Configuración de un servidor OpenLDAP

LDAP (*Lightweight Directory Access Protocol*) es un protocolo estándar de acceso a un servicio de Aller directorio distribuido, definido por la RFC 4511. Permite juntar en un arborescencia de directorio el conjunto de datos que conciernen a los diferentes objetos de una organización (cuentas de usuario, grupos, máquinas, servicios de red, edificios, etc.), y permite a los clientes LDAP acceder a los datos a través de solicitudes normalizadas.

Linux puede ser servidor y/o cliente LDAP.

1. Generalidades

En 1988, la ITU (*International Telecommunication Union*, ex-CCITT) implementó una norma que cubría los diferentes elementos necesarios para proporcionar servicios de directorio electrónico, que pudieran ser utilizables a través de una red: la norma X.500, validada a continuación por la ISO (norma ISO/IEC 9594).

Esta norma era particularmente compleja, un protocolo más simple de acceso a los servicios de mensajería derivó de ella, LDAP (*Lightweight Directory Access Protocol*). Este protocolo a continuación fue extendido para considerar un modelo completo de directorios.

Los servicios de directorios compatibles LDAP más utilizados hoy día son Microsoft ADS (*Active Directory Services*), Oracle Directory Server Enterprise Edition, IBM Tivoli Directory Server y, en el mundo del software libre, **OpenLDAP** y Apache Directory Server.

a. Estructura y terminología

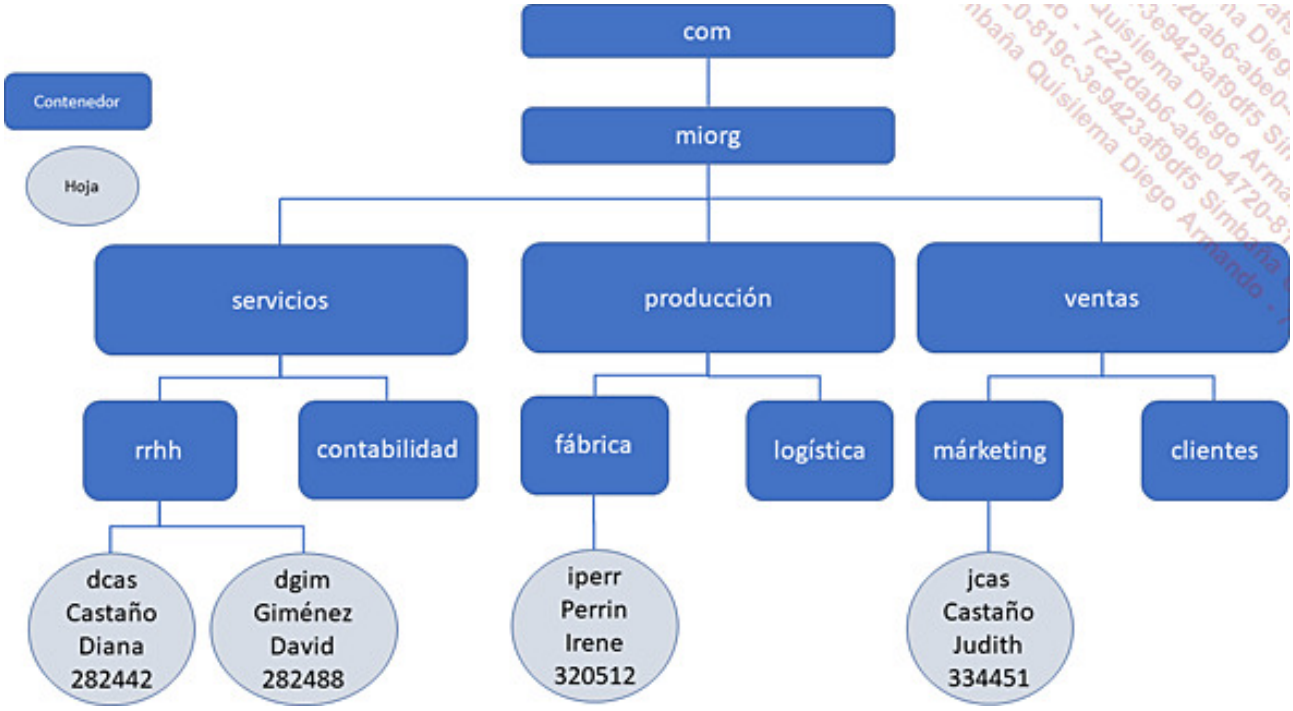
Los directorios electrónicos de tipo X.500 se basan en una estructura jerárquica, en arborescencia.

