensaje. En caso de que así sea, habría que activarla indicando *yes* a continuación.

4.4. OpenLDAP

Este paquete es la implementación de *software* libre que ofrece LDAP para sistemas Linux y BSD.

4.4.1. Instalar y configurar

Para instalar un servidor de *OpenLDAP* sobre *Ubuntu*, lo que lo vamos a hacer es instalar dos paquetes distintos, *slapd ldap-utils*. El comando que debemos de usar en dicha instalación es el siguiente:

```
sudo apt install slapd ldap-utils
```

Cuando comience el proceso de instalación, se nos solicitará una clave para la administración (dos veces, para confirmar):

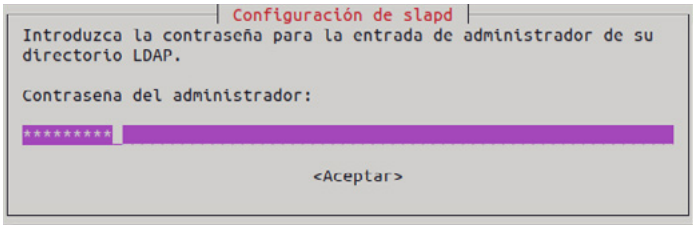

Imagen 1. Contraseña de administración

Hay que aclarar que esta contraseña es solo para el administrador de domino que se crea y no para la configuración.

Cuando ya hemos completado la instalación, podemos configurar el servicio. Para dicha configuración tenemos dos modos:

- El primero es usando los archivos de configuración que se alojan en el directorio */etc/ldap*.
- La segunda, y la más usada, es usando el comando que mostramos a continuación:

  ```
  sudo dpkg-reconfigure slapd
  ```

  Cuando lanzamos este último comando, se nos van a ir haciendo las siguientes preguntas:

- Se nos pedirá si queremos omitir la configuración del servidor, donde tendremos que responder que no para poder configurar el servidor.

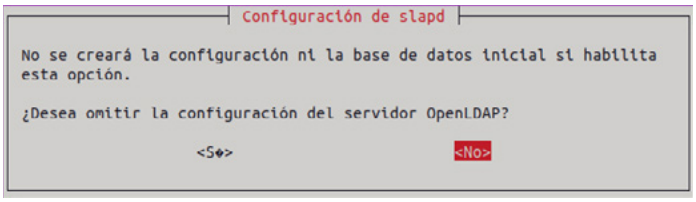

Imagen 2. Configuración *slapd* 1

- Luego nos indican que nombre de dominio se va a configurar para nuestro servicio.

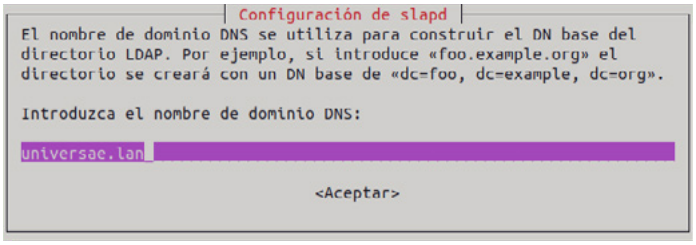

Imagen 3. Configuración de *slapd* 2

- Introducimos el nombre de la organización.

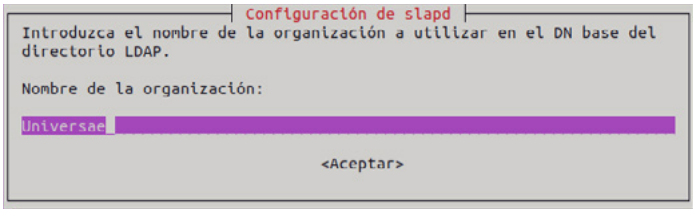

Imagen 4. Configuración de *slapd* 3

- Se nos volverá a pedir la contraseña de administrador.
- Para finalizar la instalación, tendremos dos preguntas más:
  - La primera de estas es si queremos que se borre la base de datos si purgamos el apquete que estamos configurando, a lo que recomendamos decir que sí, para evitar futuras confusiones.
  - La segunda es similar, para mover los ficheros de la base de datos en caso de desinstalación.

