Autenticació d'usuaris amb LDAP

NSS :

NSS (“Name Service Switch”) es un conjunto de librerías (con ruta /lib/libnss_* o /lib/x86_64-linux-gnu/libnss_*) que permiten a las aplicaciones programadas haciendo uso de ellas utilizar de forma coherente y común un conjunto de orígenes de datos conteniendo las equivalencias de nombres de distintos ítems, como máquinas, redes, nombres de protocolos, usuarios, grupos, etc. En otras palabras: las “aplicaciones NSS” son capaces de acceder al fichero /etc/nsswitch.conf, el cual indica qué orígenes de datos se pueden utilizar para resolver los distintos tipos de nombres que dichas aplicaciones necesitan.

Por ejemplo, para obtener la información sobre los nombres de usuarios reconocidos por el sistema, las “aplicaciones NSS” consultarán /etc/nswitch.conf para saber si la han de obtener de los ficheros locales (/etc/passwd y /etc/shadow) o bien de alguna base de datos remota (como pudiera ser un servidor Ldap), o bien complementar ambos orígenes para que si falla el predeterminado se utilice el otro. Otro ejemplo: para conocer la correspondencia entre nombres de máquinas y su ip, las “aplicaciones NSS” consultarán /etc/nswitch.conf para saber si primero han de consultar en un servidor DNS o bien pueden obtener la información del fichero /etc/hosts, o bien pueden complementar ambos orígenes en un orden determinado.

El objetivo de NSS es que las aplicaciones que hagan uso de este sistema puedan obtener este tipo de información (nombres de usuarios y sus contraseñas, nombres de máquinas, de redes, de protocolos, etc) preguntando directamente a NSS sin tener que conocer el lugar exacto donde está almacenada, (ya que para obtenerla ya se encarga NSS).

Un ejemplo de archivo /etc/nswitch.conf muy simple sería el siguiente:

```
passwd: files
group: files
shadow: files
hosts: files dns
networks: files
protocols: files
services: files
ethers: files
```

...donde se indica que la base de datos de usuarios que se va a utilizar es el fichero local /etc/passwd (por el valor “files”), la de grupos es el fichero local /etc/group, la de contraseñas es el fichero local /etc/shadow, la de nombres de máquinas será en primera instancia el fichero local /etc/hosts (ver *man hosts* para más información sobre este fichero, o también http://en.wikipedia.org/wiki/Hosts_%28file%29), y, si no se encuentra el nombre allí, entonces se procederá (ya que tras “files” está el valor “dns”) a realizar una búsqueda DNS en los servidores configurados en /etc/resolv.conf; los nombres de redes se buscarán en el fichero local /etc/networks (ver *man networks* para más información sobre este fichero), los de los protocolos en el fichero local /etc/protocols (ver *man protocols* para más información sobre este fichero), los de los servicios en el fichero local /etc/services (ver *man services* para más información sobre este fichero) y la correspondencia estática entre direcciones MAC e Ips en el fichero local /etc/ethers (ver *man ethers* para más información sobre este fichero).

PAM :

Ya hemos visto que PAM es un sistema que hace de intermediario entre los programas y los distintos métodos de autenticación, de forma que éstos sean transparentes para los primeros. Esto permite que, sin realizar modificaciones en los programas, podamos utilizar métodos que vayan desde el uso típico de un nombre de usuario y una contraseña, hasta dispositivos que faciliten identificación biométrica (lectores de huellas, de voz, de imagen, etc.). PAM complementa a NSS porque mientras éste se centra en la búsqueda y mapeo de nombres de usuarios, PAM controla la autenticación propiamente dicha.

LDAP :

LDAP (“Lightweight Directory Access Protocol”) es un protocolo de nivel de aplicación que permite acceder a un “servidor de directorio”. Por “directorio” se entiende un conjunto de datos organizados de una manera lógica y jerárquica en forma de elementos llamados “entradas”, los cuales poseen diversos atributos. Cada entrada representa un objeto que puede ser abstracto o real (una persona, un mueble, una función en la estructura de una empresa, etc). La utilidad de un servidor de directorio radica en ofrecer dichos objetos a la red de una forma centralizada (y, opcionalmente, transparentemente distribuida). Se puede entender que un servidor de directorio pueda ser equivalente a un servidor de bases de datos, pero su sistema de almacenamiento es diferente y su manera de consultar y manipular la información contenida en él también.

