

Práctica: Instalación y configuración de LDAP

Marta López de los Bueis 2ºDAW

Instalación y configuración de LDAP para autenticar

Instala los paquetes necesarios en el servidor o en una máquina cliente que quieras que se autentique en LDAP:

```
$ sudo apt install libnss-ldap libpam-ldap ldap-utils nscd
```

```
vboxuser@Ubuntu:~$ sudo apt install libnss-ldap ldap-utils nscd
[sudo] contraseña para vboxuser:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
ldap-utils ya está en su versión más reciente (2.5.18+dfsg-0ubuntu0.22.04.2).
Se instalarán los siguientes paquetes adicionales:
  ldap-auth-client ldap-auth-config libpam-ldap
Se instalarán los siguientes paquetes NUEVOS:
  ldap-auth-client ldap-auth-config libnss-ldap libpam-ldap nscd
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 24 no actualizados.
Se necesita descargar 197 kB de archivos.
Se utilizarán 852 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nscd amd64
```

Configurar NSS para Usar LDAP en Autenticación.

Edita el archivo `/etc/nsswitch.conf` y cambia las líneas `passwd`, `group` y `shadow` para incluir `ldap`:
(Si ya lo tienes incluido no hagas cambios)

passwd: compat

ldap group: compat

ldap shadow: compat ldap

```

GNU nano 0.2 /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      files systemd
group:       files systemd
shadow:      files
gshadow:     files

hosts:       files mdns4_minimal [NOTFOUND=return] dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis

```

```

passwd:      compat
ldap group:   compat
ldap shadow:  compat ldap
gshadow:     files

```

Configurar PAM para la Autenticación con LDAP

Edita los archivos de PAM para usar LDAP en la autenticación:

1) Archivo /etc/pam.d/common-auth: Agrega:

auth sufficient pam_ldap.so

```

GNU nano 6.2 /etc/pam.d/common-auth *
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth [success=3 default=ignore] pam_unix.so nullok
auth [success=2 default=ignore] pam_sss.so use_first_pass
auth [success=1 default=ignore] pam_ldap.so use_first_pass
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already
# this avoids us returning an error just because nothing sets a success c
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth optional pam_cap.so
# end of pam-auth-update config
auth sufficient pam_ldap.so

```

2) Archivo /etc/pam.d/common-account: Agrega:

account sufficient pam_ldap.so

```
# and here are more per-package modules (the "Additional" block)
account sufficient pam_localuser.so
account [default=bad success=ok user_unknown=ignore] pam_sss.so
account sufficient pam_ldap.so
```

3) Archivo /etc/pam.d/common-password:

password sufficient pam_ldap.so

```
password sufficient pam_ldap.so
```

4) Archivo /etc/pam.d/common-session:

session required pam_mkhomedir.so skel=/etc/skel umask=0077

```
session required pam_mkhomedir.so skel=etcskel umask=0077
```

Reiniciar Servicios para Aplicar Cambios

Reinicia el servicio nscd para que los cambios tomen efecto:

\$ sudo systemctl restart nscd

```
sudo systemctl restart nscd
```

Verificar la Configuración y Probar la Autenticación LDAP

Verifica que el sistema pueda obtener información del usuario asier desde LDAP:

\$ getent passwd asier

```
vboxuser@Ubuntu:~$ getent passwd asier
asier:x:1002:1002:,,,:/home/asier:/bin/bash
```

Intenta iniciar sesión en el sistema como asier (o el que tú hayas incluido) para probar la autenticación.

Puedes hacerlo desde la misma terminal con: **\$ su - asier**

```
vboxuser@Ubuntu:~$ su - asier
Contraseña:
LDAP Password:
asier@Ubuntu:~$
```