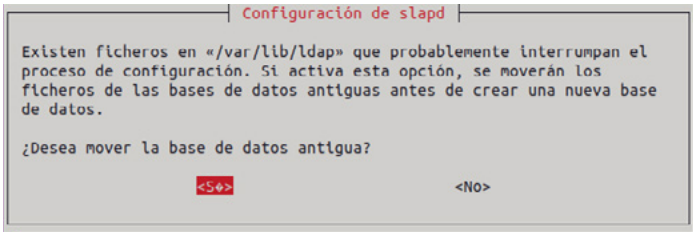

Imagen 5. Configuración de slapd 4

Una vez configurado el servicio, se habrá creado la base de datos.

Si queremos comprobar que dicho servicio se encuentra funcionando de manera correcta con dicha configuración inicial, podemos usar el comando:

```
systemctl status slapd
```

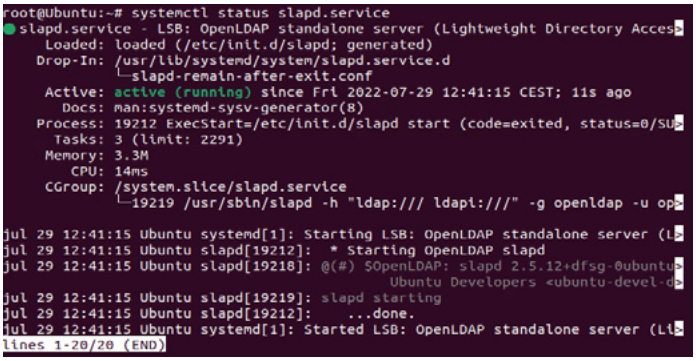

Imagen 6. Comprobación del funcionamiento del servicio

Otra de las pruebas que tenemos a disposición en el servicio *slapd* es usar el comando de a continuación:

```
ldapwhoami -H ldap:// -x
```

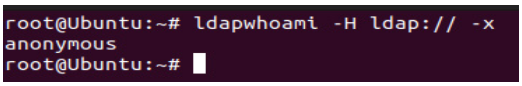

Imagen 7. Comprobación mediante comandos de LDAP

Cuando nos de la salida, debemos de ver que sea *Anonymous*, pues es la lógica ya que no hay ningún usuario configurado en el servicio LDAP.

4.4.2. Llenar la base de datos del protocolo ligero de acceso a directorio

Cuando ya tenemos instalado y con su correcta configuración el servidor de LDAP, debemos de diseña la base de datos para una posterior creación. La intención final de esto es lógicamente la inserción de los datos de usuarios.

La estructura que debemos de seguir en la creación de unidades organizativas, grupos y usuarios, es una estructura jerárquica.

Si queremos ver la información de la configuración previa que hemos hecho, podemos lanzar el comando `slapcat`.

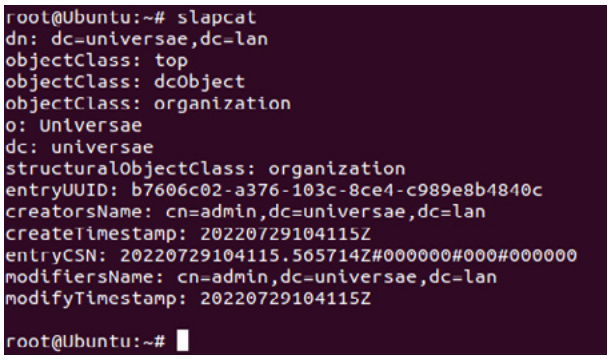

Imagen 8. Comando slapcat

Vemos en la salida de dicho comando que se muestra el DN del dominio que se definió en la configuración previa.

Creación de objetos en el servicio de directorio LDAP

Podemos almacenar en nuestros servicios de directorio cuentas Unix, pero para esto es necesario que se creen unidades organizativas. Estas unidades organizativas deben de ser primeramente dos, una para los usuarios y otra para los grupos. Una vez creadas, ya podríamos crear usuarios.