Aunque no tiene por qué ser así siempre, el tipo de información que suele encontrarse en la mayoría de ocasiones en un servidor LDAP es típicamente aquella relacionada con la autenticación centralizada de usuarios (nombre, contraseña, uid, grupo, permisos, etc), o con la autenticación centralizada de máquinas (nombre, dirección MAC, dirección IP, etc). También puede contener información complementaria de usuarios (correo, teléfonos, dirección, etc) o configuraciones centralizadas de aplicaciones y certificados, etc.

Para definir los atributos que tendrán las entradas almacenadas en un servidor LDAP podemos hacer uso de las llamadas “Reglas de Esquema”. Éstas son plantillas que especifican qué atributos formarán la entrada de forma obligatoria y cuáles de forma optativa (a modo de “esqueleto” de la entrada). La “Regla de Esquema” concreta utilizada por una entrada determinada se indica en su atributo especial objectClass; esta Regla se puede escoger de entre un conjunto de Reglas estandarizadas que ofrece todos los servidores LDAP. También podríamos crear nuestras propias Reglas de Esquema (o modificar alguna existente), pero no suele ser necesario porque las Reglas predefinidas cubren la mayoría de casos prácticos.

Entre los atributos que suelen emplearse para definir una entrada, habitualmente, encontraremos los siguientes, (aunque puede haber muchos más y diferentes, dependiendo de la Regla utilizada):

uid (user id): Identificador de la entrada. ¡No confundir con el uid de usuario!
objectClass: Indica el tipo de entrada (la Regla que la define)
cn (common name): Nombre de la persona representada en la entrada
sn (surname): Apellido de la persona.
mail: dirección de correo electrónico de la persona.
o (organization): Departamento al que pertenece la persona.
ou (organizational unit): Contenedor estructural (a modo de “carpeta”) dentro del cual está categorizada esta entrada

Tal como se puede ver, en el caso anterior se ha utilizado una Regla (muy típica, por otro lado) que hace referencia a objetos representando empleados de una empresa. En el caso de carecer de atributo “uid”, el atributo que suele hacer de identificador de la entrada suele ser “cn”.

Las entradas se organizan en una estructura jerárquica en forma de árbol invertido. Tradicionalmente, la parte superior de esta estructura refleja la jerarquía de los dominios DNS (incluso regionales) de la organización, de manera que las entradas que representan a la compañía (como “pepsi.com”, “unicef.org” o “yahoo.es”) aparecen en el árbol por encima de otras entradas que representan unidades organizativas internas. Las primeras suelen identificarse por la presencia del atributo “dc” (domain component), y para cada subdominio hay una (dc=”pepsi” y dc=”com” para “pepsi.com”, dc=”unicef” y dc=”org” para “unicef.org”, etc). Dentro de las últimas es donde se encuentra la información relativa a usuarios, máquinas, documentos o cualquier otra cosa que queramos.

Sea del tipo que sea (“domain component” o no) y represente lo que represente, toda entrada posee un único “Nombre Distinguido” -“Distinguised Name” (DN)-, que sirve para identificarla de manera unívoca. El DN, de hecho, se construye a partir del identificador de la entrada en sí misma (lo que se llama “Nombre Relativo Distinguido” -”Relative Distinguished Name” (RDN)-, y que suele ser el valor de su atributo “uid” o bien “cn” -o “ou” en el caso de las unidades organizativas-) concatenado con los identificadores de las entradas de sus antecesores separados por comas. Por ejemplo: si el DN de una entrada es “uid=pperez,ou=empleados,dc=nike,dc=es”, nos estaremos refiriendo a una entrada (cuyo RDN es

"uid=pperez") que contiene información sobre el empleado Pperez perteneciente a la sección española de Nike. Para conocer toda esa información, deberíamos observar el resto de atributos de esa entrada (objetClass, cn, givenname, sn, o,mail ...).

LDAP tiene definidas las operaciones necesarias para interrogar y actualizar el directorio (adicionar y borrar una entrada, modificar una entrada existente, cambiar el nombre de una entrada, etc). No obstante, la mayor parte del tiempo LDAP se utiliza para buscar información almacenada en el directorio: las operaciones de búsqueda permiten que en una porción del directorio se busquen entradas que cumplan con algún criterio especificado en el filtro de búsqueda.

Algunos servidores de directorio no tienen protección y permiten que cualquier persona consulte la información que contienen, pero LDAP provee un mecanismo para que los clientes se autentiquen, (o al menos confirmen su identidad) para garantizar un control de acceso y proteger así la información que el servidor contiene.

Nosotros utilizaremos la infrastructura LDAP para poder loguearnos en un PC mediante un usuario y contraseña guardados en forma de entrada dentro de un servidor de directorio, obteniendo además información adicional sobre dicho usuario para poder asignarle los permisos adecuados.