Un directorio está compuesto por objetos, que pueden contener otros objetos

opcionalmente. Los objetos de estructura se llaman **contenedores** y pueden ser de diferentes tipos: organización, dominio y unidad organizativa. Un objeto no estructurante se llama **hoja** (*leaf object*). Los diferentes datos asociados a un objeto son sus **atributos**.

Ejemplo

Directorio LDAP basado en una estructura de tipo dominio DNS.



b. Esquema

El conjunto de los tipos de objetos y de los atributos de objeto que pueden figurar en un directorio están definidos en el **esquema** del directorio.

El esquema de base del directorio puede ser extendido, para definir nuevos tipos de objetos o nuevos atributos para un tipo de objeto existente.

El tipo de un objeto (unidad organizativa OU, componente de dominio DC, etc.) se llama **clase**. Una clase de objetos está definida por el conjunto de sus **atributos**. De entre los cuales, el CN (*Common Name*), nombre simple, sirve para denominar el objeto en el interior de su contenedor.

Un esquema de directorio que administra esencialmente personas (cuentas de usuario, cuentas de grupos, etc.) se designa a menudo con la palabra esquema de "páginas blancas " (whitepages), por analogía con los antiguos directorios telefónicos de papel.

c. Designación de los objetos

Todos los objetos de un directorio se sitúan en una arborescencia. Para designar uno sin ambigüedad, hay que utilizar su CN (*Common Name*), y especificar a continuación su posición en el directorio subiendo los distintos contenedores hasta la raíz de la arborescencia. Esta designación completa se llama el DN (*Distinguished Name*), nombre distinguido.

Sintaxis de un DN

```
CN=NombreObj,clase1=nombreCont1,...,claseRoot=nombreRoot
```

Donde:

`CN=NombreObj`	Nombre simple del objeto (*Common Name*).
`claseX=nombreContX`	Clase (`OU`, `DC`…) y nombre simple del contenedor.
`claseRoot=nombreRoot`	Clase y nombre simple del contenedor raíz.

El DN, nombre distinguido, se usa para designar un objeto del directorio, es obligatorio para las autenticaciones.

Ejemplo

En el ejemplo de directorio presentado anteriormente, la cuenta de directorio de la usuaria Judith Castaño tiene como CN jcas. Su DN será:

```
CN=jcas,OU=márketing,DC=ventas,DC=miorg,DC=com
```

d. Autenticación a través de un directorio LDAP

Los directorios integran un mecanismo de seguridad, basado en la autentificación del usuario. Las solicitudes de consulta no exigen, generalmente, una autenticación y se pueden efectuar en modo anónimo. Las solicitudes de escritura necesitan, sin embargo, de una autenticación. El usuario debe proporcionar el nombre distinguido (DN) y la contraseña de una cuenta del directorio que tenga los derechos necesarios sobre los elementos que quiere gestionar. A este mecanismo de autenticación se le llama *bind*.

e. El formato LDIF

El formato estándar LDIF (*LDAP Data Interchange Format*) define el contenido de un archivo de texto que puede contener toda o una parte de los datos de un directorio LDAP. Permite efectuar operaciones de importación o exportación con un servicio de directorio LDAP. Está gestionado por múltiples herramientas LDAP.

