



Práctica 6.1 | Autenticación con LDAP

Despliegue de Aplicaciones Web

Actividad 6.1 Autenticación con LDAP

En esta actividad vamos a administrar un directorio de openLDAP y luego lo usaremos para autenticar los usuarios de una web..

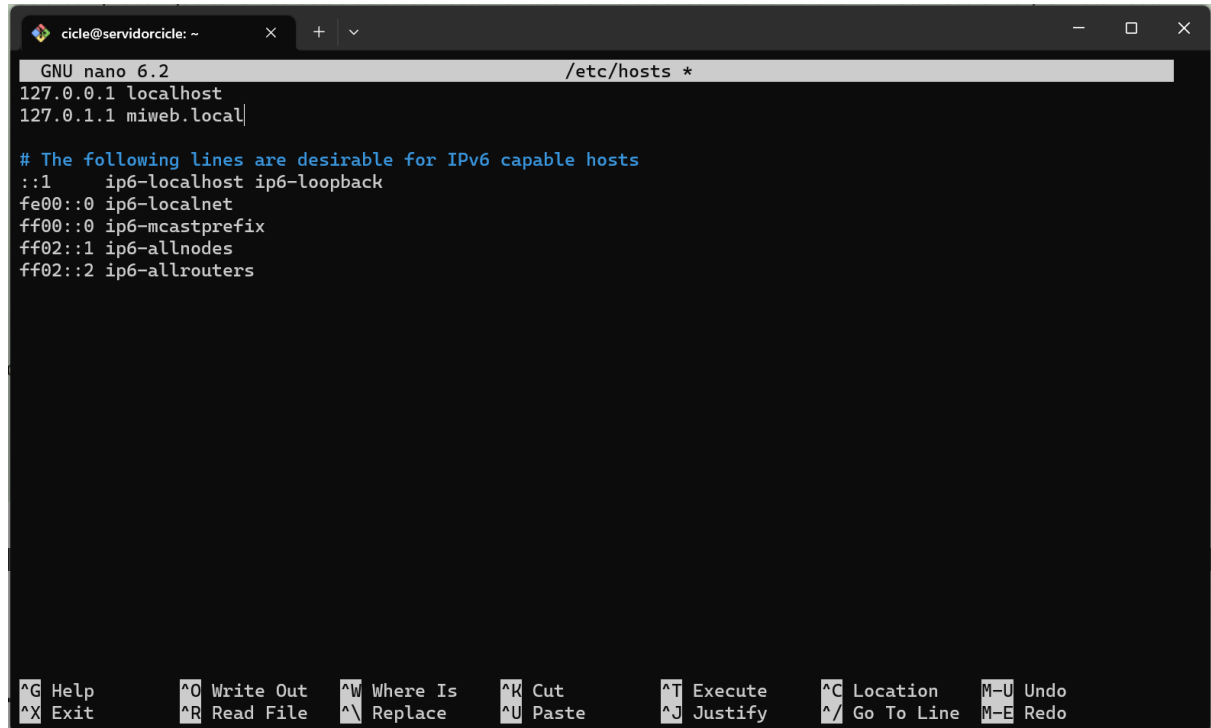
Actividad a realizar:

1. (0 puntos) Crea una nueva máquina virtual importando el archivo OVA de Ubuntu 22.04 que encuentras en el classroom en el tema de la asignatura. Luego arranca la máquina creada y inicia sesión.

2. (0,5 puntos) Instala i configura openLDAP para el dominio miweb.local

```
cicle@servidorcicle: ~  
cicle@servidorcicle:~$ sudo sudo hostname miweb.local  
cicle@servidorcicle:~$ hostname  
miweb.local  
cicle@servidorcicle:~$ |
```

```
cat: /etc/hosts: No such file or directory
cicle@servidorcicle:~$ sudo cat /etc/hostname
miweb.local
cicle@servidorcicle:~$
```



```
GNU nano 6.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 miweb.local

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

A continuación procedemos a instalar el LDAP:

```
/sudo apt-get install slapd ldap-utils
```

```
cicle@servidorcicle: ~  
command 'sdoc' from deb ruby-sdoc (1.1.0-1)  
Try: sudo apt install <deb name>  
cicle@servidorcicle:~$ sudo nano /etc/hosts  
cicle@servidorcicle:~$ sudo cat /etc/hosts  
127.0.0.1 localhost  
127.0.1.1 miweb.local  
  
