PRÁCTICA 5.2

OPERACIONES SOBRE LDAP UTILIZANDO LDAP-UTILS

FECHA DE INICIO: 16/01/2025 **FECHA DE FINALIZACIÓN ESPERADA:** 21/01/2025

RA ASOCIADO: RA5. Verifica la ejecución de aplicaciones web comprobando los parámetros de configuración de servicios de red.

Contenido

OBJETIVOS

- Conocer el propósito de LDAP y su rol en la gestión de directorios centralizados.
- Comprender cómo gestionar usuarios y recursos en un entorno centralizado.
- Aprender a gestionar servidores OpenLDAP para administrar directorios de información.

- Dominar herramientas como ldap-utils para realizar operaciones de alta, modificación, consulta y eliminación de datos.
- Facilitar la administración mediante el uso de scripts y formatos estandarizados como LDIF (LDAP Data Interchange Format) para definir entradas y modificaciones.
- Verificar el correcto funcionamiento del servidor LDAP mediante herramientas de red y comandos específicos.

ENUNCIADO

Esta tarea aborda las operaciones básicas que pueden realizarse sobre un servidor LDAP utilizando el paquete **ldap-utils**, un conjunto de herramientas cliente que se utiliza para interactuar con servidores LDAP como OpenLDAP*. Cada sección incluye los comandos necesarios, explicaciones de su funcionamiento y ejemplos de uso.

***OpenLDAP:** Es una implementación de servidor del protocolo LDAP. Actúa como el servicio principal que gestiona y almacena la base de datos del directorio jerárquico, permitiendo la autenticación y administración de usuarios y recursos en red.

---

1. Añadir entidades

Para añadir nuevas entradas al DIT (Directorio de Información de Datos), crearemos un archivo en formato LDIF con la información necesaria.

Pasos:

1. Crear el archivo **add_entradas.ldif** con el siguiente contenido:

```
# Unidad organizativa usuarios

dn: ou=usuarios,dc=daw,dc=com
objectClass: organizationalUnit
ou: usuarios

# Unidad organizativa grupos
dn: ou=grupos,dc=daw,dc=com
objectClass: organizationalUnit
ou: grupos

# Usuario homer en la unidad organizativa grupos
dn: uid=homer,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: homer
homer mail:
homer@daw.com
userPassword: homer
```

Explicación detallada de los atributos:

- **dn (Distinguished Name):**
  - Es el identificador único de una entrada en el directorio.
  - Ejemplo: dn: uid=homer,ou=grupos,dc=daw,dc=com indica que "homer" pertenece a la unidad organizativa "grupos" dentro del dominio "daw.com".
- **uid (User ID):**
  - Identificador único del usuario dentro de una organización.
  - Ejemplo: uid: homer es el identificador del usuario Homer.
- **ou (Organizational Unit):**
  - Representa una unidad organizativa dentro del directorio.
  - Ejemplo: ou=grupos agrupa a los usuarios en "grupos".
- **dc (Domain Component):**
  - Indica los componentes del dominio.
  - Ejemplo: dc=daw,dc=com representa el dominio "daw.com".
- **objectClass:**
  - Define el esquema o tipo de objeto que se está creando.
  - Ejemplo: inetOrgPerson es una clase común que representa usuarios.
- **sn (Surname):**
  - Apellido del usuario. ○ Ejemplo: sn: simpson indica que el apellido del usuario es Simpson.
- **cn (Common Name):**
  - Nombre completo del usuario.
  - Ejemplo: cn: homer especifica el nombre "Homer".
- **mail:**
  - Correo electrónico del usuario.
  - Ejemplo: mail: homer@daw.com.
- **userPassword:**
  - ○ Contraseña del usuario en formato de texto plano o encriptado. ○ Ejemplo: userPassword: homer.

