

Administración de redes Linux

LDAP II

Instalación y configuración de un servidor OpenLDAP y Gestión de Usuarios

Iria Estévez Ayres

uc3m

Universidad **Carlos III** de Madrid

Departamento de Ingeniería Telemática

Marzo 2025

Índice

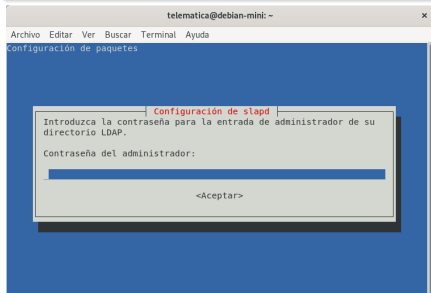
- 1 Instalación y configuración de un servidor OpenLDAP
- 2 Añadiendo grupos y usuarios al directorio LDAP
 - Añadiendo grupos y usuarios al directorio usando LDIF
 - Usando ldapmodify
 - Otras herramientas
- 3 Usando LDAP para autenticar usuarios

Apartado 1

Instalación y configuración de un servidor OpenLDAP

Instalando slapd (I)

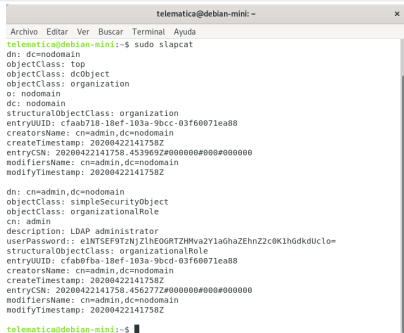
```
telematica@debian-mini:~$ sudo apt update
[sudo] password for telematica:
telematica@debian-mini:~$ sudo apt upgrade
telematica@debian-mini:~$ sudo apt install slapd
```



- Usad una password que podáis recordar fácilmente.

Instalando slapd (y II)

```
telematica@debian-mini:~$ sudo slapcat | grep dn
dn: dc=nodomain
dn: cn=admin,dc=nodomain
```



```
telematica@debian-mini: ~
Archivo Editar Ver Buscar Terminal Ayuda
telematica@debian-mini:~$ sudo slapcat
dn: dc=nodomain
objectClass: top
objectClass: dcObject
objectClass: organization
o: nodomain
dc: nodomain
structuralObjectClass: organization
entryUUID: cfaab718-18ef-103a-9bcc-03f60071ea88
creatorsName: cn=admin,dc=nodomain
createTimestamp: 20200422141758Z
entryCSN: 20200422141758.453969Z#000000#000#000000
modifiersName: cn=admin,dc=nodomain
modifyTimestamp: 20200422141758Z

dn: cn=admin,dc=nodomain
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9T2NjZlhlOGRTZHMvaZy1aGhZEHnZ2c0K1h6dkdUclo=
structuralObjectClass: organizationalRole
entryUUID: cfab0fba-18ef-103a-9bcd-03f60071ea88
creatorsName: cn=admin,dc=nodomain
createTimestamp: 20200422141758Z
entryCSN: 20200422141758.456277Z#000000#000#000000
modifiersName: cn=admin,dc=nodomain
modifyTimestamp: 20200422141758Z

telematica@debian-mini:~$
```

- Como el nombre de dominio no está configurado, debemos configurarlo.
- Usaremos `dpkg-reconfigure`
- Si estamos usando la MV `astt`, no saldrá el segundo ítem.

Configurando slapd

```
telematica@debian-mini:~$ sudo dpkg-reconfigure slapd
```

Os va a hacer una serie de preguntas...

- ¿Desea omitir la configuración del servidor OpenLDAP?
 - Obviamente, respondemos **NO**. A fin de cuentas queremos configurar este servicio.
- Nombre de dominio DNS:
 - arlinux.com
- Nombre de la organización:
 - Admon de Sistemas Linux
- Contraseña del administrador
- Base de datos a usar:
 - MDB

Configurando slapd (II)

...