# The following lines are desirable for IPv6 capable hosts  
::1 ip6-localhost ip6-loopback  
fe00::0 ip6-localnet  
ff00::0 ip6-mcastprefix  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
cicle@servidorcicle:~$ sudo apt-get install slapd ldap-utils  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
libflashrom1 libftd1-2  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
libltdl7 libodbc2  
Paquetes sugeridos:  
libssl2-modules-gssapi-mit | libssl2-modules-gssapi-heimdal odbc-postgresql tdsodbc  
Se instalarán los siguientes paquetes NUEVOS:  
ldap-utils libltdl7 libodbc2 slapd  
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 7 no actualizados.  
Se necesita descargar 1.881 kB de archivos.  
Se utilizarán 6.466 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] s
```

Para verificar que se ha instalado correctamente:

```
sudo slapcat
```

```
cicle@servidorcicle: ~  
Restarting services...  
systemctl restart cron.service packagekit.service polkit.service systemd-udevd.service udisks2.service  
Service restarts being deferred:  
/etc/needrestart/restart.d/dbus.service  
systemctl restart networkd-dispatcher.service  
systemctl restart systemd-logind.service  
systemctl restart unattended-upgrades.service  
systemctl restart user@1000.service  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
cicle@servidorcicle:~$ sudo slapcat  
dn: dc=local  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: local  
dc: local  
structuralObjectClass: organization  
entryUUID: f4d66592-5ea0-103d-8440-2751413e42c9  
creatorsName: cn=admin,dc=local  
createTimestamp: 20230324150444Z  
entryCSN: 20230324150444.981919Z#000000#000#000000  
modifiersName: cn=admin,dc=local  
modifyTimestamp: 20230324150444Z  
  
cicle@servidorcicle:~$ |
```

Para visualizar el archivo **.ldif** inicial, que viene por default

```
sudo cat /etc/ldap/slapd.d/cn\=config.ldif
```

```
cicle@servidorcicle: ~  
objectClass: dcObject  
objectClass: organization  
o: local  
dc: local  
structuralObjectClass: organization  
entryUUID: f4d66592-5ea0-103d-8440-2751413e42c9  
creatorsName: cn=admin,dc=local  
createTimestamp: 20230324150444Z  
entryCSN: 20230324150444.981919Z#000000#000#000000  
modifiersName: cn=admin,dc=local  
modifyTimestamp: 20230324150444Z  
  