Instalación y configuración del servidor OpenLDAP:

Nosotros utilizaremos el software OpenLDAP (http://www.openldap.org) sobre Debian/Ubuntu por ser uno de los más extendidos y con mayor historia y documentación, pero existen varios servidores LDAP más en el ecosistema Linux (ver cuadro adjunto):

Otros servidores LDAP libres son:

Apache Directory Server (http://directory.apache.org/apacheds). Incluye servidor Kerberos integrado.
389 Directory Server (http://directory.fedoraproject.org) . Servidor LDAP "nativo" de Fedora.
OpenDJ (https://github.com/OpenIdentityPlatform/OpenDJ)

También hay que destacar la existencia de soluciones integradas formadas por un servidor LDAP más otros servidores que complementan la funcionalidad de dicho servidor LDAP, facilitando en gran medida la integración de todos estos servicios (muy habitualmente utilizados en conjunto) entre sí. Ejemplos son:

FreeIPA (http://www.freeipa.org) : Servidor LDAP 389 Directory Server + Servidor Kerberos (tipo MIT) + Servidor DNS propio + Servidor NTP propio + Autoridad Certificadora. Es la solución elegida por Fedora
Samba4 (http://www.samba.org) : Servidor LDAP propio + Servidor Kerberos (tipo Heimdal) + Servidor DNS propio + Servidor NTP propio + Servidor de compartición de carpetas.

Por otro lado, comentar que Microsoft ofrece también una "suite" de servidor LDAP + Kerberos + DNS + NTP (entre otros) llamado "Active Directory", integrada en las versiones "Server" de sus sistemas Windows para poder almacenar y gestionar de forma centralizada la información de sus dominios de administración (usuarios, equipos, configuraciones, permisos, etc).

Los pasos a seguir para configurar un servidor LDAP que contenga la información necesaria para autenticar usuarios (y los pasos a seguir para configurar un cliente LDAP para que acceda a ella) se detallan a continuación:

1.-Deberás utilizar dos máquinas virtuales: una de ellas hará de servidor LDAP y la otra hará de cliente. Asegúrate que ambas tengan, además de una tarjeta en modo NAT para poder conectarse a Internet, una tarjeta en modo red interna con una IP fija (en este documento supondremos que tienen la 192.168.0.1 y 192.168.0.2, respectivamente) y de que la máquina que haga de cliente tenga instalado un entorno gráfico con navegador y gestor de ficheros (bastará hacer *sudo apt install gdm firefox nautilus* para ello).

a) Antes de instalar nada, a la máquina que hará de servidor LDAP dale un nombre que tenga una estructura similar a un nombre DNS (por ejemplo, en este documento usaremos el de "miservidor.midominio.local"). De hecho, la infrastructura básica de una red con servidor LDAP integrado se debería completar con un servidor DNS más pronto que tarde (para, entre otras cosas, no tener que configurar el archivo /etc/hosts de los clientes individualmente -como tendremos que hacer más adelante-), pero para no complicar más las cosas, realiza estos dos simples pasos y ya está:

> *Ejecuta el comando ***sudo hostnamectl set-hostname miservidor.midominio.local***. Esto hará que el fichero /etc/hostname contenga el nuevo nombre "tipo DNS" de nuestro servidor (lo puedes comprobar también con el comando *hostnamectl status*).
>
> *Modifica manualmente el contenido del archivo **/etc/hosts** para que 127.0.0.1 está asociado al "miservidor.midominio.local" en vez de a "localhost". Una vez hecho estos dos pasos, reinicia la máquina.
>
> NOTA: Que el nombre del servidor sea de tipo DNS es necesario para que las entradas "dc" de nuestro servidor LDAP se correspondan con los subdominios de dicho nombre. Es decir, al generar la base de datos de nuestras entradas en forma de árbol invertido, todas ellas deberán colgar de un DN base que en nuestro caso será "dc=midominio,dc=local".

b) Instala el software básico: ***sudo apt install slapd ldap-utils*** (el primer paquete es el servidor propiamente dicho, el segundo son las herramientas de administración; en Fedora reciben el nombre de "openldap-servers" y "openldap-clients", respectivamente). Durante el proceso de instalación aparecerá un mensaje que solicita la contraseña necesaria para administrar el servidor LDAP: introduce una cualquiera PERO ACUÉRDATE DE ELLA a partir de ahora.

c) Instala el software necesario para convertir el servidor LDAP en un servidor específico de autenticación: ***sudo apt install ldap-auth-config*** (se instalarán como dependencias, entre otros, los paquetes "libnss-ldap" y "libpam-ldap"). Durante el proceso de instalación aparecerá un asistente que irá solicitando diversa información:

> *Primero pide la dirección IP del servidor IP (en nuestro caso, 192.168.0.1 -es importante cambiar el principio para que sea "ldap://"-).
>
> *Después pide el DN base de nuestro servidor ("dc=midominio,dc=local")
>
> *Tras elegir la versión 3 del protocolo, a continuación indicaremos que sí queremos que las utilidades que utilicen PAM se comporten del mismo modo que si utilizáramos contraseñas locales (esto hará que las contraseñas se guarden en un archivo independiente que sólo podrá ser leido por el administrador)
>
> *Seguidamente, diremos que no es necesario identificarnos para hacer consultar a la base de datos (es mucho más sencillo realizar consultas anónimas al no tener que incluir ninguna contraseña en los clientes de la red) pero sí indicaremos el nombre de la cuenta LDAP que tendrá privilegios para realizar cambios en el directorio: debemos escribir un DN tal como "cn=admin,dc=midominio,dc=local" (donde el nombre "admin" podría ser cualquier otro) y a continuación introducir la misma contraseña que introdujimos en el apartado *b)*
>
> *Finalmente, deberemos elegir, si lo pregunta, el método "crypt" para la gestión de la encriptación de las contraseñas de los usuarios que guardaremos.

NOTA: Si más adelante observamos algún error o necesitamos efectuar alguna modificación en los datos introducidos, sólo tendremos que ejecutar el siguiente comando: *sudo dpkg-reconfigure ldap-auth-config* o bien editar directamente el archivo */etc/ldap.conf* (que es donde se han guardado todos estos datos) y reiniciar el servidor.

d) Modifica los archivos de configuración de NSS y PAM del servidor para configurar cómo el proceso de autenticación de los clientes. Concretamente:

*Modifica las siguientes líneas de /etc/nsswitch.conf para que queden así:

```
passwd: files ldap
group: files ldap
shadow: files ldap
```

*Ejecuta el comando ***sudo pam-auth-update*** y elige todos los módulos PAM para habilitarlos (aunque de forma predeterminada aparecen todos marcados, así que no hay que hacer nada aquí).

e) Configura el servidor LDAP propiamente dicho para poderlo empezar a utilizar mediante el comando ***sudo dpkg-reconfigure slapd*** . En el asistente que aparece, se nos mostrará para lo que confirmemos) el nombre DNS de nuestro servidor ("miservidor.midominio.local"), el DN base ("cn=midominio,cn=local") y la contraseña de administración que introdujimos en el primer punto, pero además nos preguntará sobre el formato interno de base de datos a usar (elegiremos "HDB"), sobre si deseamos eliminar la base de datos si desinstaláramos el servidor (contestaremos que sí) y un par más de preguntas que contestaremos con la opción por defecto.

Administración básica del directorio:

Ya tenemos el servidor LDAP funcionando (*sudo systemctl status slapd*) y escuchando en el puerto 389 TCP. Ahora deberíamos generar la estructura de entradas de nuestro directorio y rellenarlas de datos.

La forma más básica de añadir información al directorio es utilizar ficheros de texto cuyo contenido está escrito en el formato LDIF (LDAP Data Interchange Format). El formato básico de una entrada es:

```
# comentario
dn: <nombre global único>
<atributo>: <valor>
<atributo>: <valor>
...
```

Entre dos entradas consecutivas debe existir siempre una línea en blanco. Por otro lado, si una línea es demasiado larga, podemos repartir su contenido entre varias, siempre que las líneas de continuación comiencen con un carácter de tabulación o un espacio en blanco.

Una vez creados estos ficheros, para añadirlos al directorio (incluso con el servidor en marcha) podemos utilizar el comando *ldapadd* (del paquete "ldap-utils"). La mayoría de veces necesitaremos indicar cuatro parámetros: -f fichero.ldif (para indicar el fichero cuyo contenido se desea agregar), -D "cn=admin,dc=midominio,dc=local" (para indicar la cuenta con la que nos autenticaremos en el servidor LDAP para realizar la modificación del directorio; esta cuenta ha de tener privilegio para ello, y por tanto, ha de ser la cuenta indicada en el punto c) del ejercicio anterior), -W (para que se solicite la contraseña de dicha cuenta interactivamente a continuación) y -x (para indicar que esta cuenta se autenticará de forma simple).

NOTA: Todos los comandos del paquete "ldap-utils" disponen además del parámetro *-H ldapi:///ipServidor* para poder indicar el servidor LDAP contra el cual se van a ejecutar; esto es muy útil para utilizar estos comandos en un ordenador diferente del propio servidor.

