

LDAP – Configuración de Open LDAP

1. Creación de una Unidad Administrativa

En tu directorio home crea y edita un fichero ldif e incorpora la siguiente información, consistente con los parámetros configurados en la práctica anterior, para crear un nuevo objeto:

\$ nano ou.ldif

```
GNU nano 6.2                                ou.ldif *
dn: ou=despliegue,dc=daw2,dc=local
objectClass: top
objectClass: organizationalUnit
ou: despliegue
```

¿Cómo se llama el objeto que has creado?

¿De qué tipo (class) es?

¿Qué lugar ocupa en la jerarquía?

A continuación, deberemos añadir la información a la base de datos OpenLDAP. con el comando ldapadd:

```
root@sriserver:/home/alumno# ldapadd -x -D cn=admin,dc=daw2,dc=local -W -f ou.ldif
Enter LDAP Password:
adding new entry "ou=despliegue,dc=daw2,dc=local"
```

Ejecuta el comando para ver la configuración del LDAP:

```
root@sriserver:/home/alumno# slapcat
dn: dc=daw2,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw2
dc: daw2
structuralObjectClass: organization
entryUUID: 2abd7d52-2568-103d-8943-5b94eb5a2f8e
creatorsName: cn=admin,dc=daw2,dc=local
createTimestamp: 20230110192437Z
entryCSN: 20230110192437.823762Z#000000#000#000000
modifiersName: cn=admin,dc=daw2,dc=local
modifyTimestamp: 20230110192437Z

dn: ou=despliegue,dc=daw2,dc=local
objectClass: top
objectClass: organizationalUnit
ou: despliegue
structuralObjectClass: organizationalUnit
entryUUID: 560aa272-2569-103d-8b31-e59629381d01
creatorsName: cn=admin,dc=daw2,dc=local
createTimestamp: 20230110193259Z
entryCSN: 20230110193259.968118Z#000000#000#000000
modifiersName: cn=admin,dc=daw2,dc=local
modifyTimestamp: 20230110193259Z
```

2. Creación de un Grupo

En tu directorio home crea y edita un nuevo fichero group.ldif e incorpora la siguiente información:

```
GNU nano 6.2 group.ldif *
dn: cn=grupo,ou=despliegue,dc=daw2,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: grupo_
```

Incorpora la información a la base de datos OpenLDAP. con el comando ldapadd:

```
root@sriserver:~# ldapadd -x -D cn=admin,dc=daw2,dc=local -W -f group.ldif
Enter LDAP Password:
adding new entry "cn=grupo,ou=despliegue,dc=daw2,dc=local"
```

Ejecuta el comando para ver la configuración del LDAP:

```
dn: cn=grupo,ou=despliegue,dc=daw2,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: grupo
structuralObjectClass: posixGroup
entryUUID: e309886e-2569-103d-8b32-e59629381d01
creatorsName: cn=admin,dc=daw2,dc=local
createTimestamp: 20230110193656Z
entryCSN: 20230110193656.519655Z#000000#000#000000
modifiersName: cn=admin,dc=daw2,dc=local
modifyTimestamp: 20230110193656Z
```

2. Creación de un Usuario Para añadir un usuario, repetimos el proceso anterior, pero lo primero será evitar que la contraseña del usuario se almacene en texto plano dentro del archivo ldif.

Para lograrlo, usaremos el comando slappasswd que produce, a partir de la contraseña original, un hash utilizando el algoritmo SHA-1 (aunque podríamos cambiar el algoritmo que se aplique usando el argumento -h). Ese hash habrá que anotarlo para usarlo en el fichero ldif

Elige (y recuerda) una contraseña para ese usuario. Comprueba la robustez de esa contraseña en la página PasswordMonster. Utiliza una contraseña al menos “Strong” (y adjúntala en la práctica). Por lo tanto, comenzamos ejecutando el comando slappasswd:

```
YouCantGetThisOne2023
Very Strong
root@sriserver:~# slappasswd
New password:
Re-enter new password:
{SSHA}yrzfn2gnLs0q4sa2aquHG8gsMovt0EIz
```