- ¿Desea que se borre la base de datos cuando se purgue el paquete slapd?
 - **NO**. No tiene sentido arriesgarse a perder la base de datos por error.
- ¿Desea mover la base de datos antigua?
 - Esto se pregunta si ya hay una configuración previa.
 - Respondemos que **Sí**, para iniciar una base de datos nueva.

```
telematica@debian-mini:~$ sudo slapcat | grep dn
dn: dc=arlinux,dc=com
dn: cn=admin,dc=arlinux,dc=com
```

Haciendo comprobaciones (I)

```
telematica@debian-mini:~$ ldapsearch -x -b dc=arlinux,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=arlinux,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# arlinux.com
dn: dc=arlinux,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: Admon de Sistemas Linux
ou: arlinux
dc: arlinux

# admin, arlinux.com
dn: cn=admin,dc=arlinux,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```


Haciendo comprobaciones (II)

Ejercicios en clase

Ejecutad cada uno de los siguientes comandos e indicad qué ocurre en cada caso:

- 1 `ldapsearch -x -b dc=arlinux,dc=com dn`
- 2 `ldapwhoami -x -H ldapi:///`
- 3 `ldapsearch -x -H ldapi:/// -LLL -s base -b "" namingContexts`
- 4 `sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b "cn=config"`
- 5 Usa `grep olcRootDN` para quedarte con las líneas que contengan dicha cadena.
¿Qué ocurre? ¿Qué es `olcRootDN`? El DN del administrador
- 6 ¿Qué significa `-H ldapi:///`? ¿a qué se refiere? Es una URI, indica que el protocolo a usar es `ldapi`
- 7 ¿Para qué vale `-Y EXTERNAL`?

Autenticación externa

Apartado 2

Añadiendo grupos y usuarios al directorio LDAP

Nuestro primer LDIF

Crea este fichero: grupos.ldif

```
dn: ou=gente,dc=arlinux,dc=com
objectClass: organizationalUnit
ou: gente
```

```
dn: ou=grupo,dc=arlinux,dc=com
objectClass: organizationalUnit
ou: grupo
```

- LDIF es un formato que se usa para poder añadir, modificar y borrar entradas en un directorio LDAP.

No te olvides de dejar una línea en blanco entre entradas

Añadiendo grupos con LDIF (I)

```
telematica@debian-mini:~$ sudo apt install ldap-utils ldapscripts
```

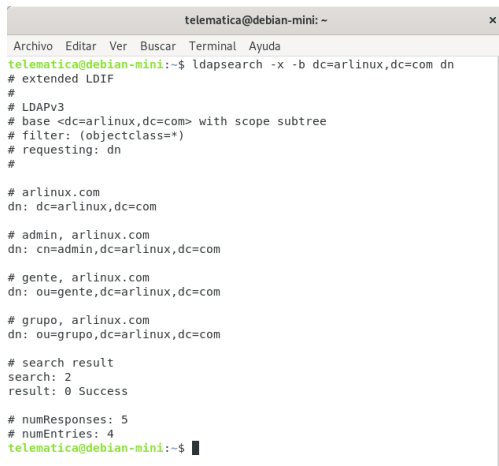
- Existen 2 utilidades semejantes para modificar el árbol de LDAP.
- slapadd obliga a reiniciar el servidor para que se apliquen los cambios.
- Usaremos ldapadd (incluido en el paquete ldap-utils, que te permite no reiniciar).

