10 Guía Servidor LDAP

MATERIAL

- Los contenidos de la unidad y esta guía
- Máquinas Virtuales Ubuntu 22.04 Desktop (1 Servidor DNS + 1 Servidor Web y Tomcat).
- Virtualbox
- Ordenador con S.O. Windows 10.
- Navegador para comprobar la realización de la tarea.
- Procesador de textos para elaborar la documentación y los archivos de la tarea.
- Acceso a Internet.

10.1 Instalación Servidor LDAP

1. **Realizar la instalación del Servidor LDAP.**

   Lo primero que haremos es modificar el /etc/hosts para indicar un FQDN a nuestro servidor.

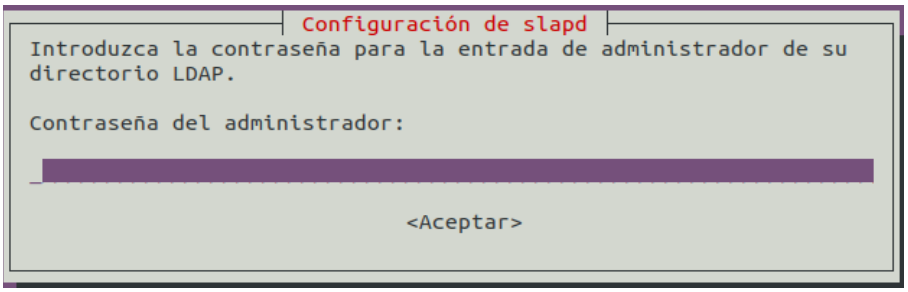
   #sudo nano /etc/hosts

```
 GNU nano 4.8                          /etc/hosts
127.0.0.1       localhost
127.0.1.1       informatica-VirtualBox
192.168.1.137   dpl-daw.ldap

# 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 realizar la instalación del Servidor LDAP.

#sudo apt install slapd ldap-utils

Comienza la instalación y se nos solicita introducir una contraseña para el administrador del directorio LDAP.



Una vez concluye la instalación, verificamos que se ha instalado ejecutando:

#sudo slapcat

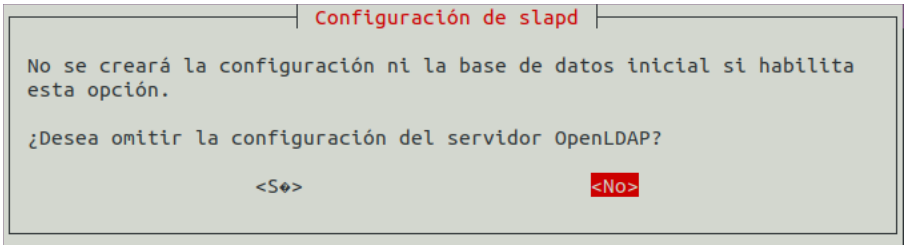
```
informatica@informatica-VirtualBox:~$ sudo slapcat
dn: dc=nodomain
objectClass: top
objectClass: dcObject
objectClass: organization
o: nodomain
dc: nodomain
structuralObjectClass: organization
entryUUID: cdd837bc-0966-103c-9867-63a3ce91f513
creatorsName: cn=admin,dc=nodomain
createTimestamp: 20220114091922Z
entryCSN: 20220114091922.245170Z#000000#000#000000
modifiersName: cn=admin,dc=nodomain
modifyTimestamp: 20220114091922Z