Ejemplo

Definición de la cuenta de usuario de Judith Castaño, del ejemplo anterior, en formato LDIF:

```
dn: CN=jcas,OU=márketing,DC=ventas,DC=minorg,DC=com
objectClass: person
cn: jcas
sn: Castaño
gn:Judith
NumPuesto: 334451
```

2. El servidor OpenLDAP

OpenLDAP es el servidor LDAP open source más utilizado en Linux. Lo proporcionan los paquetes de software `openldap-servers` (Red Hat) o `slapd` (Debian).

Ejemplo

Instalación del paquete `slapd` en una distribución Debian 10.

```
apt-get install slapd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 libodbc1
Paquetes sugeridos:
 libmyodbc odbc-postgresql tdsodbc unixodbc-bin ldap-utils libsasl2-modules-
gssapi-mit | libsasl2-modules-gssapi-heimdal
Se instalarán los siguientes paquetes NUEVOS:
 libodbc1 slapd
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 1.660 kB de archivos.
Se utilizarán 16,7 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
[...]
```

La instalación solicita la contraseña de la cuenta de administración del directorio.

```
[...]
Configurando slapd (2.4.47+dfsg-3+deb10u6) ...
 Creating new user openldap... done.
 Creating initial configuration... done.
 Creating LDAP directory... done.
Procesando disparadores para systemd (241-7~deb10u8) ...
Procesando disparadores para man-db (2.8.5-2) ...
Procesando disparadores para libc-bin (2.28-10) ..
```

a. Gestión del servicio

El servidor OpenLDAP está gestionado por un script `init System V` o a través de `systemd`. El nombre del script y del servicio `systemd` es en general `slapd`.

Ejemplo

Script de inicio y situación del servicio del servidor LDAP después de haberlo instalado en una distribución Debian 10:

```
ls /etc/init.d/slap*
/etc/init.d/slapd
systemctl status slapd
  slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
  Loaded: loaded (/etc/init.d/slapd; generated)
  Active: active (running) since Sun 2021-11-07 21:15:40 CET; 1min 35s ago
    Docs: man:systemd-sysv-generator(8)
   Tasks: 3 (limit: 2347)
  Memory: 3.1M
  CGroup: /system.slice/slapd.service
          11570 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F
/etc/ldap/slapd.d

nov 07 21:15:40 pc-220 systemd[1]: Starting LSB: OpenLDAP standalone server (Lightweight
Directory Access Protocol)...
nov 07 21:15:40 pc-220 slapd[11570]: slapd starting
nov 07 21:15:40 pc-220 systemd[1]: Started LSB: OpenLDAP standalone server (Lightweight
Directory Access Protocol).
nov 07 21:15:40 pc-220 slapd[11559]: Starting OpenLDAP: slapd.
```

Situación del servicio del servidor LDAP después de haberlo instalado en una distribución CentOS 7:

```
systemctl status slapd
  slapd.service - OpenLDAP Server Daemon
  Loaded: loaded (/usr/lib/systemd/system/slapd.service; disabled;
vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:slapd
          man:slapd-config
          man:slapd-hdb
          man:slapd-mdb
          file:///usr/share/doc/openldap-servers/guide.html
```

b. Configuración del servicio de directorio

En un entorno elemental, como el que se tiene que conocer para la certificación LPIC-2, la configuración inicial es relativamente simple. Básicamente hay que determinar el contexto de base y el punto de inicio de la arborescencia en el que se encuentran todos los objetos del directorio.

La configuración principal se encuentra en el archivo `slapd.conf` (o, en las versiones recientes, en `ldap.conf`), generalmente situado en el directorio `/etc/ldap` o `/etc/openldap`. Este archivo contiene en particular la declaración de la cuenta de administración del directorio así como su contraseña.

Algunas versiones de OpenLDAP usan el directorio `slapd.d` (en `/etc/ldap` o `/etc/openldap`). En ese caso, los elementos almacenados en el directorio son gestionados dinámicamente por el servicio de gestión de configuración, `slapd-config`.

Definición del contexto de base

```
suffix      "dc=DominioRaíz"
```

Donde `DominioRaíz` representa el contexto principal, punto de inicio de la arborescencia.