2.- a) Crea un fichero llamado “base.ldif” con el contenido mostrado a continuación y seguidamente agrégalo al directorio con el comando: *ldapadd -x -D cn=admin,dc=midominio,dc=local -W -f base.ldif* . Con esto habrás generado dos entradas de tipo “unidad organizativas” que servirán para contener (a modo de “carpetas”) los usuarios y grupos que generaremos a continuación.

```
dn: ou=usuarios,dc=midominio,dc=local
objectClass: organizationalUnit
ou: usuarios

dn: ou=grupos,dc=midominio,dc=local
objectClass: organizationalUnit
ou: grupos
```

b) Crea un fichero llamado “grupos.ldif” con el siguiente contenido y seguidamente agrégalo al directorio con un comando similar al del apartado anterior:

```
dn: cn=grupoldap,ou=grupos,dc=midominio,dc=local
objectClass: posixGroup
cn: grupoldap
gidNumber: 10000
```

c) Crea un fichero llamado “usuarios.ldif” con el siguiente contenido y seguidamente agrégalo al directorio con un comando similar al del apartado anterior:

> NOTA: Tal como se puede ver, cada objeto “usuario” está formado a partir de la unión de diferentes tipos predefinidos de objeto (posixAccount, shadowAccount, inetOgPerson), donde cada uno aporta un determinado conjunto de atributos: posixAccount incluye la información que encontraríamos en el archivo /etc/passwd clásico, shadowAccount incluye la información que encontraríamos en el archivo /etc/shadow clásico y inetOrgPerson incluye información extra del usuario dentro de la organización (como el correo, cód. postal...).
>
> NOTA: Hay que tener **muy en cuenta** que al añadir nuevos usuarios los valores de los atributos uidNumber y homeDirectory (además de userPassword) deben ser diferentes para cada usuario. Lo mismo ocurre con el atributo gidNumber para los grupos. Además, los valores de uidNumber y gidNumber no deben coincidir con el uid y gid de ningún usuario y grupo local de los clientes.

```
dn: uid=usu1ldap,ou=usuarios,dc=midominio,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: usu1ldap
sn: Lopez
givenName: Juan
cn: Juan Lopez
displayName: Juan Lopez
uidNumber: 3000
gidNumber: 10000
userPassword: XXX
gecos: Es muy tonto
loginShell: /bin/bash
homeDirectory: /home/jlopez
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: juan.lopez@gmail.com
postalCode: 29000

####################LINEA EN BLANCO#######################
```

dn: uid=usu2ldap,ou=usuarios,dc=midominio,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: usu2ldap
sn: Perez
givenName: Perico
cn: Pedro Perez
displayName: Pedro Perez
uidNumber: 3001
gidNumber: 10000
userPassword: XXX
gecos: Es un crack
loginShell: /bin/bash
homeDirectory: /home/pperez
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: pedrito@yahoo.es
postalCode: 29001

d) Ahora podemos comprobar si el contenido anterior se ha añadido correctamente. Para ello podemos usar el comando ldapsearch (del paquete "ldap-utils"), el cual permite hacer una búsqueda en el directorio. Concretamente, ejecuta ***ldapsearch -x -LLL -b "dc=midominio,dc=local" uid=usu1ldap sn givenName*** Con este comando de ejemplo estaremos buscando un usuario con uid=usu1ldap y pediremos que nos muestre el contenido de los atributos sn y givenName (se puede no pedir ningún atributo en concreto: en ese caso se muestran todos). El parámetro -LLL sirve para utilizar ldapsearch en modo "no verboso" y el parámetro -b sirve para indicar el DN base a partir del cual se empezará la búsqueda por las entradas inferiores del árbol.

> NOTA: Fijarse que ahora no ha sido necesario utilizar los parámetros -D y -W porque en el apartado c) del primer ejercicio indicamos que para realizar consultas no se necesitaba realizar ninguna autenticación.