dn: cn=admin,dc=nodomain
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9Z2NYZUhWQ3B2Z3l4UFFKRkZaWERiN25kVjhzRkJMNGo=
```

2. Configurar el Servidor LDAP en Ubuntu 22.04 LTS.

Configuramos el servicio de directorio LDAP, apoyándonos en el asistente slapd.

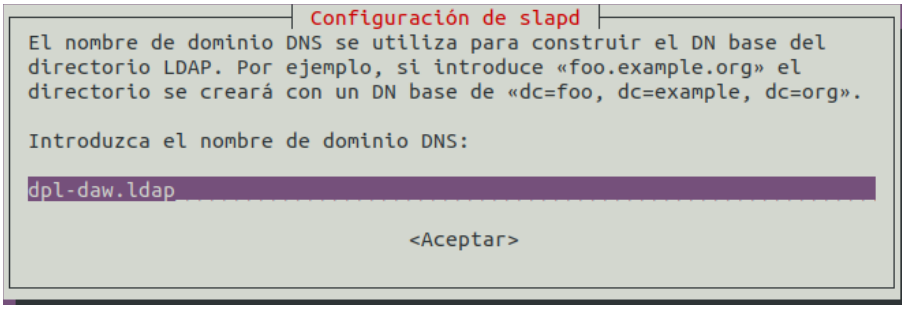
#sudo dpkg-reconfigure slapd

El primer diálogo que nos aparece nos pregunta si queremos omitir la configuración de OpenLDAP. Elegimos **No**.



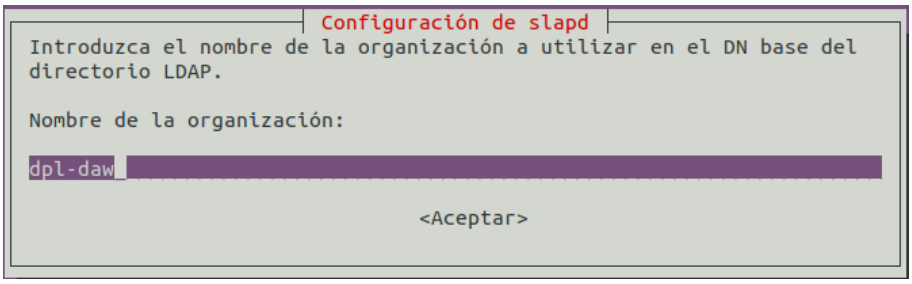
A continuación nos pregunta por el dominio en el que se encuentra nuestro servidor, esto va a formar parte del DN del directorio LDAP. Al haberlo indicado anteriormente en el fichero /etc/hosts, automáticamente el asistente lo recoge y solo debemos darle a **OK**.

Lo he introducido manualmente porque no lo ha cogido en automático pongo dentro **dpl-daw.ldap** y Aceptamos.

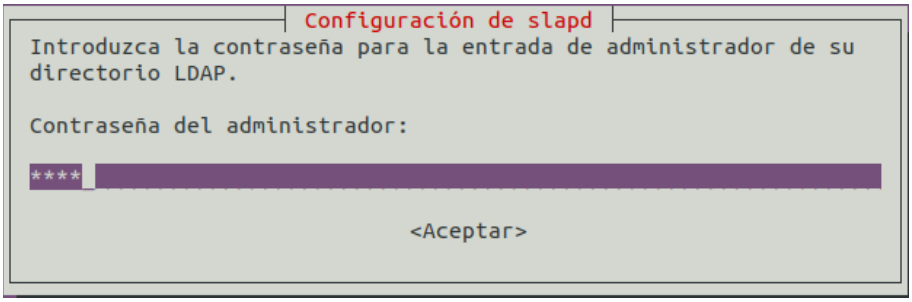


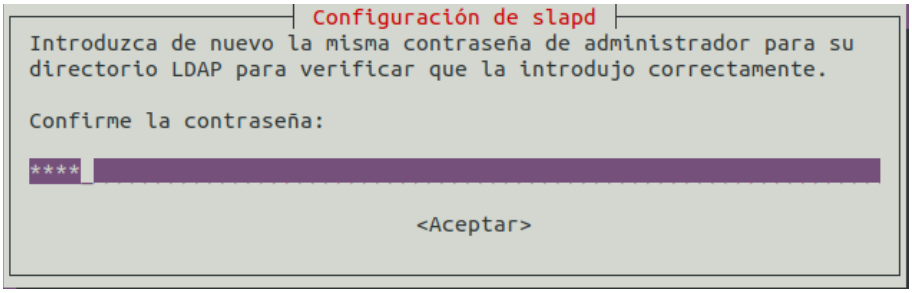
Nos pregunta el nombre de la organización. En este caso le voy a poner:

dpl-daw

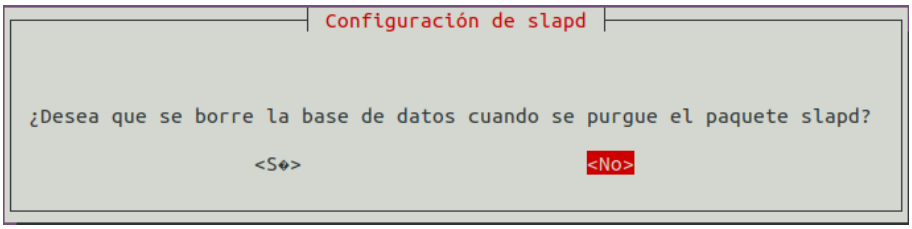


Nos vuelve a preguntar la contraseña, la que introduzcamos ahora será la definitiva, podemos poner la misma. Va a solicitarla dos veces por seguridad para evitar errores tipográficos.

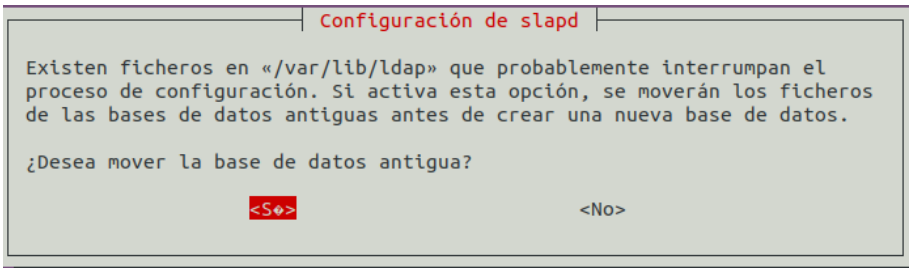




El siguiente diálogo nos pregunta si queremos que se elimine la base de datos LDAP, al borrar el paquete slapd del sistema. Elegimos **No**.



Por último nos pregunta si queremos mover los datos de alguna base de datos antigua de directorio LDAP a la nueva que estamos configurando. En nuestro caso, como no tenemos ninguna antigua no va afectar en nada, lo dejaremos en SI y finalizaremos la configuración.




