Práctica Servidor LDAP y Samba

Supongamos que queremos montar un servidor LDAP para el dominio **empresa.local** en la **red 10.0.0.0/8**.

Índice

Andrés Julián Mayor Leirós
IES San Clemente

Configuración del servidor LDAP

1 Configurar la red en el equipo servidor

Creamos en VirtualBox la “Red NAT” 10.0.0.0/8 sin DHCP y asignamos las máquinas virtuales correspondientes al servidor esta “Red NAT”.

Configuramos la red en el equipo servidor[1] (10.0.0.10), comprobando si no hemos cometido algún error al definir la puerta de enlace (gateway) o los servidores DNS (nameservers) **haciendo un ping a algún servidor externo** que sepamos que siempre está disponible como la página web de Google.

2 Nombre de equipo y resolución empleando /etc/hosts

El nombre del equipo se configura en el fichero /etc/hostname. El contenido de este fichero será el nombre del equipo, por ejemplo,

1 Tendremos que modificar el contenido de los ficheros /etc/network/interfaces y /etc/resolv.conf

```
servidor.empresa.local
```

Es conveniente también configurar el fichero /etc/hosts. Este fichero cumple las funciones del servidor DNS de la red cuando no disponemos de uno. En este fichero tenemos un contenido similar al siguiente:

```
127.0.0.1          localhost
127.0.1.1          ...
...
```

En este caso, lo que hay que hacer es cambiar en el servidor todo el contenido de la segunda línea (127.0.1.1 ...) por el siguiente:

```
10.0.0.10  servidor.empresa.local  servidor
```

3 Modificar y actualizar los repositorios

Modificamos el fichero de configuración necesario para indicar que emplearemos los repositorios oficiales para el servidor (/etc/apt/sources.list) y actualizamos la lista de paquetes disponibles en el repositorio ejecutando en la consola el comando:

```
$ sudo apt update
```

4 Instalar LDAP

En este caso instalaremos los paquetes slapd (el servicio LDAP) y ldap-utils (nos proporciona herramientas para interaccionar con el servicio LDAP).

Ejecutamos en una consola:

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

Durante la instalación nos solicitará la contraseña que deseamos establecer para el administrador LDAP[2] y que la confirmemos.

Una vez finalice la instalación del servicio LDAP es conveniente **confirmar si la instalación se realizó correctamente** mostrando el contenido de la base de datos LDAP ejecutando el comando:

```
$ sudo slapcat
```

A través de su salida podemos ver si ya ha cogido bien los datos (aparece una entrada para cn=admin,dc=instituto,dc=local y no aparece dc=nodomain).

```
$ sudo slapcat
dn: dc=empresa,dc=local
objectClass: top
objectClass: dcObject
```

2 Esta contraseña, por motivos de seguridad, debería cumplir una serie de requisitos de seguridad (tener más de 10 caracteres y contener mayúsculas, minúsculas, dígitos numéricos y signos de puntuación) y ser diferente que la contraseña del usuario administrador local del servidor

Andrés Julián Mayor Leirós IES San Clemente

```
objectClass: organization
o: empresa.local
dc: empresa
structuralObjectClass: organization
entryUUID: e33fc814-e5b9-1038-8243-39a2e6b74e62
creatorsName: cn=admin,dc=instituto,dc=local
createTimestamp: 20190328152831Z
entryCSN: 20190328152831.511390Z#000000#000#000000
modifiersName: cn=admin,dc=instituto,dc=local
modifyTimestamp: 20190328152831Z

dn: cn=admin,dc=empresa,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword::
e1NTSEF9WDIzUEJxbXgycUU3M1dRUmppTVYrZE91U0RNMWswSHE=
structuralObjectClass: organizationalRole
entryUUID: e340fedc-e5b9-1038-8244-39a2e6b74e62
creatorsName: cn=admin,dc=instituto,dc=local
createTimestamp: 20190328152831Z
entryCSN: 20190328152831.519463Z#000000#000#000000
modifiersName: cn=admin,dc=instituto,dc=local
modifyTimestamp: 20190328152831Z
```