Otros comandos importantes del paquete "ldap-util" son *ldapdelete* y *ldapmodify*. Un ejemplo del primero (bastante evidente) podría ser: ***ldapdelete -x -D "cn=admin,dc=midominio,dc=local" -W "uid=usu2ldap,ou=usuarios,dc=midominio,dc=local"*** . El segundo tiene tres formas de modificar una entrada: añadiendo un nuevo atributo, eliminando un atributo existente o modificando el valor de un atributo. Para cambiar el uidNumber de un usuario, por ejemplo, podríamos hacer ***ldapmodify -x -D "cn=admin,dc=midominio,dc=local" -W -f fichero.cambios*** donde "fichero.cambios" debería tener un contenido como el siguiente (donde se especifica qué entradas se quieren modificar y de qué manera):

dn:uid=usu2ldap,ou=usuarios,dc=midominio,dc=local
replace:uidNumber
uidNumber:3002

La información anterior la podríamos haber introducido directamente desde la entrada estándar si no hubiéramos especificado el parámetro -f. Para añadir un atributo nuevo deberíamos escribir:

dn:uid=usu2ldap,ou=usuarios,dc=midominio,dc=local
add:jpegPhoto
jpegPhoto:file:///tmp/foto.png

Y para borrarlos:

dn:uid=usu2ldap,ou=usuarios,dc=midominio,dc=local
delete:jpegPhoto

3.-a) Modifica el atributo “gecos” del usuario Juan López para que muestre la descripción: “Ronca”. Comprueba mediante *ldapsearch* que el cambio lo has realizado correctamente

b) Añade el atributo “jpegPhoto” del usuario Juan López indicando la ruta (ficticia) de su foto identificativa. Comprueba mediante *ldapsearch* que el cambio lo has realizado correctamente

c) Elimina el atributo “jpegPhoto” anterior.Comprueba mediante *ldapsearch*que el cambio lo has realizado correctamente

Administración gráfica del directorio:

Los comandos del paquete “ldap-utils” no son las únicas herramientas que disponemos para manipular las entradas del directorio. Otro conjunto de comandos de consola específicamente pensadas para gestionar entradas de usuarios y grupos (pero dependientes de “ldap-utils” en su base) son los incluidos en el paquete “ldapscripts” (http://contribs.martymac.org). A partir de la configuración establecida en el archivo /etc/ldapscripts/ldapscripts.conf, podremos utilizar comandos específicos como *ldapadduser, ldapsetpasswd, ldapdeleteuser,* etc.

No obstante, a la larga necesitaremos alguna herramienta gráfica para realizar este trabajo de una forma más cómoda y rápidamente. Entre las aplicaciones gráficas de administración de directorio podemos destacar **Apache Studio** (http://directory.apache.org/studio) y **Jxplorer** (http://jxplorer.org), ambas multiplataforma. Además, si no nos importa instalar en nuestra máquina de administración un servidor web (Apache + Php), podemos utilizar también **phpLdapAdmin** (http://phpldapadmin.sourceforge.net, algo obsoleta) o **LAM** (https://www.ldap-account-manager.org).

4.-a) Arranca la máquina cliente, la cual utilizaremos ahora mismo como máquina de administración del directorio ofrecido por la máquina servidora. Instala LAM (***sudo apt install ldap-account-manager***); verás como se instala el servidor web Apache como dependencia. Una vez instalado, ejecuta un navegador y escribe **http://127.0.0.1/lam** para acceder a la página inicial de LAM

> NOTA: Si quisiéramos tener la documentación de LAM fácilmente accesible, podríamos hacer un acceso directo que apuntara a ella dentro de la carpeta pública de Apache. Es decir: para consultar la documentación en http://127.0.0.1/lam-docs, ejecutar *ln -s /usr/share/doc/ldap-account-manager/docs/manual /var/www/html/lam-docs*

b) Primero hay que configurar LAM para que pueda contactar con nuestro servidor LDAP. Concretamente, hay que ir al botón “LAM configuration” de la pantalla principal, y allí al enlace “Edit server profiles”, donde teclearemos la contraseña “lam” (sin comillas). A partir de aquí:

En la sección “General settings” debemos indicar:
- *Server address: **ldap://192.168.0.1:389**
- *Activate TLS: no
- *Tree suffix: “dc=midominio,dc=local”

Y más abajo, en “Security settings”:
- *List of valid users: “cn=admin,dc=midominio,dc=local”

Opcionalmente, en la sección “Account types” podemos indicar:
- *Users LDAP suffix: “ou=usuarios,dc=midominio,dc=local”
- *Groups LDAP suffix: “ou=grupos,dc=midominio,dc=local”

*Mediante el botón “X”, eliminar las cuentas de tipo “Hosts” y “Samba domains”, que no usaremos

> NOTA: Opcionalmente, en la sección “Modules” podemos mover el módulo “Samba 3” (sambaSamAccount) a la lista de módulos disponibles, tanto en la sección “Users” como “Groups”, ya que no lo usaremos.

