Uso de un cliente LDAP

Además de sus funcionalidades de cliente LDAP, para la identificación y la autenticación de los usuarios, Linux dispone de comandos que permiten interactuar con el servidor LDAP. Estos comandos se proporcionan con el paquete de software `ldap-utils` (Debian) o `openldap-clients` (Red Hat).

1. Archivo de configuración del cliente

Aunque no sea obligatorio, el archivo de configuración permite definir opciones y valores por defecto, que pueden ser usados por la biblioteca LDAP. Este archivo, `slapd.conf` (o, en versiones recientes, `ldap.conf`), se encuentra, por defecto, en el directorio `/etc/ldap` o `/etc/openldap`.

El archivo permite definir variables, valores por defecto para los comandos que usan la biblioteca, entre ellos:

`BASE`	Sufijo del directorio por defecto.
`URI`	URI de los servidores LDAP por defecto.
`HOST`	Nombre de host o dirección de los servidores LDAP por defecto.

Ejemplo

Valores por defecto para los comandos LDAP de un cliente LDAP:

```
BASE    dc=intra,dc=es
URI     ldap://servldap.intra.es ldap:// servldap1.intra.es:666
HOST    servldap.intra.es
```

2. Interrogación del directorio: ldapsearch

El comando `ldapsearch` permite efectuar solicitudes de interrogación al directorio LDAP y recuperar el resultado en el formato normalizado LDIF (*LDAP Data Interchange Format*).

Este comando admite múltiples opciones. Permite obtener toda la información o una parte de ella almacenada en la arborescencia del directorio LDAP del servidor.

El caso más simple consiste en solicitar la exportación total de toda la información del directorio local (equivalente del comando `slapcat`). Esto permite comprobar la presencia de un objeto o que el servidor de directorio responde a la solicitudes.

Sintaxis para mostrar el contenido de un directorio

```
ldapsearch [-x] -b Sufijo
```

Donde:

`-x`	Solicitud anónima (sin contraseña).
`-b Sufijo`	Identificador del directorio que se va a interrogar.

Ejemplo

```
ldapsearch -x -b dc=midns,dc=es
# extended LDIF
#
```

```
# LDAPv3
# base <dc=midns,dc=es> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# midns.es
dn: dc=midns,dc=es
objectClass: top
objectClass: dcObject
objectClass: organization
o: midns.es
dc: midns

# admin, midns.es
dn: cn=admin,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# pba, midns.es
dn: cn=pba,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: pba
description: LDAP user

# user1, midns.es
dn: cn=user1,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: user1
description: LDAP user

# search result
search: 2
result: 0 Success

# numResponses: 5
```

```
# numEntries: 4
```

Sintaxis con criterios de selección

```
ldapsearch -x -D dn_admin [ -W | -w Contraseña] -h ip_servidor -b contexto -s
sub atributo=valor
```

Donde:

`-x`	Autenticación simple.
`-D dn_admin`	DN de la cuenta de usuario que realiza la solicitud.
`-W | -w Contraseña`	Contraseña de la cuenta (`-W`, tecleada en la entrada estándar).
`-h ip_servidor`	Dirección IP del servidor LDAP que se va a interrogar.
`-b contexto`	Contexto de inicio de la búsqueda.
`-s sub`	Búsqueda recursiva a partir del contexto de inicio.
`atributo=valor`	Criterio de selección. Caracteres joker (`*`, …) autorizados en `valor`.

Ejemplo

Búsqueda de todos los usuarios del directorio cuyo nombre empieza por `us`.

```
ldapsearch -x -D cn=pba,dc=midns,dc=es -W -s sub -b dc=midns,dc=es cn=us*
Enter LDAP Password: XXX
# extended LDIF
#
# LDAPv3
# base <dc=midns,dc=es> with scope subtree
# filter: cn=us*
# requesting: ALL
#

# user1, midns.es
dn: cn=user1,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: user1
description: LDAP user

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

3. Gestión de la contraseña: ldappasswd

El comando `ldappasswd` permite asignar una contraseña cifrada a un usuario del directorio.

Sintaxis

```
ldappasswd [-x] [-D dn_solicitante] [ -W | -w Contraseña] [-h ip_servidor] [-S | -s ContraseñaUsuario] [DNUsuario]
```

Donde :

`-x`	Autenticación simple.
`-D dn_solicitante`	DN de la cuenta que efectúa la solicitud.
`-W | -w Contraseæa`	Contraseña del solicitante (`-W`, tecleada en la entrada estándar).
`-h ip_servidor`	Dirección IP del servidor LDAP que se va a interrogar.
`-S | -s ContraseæaUsuario`	Nueva contraseña (`-S`, tecleada en la entrada estándar).
`DNUsuario`	DN de la cuenta que se tiene que cambiar la contraseña.

Sin argumentos, el comando modifica la contraseña del usuario actual, en el directorio del servidor local.

Ejemplo

Modificación de la contraseña de un usuario, hecha por el administrador del directorio.

```
ldappasswd -x -D cn=admin,dc=midns,dc=es -w contraseñaroot -s contraseña
cn=user1,dc=midns,dc=es
```

Lo comprobamos, interrogando al directorio con la cuenta de administración:

```
ldapsearch -x -D cn=admin,dc=midns,dc=es -W -s sub -b dc=midns,dc=es
cn=user1 Enter LDAP Password: XXX
# extended LDIF
#
# LDAPv3
```

```
# base <dc=midns,dc=es> with scope subtree
# filter: cn=user1
# requesting: ALL
#

# user1, midns.es
dn: cn=user1,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: user1
description: LDAP user
userPassword:: e1NTSEF9VTVaUTQ2bDQrTDZVbEQwbHpmMGRlVm5oVTdIWXVpUXU=

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

La contraseña del usuario se ha almacenado cifrada en el directorio.