Si NO ha recogido bien los datos normalmente se debe a que hemos cubierto mal el contenido de /etc/hosts[3] y debemos reconfigurar el servicio ejecutando el comando:

```
$ sudo dpkg-reconfigure slapd
```

5 Añadir entradas al árbol LDAP

Ahora debemos añadir unidades organizativas, grupos o usuarios al árbol LDAP **empleando ficheros LDIF o** bien instalando alguna herramienta que nos permita gestionar el árbol LDAP **a través de** la interfaz gráfica como puede ser **LDAP Account Manager**.

a) A través de ficheros LDIF

Se verá en el módulo de “Administración de Sistemas Operativos” de 2ª Curso de ASIR

b) A través de una interfaz gráfica

Podemos instalar en el servidor LDAP Account Manager para poder configurar y gestionar a través de cualquier navegador web que abramos un equipo cualquiera de nuestra red. Para

3 Deberíamos revisar su contenido y corregirlo porque el contenido del fichero /etc/hosts también afecta a otras funciones (como por ejemplo sudo)

poder hacerlo necesitamos instalar en el servidor el paquete ldap-account-manager ejecutando el siguiente comando:

```
$ sudo apt install ldap-account-manager
```

Finalizada la instalación de este paquete, ya podemos desde cualquier equipo de la red con interfaz gráfica, como por ejemplo el equipo cliente, acceder a un navegador web y visitar la URL http://*172.16.0.10*/lam[4] para gestionar LDAP tal y como se describe en el apartado 4 de la configuración en el equipo cliente.

Configuración del cliente LDAP

1 Configurar la red en el equipo cliente

Asignamos a la máquina virtual cliente correspondiente la misma "Red NAT" que asignamos al servidor y configuramos la red en el equipo cliente (10.1.0.20), comprobando si no hemos cometido algún error al definir la puerta de enlace (gateway) o los servidores DNS (nameservers) haciendo un ping a algún servidor externo que sepamos que siempre está disponible como la página web de Google

2 Nombre de equipo y resolución empleando /etc/hosts

El nombre del equipo se configura en el fichero /etc/hostname. El contenido de este fichero será el nombre del equipo, por ejemplo,

```
cliente-01.empresa.local
```

Es conveniente también configurar el fichero /etc/hosts. Este fichero cumple las funciones del servidor DNS de la red cuando no disponemos de uno. En este fichero tenemos un contenido similar al siguiente:

```
127.0.0.1          localhost
127.0.1.1          ...
...
```

En este caso, lo que hay que hacer es cambiar en el cliente todo el contenido de la segunda línea (127.0.1.1 ...) por el siguiente:

```
10.1.0.20  cliente-01.empresa.local  cliente-01
```

3 Actualizar los repositorios

Modificamos el fichero de configuración necesario para indicar que emplearemos los repositorios oficiales tanto para el servidor como el cliente y actualizamos la lista de paquetes disponibles en el repositorio ejecutando en la consola el comando:

```
$ sudo apt update
```

4 O http://www.instituto.local en caso de que tengamos configurado correctamente en nuestra red un servidor DNS

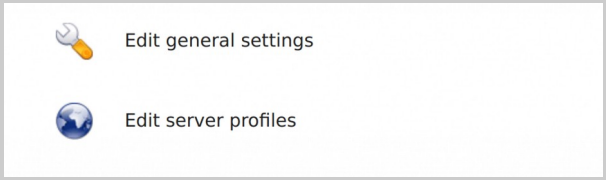
4 LDAP Account Manager

Si hemos instalado en el servidor LDAP Account Manager, necesitamos configurarlo para poder *conectar* con el servicio LDAP instalado en el servidor. Para ello realizaremos los siguientes pasos:

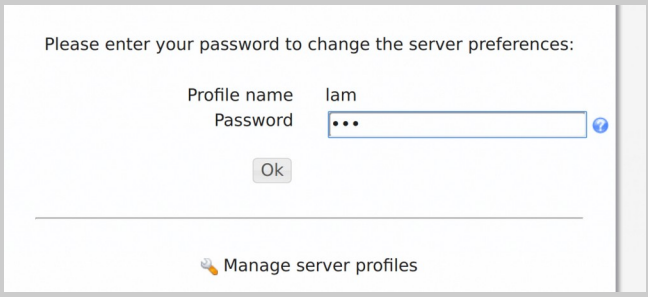
a) Abrimos un navegador web e introducimos la dirección URL para acceder al LDAP Accounr Manager instalado en el servidor:

```
http://172.16.0.10/lam
```

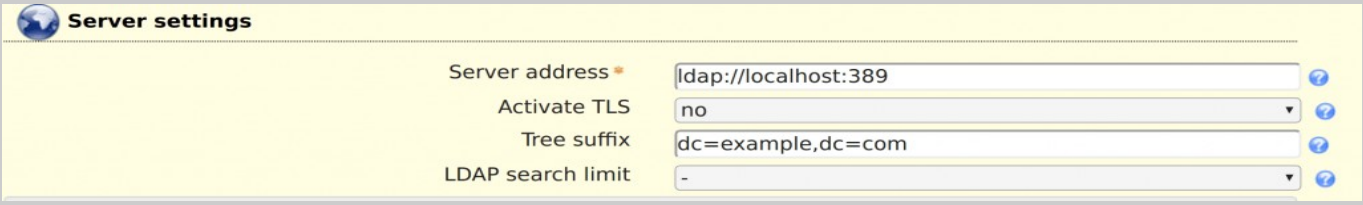
b) Editamos y configuramos el perfil del servidor. Para ello pulsamos en el enlace que hay en la parte superior derecha “LAM Configuration”



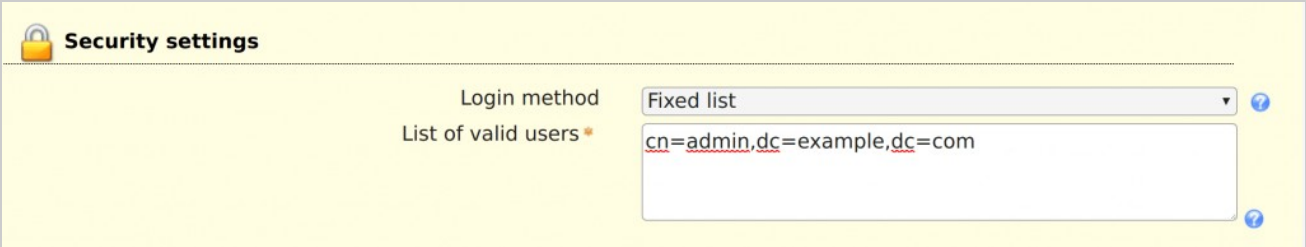
c) Pulsamos en “Edit Server Profiles” e introducimos la contraseña por defecto, lam[5]



d) Cambiamos la dirección del servidor LDAP y el sufijo del árbol LDAP modificando los datos que figuran por los nuestros (example.com por empresa.local)



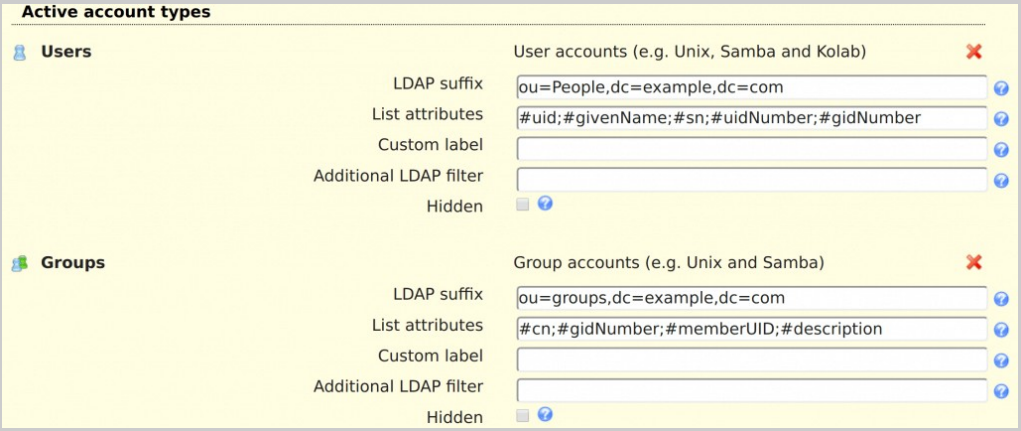
e) Cambiamos el acceso para que en vez de intentar logearse con Manager lo haga con el usuario admin en la sección de “Security Settings”