cicle@servidorcicle:~$ sudo cat /etc/ldap/slapd.d/cn\=config.ldif  
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.  
# CRC32 026aa1dd  
dn: cn=config  
objectClass: olcGlobal  
cn: config  
olcArgsFile: /var/run/slapd/slapd.args  
olcLogLevel: none  
olcPidFile: /var/run/slapd/slapd.pid  
olcToolThreads: 1  
structuralObjectClass: olcGlobal  
entryUUID: f4cd051a-5ea0-103d-81aa-c767a7967aa4  
creatorsName: cn=config  
createTimestamp: 20230324150444Z  
entryCSN: 20230324150444.920469Z#000000#000#000000  
modifiersName: cn=config  
modifyTimestamp: 20230324150444Z  
cicle@servidorcicle:~$
```

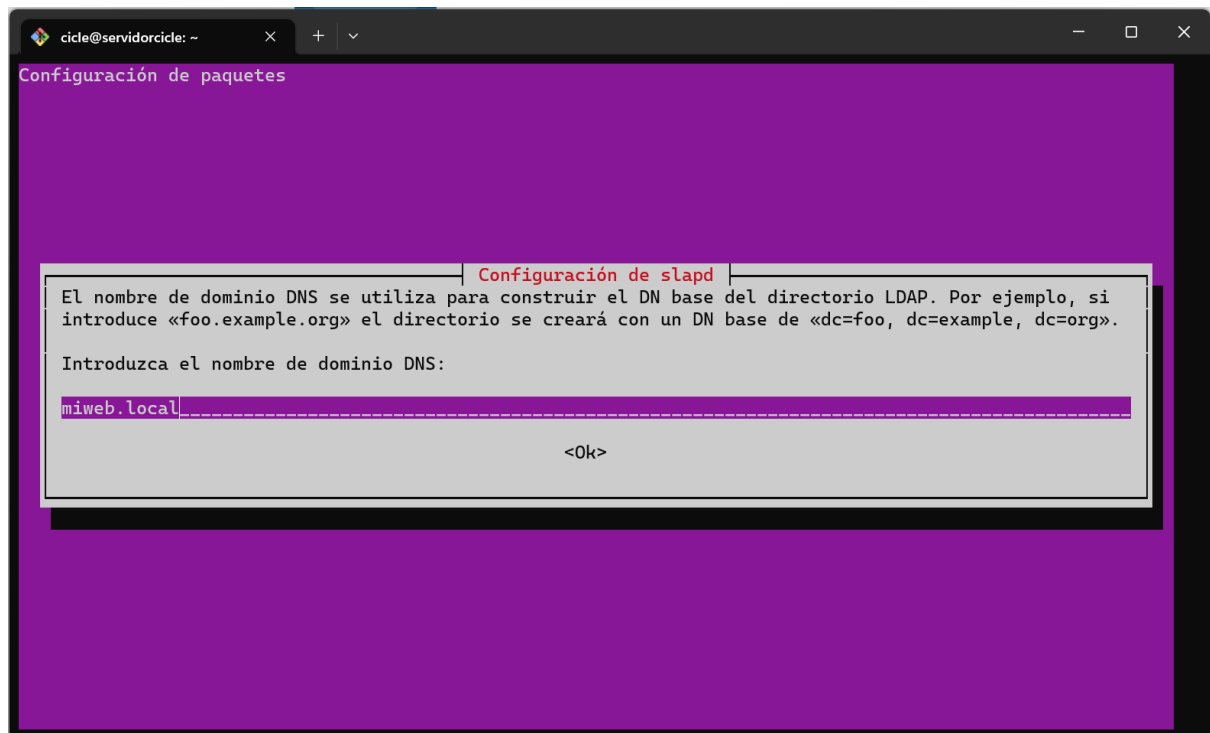
```
sudo service slapd status
```

```
cicle@servidorcicle: ~  
olcToolThreads: 1  
structuralObjectClass: olcGlobal  
entryUUID: f4cd051a-5ea0-103d-81aa-c767a7967aa4  
creatorsName: cn=config  
createTimestamp: 20230324150444Z  
entryCSN: 20230324150444.920469Z#000000#000#000000  
modifiersName: cn=config  
modifyTimestamp: 20230324150444Z  
cicle@servidorcicle:~$ sudo service slapd status  
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)  
   Loaded: loaded (/etc/init.d/slapd; generated)  
   Drop-In: /usr/lib/systemd/system/slapd.service.d  
            └─slapd-remain-after-exit.conf  
   Active: active (running) since Fri 2023-03-24 15:04:46 UTC; 5min ago  
     Docs: man:systemd-sysv-generator(8)  
  Process: 34858 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)  
    Tasks: 3 (limit: 2238)  
   Memory: 3.3M  
      CPU: 56ms  
   CGroup: /system.slice/slapd.service  
           └─34865 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d  
  
mar 24 15:04:46 miweb.local systemd[1]: Starting LSB: OpenLDAP standalone server (Lightweight Directory Acc  
mar 24 15:04:46 miweb.local slapd[34858]: * Starting OpenLDAP slapd  
mar 24 15:04:46 miweb.local slapd[34864]: @(#) $OpenLDAP: slapd 2.5.14+dfsg-0ubuntu0.22.04.1 (Feb 17 2023 2  
           Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>  
mar 24 15:04:46 miweb.local slapd[34865]: slapd starting  
mar 24 15:04:46 miweb.local slapd[34858]: ...done.  
mar 24 15:04:46 miweb.local systemd[1]: Started LSB: OpenLDAP standalone server (Lightweight Directory Acce  
Lines 1-20/20 (END)
```

Ahora vamos a reconfigurar el servidor de LDAP para que escuche nuestro nombre de servidor local:

```
sudo dpkg-reconfigure slapd
```

Le damos a “NO” y luego indicamos el nombre del dominio que hemos escogido.



Posteriormente, nos pedirá introducir la contraseña para el usuario administrador. Le damos NO a “*desea que se elimine la bbdd...?*”. Y a SÍ cuando nos pregunte si deseamos mover la antigua bbdd .

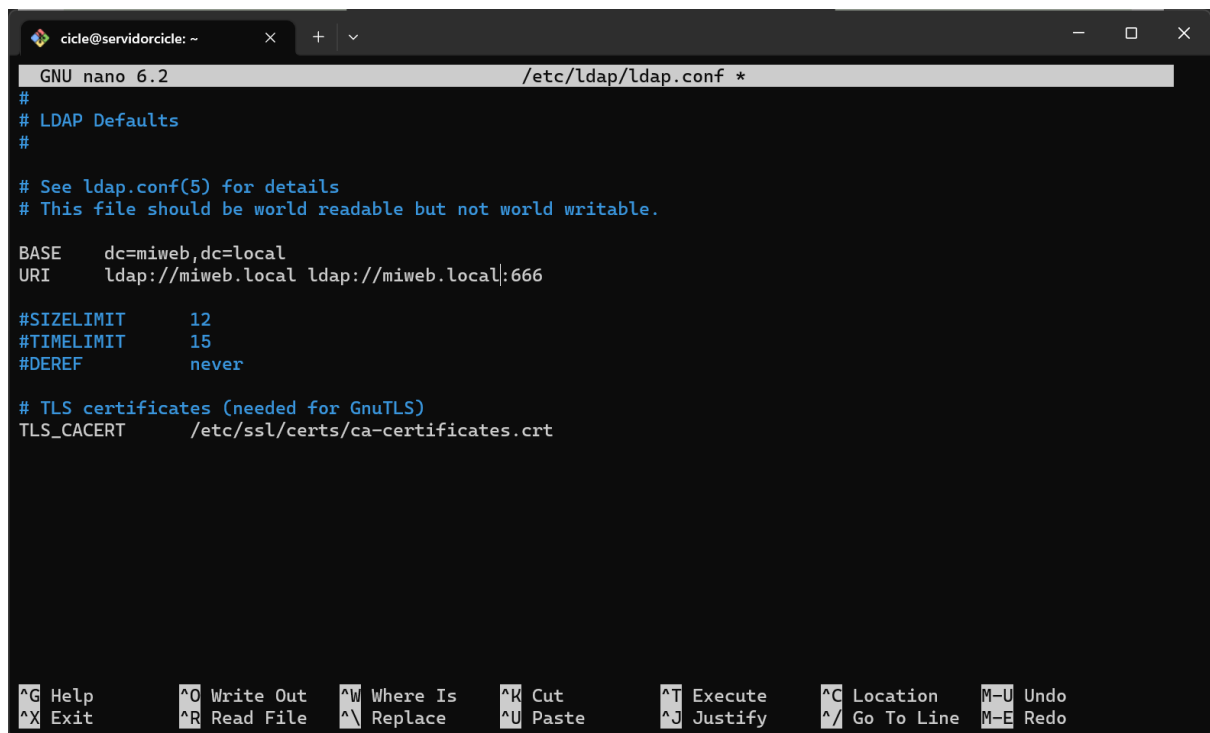
Este es el resultado final

```
cicle@servidorcicle:~$ sudo dpkg-reconfigure slapd
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.14+dfsg-0ubuntu0.22.04.1... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
cicle@servidorcicle:~$
```

Ahora cambiaremos el /etc/hostname y /etc/hosts en daw.local

Una vez tengamos los nombres cambiados editaremos en el archivo
/etc/ldap/ldap.conf

Descomentaremos las líneas de BASE y URI y pondremos el nombre de nuestro dominio.



```
GNU nano 6.2 /etc/ldap/ldap.conf *
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=miweb,dc=local
URI      ldap://miweb.local ldap://miweb.local:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo
```

Para comprobar la conexión con el servidor:

```
ldapsearch -x
```

```
cicle@servidorcicle: ~  
cicle@servidorcicle:~$ sudo nano /etc/ldap/ldap.conf  
cicle@servidorcicle:~$ ldapsearch -x  
# extended LDIF  
#  
# LDAPv3  
# base <dc=miweb,dc=local> (default) with scope subtree  
# filter: (objectclass=*)  
# requesting: ALL  
#  
# miweb.local  
dn: dc=miweb,dc=local  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: leslie  
dc: miweb  
  
# search result  
search: 2  
result: 0 Success  
  
# numResponses: 2  
# numEntries: 1  
cicle@servidorcicle:~$ |
```

```
sudo cat /etc/hosts  
sudo cat /etc/ldap/ldap.conf
```

```
cicle@miweb: ~  
cicle@miweb:~$ sudo cat /etc/hosts  
127.0.0.1 localhost  
127.0.1.1 miweb.local  
  
# The following lines are desirable for IPv6 capable hosts  
::1 ip6-localhost ip6-loopback  
fe00::0 ip6-localnet  
ff00::0 ip6-mcastprefix  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
cicle@miweb:~$ sudo cat /etc/ldap/ldap.conf  
#  
# LDAP Defaults  
#  
# See ldap.conf(5) for details  
# This file should be world readable but not world writable.  
  