2. Ejecuta el siguiente comando para añadir estas entradas al servidor LDAP:

```
ldapadd -x -D cn=admin,dc=daw,dc=com -W -f add_entradas.ldif
```

- **-x**: Utiliza autenticación simple.

- **-D**: Define el usuario administrador.
- **-W**: Solicita la contraseña.
- **-f**: Especifica el archivo LDIF a procesar.

---

2. Búsquedas

El comando **ldapsearch** permite consultar la información almacenada en el DIT.

Ejemplos:

1. Consultar todo el DIT: `ldapsearch -x -b dc=daw,dc=com`

2. Mostrar sólo el atributo **mail** de todas las entradas: `ldapsearch -x -LLL -b dc=daw,dc=com mail`

3. Mostrar todos los atributos de las entidades con clase **inetOrgPerson**:

```
ldapsearch -x -LLL -b dc=daw,dc=com "objectClass=inetOrgPerson"
```

4. Mostrar las entidades de clase **inetOrgPerson** cuyo **cn** es "homer":

```
ldapsearch -x -LLL -b dc=daw,dc=com "(&(objectClass=inetOrgPerson)(cn=homer))"
```

---

3. Modificar entidades

Para modificar entradas existentes en el DIT, crearemos un archivo LDIF con las modificaciones necesarias.

Pasos:

1. Crear el archivo **modify_entradas.ldif** con el siguiente contenido:

```
dn: uid=bart,ou=grupos,dc=daw,dc=com
add: mobile
mobile: 999999999

dn: uid=bart,ou=grupos,dc=daw,dc=com
delete: mail

dn: uid=homer,ou=grupos,dc=daw,dc=com
changetype: modify
replace: mail
```

```
mail: homersimpson@daw.com
```

Explicación detallada:

- **add:**
  - Añade un nuevo atributo a la entrada especificada.
  - Ejemplo: `add: mobile` añade el atributo de teléfono móvil.
- **delete:**
  - Elimina un atributo existente de la entrada.
  - Ejemplo: `delete: mail` elimina el correo electrónico.
- **replace:**
  - Reemplaza el valor actual de un atributo.
  - Ejemplo: `replace: mail` cambia el correo electrónico de Homer.
- **changetype:**
  - Define el tipo de cambio a realizar (e.g., modify).

2. Ejecutar el siguiente comando para aplicar las modificaciones:

```
ldapmodify -x -D cn=admin,dc=daw,dc=com -W -f modify_entradas.ldif
```

3. Verificar los cambios realizando una búsqueda:

```
ldapsearch -x -b dc=daw,dc=com
```

---

4. Eliminar entidades

Para eliminar entradas del DIT, crearemos un archivo LDIF que contenga las entradas a borrar.

Pasos:

1. Crear el archivo **delete_entradas.ldif** con el siguiente contenido:

```
uid=homer,ou=grupos,dc=daw,dc=com
uid=bart,ou=grupos,dc=daw,dc=com
ou=usuarios,dc=daw,dc=com
ou=grupos,dc=daw,dc=com
```

2. Ejecutar el siguiente comando para eliminar las entradas:

```
ldapdelete -x -D cn=admin,dc=daw,dc=com -W -f delete_entradas.ldif
```

Explicación detallada:

- **ldapdelete:**
  - Elimina las entradas especificadas en el archivo LDIF.
  - Ejemplo: `uid=homer,ou=grupos,dc=daw,dc=com` elimina al usuario Homer.

3. Verificar que las entradas han sido eliminadas:

```
ldapsearch -x -b dc=daw,dc=com
```

DOCUMENTACIÓN

Deberás documentar los procedimientos indicando:

- los pasos realizados (comandos, modificaciones a ficheros de configuración y rutas de los mismos, etc.).

- capturas de pantalla que demuestren que se han logrado los objetivos planteados.