5 Por motivos de seguridad lo primero que deberíamos hacer es cambiar la contraseña del perfil en la página de configuración general (General Settings)

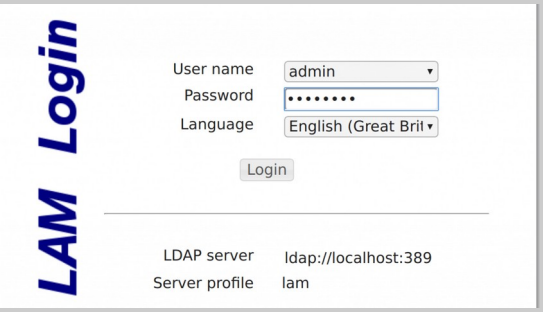
Andrés Julián Mayor Leirós IES San Clemente

f) Cambiamos a la pestaña de “Account Types” o Tipos de Cuentas y cambiamos el sufijo LDAP y las unidades organizativas (people por Usuarios, groups por Grupos y example.com por instituto.local)



g) Los usuarios y grupos LDAP definidos a través de LDAP Account Manager se crean por defecto con uids y gids a partir de 10000. Si deseamos que se realicen a partir de otro número podemos realizarlo yendo a la pestaña “Module Settings” y actualizaremos el valor al que deseemos en el apartado correspondiente.

h) Por último, guardaremos los cambios y ya podremos validarnos con la cuenta del usuario admin del servidor LDAP e introduciendo su contraseña.



i) La primera vez nos saldrá un mensaje de que si queremos que se creen las unidades organizativas Usuarios y Grupos. Aceptamos, y ya podemos crear gestionar LDAP a través de interfaz web, gestionando, por ejemplo, unidades organizativas, grupos, usuarios, modificando el esquema, etc.

- Creamos los grupos GLDAP, Gdireccion, Ginformaticos, Gtrabajadores, Gcontables, Gventas
- Creamos las siguientes cuentas de usuario:
  - Director, que tiene como grupo principal GLDAP y como grupo secundario Gdireccion
  - Informatico, que tiene como grupo principal GLDAP y como grupo secundario Ginformaticos
  - contable, que tiene como grupo principal GLDAP y como grupos secundarios Gtrabajadores y Gcontables
  - ventas, que tiene como grupo principal GLDAP y como grupos secundarios Gtrabajadores y Gventas

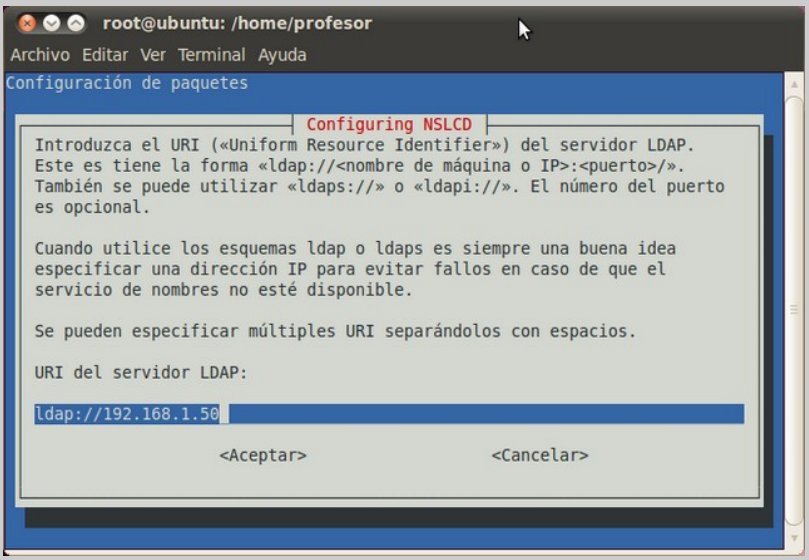
5 Autenticación del cliente empleando el servidor LDAP