```
telematica@debian-mini:~$ sudo ldapadd -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f grupos.ldif
Enter LDAP Password:
adding new entry "ou=gente,dc=arlinux,dc=com"

adding new entry "ou=grupo,dc=arlinux,dc=com"
```

- `-D "cn=admin,dc=arlinux,dc=com"` especifica que nos autenticamos contra el nodo admin (ganando así también estos privilegios).

Añadiendo grupos con LDIF (y II)



```
telematica@debian-mini: ~
Archivo Editar Ver Buscar Terminal Ayuda
telematica@debian-mini:~$ ldapsearch -x -b dc=arlinux,dc=com dn
# extended LDIF
#
# LDAPv3
# base <dc=arlinux,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: dn
#
# arlinux.com
dn: dc=arlinux,dc=com

# admin, arlinux.com
dn: cn=admin,dc=arlinux,dc=com

# gente, arlinux.com
dn: ou=gente,dc=arlinux,dc=com

# grupo, arlinux.com
dn: ou=grupo,dc=arlinux,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
telematica@debian-mini:~$
```

LDAP schemas

- Tal y como se comentó en la clase anterior, LDAP usa *schemas* para definir los campos de los objetos.
- Vamos a usar el siguiente *schema*
- Se puede encontrar en el fichero `/etc/ldap/schema/nis.schema`
- También usaremos el schema `/etc/ldap/schema/inetorgperson.schema`

```
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'  
    DESC 'Abstraction of an account with POSIX attributes'  
    SUP top AUXILIARY  
    MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )  
    MAY ( userPassword $ loginShell $ gecos $ description ) )
```

```
objectclass ( 1.3.6.1.1.1.2.1 NAME 'shadowAccount'  
    DESC 'Additional attributes for shadow passwords'  
    SUP top AUXILIARY  
    MUST uid  
    MAY ( userPassword $ shadowLastChange $ shadowMin $  
        shadowMax $ shadowWarning $ shadowInactive $  
        shadowExpire $ shadowFlag $ description ) )
```

```
objectclass ( 1.3.6.1.1.1.2.2 NAME 'posixGroup'  
    DESC 'Abstraction of a group of accounts'  
    SUP top STRUCTURAL  
    MUST ( cn $ gidNumber )  
    MAY ( userPassword $ memberUid $ description ) )
```

Generando el fichero de atributos de un usuario

- En nuestro caso, usaremos un usuario existente en el sistema.
- Crearemos el usuario con adduser

```
telematica@debian-mini:~$ sudo adduser ada
Añadiendo el usuario `ada' ...
Añadiendo el nuevo grupo `ada' (1001) ...
Añadiendo el nuevo usuario `ada' (1001) con grupo `ada' ...
Creando el directorio personal `/home/ada' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para ada
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
Nombre completo []: Ada Lovelace
Número de habitación []: online
Teléfono del trabajo []: 1010
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n]
telematica@debian-mini:~$ getent passwd | grep ada
ada:x:1001:1001:Ada Lovelace,online,1010,:/home/ada:/bin/bash
```

- Calcularemos el hash de una password (que no coincida con la de ningún usuario)

```
telematica@debian-mini:~$ /usr/sbin/slappasswd
New password:
Re-enter new password:
{SSHA}BsBwHRWo3bhdiDjBLZqQChHVT+ctsKYV
```

Fichero usuario.ldif

```
dn: uid=ada,ou=gente,dc=arlinux,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: ada
cn: ada
givenName: Ada
sn: Byron
userPassword: {SSHA}BsBwHRWo3bhdiDjBLZqQChHVT+ctsKYV
loginShell: /bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/ada
shadowMax: 60
shadowMin: 1
shadowWarning: 7
shadowInactive: 7
shadowLastChange: 0

dn: cn=ada,ou=grupo,dc=arlinux,dc=com
objectClass: posixGroup
cn: ada
gidNumber: 1001
memberUid: ada
```


Añadiendo el usuario y grupo

```
telematica@debian-mini:~$ sudo ldapadd -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f usuario.ldif
Enter LDAP Password:
adding new entry "uid=ada,ou=gente,dc=arlinux,dc=com"
adding new entry "cn=ada,ou=grupo,dc=arlinux,dc=com"
```

```
telematica@debian-mini:~$ ldapsearch -x -b ou=gente,dc=arlinux,dc=com dn
# extended LDIF
#
# LDAPv3
# base <ou=gente,dc=arlinux,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: dn
#
# gente, arlinux.com
dn: ou=gente,dc=arlinux,dc=com