4. Incorporación de objetos en el directorio usando ldapadd

El comando `ldapadd` añade un objeto, descrito en formato LDIF, en el directorio.

Sintaxis

```
ldapadd [-x] [-D dn_Admin] [ -W | -w contraseña] [-h ip_servidor]
[-f archivoLDIF]
```

Donde:

`-x`	Autenticación simple.
`-D dn_Admin`	DN de la cuenta del administrador.
`-W | -w contraseæa`	Contraseña del administrador (`-W`, tecleada en la entrada estándar).
`-h ip_servidor`	Dirección IP del servidor LDAP que se va a interrogar.
`-f archivoLDIF`	Camino de acceso al archivo LDIF.

Sin la opción `-f`, el comando lee en la entrada estándar los datos que se tienen que añadir al directorio.

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 quiere añadir al directorio:

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

Añadimos el objeto en el directorio local:

```
ldapadd -D cn=admin,dc=midns,dc=es -W -f ldap.ldif
```

```
Enter LDAP Password: XXX
adding new entry "cn=trinidad,dc=midns,dc=es"
```

Comprobamos la presencia del nuevo usurario en el directorio:

```
ldapsearch -x -D cn=admin,dc=midns,dc=es -W -s sub -b dc=midns,dc=es cn=trinidad
Enter LDAP Password: XXX
[...]
# trinidad, midns.es
dn: cn=trinidad,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: trinidad
userPassword:: bWFyaWU=
description: LDAP user

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

La cuenta de usuario se ha creado correctamente.

5. Modificación de objetos: ldapmodify

El comando `ldapmodify` modifica un objeto existente, descrito en formato LDIF, en el directorio.

Sintaxis

```
ldapmodify [-x] [-D dn_Admin] [ -W | -w contraseña] [-h ip_servidor]
```

[-f ArchivoLDIF]

Donde:

`-x`	Autenticación simple.
`-D dn_Admin`	DN de la cuenta del administrador.
`-W | -w Contraseña`	Contraseña del administrador (`-W`, tecleada en la entrada estándar).
`-h ip_servidor`	Dirección IP del servidor LDAP que se va a interrogar.
`-f archivoLDIF`	Camino de acceso al archivo LDIF.

Sin la opción `-f`, el comando lee en la entrada estándar los datos que se tendrán que añadir al directorio.

Ejemplo

Modificación de una cuenta de usuario en el directorio:

Creamos un archivo en formato LDIF, para modificar el atributo `description` de una cuenta de usuario en el directorio:

```
vi ldapactualizacion.ldif
dn: cn=trinidad,dc=midns,dc=es
changetype: modify
replace: description
description: Cuenta de Trinidad Fernández
```

Modificamos la cuenta de usuario:

```
ldapmodify -D cn=admin,dc=midns,dc=es -W -f ldapactualizacion.ldif
Enter LDAP Password: XXX
modifying entry "cn=trinidad,dc=midns,dc=es"
```

Comprobamos la modificaicón:

```
ldapsearch -x -D cn=admin,dc=midns,dc=es -W -s sub -b dc=midns,dc=es
cn=trinidad
Enter LDAP Password: XXX
[...]
# trinidad, midns.es
dn: cn=trinidad,dc=midns,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: trinidad
userPassword:: bWFyaWU=
description: Cuenta de Trinidad Fernández

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

6. Supresión de objetos: ldapdelete

El comando `ldapdelete` suprime el objeto existente que será determinado por su DN.

Sintaxis

```
ldapdelete [-x] [-D dn_Admin] [ -W | -w contraseña] [-h ip_servidor] DNobj
```

Donde:

`-x`	Autenticación simple.
`-D dn_Admin`	DN de la cuenta del administrador.
`-W | -w contraseæa`	Contraseña del administrador (`-W`, tecleada en la entrada estándar).
`-h ip_servidor`	Dirección IP del servidor LDAP que se va a interrogar.
`DNobj`	DN del objeto que se va a suprimir.

Ejemplo

Supresión de una cuenta de usuario en el directorio del servidor local:

```
ldapdelete -D cn=admin,dc=midns,dc=es -W cn=user1,dc=midns,dc=es
Enter LDAP Password: XXX
```

Comprobamos la supresión:

```
ldapsearch -x -D cn=admin,dc=midns,dc=es -W -s sub -b dc=midns,dc=es cn=u*
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=midns,dc=es> with scope subtree
# filter: cn=u*
# requesting: ALL
#

# search result
search: 2
result: 0 Success
```

```
# numResponses: 1
```

La cuenta de usuario se ha suprimido.

7. Herramientas gráficas

Existen diferentes herramientas gráficas que facilitan la gestión de los servidores LDAP y de sus directorios. Podemos citar:

- LDAP Admin Tool.
- LDAP Admin Windows LDAP Manager.
- LDAP Tool Box White Pages.
- LEX - The LDAP Explorer.
- phpLDAPadmin.
- Apache Directory Studio.
- JXplorer Java LDAP Browser.
- NetTools LDAP Search.
- Softerra LDAP Administrator.
- web2ldap.
- Active Directory Explorer.