Para hacer que el cliente se pueda validar contra el servidor LDAP tenemos que instalar el paquete libpam-ldapd:

```
$ sudo apt install libpam-ldapd
```

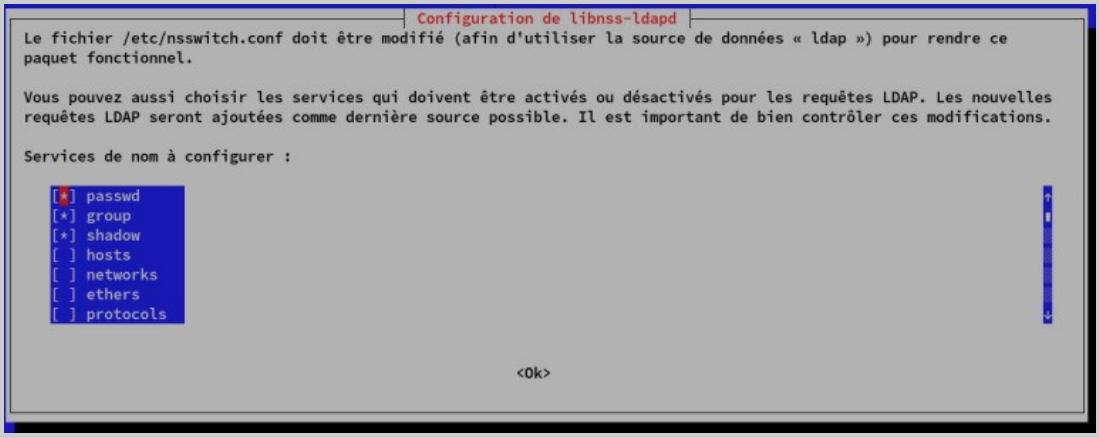
respondiendo a las preguntas que nos plantean:

a) La dirección del servidor LDAP, que **en nuestro caso sería ldap://10.0.0.10**



b) El nombre distinguido de la base de búsquedas de LDAP, que **en nuestro caso sería dc=empresa,dc=local**

c) Y finalmente debemos indicar los servicios que se habilitarán para realizar búsquedas LDAP (passwd, group y shadow)



d) Una vez finalice la instalación es conveniente ejecutar los comandos:

```
$ sudo getent passwd
```

```
$ sudo getent group
```

y comprobar que si se ven los usuarios/grupos que ya hemos creado en el servidor LDAP.

Andrés Julián Mayor Leirós IES San Clemente

Si no logramos ver los usuarios y grupos ya definidos en LDAP se deberá probablemente a que hemos introducido algún valor incorrectamente. Para solucionarlo podemos volver a comprobar los valores reconfigurando dos paquetes:

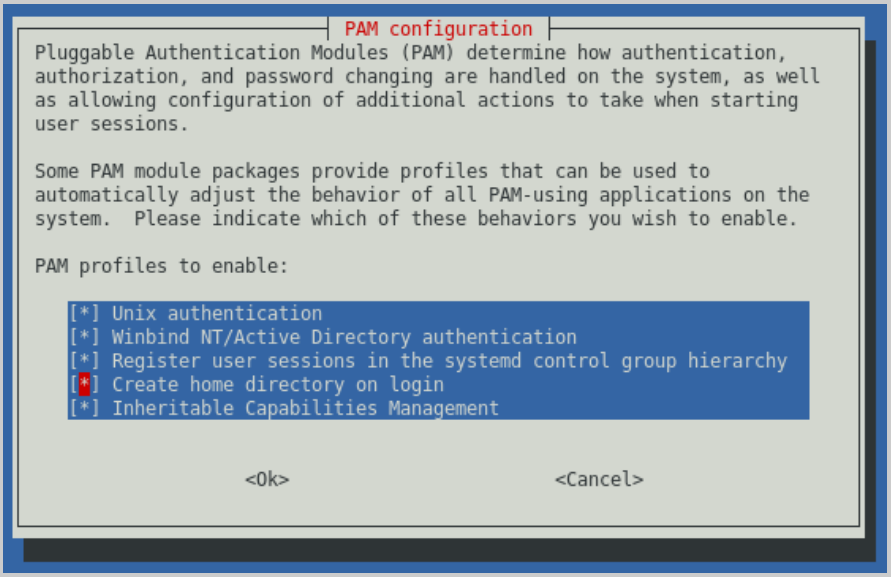
```
$ sudo dpkg-reconfigure nslcd
```

```
$ sudo dpkg-reconfigure libnss-ldapd
```