# ada, gente, arlinux.com
dn: uid=ada,ou=gente,dc=arlinux,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Indica qué ocurre si ejecuto este comando:

```
❹ ldapsearch -x -LLL -b "dc=arlinux,dc=com" '(objectclass=*)' uid givenName sn
```

Comprobando y modificando la password LDAP de un usuario

```
telematica@debian-mini:~$ ldapwhoami -vvv -D "cn=admin,dc=arlinux,dc=com" -x -W
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
dn:cn=admin,dc=arlinux,dc=com
Result: Success (0)
telematica@debian-mini:~$ ldappasswd -H ldapi:/// -x -D "cn=admin,dc=arlinux,dc=com" -W -S "uid=ada,ou=gente,dc=arlinux,dc=com"
```

```
New password:
Re-enter new password:
Enter LDAP Password:
telematica@debian-mini:~$ ldapwhoami -vvv -D "uid=ada,ou=gente,dc=arlinux,dc=com" -x -W
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
dn:uid=ada,ou=gente,dc=arlinux,dc=com
Result: Success (0)
```

Borrando el usuario y el grupo

```
telematica@debian-mini:~$ ldapdelete -x -W -H ldapi:/// -D "cn=admin,dc=arlinux,dc=com"
"uid=ada,ou=gente,dc=arlinux,dc=com"
Enter LDAP Password:
telematica@debian-mini:~$ ldapdelete -x -W -H ldapi:///
-D "cn=admin,dc=arlinux,dc=com" "cn=ada,ou=grupo,dc=arlinux,dc=com"
Enter LDAP Password:
```

Uso de ldapmodify para la gestión de usuarios y grupos

- Edita tu fichero usuario.ldif
- En cada entrada a añadir debes añadir en segundo lugar la línea `changetype:add`

```
dn: uid=ada,ou=gente,dc=arlinux,dc=com
changetype:add
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: ada
cn: ada
givenName: Ada
sn: Byron
loginShell: /bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/ada
```

```
dn: cn=ada,ou=grupo,dc=arlinux,dc=com
changetype:add
objectClass: posixGroup
cn: ada
gidNumber: 1001
memberUid: ada
```

```
telematica@debian-mini:~$ sudo ldapmodify -x -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f usuario.ldif
[sudo] password for telematica:
Enter LDAP Password:
adding new entry "uid=ada,ou=gente,dc=arlinux,dc=com"

adding new entry "cn=ada,ou=grupo,dc=arlinux,dc=com"
```

Borrando usuarios

Fichero: charles.ldif

```
dn: uid=charles,ou=gente,dc=arlinux,dc=com
changetype: add
objectClass: top
objectClass: account
uid: charles
```

Fichero: rmcharli.ldif

```
dn: uid=charles,ou=gente,dc=arlinux,dc=com
changetype: delete
```

```
telematica@debian-mini:~$ sudo ldapmodify -x -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f charles.ldif
Enter LDAP Password:
adding new entry "uid=charles,ou=gente,dc=arlinux,dc=com"
```

```
telematica@debian-mini:~$ ldapsearch -x -b ou=gente,dc=arlinux,dc=com dn | grep dn
# requesting: dn
```

```
dn: ou=gente,dc=arlinux,dc=com
dn: uid=ada,ou=gente,dc=arlinux,dc=com
dn: uid=charles,ou=gente,dc=arlinux,dc=com
```

```
telematica@debian-mini:~$ sudo ldapmodify -x -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f rmcharli.ldif
Enter LDAP Password:
deleting entry "uid=charles,ou=gente,dc=arlinux,dc=com"
```

Añadiendo atributos a un usuario

Formato básico del fichero LDIF

```
dn: entrada_a_modificar
changetype: modify
add: tipo_de_atributo
attribute_type: valor_a_actualizar
```

Fichero cambio.ldif

```
dn: uid=ada,ou=gente,dc=arlinux,dc=com
changetype: modify
add: mail
mail: ada.byron@arlinux.com
mail: abyron@arlinux.com
-
add: mobile
mobile: 0101010101
```