Añadir entradas

Creamos el archivo add_entradas.ldif con el siguiente comando:

nano ~/add_entradas.ldif (en mi caso en la raíz)

añadimos el siguiente contenido:

```
  GNU nano 6.2              /home/adrian/add_entradas.ldif
# Unidad organizativa usuarios
dn: ou=usuarios,dc=daw,dc=com
objectClass: organizationalUnit
ou: usuarios

# Unidad organizativa grupos
dn: ou=grupos,dc=daw,dc=com
objectClass: organizationalUnit
ou: grupos

# Usuario homer en la unidad organizativa grupos
dn: uid=homer,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: homer
sn: simpson
cn: homer
mail: homer@daw.com
userPassword: homer

# Usuario bart en la unidad organizativa grupos
dn: uid=bart,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: bart
sn: simpson
cn: bart
mail: bart@daw.com
userPassword: bart
```

Ahora añadiríamos las entradas al servidor LDAP con el siguiente comando:

ldapadd -x -D cn=admin,dc=daw,dc=com -W -f ~/add_entradas.ldif

```
adrian@servidor-ubuntu:~$ ldapadd -x -D cn=admin,dc=daw,dc=com -W -f ~/add_e
ntradas.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=daw,dc=com"

adding new entry "ou=grupos,dc=daw,dc=com"

adding new entry "uid=homer,ou=grupos,dc=daw,dc=com"

adding new entry "uid=bart,ou=grupos,dc=daw,dc=com"

adrian@servidor-ubuntu:~$
```

Búsquedas

ldapsearch -x -b dc=daw,dc=com

```
adrian@servidor-ubuntu:~$ ldapsearch -x -b dc=daw,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=daw,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# daw.com
dn: dc=daw,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw.com
dc: daw

# usuarios, daw.com
dn: ou=usuarios,dc=daw,dc=com
objectClass: organizationalUnit
ou: usuarios

# grupos, daw.com
dn: ou=grupos,dc=daw,dc=com
objectClass: organizationalUnit
ou: grupos

# homer, grupos, daw.com
dn: uid=homer,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: homer
sn: simpson
cn: homer
mail: homer@daw.com

# bart, grupos, daw.com
dn: uid=bart,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
```

Realizar Búsquedas

Mostrar todas las entradas del DIT:

ldapsearch -x -b dc=daw,dc=com

```
adrian@servidor-ubuntu:~$ ldapsearch -x -b dc=daw,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=daw,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# daw.com
dn: dc=daw,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw.com
dc: daw

# usuarios, daw.com
dn: ou=usuarios,dc=daw,dc=com
objectClass: organizationalUnit
ou: usuarios

# grupos, daw.com
dn: ou=grupos,dc=daw,dc=com
objectClass: organizationalUnit
ou: grupos

# homer, grupos, daw.com
dn: uid=homer,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: homer
sn: simpson
cn: homer
mail: homer@daw.com
```

Mostrar sólo los correos electrónicos:

ldapsearch -x -LLL -b dc=daw,dc=com mail

```
adrian@servidor-ubuntu:~$ ldapsearch -x -LLL -b dc=daw,dc=com
dn: dc=daw,dc=com

dn: ou=usuarios,dc=daw,dc=com

dn: ou=grupos,dc=daw,dc=com

dn: uid=homer,ou=grupos,dc=daw,dc=com
mail: homer@daw.com

dn: uid=bart,ou=grupos,dc=daw,dc=com
mail: bart@daw.com

adrian@servidor-ubuntu:~$
```

Mostrar las entidades de clase inetOrgPerson:

ldapsearch -x -LLL -b dc=daw,dc=com "objectClass=inetOrgPerson"

```
adrian@servidor-ubuntu:~$ ldapsearch -x -LLL -b dc=daw,dc=com "objectClass=i
netOrgPerson"
dn: uid=homer,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: homer
sn: simpson
cn: homer
mail: homer@daw.com

dn: uid=bart,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: bart
sn: simpson
cn: bart
mail: bart@daw.com
```