Una vez hecho esto, guardamos los cambios (la configuración de LAM se guarda en /usr/share/ldap-account-manager/config/lam.conf) y ya podremos iniciar sesión en el servidor con el usuario admin y la contraseña indicada en el primer ejercicio. Cancela el aviso que se muestra, pulsa “Tree view” y ya podrás administrar las entradas de una forma cómoda y fácil.

c) Crea un nuevo usuario copiando todos los datos del usuario Perico (a modo de plantilla) con la opción adecuada. Acuérdate sobre todo de cambiar el uidNumber y el homeDirectory del usuario nuevo (además de los otros posibles campos que desees, como el cn, etc).

NOTA: También puedes crear nuevos usuarios a partir de una plantilla preparada en el "Profile editor"

Copias de seguridad del directorio:

Siempre debemos tener a mano un archivo con la copia de seguridad de los datos contenidos en el directorio. Este archivo puede ser generado mediante la opción de exportación de LAM, o bien mediante el comando *sudo slapcat* (sólo ejecutable desde el servidor). Por defecto muestra por pantalla el contenido completo del directorio LDAP en formato LDIF pero podemos volcarlo a un fichero con el parámetro -l, así: **slapcat -l backup.ldif.** Si sólo queremos obtener los datos de un subconjunto del árbol, podemos usar el parámetro -b como viene siendo habitual. Para reestablecer la copia, tan sólo deberemos usar el comando *ldapadd*

5.-a) Crea la copia de seguridad de todo el directorio (con slapcat o LAM, da igual)

b) Borra las unidades organizativas "usuarios" y "grupos" (con todo lo que contienen): usa LAM para ello

c) Comprueba con *ldapsearch* que efectivamente los datos sobre los usuarios se han perdido.

d)Restaura la copia de seguridad y comprueba con *ldapsearch* que efectivamente los datos se han recuperado

Autenticación mediante LDAP en máquinas cliente:

6.-a) Modifica el fichero /etc/hosts de la/s máquina/s cliente/s para que 192.168.0.1 apunte a "miservidor.midominio.local" y reinicia.

b) Repite los apartado c) y d) del punto nº1, esta vez para instalar y configurar los paquetes necesarios que permitan utilizar NSS y PAM como clientes de autenticación y conectarlos al servidor LDAP ya funcional. Las respuestas a dar en el asistente que aparecen son exactamente las mismas que las que se dieron en su momento

NOTA: Es interesante observar en este sentido los cambios producidos automáticamente tras este proceso en los ficheros /etc/pam.d/common-auth, /etc/pam.d/common-account y /etc/pam.d/common-password.

c) Descomenta todas las líneas del archivo /etc/ldap/ldap.conf (correspondiente a la configuración del cliente) y modifica las líneas BASE y URI para que queden así:

BASE dc=midominio,dc=local
URI ldap://miservidor.midominio.local

d) Ejecuta el comando ***getent passwd*** (o ***getent shadow***) para ver si todo ha ido bien. Este comando obtiene las entradas disponibles en los diversos orígenes especificados dentro de /etc/nsswitch.conf para la categoría indicada ("passwd" o "shadow", respectivamente). La gracia está en que este comando junta la información local ("files") con la obtenida a través de la red ("ldap"), por lo que deberíamos ver al mismo tiempo los usuarios locales y los usuarios LDAP.

e) El cliente ya está listo para que nos autentiquemos con una cuenta del servidor LDAP. Sin embargo, si ahora nos identificáramos en el cliente con la cuenta usu1ldap, por ejemplo, encontraríamos que no existe su carpeta personal (/home/jlopez) en el equipo cliente. Lógicamente, podríamos crear dicha carpeta a mano, pero habría que repetir el proceso en cada uno de los clientes en los que el usuario vaya a iniciar sesión. Si queremos que la carpeta se cree automáticamente cuando el usuario inicie sesión por primera vez en un equipo, deberemos hacer uso de un módulo PAM llamado "pam_mkhomedir". Esto lo conseguimos haciendo

una pequeña modificación en el archivo /etc/pam.d/common-session del cliente; concretamente, tenemos que añadir una nueva línea al principio de ese archivo con este contenido:

session required pam_mkhomedir.so skel=/etc/skel umask=0022

f) Ya podemos loguearnos con los usuarios LDAP en un terminal virtual. Pruébalo.