- Si el atributo lo admite, se pueden añadir varios valores (atributo mail).
- Se pueden añadir varios atributos a la vez.

```
telematica@debian-mini:~$ sudo ldapmodify -x -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f cambio.ldif
Enter LDAP Password:
modifying entry "uid=ada,ou=gente,dc=arlinux,dc=com"
```

Modificando atributos de un usuario

Formato básico del fichero LDIF

```
dn: entrada_a_modificar
changetype: modify
replace: tipo_de_atributo
attribute_type: valor_a_actualizar
```

Fichero cambio2.ldif

```
dn: uid=ada,ou=gente,dc=arlinux,dc=com
changetype: modify
replace: mail
mail: ada.lovelace@arlinux.com
```

- Si el atributo tiene valores (en nuestro ejemplo el atributo mail), los reemplaza a todos.
- Comprobadlo haciendo ldapsearch.

```
telematica@debian-mini:~$ sudo ldapmodify -x -D "cn=admin,dc=arlinux,dc=com" -W -H ldapi:/// -f cambio2.ldif
Enter LDAP Password:
modifying entry "uid=ada,ou=gente,dc=arlinux,dc=com"
```

Borrando atributos de un usuario

Borra todos los valores

```
dn: entrada_a_modificar
changetype: modify
delete: tipo_de_atributo
```

Fichero cambio3.ldif

```
dn: uid=ada,ou=gente,dc=arlinux,dc=com
changetype: modify
add: mail
mail: abyron@arlinux.com
-
add: title
title: manager
-
add: title
title: desarrolladora
```

Borra uno determinado

```
dn: entrada_a_modificar
changetype: modify
delete: tipo_de_atributo
attribute_type: valor_a_actualizar
```

Fichero cambio4.ldif

```
dn: uid=ada,ou=gente,dc=arlinux,dc=com
changetype: modify
delete: title
-
delete: mail
mail: ada.lovelace@arlinux.com
```

- 9 Aplica las modificaciones en orden y explica qué ha ocurrido.
- 10 Vuelve a añadir los dos campos title. Ahora quiero modificar el atributo title: manager y cambiarlo a title: informatica sin borrar el otro. Indica el contenido del fichero LDIF

Renombrando entradas

fichero LDIF

```
dn: entrada_a_modificar
changetype: modrdn
newrdn: nuevo_rdn
deleteoldrdn: 0_o_1
```

- Cambia el valor del rdn.
- Puede (deleteoldrdn a 1) o no (deleteoldrdn a 0) borrarse el anterior rdn.

Vuelve a añadir a Charles con el fichero charles.ldif

Fichero charles2.ldif

```
dn: uid=charles,ou=gente,dc=arlinux,dc=com
changetype: modrdn
newrdn: uid=charlie
deleteoldrdn: 0
```

Fichero charles3.ldif

```
dn: uid=charlie,ou=gente,dc=arlinux,dc=com
changetype: modrdn
newrdn: uid=babbage
deleteoldrdn: 1
```

```
dn: uid=babbage,ou=gente,dc=arlinux,dc=com
changetype: modify
delete: uid
uid: charles
```

11 Aplica las modificaciones en orden y explica qué ha ocurrido.

Moviendo una entrada

fichero LDIF

```
dn: entrada_a_modificar
changetype: modrdn
newrdn: nuevo_rdn
deleteoldrdn: 0_o_1
newsuperior: nuevo_nodo_padre
```

- Es una opción de modrdn

Fichero charles4.ldif

```
dn: ou=matematicos,ou=gente,dc=arlinux,dc=com
changetype: add
objectClass: organizationalUnit
ou: matematicos

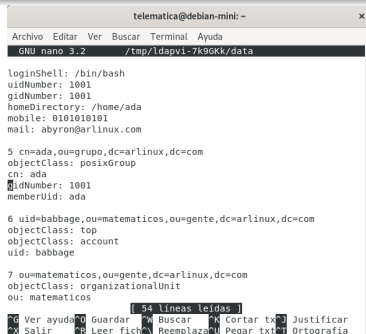
dn: uid=babbage,ou=gente,dc=arlinux,dc=com
changetype: modrdn
newrdn: uid=babbage
deleteoldrdn: 0
newsuperior: ou=matematicos,ou=gente,dc=arlinux,dc=com
```

- 12 Aplica las modificaciones en orden y explica qué ha ocurrido.
- 13 Antes de seguir con el siguiente apartado, borra este usuario.