```
informatica@informatica-VirtualBox:~$ sudo dpkg-reconfigure slapd
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.4.49+dfsg-2ubuntu1.8... d
one.
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
```

Si volvemos a jecutar el slapcat, comprobamos que se han modificado los atributos.

#sudo slapcat

```
informatica@informatica-VirtualBox:~$ sudo slapcat
[sudo] contraseña para informatica:
dn: dc=dpl-daw,dc=ldap
objectClass: top
objectClass: dcObject
objectClass: organization
o: dpl-daw
dc: dpl-daw
structuralObjectClass: organization
entryUUID: 86bce1ec-096c-103c-8cd8-6d9020d712d4
creatorsName: cn=admin,dc=dpl-daw,dc=ldap
createTimestamp: 20220114100019Z
entryCSN: 20220114100019.928196Z#000000#000#000000
modifiersName: cn=admin,dc=dpl-daw,dc=ldap
modifyTimestamp: 20220114100019Z

dn: cn=admin,dc=dpl-daw,dc=ldap
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9OXBXY0UyVkpOTng5ZnM4NzlXbWtwdHZqRnorM3doaU8=
```

3. **Crear dos grupos y en cada grupo dos usuarios con sus respectivas contraseñas.**

   Con nuestro servicio instalado y configurado, el siguiente paso es crear la estructura básica del directorio. Es decir, crearemos la estructura jerárquica del árbol (***DIT – Directory Information Tree***).

   Una de las formas más sencillas de añadir entradas al directorio es mediante ficheros **LDIF (*LDAP Data Interchange Format*)**. Básicamente se tratan de ficheros en texto plano con un formato particular que debemos conocer para poder construirlos correctamente. El formato básico de una entrada es el siguiente:

```
# comentario
dn: <nombre distintivo único>
<atributo>: <valor>
<atributo>: <valor>
...
```

Procedemos a crear el fichero base que contenga los objetos básicos del directorio.

#nano base.ldif

En él vamos a crear dos entradas referentes a **unidades organizativas: «usuarios» y «grupos»**. Las unidades organizativas, como su propio nombre indica, son atributos que nos van a servir para estructurar de forma idónea nuestro árbol del directorio LDAP. Estas dos entradas serán la base de nuestro árbol ya que de ellas dependerán varias entradas más adelante.

```
  GNU nano 4.8                          base.ldif
dn: ou=usuarios,dc=dpl-daw,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: usuarios

dn: ou=grupos,dc=dpl-daw,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: grupos
```

Tras crear el fichero base.ldif lo cargamos en LDAP con la siguiente orden.

#sudo ldapadd -x -D cn=admin,dc=dpl-daw,dc=ldap -W -f base.ldif

-x = Autenticación Simple.

-D= Unir a DN (Distinguished Name, Nombre distinguido)

-W= Solicitud de contraseña de validación.

-f= Directorio de lectura de operaciones

