# 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: en cada máquina cliente donde el usuario inicie sesión por primera vez se creará una nueva carpeta personal local. Por tanto, 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. NFS tiene la capacidad de "compartir" una misma carpeta (o más) en todos los equipos-cliente que deseemos, de manera que podríamos configurarlo para que dicha carpeta fuera precisamente la carpeta personal del usuario concreto que se haya logueado en un equipo-cliente cualquiera. A esto se le llama "perfil móvil" de usuario. De esta forma, un usuario encontrará disponible su misma carpeta personal en todos los equipos cliente donde inicie sesión, sea cual sea este.

**1.-a)** Instala el servidor NFS en la misma máquina que hace de servidor LDAP (***sudo apt install nfs-kernel-server*** en Ubuntu; ***sudo dnf install nfs-utils*** en Fedora) y crea una carpeta que alojará las carpetas personales de los usuarios. Por ejemplo, si decidimos que esta carpeta sea “/opt/perfiles”, haz entonces:

***sudo mkdir /opt/perfiles && sudo chown nobody:nogroup /opt/perfiles***

NOTA: El comando *chown* anterior es para mejorar la seguridad, ya que con él hacemos que solo el usuario sin privilegios *nobody* tenga permisos de escritura en "/opt/perfiles". Atención: en sistemas Fedora el grupo predefinido "nogroup" no existe sino que se llama "nobody" (como el usuario), así que el comando chown anterior deberá escribirse así: *sudo chown nobody:nobody /opt/perfiles*

**b)** Modifica el archivo "/etc/exports" para compartir el directorio anterior con permisos de lectura/escritura para todos los usuarios (¡y reinicia el servidor!). Es decir, escribe en ese archivo una línea como esta:

```
/opt/perfiles       *(rw)
```

**c)** Crea, también en el servidor NFS, las carpetas personales individuales de cada usuario, asignar a cada una su propietario respectivo y establecer los permisos adecuados para que solo és pueda acceder a ella. Es decir:

***sudo mkdir /opt/perfiles/jlopez*** && ***sudo chown 3001:10000 /opt/perfiles/jlopez && sudo chmod 700 /opt/perfiles/jlopez***
***sudo mkdir /opt/perfiles/pperez && sudo chown 3002:10000 /opt/perfiles/pperez && sudo chmod 700 /opt/perfiles/pperez***

NOTA: Fijarse que no podemos ejecutar el comando *chown* con los usuarios LDAP porque éstos no están reconocidos como usuarios válidos en el propio servidor.

**d)** Modifica las cuentas de usuario LDAP existentes para indicar que su carpeta personal (atributo "homeDirectory") se encuentra ahora dentro de la carpeta "/opt/punto" (es decir, es "/opt/punto/jlopez" o "/opt/punto/pperez" o...). Es decir, ejecuta el siguiente comando...:

***ldapmodify -D cn=admin -W -f homes.ldif***

...donde "homes.ldif" ha de tener un contenido similar a este:

```
dn:uid=usu1ldap,ou=usuarios,dc=midominio,dc=net
changetype:modify
replace:homeDirectory
homeDirectory:/opt/punto/jlopez

dn:uid=usu2ldap,ou=usuarios,dc=midominio,dc=net
changetype:modify
replace:homeDirectory
homeDirectory:/opt/punto/pperez
```

**e)** Pasa ahora a la/s máquina/s cliente/s. Crea una carpeta en cada una de ellas que hará de punto de montaje de los perfiles móviles. Si decidimos que este punto de montaje sea la carpeta “/opt/punto”, el comando a ejecutar es:

***sudo mkdir /opt/punto***

> NOTA: Ahora no hace falta ejecutar ningún comando *chown* para rebajar permisos porque en cuanto se realice el montaje automáticamente se le asignará el propietario y grupo de la carpeta remota montada ("/opt/perfiles"), el cual ya es precisamente *nobody*

**f)** Haz que el montaje de “/opt/perfiles” en “/opt/punto” se produzca nada más arrancar la máquina cliente. Para ello, añade la siguiente línea al archivo /etc/fstab de cada cliente y después reinicíalo o ejecuta *mount -a*

```
miservidor.midominio.net:/opt/perfiles  /opt/punto  nfs4  auto  0  0
```

**h)** Inicia sesión gráfica en la máquina cliente con un usuario LDAP. Abre un terminal y ejecuta el comando *pwd*. ¿Qué ves? Seguidament abre el Gedit, escribe cualquier cosa en el documento recién abierto y guárdalo en la carpeta personal de ese usuario. Confirma que no has tenido ningún problema a la hora de guardarlo y comprueba que dicha carpeta personal es remota observando (como "root") que, efectivamente, ese documento se ha creado en el servidor (dentro de la subcarpeta "/opt/perfiles/carpeta_personal" correspondiente).

**g)** El usuario LDAP con el que has iniciado sesión en la máquina cliente, ¿puede ver el contenido de la carpeta personal de cualquier otro usuario LDAP?