Herramientas: ldapvi

```
telematica@debian-mini:~$ sudo apt install ldapvi
telematica@debian-mini:~$ ldapvi -D cn=admin,dc=arlinux,dc=com -h ldapi:/// -b dc=arlinux,dc=com
--- Login
Type M-h for help on key bindings.
Filter or DN: cn=admin,dc=arlinux,dc=com
Password: *****
8 entries read

Select an editor. To change later, run 'select-editor'.
 1. /bin/nano          <---- easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny
Choose 1-3 [1]: 1
```



```
telematica@debian-mini: -
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 3.2 /tmp/ldapvi-7k9GKk/data

loginShell: /bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/ada
mobile: 0101010101
mail: abyron@arlinux.com

5 cn=ada,ou=grupo,dc=arlinux,dc=com
objectClass: posixGroup
cn: ada
uidNumber: 1001
memberUid: ada

6 uid=babbage,ou=matematicos,ou=gente,dc=arlinux,dc=com
objectClass: top
objectClass: account
uid: babbage

7 ou=matematicos,ou=gente,dc=arlinux,dc=com
objectClass: organizationalUnit
ou: matematicos

[ 54 líneas leídas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar texto ^J Justificar
^X Salir ^R Leer fichero ^L Reemplazar ^U Pegar texto ^T Ortografía
```

Apartado 3

Usando LDAP para autenticar usuarios

Usando LDAP como fuente de datos para NSS (I)

- El sistema NSS (Name Server Switch) es un sistema modular diseñado para definir o recuperar información de directorios del sistema.
- Para usar LDAP como fuente de datos de NSS es necesario instalar el paquete `libnss-ldapd`.

```
telematica@debian-mini:~$ sudo apt install libnss-ldapd
```

No en todas las distribuciones pregunta las mismas opciones de configuración:

- Servidor ldap
 - `ldapi:///`
- DN de la base de búsquedas
 - `dc=arlinux,dc=com`
- Indique los servicios de nombre a configurar:
 - `passwd`
 - `group`
- Versión de LDAP
 - `3`
- ¿Requiere login la base de datos?
 - `No`

- ¿Dar privilegios especiales al root?
 - `Sí`
- ¿Desea hacer que la configuración sólo la pueda leer o escribir el propietario?
 - `No`
- Cuenta LDAP para el root
 - `cn=admin,dc=arlinux,dc=com`
- Contraseña para la cuenta LDAP de root
 - `Dejadla en blanco`

Usando LDAP como fuente de datos para NSS (II)

```
telematica@debian-mini:~$ sudo nano /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 ldap
group:       files systemd ldap
shadow:      files
gshadow:     files
```

```
telematica@debian-mini:~$ getent passwd | grep ada
ada:x:1001:1001:Ada Lovelace,online,1010,:/home/ada:/bin/bash
ada:x:1001:1001:ada:/home/ada:/bin/bash
telematica@debian-mini:~$ su ada
```

- Si se quiere que sea la primera base de datos en la que se busca, se debe colocar ldap antes.
- Así el usuario se autenticará antes con la password de LDAP y después con la del sistema
- En la próxima clase seguiremos trabajando con autenticación y permisos con ldap.

Administración de redes Linux

LDAP II

Instalación y configuración de un servidor OpenLDAP y Gestión de Usuarios

Iria Estévez Ayres

uc3m

Universidad **Carlos III** de Madrid

Departamento de Ingeniería Telemática

Marzo 2025