Para crear las unidades organizativas, debemos de crear un fichero que tenga extensión `.ldif` en nuestra carpeta de trabajo. LA estructura de dicho fichero debe de ser la siguiente:

```
dn: ou=unidad_organizativa,dc=dominio,dc=dominio
objectClass: organizationalUnit
objetcClass: top
ou: unidad_organizativa
description: descripción de la unidad
```

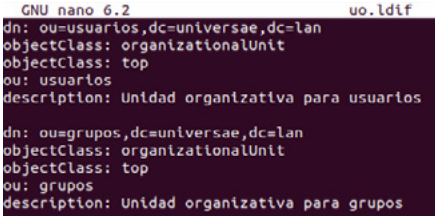

Imagen 9. Fichero para unidades organizativas

Vamos a indicar ahora que significan los distintos atributos que hemos especificado anteriormente:

- El atributo `dn` nos indica la ruta absoluta de la que va a formar parte el objeto de tipo `ou`, es decir, unidad organizativa.
- El atributo `objectClass` indica de que clase es el atributo que se está creando.
- La segunda clase, `top`, no es obligatorio que se ponga, pero se hace con la intención de que la clase `organizationalUnit` herede de ella. Esto es aconsejable.
- El último de los atributos también es opcional, ya que es una simple descripción.

Para crear usuarios, de nuevo creamos un fichero con la misma extensión y estructura:

```
dn:  cn=usuario,ou=unidad_organizativa,dc=dominio,dc=dominio
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
obejctClass: top
cn: usuario
gidNumber: gid
homeDirectory: directorio_usuario
loginShell: /bin/bash
sn: información_complementaria (second name)
uid: login
uidNumber: uid
userPassword: contraseña
```

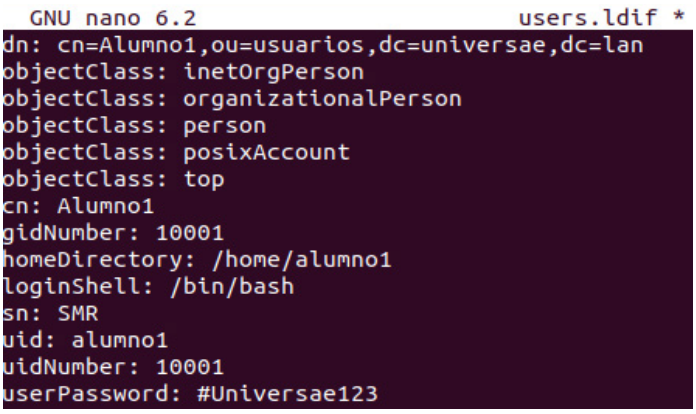

Imagen 10. Fichero para usuarios

En este caso, los atributos que debemos tener en cuenta son:

- El atributo `dn` indica la ruta absoluta donde se va a alojar el usuario creado, que es de tipo *cn, Common Name*.
- Los atributos de `objectClass`, en los que hemos definido varias clases.
- `gidNumber`, el GID del grupo principal de usuario.
- `homeDirectory`, el directorio *home* del usuario.
- `loginShell`, el *Shell* de Linux en el que iniciará sesión el usuario, por defecto, */bin/bash*.
- `sn`, es información complementaria o *Second Name*.
- `uid` es el nombre que usará el usuario para *loguear*.
- `uidNumber` hace referencia al UID del usuario.
- `userPassword` es la contraseña que el usuario debe de indicar para autenticar.

Podemos añadir a estas definiciones tam bién cualquiera atributo que empiece por *shadow* y se encuentre definido en el fichero */etc/shadow* para indicar que se apliquen estos efectos a los campos de dicho fichero.

Para los grupos, podemos crear un mismo fichero de nuevo con la misma extensión, y una estructura bastante similar.

Imagen 11. Fichero para grupos

Hay que destacar dos atributos que cambian con respecto al usuario:

- `gidNumber:` se indica cual será el GID del grupo.
- `memberUid:` para indicar el UID de los miembros que se albergarán.

Para finalizar, si queremos dar de alta las unidades organizativas, los usuarios y los grupos en el servicio de directorio, debemos de hacerlo con el siguiente comando:

```
ldapadd -c -x -D cn=admin,dc=dominio,dc=dominio -W -f
fichero.ldif
```

```
root@Ubuntu:~# ldapadd -c -x -D cn=admin,dc=universae,dc=lan -W -f uo.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=universae,dc=lan"
ldap_add: Already exists (68)

adding new entry "ou=grupos,dc=universae,dc=lan"

root@Ubuntu:~#
```

Imagen 12. Añadir unidades organizativas

```
root@Ubuntu:~# ldapadd -c -x -D cn=admin,dc=universae,dc=lan -W -f users.ldif
Enter LDAP Password:
adding new entry "cn=Alumno1,ou=usuarios,dc=universae,dc=lan"
```