BASE dc=miweb,dc=local  
URI ldap://miweb.local ldap://miweb.local:666  
  
#SIZELIMIT 12  
#TIMELIMIT 15  
#DEREF never  
  
# TLS certificates (needed for GnuTLS)  
TLS_CACERT /etc/ssl/certs/ca-certificates.crt  
cicle@miweb:~$ |
```

3. (1,5 puntos) Mediante comandos crea los siguientes usuarios y grupos.

- **Informaticos** (*juan, javier, pedro, tomas, miquel, martin, sandra, sonia, rosa*)

- **Programacion** (juan, pedro, sandra)
- **Administracion** (sonia, rosa, javier)
- **Helpdesk** (martin, tomas)
- **Contabilidad** (jhonny, otto, james)
 - **Facturacion** (jhonny, otto)
 - **Consultores** (james)
- **Usuarios** (jcarlos, daniel, vicente, maria, eva, ana)

Los nombres en azul son grupos y en naranja los usuarios. Los usuarios deben tener establecidos de forma coherente los siguientes campos:

- **businessCategory**
- **title**
- **departmentNumber**
- **employeeNumber**
- **mobile**

Los usuarios deben tener todos nombre, apellidos y el password establecido a cicle.

Creamos los 3 archivos ldif. Y luego ejecutamos cada uno de ellos

```

GNU nano 6.2 informaticos.ldif
dn:ou=informaticos,dc=daw,dc=local
objectclass:organizationalUnit
ou:informaticos

dn:cn=juan,ou=informaticos,dc=daw,dc=local
objectClass:inetOrgPerson
uid:juan
cn:cicle
sn:cicle
userPassword:cicle
businessCategory:informaticos
title:Programador
departmentNumber:1
employeeNumber:101
mobile:123456789

dn:cn=javier,ou=informaticos,dc=daw,dc=local
objectClass:inetOrgPerson
uid:javier
cn:cicle
sn:cicle
userPassword:cicle
businessCategory:informaticos
title:Programador
departmentNumber:1
employeeNumber:102
  
```



```
cicle@miweb: ~  
MINGW64/c/Users/lesli/Docu  
member:cn=pedro,ou=informaticos,dc=daw,dc=local  
member:cn=sandra,ou=informaticos,dc=daw,dc=local  
  
dn:cn=administracion,ou=informaticos,dc=daw,dc=local  
objectclass:groupOfNames  
cn:administracion  
member:cn=sonia,ou=informaticos,dc=daw,dc=local  
member:cn=rosa,ou=informaticos,dc=daw,dc=local  
member:cn=javier,ou=informaticos,dc=daw,dc=local  
  
dn:cn=helpdesk,ou=informaticos,dc=daw,dc=local  
objectclass:groupOfNames  
cn:helpdesk  
member:cn=martin,ou=informaticos,dc=daw,dc=local  
member:cn=tomas,ou=informaticos,dc=daw,dc=local  
  
cicle@miweb:~$ sudo nano informaticos.ldif  
cicle@miweb:~$ sudo nano contabilidad.ldif  
cicle@miweb:~$ ls  
contabilidad.ldif  informaticos.ldif  
cicle@miweb:~$ sudo nano usuarios.ldif  
cicle@miweb:~$ ls  
contabilidad.ldif  informaticos.ldif  usuarios.ldif  
cicle@miweb:~$
```

Y ejecutamos los archivos

```
sudo ldapadd -D cn=admin,dc=miweb,dc=local -W -f informaticos.ldif -c
```

```
cicle@miweb: ~  
MINGW64/c/Users/lesli/Docu  
cicle@miweb:~$ sudo ldapadd -D cn=admin,dc=miweb,dc=local -W -f informaticos.ldif -c  
Enter LDAP Password:  
adding new entry "ou=informaticos,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=juan,ou=informaticos,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=javier,ou=informaticos,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=pedro,ou=informaticos,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=tomas,ou=informaticos,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=miquel,ou=informaticos,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=martin,ou=informaticos,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge
```