```
informatica@informatica-VirtualBox:~$ sudo ldapadd -x -D cn=admin,dc=dpl-daw,dc=
ldap -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=dpl-daw,dc=ldap"

adding new entry "ou=grupos,dc=dpl-daw,dc=ldap"
```

Tras cargar las entradas pasamos a crear nuevas entradas que colgarán de las unidades organizativas. Creamos una entrada para un **grupo** y una entrada para un **usuario**.

Antes de empezar, por seguridad **generaremos una contraseña cifrada** con la siguiente orden.

#slappasswd

Nos pedirá la contraseña dos veces

```
informatica@informatica-VirtualBox:~$ slappasswd
New password:
Re-enter new password:
{SSHA}V53LYZvQFUadVkJ7qU+W+jF5uIFhabj+
```

Y obtendremos la clave cifrada por el algoritmo criptográfico SSHA.

Ahora que tenemos la contraseña cifrada creamos nuestro fichero **content.ldif**, donde vamos a crear dos entradas:

- Dos **grupos, uno** llamado **griegos** y otro **romanos** que colgará de la unidad organizativa grupos.
- Los usuarios se distribuirán de la siguiente manera en los grupos:
  - Grupo griegos. Atenea y Cronos.
  - Grupo romanos. Minerva y Saturno.

Inicialmente voy aprovechar que tenemos creado el archivo **base.ldif para hacer una copia a content.ldif**.

#cp base.ldif content.ldif

Editamos content.ldif para declarar la estructura indicada.

#nano content.ldif

```
  GNU nano 4.8                          content.ldif
dn: ou=usuarios,dc=dpl-daw,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: usuarios

dn: ou=grupos,dc=dpl-daw,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: grupos

dn: uid=minerva,ou=usuarios,dc=dpl-daw,dc=ldap
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: minerva
sn: minerva
uid: minerva
userPassword: {SSHA}V53LYZvQFUadVkJ7qU+W+jF5uIFhabj+
dn: uid=saturno,ou=usuarios,dc=dpl-daw,dc=ldap
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: saturno
sn: saturno
uid: saturno
userPassword: {SSHA}V53LYZvQFUadVkJ7qU+W+jF5uIFhabj+

dn: uid=cronos,ou=usuarios,dc=dpl-daw,dc=ldap
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: cronos
sn: cronos
uid: cronos
userPassword:
```

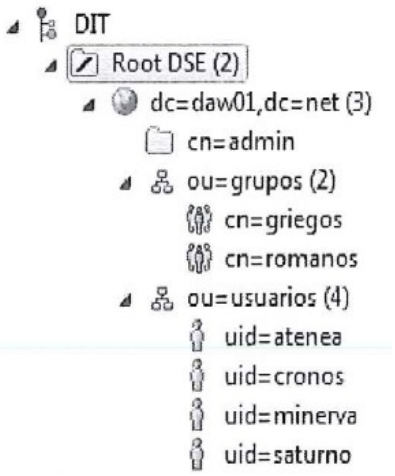
```
dn: uid=atenea,ou=usuarios,dc=dpl-daw,dc=ldap
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: atenea
sn: atenea
uid: atenea
userPassword: {SSHA}V53LYZvQFUadVkJ7qU+W+jF5uIFhabj+

dn: cn=romanos,ou=grupo,dc=dpl-daw,dc=ldap
objectClass: groupOfUniqueNames
objectClass: top
cn: romanos
uniqueMember: uid=minerva,ou=usuarios,dc=dpl-daw,dc=ldap
uniqueMember: uid=saturno,ou=usuarios,dc=dpl-daw,dc=ldap

dn: cn=griegos,ou=grupo,dc=dpl-daw,dc=ldap
objectClass: groupOfUniqueNames
objectClass: top
cn: romanos
uniqueMember: uid=atenea,ou=usuarios,dc=dpl-daw,dc=ldap
uniqueMember: uid=cronos,ou=usuarios,dc=dpl-daw,dc=ldap
```

De la misma forma que anteriormente, procedemos a cargar las entradas en el directorio LDAP ejecutando la siguiente instrucción.

#sudo ldapadd -x -D cn=admin,dc=dpl-daw,dc=ldap -W -f content.ldif

```
informatica@informatica-VirtualBox:~$ sudo ldapadd -x -D cn=admin,dc=dpl-daw,dc=
ldap -W -f content.ldif
[sudo] contraseña para informatica:
Enter LDAP Password:
adding new entry "ou=usuarios,dc=dpl-daw,dc=ldap"
ldap_add: Already exists (68)
```

DIT. Estructura del directorio de información.



Hay herramientas para administrar el LDAP como son el phpLDAPadmin o IDEs de desarrollo como el Eclipse entre otros, de manera que se puede gestionar de manera gráfica.