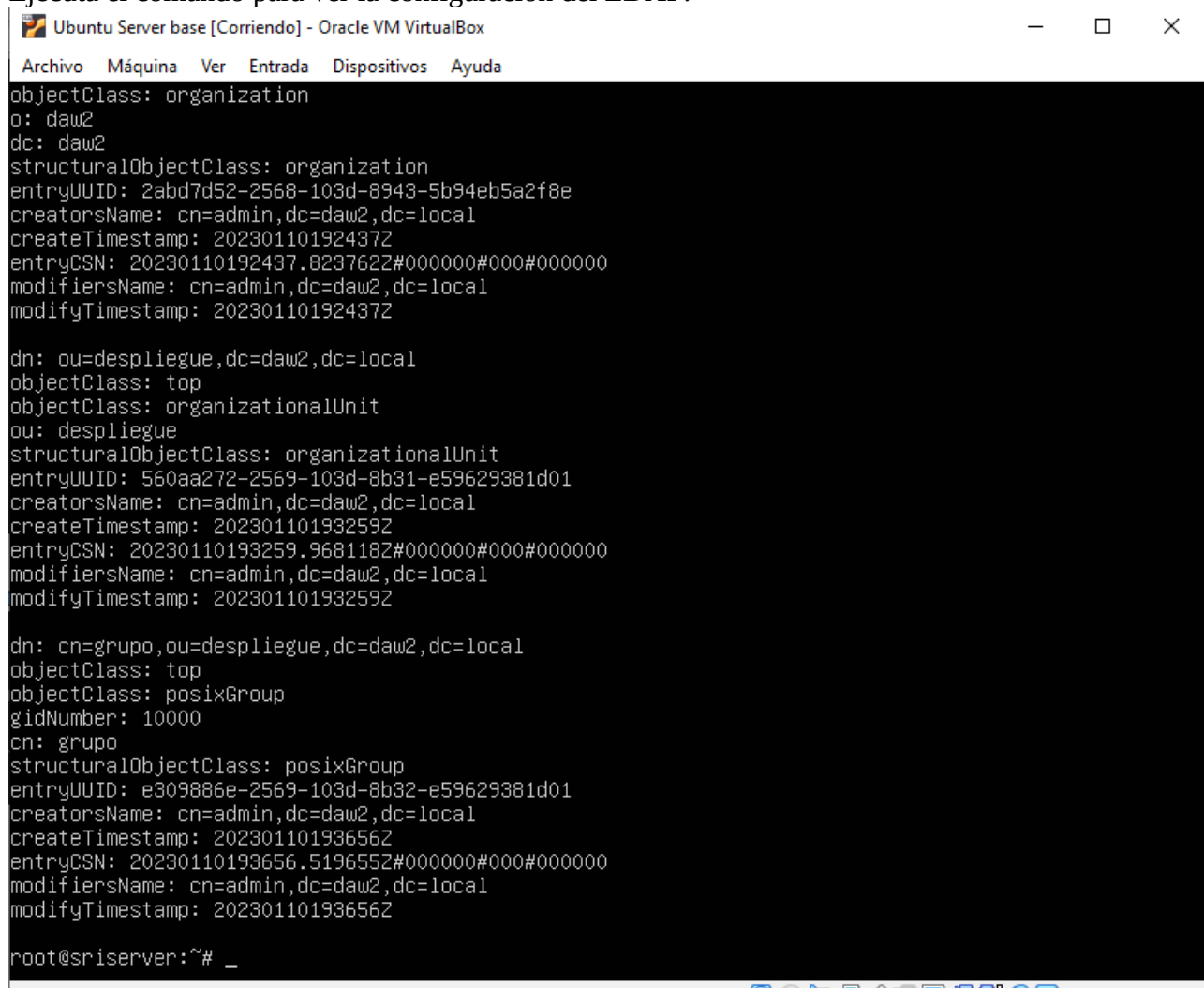
Al momento, obtendremos la cadena, codificada con hash SHA-1, que equivale a la contraseña que hemos escrito. Debemos copiarla para utilizarla en el archivo `ldif` que crearemos a continuación.

```
GNU nano 6.2 user.ldif *
dn: uid=usuario,ou=despliegue,dc=daw2,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: usuario
cn: usuario
uid: usuario
ou: grupo
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/usuario
loginShell: /bin/bash
userPassword: yrzfn2gnLs0q4sa2aquHG8gsMovt0EIz
sn: apellido
mail: usuario@daw2.com
givenName: nombre
```

Incorpora la información a la base de datos OpenLDAP. con el comando `ldapadd`:

```
root@sriserver:~# ldapadd -x -D cn=admin,dc=daw2,dc=local -W -f user.ldif
Enter LDAP Password:
adding new entry "uid=usuario,ou=despliegue,dc=daw2,dc=local"
ldap_add: Type or value exists (20)
        additional info: cn: value #0 provided more than once
```

Ejecuta el comando para ver la configuración del LDAP:



The screenshot shows a terminal window titled "Ubuntu Server base [Corriendo] - Oracle VM VirtualBox". The terminal output displays LDAP entry details for three entries: an organization entry, an organizational unit entry, and a posix group entry. The organization entry has dn: `o=daw2` and objectClass: `organization`. The organizational unit entry has dn: `ou=despliegue,dc=daw2,dc=local` and objectClass: `organizationalUnit`. The posix group entry has dn: `cn=grupo,ou=despliegue,dc=daw2,dc=local` and objectClass: `posixGroup`. The terminal ends with the prompt `root@sriserver:~#`.

```
objectClass: organization
o: daw2
dc: daw2
structuralObjectClass: organization
entryUUID: 2abd7d52-2568-103d-8943-5b94eb5a2f8e
creatorsName: cn=admin,dc=daw2,dc=local
createTimestamp: 20230110192437Z
entryCSN: 20230110192437.823762Z#000000#000#000000
modifiersName: cn=admin,dc=daw2,dc=local
modifyTimestamp: 20230110192437Z

dn: ou=despliegue,dc=daw2,dc=local
objectClass: top
objectClass: organizationalUnit
ou: despliegue
structuralObjectClass: organizationalUnit
entryUUID: 560aa272-2569-103d-8b31-e59629381d01
creatorsName: cn=admin,dc=daw2,dc=local
createTimestamp: 20230110193259Z
entryCSN: 20230110193259.968118Z#000000#000#000000
modifiersName: cn=admin,dc=daw2,dc=local
modifyTimestamp: 20230110193259Z

dn: cn=grupo,ou=despliegue,dc=daw2,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: grupo
structuralObjectClass: posixGroup
entryUUID: e309886e-2569-103d-8b32-e59629381d01
creatorsName: cn=admin,dc=daw2,dc=local
createTimestamp: 20230110193656Z
entryCSN: 20230110193656.519655Z#000000#000#000000
modifiersName: cn=admin,dc=daw2,dc=local
modifyTimestamp: 20230110193656Z

root@sriserver:~#
```

3. Recuperar Información del Usuario Por último, podemos comprobar que el contenido anterior se recupera correctamente. Para lograrlo podemos utilizar el comando `ldapsearch`, que nos permite hacer una búsqueda en el directorio.:

```
root@sriserver:~# ldapsearch -xLLL -b "dc=daw2,dc=local" uid=usuario sn givenName cn
```