```
sudo ldapadd -D cn=admin,dc=miweb,dc=local -W -f contabilidad.ldif -c
```

```
cicle@miweb: ~  
MINGW64/c/Users/lesli/Docu  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
cicle@miweb:~$ sudo ldapadd -D cn=admin,dc=miweb,dc=local -W -f contabilidad.ldif -c  
Enter LDAP Password:  
adding new entry "ou=contabilidad,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=jhonny,ou=contabilidad,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=otto,ou=contabilidad,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=james,ou=contabilidad,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=facturacion,ou=contabilidad,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=consultores,ou=contabilidad,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
cicle@miweb:~$ |
```

```
sudo ldapadd -D cn=admin,dc=miweb,dc=local -W -f usuarios.ldif -c
```

```
cicle@miweb: ~  
MINGW64/c/Users/lesli/Docu  
cicle@miweb:~$ sudo ldapadd -D cn=admin,dc=miweb,dc=local -W -f usuarios.ldif -c  
Enter LDAP Password:  
adding new entry "ou=usuarios,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=jcarlos,ou=usuarios,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=daniel,ou=usuarios,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=vicente,ou=usuarios,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=maria,ou=usuarios,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=eva,ou=usuarios,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge  
  
adding new entry "cn=ana,ou=usuarios,dc=daw,dc=local"  
ldap_add: Server is unwilling to perform (53)  
    additional info: no global superior knowledge
```

4. (0,5 puntos) Mediante comandos elimina el usuario martin.

```
cicle@miweb:~$ ldapdelete -W -D "cn=admin,dc=miweb,dc=local" "cn=martin,ou=informaticos,dc=miweb,dc=local"  
Enter LDAP Password:  
cicle@miweb:~$ |
```

5. (0,5 puntos) Mediante comandos elimina el grupo Consultores.

```
cicle@miweb:~$ ldapdelete -W -D "cn=admin,dc=miweb,dc=local" "cn=consultores,ou=contabilidad,dc=miweb,dc=local"
Enter LDAP Password:
cicle@miweb:~$
```

6. (0,5 puntos) Genera un archivo Idif con la información necesaria para generar toda la información de usuarios y grupos pedida en el punto 3. Entrega el archivo generado.

Archivo entregado en la carpeta llamado leslie.ldif

7. (1,25 punto) Crea una web con informacion de una empresa de construcción de barcos. Debe tener una página principal con información de a que se dedica la empresa y un menú con enlaces. Crea tres carpetas llamadas administracion, nominas, informacion y dentro añade un archivo index.html con tu nombre y el nombre de la carpeta.

8. (1,25 punto) Protege la ruta relativa administracion mediante ldap para que sólo puedan acceder los usuarios del grupo administracion. Comprueba que funciona para los usuarios correctos.

9. (1,25 punto) Protege la ruta relativa nominas mediante ldap para que sólo pueda acceder el usuario otto. Comprueba que funciona para los usuarios correctos.

10. (1 punto) Protege la ruta relativa informacion mediante ldap para que sólo puedan acceder los usuarios autenticados. Comprueba que funciona para los usuarios correctos.

11. (0,5 puntos) Instala en local Apache Directory Studio y crea una conexión con el servidor ldap de la máquina virtual.

12. (1,25 punto) Mediante Apache Directory Studio añade una unidad organizativa jefes y añade un usuario llamado masterfirst que es el usuario del jefe. Rellena de forma coherente la misma información para el usuario.

Para responder a las diferentes actividades debes entregar un documento con capturas de pantalla a tamaño completo de la pantalla de tu ordenador que sean visibles correctamente de todo el proceso realizado para realizar y comprobar que se ha realizado correctamente la actividad.

Si con esas capturas de pantalla no se puede demostrar que has realizado correctamente el apartado oportuno del examen este apartado tendrá una nota de 0. Si las capturas no permiten ver con claridad la información, la nota de

ese apartado es de 0. Si las capturas realizadas son reutilizadas o copiadas la nota es de 0.

A entregar:

- ***Debes entregar un documento de texto con las capturas de pantalla (con el número de cada apartado).***
- ***Debes entregar un archivo LDIF con lo que se pide en el apartado 6. 2***