Si ya somos capaces de ver los usuarios y grupos definidos en LDAP, **aún no podemos validarnos porque la carpeta personal de los usuarios no se crea automáticamente**. Debemos actualizar el PAM (los módulos de autenticación) para que el equipo cliente *se entere* de que debe intentar logearse contra el servidor LDAP y en tal caso crear la carpeta personal del usuario. Esto lo haremos ejecutando el comando:

```
$ sudo pam-auth-update
```

y marcando la opción “Create home directory on login”[6]



En caso de querer mejorar la seguridad y no permitir que los usuarios pertenecientes al mismo grupo de usuarios al que pertenece un usuario puedan acceder (aunque sólo sea en modo lectura) a su carpeta personal, antes de ejecutar el comando anterior podemos realizar un cambio en el fichero **/usr/share/pam-configs/mkhomedir** añadiendo o modificando la **opción umask y estableciéndolo el valor 0077**

```
 GNU nano 4.3                                  /usr/share/pam-configs/mkhomedir
Name: activate mkhomedir
Default: yes
Priority: 900
Session-Type: Additional
Session:
        required                        pam_mkhomedir.so umask=0022 skel=/etc/skel
```

Ya sólo tenemos que reiniciar el equipo cliente para poder validarnos con un usuario de LDAP.

6 Se podría ejecutar pam-auth-update --enable homedir

Andrés Julián Mayor Leirós IES San Clemente

En caso de que no deseemos que aparezcan en la pantalla de inicio los usuarios locales (y los de LDAP una vez nos hayamos logeados una vez) modificamos el contenido del fichero /etc/gdm3/greeter.dconf-defaults descomentando la línea

```
disable-user-list=true
```

Al iniciar sesión, nos fijamos en que al introducir la contraseña aparece un mensaje indicando que se está creando el directorio *home* antes de mostrarnos de forma definitiva el escritorio.

Servicio Samba

1 Añadir y particionar un disco en el servidor

Añade al servidor LDAP un segundo disco de 6 GB y empleando fdisk crea **dos particiones lógicas** de aproximadamente 3 GB y formatéalas en ext4. Crea debajo del directorio /mnt dos carpetas: Comun y Personales.

Monta manualmente una de las particiones lógicas en /mnt/Comun y desmóntala. Si realizamos el montaje de forma manual de las particiones lógicas en los dos directorios anteriores, al reiniciar el ordenador, aparecerán desmontadas.

- ¿Qué tenemos que hacer para que no sea así?
- ¿Qué fichero hay que modificar?
- ¿Qué comando debemos ejecutar después de modificar el fichero anterior para comprobar que no hemos cometido errores y no tener problemas al reiniciar el equipo?
- Si cambiamos el disco de puerto SATA ¿qué ocurriría? ¿Qué tenemos que hacer en el fichero para no tener problemas en este caso? Realiza los cambios pertinentes

Crea debajo de Comun las carpetas Informáticos, Trabajadores y Resultados, y dentro de la carpeta Trabajadores las carpetas Contables y Ventas.

Crea debajo de Personales una carpeta con el *login* de cada usuario definido en el servidor LDAP.