Declaración de la cuenta de administración del dominio

```
rootdn      "cn=CuentaAdmin,dc=DominioRaíz"
```

Donde `CuentaAdmin` representa la cuenta del administrador del directorio.

Declaración de la contraseña de la cuenta de administración del dominio

```
rootpw {TypeCrypt}contraseña_cifrada
```

Donde `TypeCrypt` representa el algoritmo de hash usado para cifrar la contraseña (`SHA1`, `MD5` o `crypt`).

Se puede especificar una contraseña sin cifrar, aunque esté desaconsejado por razones de seguridad. La sintaxis es la siguiente:

```
rootpw contraseña_no_cifrada
```

Nivel de registro

```
Loglevel Número
```

Donde `Nœmero` es un número que combina los diferentes valores de los tipos de eventos que se querrán registrar en archivo registro del daemon de registros (`syslogd` o equivalente), enviados por el servidor LDAP.

Los archivos que constituyen la base de datos del directorio se encuentran, por defecto, en el directorio `/var/lib/ldap` . Por seguridad, este directorio y los archivos que se encuentran dentro deberán estar asociados a la cuenta de servicio de OpenLDAP (generalmente la cuenta de usuario `ldap` o `openldap`). Por otro lado, esta cuenta debe tener los derechos de escritura en el directorio y en los archivos que se encuentran en su interior.

Ejemplo

Implementación de control de acceso en el directorio y los archivos.

```
chown -R ldap:ldap /var/lib/ldap
ls -ld /var/lib/ldap /var/lib/ldap/*
drwx------. 2 ldap ldap     126 24 oct   05:03 /var/lib/ldap
-rw-r--r--. 1 ldap ldap    2048 24 oct   02:35 /var/lib/ldap/alock
-rw-------. 1 ldap ldap  262144 24 oct   02:35 /var/lib/ldap/__db.001
```

```
-rw-------. 1 ldap ldap    32768 24 oct   02:35 /var/lib/ldap/__db.002
-rw-------. 1 ldap ldap    49152 24 oct   02:35 /var/lib/ldap/__db.003
-rw-------. 1 ldap ldap     8192 24 oct   02:35 /var/lib/ldap/dn2id.bdb
-rw-------. 1 ldap ldap    32768 24 oct   02:35 /var/lib/ldap/id2entry.bdb
-rw-------. 1 ldap ldap 10485760 24 oct   02:35 /var/lib/ldap/log.0000000001
```

c. Generación de una contraseña cifrada: slappasswd

El comando `slappasswd` escribe en la salida estándar, a partir de una cadena de caracteres, la cadena de caracteres `{TypeCrypt}contraseæa_cifrada` .

Ejemplo

```
slappasswd -s contraseña
{SSHA}ifnqWW/158iL6d0vbCkwuDjE+JZVo9xf
```

Declaramos la contraseña en el archivo de configuración:

```
vi /etc/ldap/ldap.conf
[...]
rootpw {SSHA}ifnqWW/158iL6d0vbCkwuDjE+JZVo9xf
[...]
```

d. Control de la configuración: slaptest

El comando `slaptest` permite comprobar el contenido de los archivos de configuración del servicio de directorios.

Sintaxis

```
slaptest -u -v
```

Donde:

`-v`	Visualización detallada.
`-u`	Solamente comprueba el archivo de configuración.

Ejemplo

```
slaptest -u -v
config file testing succeeded
```

e. Inicio del servidor

Una vez que se haya comprobado la configuración, iniciamos el servicio `slapd`, con el script de arranque o a través de `systemd`.

Ejemplo

```
systemctl start slapd
ps -ef | grep slapd
openldap  9387     1  0 16:34 ?        00:00:00 /usr/sbin/slapd -h
ldap:/// ldapi:/// -g openldap -u openldap -F /etc/ldap/slapd.d
```

f. Herramientas LDIF

Varios comandos usan el formato LDIF para exportar o modificar el contenido del directorio.

El comando `slapcat` exporta en formato LDIF todo o una parte del contenido del directorio.