Imagen 13. Añadir usuarios

```
root@Ubuntu:~# ldapadd -c -x -D cn=admin,dc=universae,dc=lan -W -f groups.ldif
Enter LDAP Password:
adding new entry "cn=alumnos,ou=grupos,dc=universae,dc=lan"

root@Ubuntu:~#
```

Imagen 14. Añadir grupos

4.4.3. Comandos básicos del protocolo ligero de acceso a directorio

Búsqueda de objetos en el servicio de directorio LDAP

La información que hemos creado y almacenado anteriormente es susceptible de ser buscada para mirar datos o información concreta. Esta búsqueda se puede hacer a través de comandos en el servicio de directorio LDAP. El comando para buscar es `ldapsearch`, que tiene numerosas opciones y no las vamos a explicar todas. En los siguientes ejemplos tenemos algunas:

- Buscar toda la información de un usuario:

```
root@Ubuntu:~# ldapsearch -xLLL -b dc=universae,dc=lan uid=alumno1
dn: cn=Alumno1,ou=usuarios,dc=universae,dc=lan
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Alumno1
gidNumber: 10001
homeDirectory: /home/alumno1
loginShell: /bin/bash
sn: SMR
uid: alumno1
uidNumber: 10001

root@Ubuntu:~#
```

Imagen 15. Búsqueda de usuario

- Buscar toda la información de un grupo:

```
root@Ubuntu:~# ldapsearch -xLLL -b dc=universae,dc=lan cn=alumnos
dn: cn=alumnos,ou=grupos,dc=universae,dc=lan
objectClass: posixGroup
objectClass: top
cn: alumnos
gidNumber: 10001
memberUid: alumno1

root@Ubuntu:~#
```

Imagen 16. Búsqueda de grupos

Borrar objetos en el servicio de directorio LDAP

Los objetos que creamos en el directorio también se pueden borrar con el comando `ldapdelete`. De nuevo, como pasaba con el comando anterior, ten2emos muchísimas opciones para borrar todo tipo de objetos.

En nuestro ejemplo, borramos un usuario.

```
root@Ubuntu:~# ldapdelete -x -W -D cn=admin,dc=universae,dc=lan "cn=alumno1,ou=
usuarios,dc=universae,dc=lan"
Enter LDAP Password:
root@Ubuntu:~# ldapsearch -xLLL -b dc=universae,dc=lan uid=alumno1
root@Ubuntu:~#
```

Imagen 17. Borrado de usuario

Modificación de objetos en el servicio de directorio LDAP

Ya hemos visto como crear, buscar y borrar objetos del servicio de directorio LDAP, y ahora le toca el turno a como modificar los objetos.

Para realizar estas modificaciones hay que tener en cuenta que se hacen sobre los atributos que hemos descrito cuando los hemos creado. El comando que debemos de usar es `ldapmodify`, con muchas opciones, por supuesto.

Estas modificaciones se hacen a tr5avñes de un nuevo fichero creado también con extensión *.ldif* y es muy similar a la creación de los objetos.

En el siguiente cuadro podemos ver las tres opciones que tenemos de modificación:

Opciones de modificación de objetos en LDAP	
Comando	**Acción**
`add`	Añade un atributo al objeto, al cual hay que darle un valor.
`replace`	Cambia el valor de un atributo ya definido, habrá que indicar dicho valor.
`delete`	Elimina uno de los atributos especificados.

Tenemos a continuación ejemplos de cómo se haría cada una de las modificaciones que hemos nombrado en el cuadro anterior:

- Cambiar un atributo:

```
  GNU nano 6.2                    cambiar_usuarios.ldif *
dn: cn=alumno1,ou=usuarios,dc=universae,dc=lan
changetype: modify
replace: homeDirectory
homeDirectory: /home/alumno
```

Imagen 18. Cambiar un atributo 1

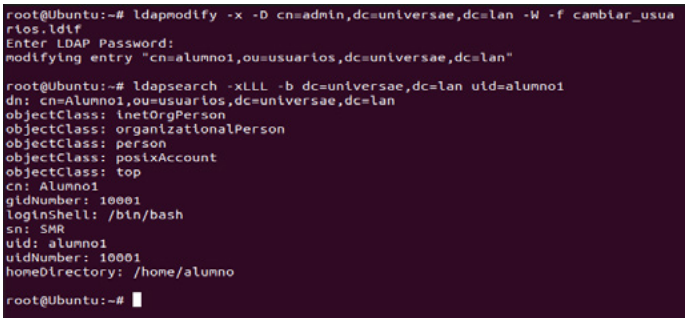

Imagen 19. Cambiar un atributo 2

- Añadir un nuevo atributo:

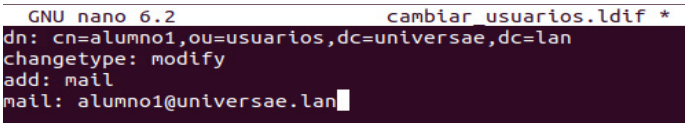

Imagen 20. Añadir un atributo 1

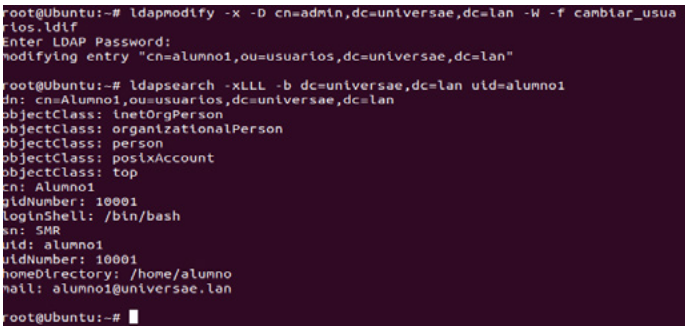

Imagen 21. Añadir un atributo 2

- Eliminar un atributo existente:

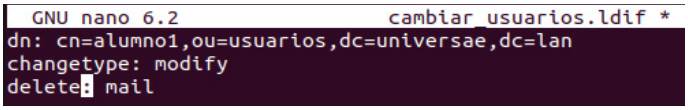

Imagen 22. Eliminar un atributo 1

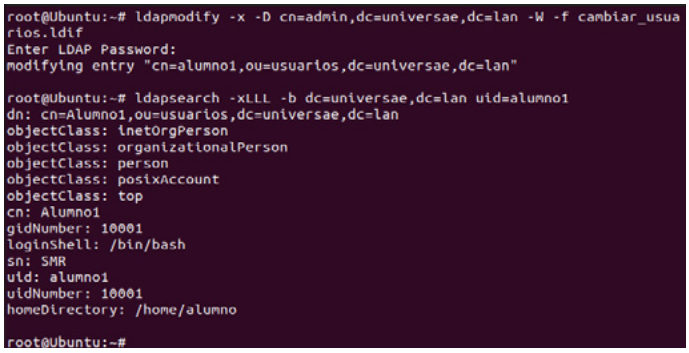

Imagen 23. Eliminar un atributo 2

Hay que saber también, que se pueden cambiar varios atributos a la vez con el mismo fichero, pero separando cada atributo por una línea compuesta únicamente de un guion, "-".

4.4.4. Política de contraseñas

Para implementar las directivas de contraseñas en *OpenLDAP* se usan la superposición de directivas de contraseñas definidas como *ppolicy*. Esta es la más reciente de las implementaciones de las propuestas de directivas de contraseña IETF para LDAP. Entre los mecanismos que nos incluye podemos destacar:

- Envejecimiento de contraseñas, hay desde mínimas y máximas.
- Calidad de contraseñas.
- Bloqueo de cuentas de manera automática.
- Reutilización de contraseñas y control de duplicación.
- Hay ciertos tiempos de espera de la cuenta.
- Se debe restablecer la contraseña de manera obligatoria en ciertos casos.
- El contenido de la contraseña debe de ser aceptable.
- Inicios de sesión de gracia para que se pueda iniciar sesión con contraseñas caducadas durante un pequeño periodo de tiempo una vez pasada la fecha de caducidad.

4.5. phpLdapAdmin

Para administrar el servidor de LDAP de manera más amigable y sencilla tenemos a nuestra disposición una herramienta gráfica vía web, que es *phpLdapAdmin*. La vista que se nos muestra se basa en árbol jerárquico, que nos permite navegar sobre todo el directorio además de incluir funciones de búsqueda, lo que ayuda a la hora de consultas y gestiones del directorio.

Para instalar esto deberemos de instalar el paquete `phpldapadmin` y este mismo instalará todas las dependencias necesarias.

