

INSTALACIÓN DE “OpenLDAP” EN SO LINUX

La instalación que se va a realizar es el servidor OpenLDAP, llamado slapd, y sus utilidades, que es el servicio DNS para SO Linux bajo la versión de Debian y, más concretamente, de Kali Linux. La instalación se puede realizar en una máquina virtual que posee una imagen de este sistema operativo o en una máquina física. El procedimiento de instalación es el siguiente:

1. Para comenzar, habría que tener conexión a Internet y actualizados los repositorios de la máquina virtual o física en la que vayamos a instalar el servicio de directorio LDAP.

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

2. Saldrá una pantalla informativa, tras la instalación, que se podrá salir de ella pulsando “q”. Posteriormente el servicio pedirá una contraseña de administrador: se tecleará **admin** dos veces, aunque se puede teclear la que se crea oportuna.

IMPORTANTE: Esta contraseña será la del usuario que tendrá control total de la administración sobre el directorio que vamos a montar. Por eso, en un caso real, esta contraseña deberá ser una **contraseña robusta**.

3. A continuación, se va a configurar slapd mediante el siguiente comando, y en la pantalla se dejará seleccionada la opción por defecto (**NO**).

```
dpkg-reconfigure slapd
```

4. Cuando se pulse esta opción, saldrá otra pantalla donde habrá que teclear el dominio que sea necesario instalar en el servicio de directorio, en nuestro caso **ejemplo.com**. A continuación, se pondrá el nombre de la organización, que será **ejemplo**, siguiendo la nomenclatura anterior.
5. El siguiente paso sería teclear de nuevo la contraseña de administrador dos veces, que en nuestro caso, sería **admin**. Por último, pregunta la configuración si se quiere

purgar la base de datos; la respuesta más adecuada es **SI** (aunque no pasa nada si de deja por defecto en NO). Posteriormente, pregunta si se quiere mover la base de datos de LDAP anterior; la respuesta es **SÍ**.

6. Ya se tiene instalado el servicio de directorio LDAP, por lo que lo único que nos queda es subir el servicio y bajar el servicio, y esto se realiza con los siguientes comandos:

```
service slapd start
```

```
service slapd stop
```

```
ps -efl | grep slapd (Con ésto vemos un listado de los procesos activos y comprobamos también que está corriendo el servicio de directorio)
```

7. Una vez que levantemos el servicio, el servidor LDAP estará escuchando por el puerto 389 de TCP y UDP. Para conexiones seguras mediante SSL sería el puerto 636.
8. Otros comandos que nos permiten gestionar LDAP son los siguientes:
 - **service slapd reload**. Permite recargar la configuración del servicio sin reiniciarlo.
 - **service slapd restart**. Reinicia el servicio.
 - **service slapd force-reload**. Fuerza la recarga de la configuración del servicio.
 - **service slapd status**. Comprueba si el servicio está activo o inactivo.
9. Se van a detallar algunas herramientas del servidor LDAP. Para mostrar la información que tenemos se debe teclear el siguiente comando:

```
slapcat
```

```
slapdd: permite insertar entradas desde un fichero LDIF.
```

```
slapindex: regenera los índices.
```

```
slappasswd: sirve para obtener una contraseña encriptada.
```

10. Por último, veremos algunos comandos para agregar información al servicio de directorio LDAP desde el punto de vista del cliente, como son los siguientes:

- **ldapsearch**: para seleccionar los objetos de un directorio a partir de cierta raíz del árbol de directorio. Un ejemplo de sentencia sería la siguiente (buscaría todos los objetos dentro de nuestro dominio ejemplo.com):

```
ldapsearch -b "dc=ejemplo,dc=com" "objectclass=*" 
```

- **ldapmodify**: para modificar los objetos de un directorio a partir de cierta raíz del servicio de directorio. Un ejemplo sería:

```
ldapmodify -D cn=admin,dc=ejemplo,dc=com -W admin -f Modify.ldif -c 
```

La línea anterior permite conectarnos como administrador a nuestro dominio ejemplo.com y modificar en el servicio de directorio la información contenida en el fichero Modify.ldif. La opción -c permite reportar los errores.

- **ldapadd**: para añadir objetos a nuestro servicio de directorio.

```
ldapadd -D cn=admin,dc=ejemplo,dc=com -W admin -f Add.ldif -c 
```

La línea anterior permite conectarnos como administrador a nuestro dominio ejemplo.com e introducir en el servicio de directorio el fichero Add.ldif. La opción -c permite reportar errores.

- **ldapdelete**: para borrar entradas de nuestro servicio de directorio.

```
ldapdelete -D "cn=root,dc=ejemplo,dc=com">cn=Juan Muñoz,  
ou=usuarios, dc=ejemplo,dc=com 
```