Sintaxis

```
slapcat [-v] [-a Filtro] [-s dnSubArb] [-b Sufijo] [-l ArchivoLDIF]
```

Donde:

`-v`	Visualización detallada.
`-b Sufijo`	Identificador del directorio que se tendrá que modificar.
`-l ArchivoLDIF`	Archivo LDIF que se quiera integrar en el directorio.
`-a Filtro`	Criterios de selección de los objetos que se quieran extraer.
`-s dnSubArb`	DN de la parte de la arborescencia que se va a extraer.

Sin la opción `-l`, el comando escribe en formato LDIF en la salida estándar. Sin la opción `-b`, el comando usa el directorio por defecto del servidor local.

Ejemplo

Visualización en formato LDIF el contenido por defecto del directorio del servidor OpenLDAP local:

slapcat

```
dn: dc=midns,dc=es
objectClass: top
objectClass: dcObject
objectClass: organization
o: midns.es
dc: midns
structuralObjectClass: organization
entryUUID: de2349d6-3929-103a-92c4-c56d053d88fc
creatorsName: cn=admin,dc=midns,dc=es
createTimestamp: 20200602143410Z
entryCSN: 20200602143410.751379Z#000000#000#000000
modifiersName: cn=admin,dc=midns,dc=es
```

```
modifyTimestamp: 20200602143410Z

dn: cn=admin,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9QkxZZkUxTXE5ODFRcUZQRmxVQTFGNzhycDU4L01TaTE=
structuralObjectClass: organizationalRole
entryUUID: de2896e8-3929-103a-92c5-c56d053d88fc
creatorsName: cn=admin,dc=midns,dc=es
createTimestamp: 20200602143410Z
entryCSN: 20200602143410.786222Z#000000#000#000000
modifiersName: cn=admin,dc=mindns,dc=es
modifyTimestamp: 20200602143410Z
```

El comando `slapadd` añade un elemento en el directorio.

Sintaxis corriente

```
slapadd [ -v] [-b Sufijo] [-f ArchivoLDIF]
```

Donde:

`-v`	Visualización detallada.
`-b Sufijo`	Identificador del directorio que se quiera modificar.
`-l ArchivoLDIF`	Archivo LDIF que se quiere integrar en el directorio.

Sin la opción `-l`, el comando lee los elementos que tendrá que añadir al directorio de la entrada estándar.
Sin la opción `-b`, el comando usa el directorio por defecto del servidor local.

Ejemplo

Incorporación de una cuenta de usuario en el directorio:

Creamos un archivo en formato LDIF, con los atributos de base del objeto que se quiera añadir en el directorio:

```
vi ldap.ldif
dn: cn=alejandro,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: alejandro
userPassword:alejandro
description: LDAP user
structuralObjectClass: organizationalRole
```

Añadimos el objeto:

```
slapadd -l ldap.ldif
_#################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

Comprobamos el contenido del directorio:

```
slapcat
[...]
dn: cn=alejandro,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: alejandro
userPassword:: cGJh
description: LDAP user
structuralObjectClass: organizationalRole
entryUUID: bbac6c88-39b6-103a-84c0-8bc37ab292fb
creatorsName: cn=admin,dc=midns,dc=es
createTimestamp: 20200603072231Z
entryCSN: 20200603072231.968746Z#000000#000#000000
```

```
modifiersName: cn=admin,dc=midns,dc=es
modifyTimestamp: 20200603072231Z
```

Se ha añadido el objeto.

g. Índice del directorio

El comando `slapindex` permite indexar o volver a indexar el contenido del directorio, para mejorar el rendimiento de este. Este comando tiene que ser ejecutado con la cuenta de usuario del servicio del servidor OpenLDAP (a través del comando `sudo -u`, por ejemplo).

El comando debería ser ejecutado cuando el servidor no esté corriendo. Este comando puede tomar mucho tiempo en ejecutarse.

Sintaxis

```
slapindex [-v] -b Sufijo
```

Donde:

`-v`	Visualización detallada.
`-b Sufijo`	Identificador del directorio que tendrá que modificarse.

Ejemplo

```
sudo -u openldap slapindex
```