2 Servidor Samba

Instala el servidor Samba en el servidor y configúralo para exportar Comun y Personales para toda la red local. Las dos carpetas se exportarán con permisos de compartición de escritura. La carpeta Personales debe compartirse de forma oculta y no estar disponible para usuarios invitados o anónimos. La carpeta Comun puede permitir el acceso a usuarios anónimos.

Añade los usuarios de LDAP a la base de datos de usuarios de Samba.

- ¿Qué fichero tenemos que modificar?

- ¿Qué líneas tenemos que añadir?
- ¿Qué tenemos que hacer una vez modificamos el fichero?
- ¿Como comprobamos en el servidor que las carpetas están compartidas?

3 Cliente Linux Samba

Instala en un equipo cliente Linux los paquetes necesarios para poder acceder a las carpetas compartidas en el servidor Samba. ¿Qué comando ejecutaremos en el cliente para comprobar que podemos ver las carpetas compartidas en el servidor Samba?

Crea en el equipo cliente debajo del directorio /mnt la carpeta Datos. Comprueba si puedes montar **manualmente** la carpeta Comun exportada por el servidor Samba en la carpeta /mnt/Datos del equipo cliente.

En este caso, si quisieras que se realizara el montaje de forma automática al reiniciar el ordenador ¿Qué fichero tendrías que modificar? ¿Cual debería ser su contenido?

La desventaja de montar de la forma anterior es que para poder usar las carpetas exportadas por Samba tenemos que buscar en Nautilus (el gestor de ficheros) el punto de montaje.

- ¿Qué otra forma tenemos para realizar el montaje para que de forma automática nos aparezca una unidad de red en el Nautilus? ¿Qué paquete tenemos que instalar?
- ¿Cual es el fichero de configuración que tenemos que modificar y cual será su contenido?

Modifica el contenido del fichero de configuración anterior para que:

- La carpeta /mnt/Comun exportada por el servidor Samba aparezca como la unidad de red Datos a cada uno de los usuarios LDAP
- A cada usuario de LDAP le aparezca una unidad de red llamada Personal conectada directamente con la carpeta que tiene cada usuario con su nombre debajo de la carpeta /mnt/Personales del servidor.

4 Permisos

Cuando tenemos múltiples grupos de usuarios los comandos chown, chgrp y chmod no nos llega para poder establecer permisos. ¿Qué tendríamos que emplear en ese caso?

Modifica en el servidor los permisos en /mnt/Comun/Informaticos para que los miembros de Ginformaticos tengan permisos de control total sobre esa carpeta y los de GDireccion puedan acceder en modo leer y recorrer.

Modifica en el servidor los permisos en /mnt/Comun/Trabajadores para que los miembros de Gdireccion, Ginformaticos y Gtrabajadores tengan permisos de lectura sobre esa carpeta.

Modifica en el servidor los permisos en /mnt/Comun/Trabajadores/Contables para que los miembros de Gdireccion tengan permisos de lectura sobre esa carpeta y los de Ginformaticos y Gcontables tengan todos los permisos.

Modifica en el servidor los permisos en /mnt/Comun/Trabajadores/Ventas para que los miembros de Gdireccion tengan permisos de lectura sobre esa carpeta y los de Ginformaticos y Gventas tengan todos los permisos.

Modifica en el servidor los permisos en /mnt/Comun/Resultados para que cualquier usuario pueda escribir.

Modifica en el servidor los permisos de cada carpeta de usuario en /mnt/Personales para que unicamente el usuario correspondiente tenga control total sobre la carpeta.

Comprueba en el equipo cliente Linux que al acceder con cada uno de los usuarios de LDAP aparecen en Nautilus las unidades de red Datos y Personal y que los permisos son los correctos.

5 Cliente Windows

Configura un equipo Windows 10 para que trabaje en la misma red que el servidor Samba.

Trata de acceder a la carpeta Comun del servidor ¿Te pide contraseña? ¿Puedes acceder a Resultados? ¿Y escribir?

Trata de acceder a la carpeta Personales del servidor ¿Te pide contraseña para acceder? Una vez accedes con un usuario y su contraseña ¿a qué carpeta puedes acceder y escribir?

Andrés Julián Mayor Leirós
IES San Clemente