g) Un inconveniente que aún tenemos es que con la configuración actual los usuarios LDAP no pueden cambiar sus propias contraseñas (prueba de ejecutar el comando *passwd* para comprobarlo). Para solucionarlo, deberemos cambiar (con el usuario local que pueda utilizar sudo) el archivo /etc/pam.d/common-password; concretamente debemos borrar las palabras use_authtok try_first_pass de la línea que usa pam_ldap.so. Vuelve a iniciar sesión con un usuario LDAP y comprueba que ahora sí que puedes utilizar el comando *passwd* para cambiar su contraseña

h) Ya podemos loguearnos también con un display manager. El problema es que tanto Gdm como Lightdm sólo incluyen en la lista de usuarios para seleccionar a aquellos que ya conoce (es decir, que han iniciado sesión al menos alguna vez). En el caso de Gdm esto no es demasiado problema porque él mismo ofrece la posibilidad mediante el botón "¿No estás listado?" de introducir el nombre y contraseña que deseemos y así añadir ese nuevo usuario a la lista en próximos inicios, pero en el caso de LightDM, para obligar a que pregunte un nombre de cuenta debemos editar el archivo /etc/lightdm/lightdm.conf y añadir las líneas allow-guest=false y greeter-hide-users=true.

Perfiles móviles con NFS :

Tal como hemos dejado la configuración de los usuarios LDAP hasta ahora, aunque inician sesión correctamente, todavía hay algo que no queda demasiado elegante: un usuario que vaya itinerando entre varios equipos cliente acabará teniendo una carpeta personal en cada uno de los equipos y su contenido no se sincronizará. Es decir, si crea un archivo en el cliente A, no lo encontrará en su carpeta cuando inicie sesión desde el cliente B. Esto es porque LDAP sólo se encarga de autenticar a los usuarios.

Tenemos que conseguir unir las posibilidades de autenticación centralizada en el servidor que ofrece LDAP con la capacidad de almacenamiento centralizado que aporta NFS. El resultado serán los perfiles móviles de usuario. Es decir, un usuario encontrará su carpeta personal en todos los equipos cliente donde inicie sesión. Para ello deberemos recordar cómo funcionaba un servidor NFS (documento anterior de este tema):

7.-a) Instala el servidor NFS en la misma máquina que hace de servidor LDAP (***sudo apt install nfs-kernel-server***) y crea una carpeta que alojará las carpetas personales de los usuarios. Si decidimos que esta carpeta sea "/opt/perfiles", haremos: ***sudo mkdir /opt/perfiles && sudo chown nobody:nogroup /opt/perfiles*** .

b) Debes crear también las carpetas personales individuales de cada usuario (***sudo mkdir /opt/perfiles/jlopez, sudo mkdir /opt/perfiles/pperez***, etc) y asignar a cada una su propietario respectivo (***sudo chown usu1ldap:grupoldap /opt/perfiles/jlopez, sudo chown usu2ldap:grupoldap /opt/perfiles/pperez***...)

> NOTA: Fijarse que podemos ejecutar el comando chown con los usuarios LDAP porque éstos también están reconocidos como usuarios válidos en el propio servidor.

c) Modifica el archivo /etc/exports para compartir el directorio anterior como fsid=0 con permisos de lectura/escritura para todos los usuarios (y reiniciar el servidor). Debería quedar una línea parecida a ésta:

/opt/perfiles *(rw,fsid=0)

d) Crea una carpeta en cada equipo cliente que hará de punto de montaje de los perfiles móviles. Si decidimos que el punto de montaje sea la carpeta "/opt/punto", los comandos a ejecutar son: ***sudo mkdir /opt/punto && sudo chmod 777 /opt/punto***

e) Haz que el montaje de “/opt/perfiles” en “/opt/punto” se produzca nada más arrancar la máquina cliente. Para ello, debemos añadir la siguiente línea al archivo /etc/fstab de cada cliente (¡y después reiniciarlo o ejecutar *mount -a*!):

```
192.168.0.1:/ /opt/punto nfs4 auto,rw,noatime 0 0
```

f) Modifica las cuentas de usuario LDAP existentes (con LAM, por ejemplo) para indicar que su carpeta personal (atributo homeDirectory) se encuentra dentro de la carpeta /opt/punto (por ejemplo, /opt/punto/jlopez, /opt/punto/pperez,...).

g) Ve a la máquina cliente e instala el paquete «nfs-common».

h) Inicia sesión en un terminal virtual de la máquina cliente con un usuario LDAP y crea en su carpeta personal un archivo (con *touch* mismo). Comprueba que dicha carpeta personal es remota observando que efectivamente el fichero se ha creado en el servidor, dentro de la subcarpeta /opt/perfiles/carpeta_personal correspondiente.

i) Inicia sesión gráfica en la máquina cliente con un usuario LDAP, abre el Nautilus y crea una carpeta dentro del escritorio. Comprueba que dicha carpeta se ha creado en el servidor, dentro de la subcarpeta /opt/perfiles/carpeta_personal/Dekstop correspondiente.