Una vez realizado esto, para la conexión usaremos la siguiente dirección en el navegador web:

http://localhost/phpldapadmin

4.6. LDAP sobre SSL/TLS con OpenLDAP

Con *OpenLDAP* tenemos la opción de configuración que nos permite realizar conexiones cifradas con *OpenSSL*.

Por lo general, las consultas que el servidor de LDAP recibe vienen dadas por el puerto 389, el del protocolo LDAP. Pero estas vienen sin cifrar. Por otro lado, si lo que queremos es establecer un cifrado de los datos mediante SSL, necesitaremos que se use el puerto 636, que es el que viene dado para el protocolo LDAP seguro o *ldaps*.

Para que todo esto cobre un sentido, debemos de tener un certificado firmado por una entidad certificadores y realizar una configuración de *slapd* que permita el uso de dichos certificados. Los pasos que vamos a ir realizando para esto son los siguientes:

1. Establecer una nueva entidad certificadora.
2. Crear petición de firma de certificado del servidor.
3. Firmar el certificado con la autoridad certificadora.
4. Copiar los certificados a la carpeta que queramos, renombrarlos y protegerlos.
5. Configurar *slapd* para que use los certificados.
6. Modificar el script de inicio de *slapd* para que use el protocolo seguro *ldaps*.
7. Reiniciar *slapd*.

Es por esto por lo que el paso que debemos seguir una vez que hemos instalado y configurado *OpenLDAP* es configurar SSL/TLS para conseguir un mayor nivel de seguridad en las comunicaciones entre servidor y clientes, aunque realmente antes la seguridad era prácticamente nula.

Da igual el entorno sobre el que trabajemos, porque *OpenLDAP* no nos permite trabajar con un certificado autofirmado, es decir, es imprescindible trabajar con un certificado válido. Entonces para esto, tenemos diversas alternativas: adquirir un certificado firmador por una entidad reconocida, generar un certificado gratuito o crear nuestra propia autoridad certificadora autofirmada.

Si quisiéramos realizar dichas opciones, deberíamos de usar el comando **openssl**.

4.7. Redes heterogéneas

Una de las principales funciones de un correcto sistema en red es el almacenamiento de la información para facilitar su gestión. Lo más común actualmente es que las empresas tengan varios entornos de red heterogéneos, es decir, que existan varios tipos de plataformas presentes y con distintas redes virtuales conectadas físicamente e incluso distribuidas geográficamente.

Una correcta red heterogénea con un servidor LDAP a modo de ejemplo puede ser como la siguiente imagen:

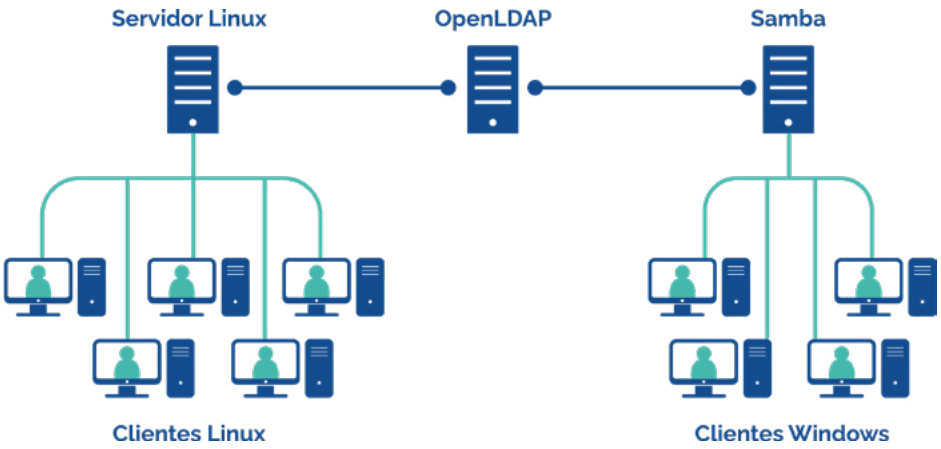

Imagen 24. Red heterogénea

Para que nuestro servicio LDAP esté siempre disponible, podemos usar las mejores soluciones gratuitas actuales, por ejemplo, integrarlo con PAM para la autenticación de clientes Linux y con Samba para la autenticación de clientes Windows. Además, como hemos hablado antes todos los datos deben de ir protegidos con *TLS*.

www.universae.com