Mostrar las entidades con cn=homer:

```
adrian@servidor-ubuntu:~$ ldapsearch -x -LLL -b dc=daw,dc=com "(&(objectClas
s=inetOrgPerson)(cn=homer))"
dn: uid=homer,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: homer
sn: simpson
cn: homer
mail: homer@daw.com

adrian@servidor-ubuntu:~$
```

Modificar Entidades

Creamos el archivo modify_entradas.ldif con el siguiente comando:

nano ~/modify_entradas.ldif (en mi caso en la raíz)

```
  GNU nano 6.2          /home/adrian/modify_entradas.ldif
dn: uid=bart,ou=grupos,dc=daw,dc=com
add: mobile
mobile: 999999999

dn: uid=bart,ou=grupos,dc=daw,dc=com
delete: mail

dn: uid=homer,ou=grupos,dc=daw,dc=com
changetype: modify
replace: mail
mail: homersimpson@daw.com
```

ldapmodify -x -D cn=admin,dc=daw,dc=com -W -f modify_entradas.ldif

```
adrian@servidor-ubuntu:~$ ldapmodify -x -D cn=admin,dc=daw,dc=com -W -f modi
fy_entradas.ldif
Enter LDAP Password:
modifying entry "uid=bart,ou=grupos,dc=daw,dc=com"

modifying entry "uid=bart,ou=grupos,dc=daw,dc=com"

modifying entry "uid=homer,ou=grupos,dc=daw,dc=com"

adrian@servidor-ubuntu:~$
```

```
adrian@servidor-ubuntu:~$ ldapsearch -x -b dc=daw,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=daw,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# daw.com
dn: dc=daw,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw.com
dc: daw

# usuarios, daw.com
dn: ou=usuarios,dc=daw,dc=com
objectClass: organizationalUnit
ou: usuarios

# grupos, daw.com
dn: ou=grupos,dc=daw,dc=com
objectClass: organizationalUnit
ou: grupos

# homer, grupos, daw.com
dn: uid=homer,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: homer
sn: simpson
cn: homer
mail: homersimpson@daw.com

# bart, grupos, daw.com
dn: uid=bart,ou=grupos,dc=daw,dc=com
objectClass: inetOrgPerson
uid: bart
sn: simpson
cn: bart
```

Eliminar Entidades

nano ~/delete_entradas.ldif

```
  GNU nano 6.2                  delete_entradas.ldif
uid=homer,ou=grupos,dc=daw,dc=com
uid=bart,ou=grupos,dc=daw,dc=com
ou=usuarios,dc=daw,dc=com
ou=grupos,dc=daw,dc=com
```

Ejecutar el comando para eliminar:

ldapdelete -x -D cn=admin,dc=daw,dc=com -W -f delete_entradas.ldif

```
adrian@servidor-ubuntu:~$ ldapdelete -x -D cn=admin,dc=daw,dc=com -W -f dele
te_entradas.ldif
Enter LDAP Password:
adrian@servidor-ubuntu:~$
```

Verificamos

```
adrian@servidor-ubuntu:~$ ldapsearch -x -D "cn=admin,dc=daw,dc=com" -W -b "d
c=daw,dc=com"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=daw,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# daw.com
dn: dc=daw,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw.com
dc: daw

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
adrian@servidor-ubuntu:~$
```

(Solución 2)

```
adrian@servidor-ubuntu:~$ ldapdelete -x -D cn=admin,dc=daw,dc=com -W uid=hom
er,ou=grupos,dc=daw,dc=com
Enter LDAP Password:
adrian@servidor-ubuntu:~$ ldapdelete -x -D cn=admin,dc=daw,dc=com -W uid=bar
t,ou=grupos,dc=daw,dc=com
Enter LDAP Password:
adrian@servidor-ubuntu:~$ ldapdelete -x -D cn=admin,dc=daw,dc=com -W ou=usua
rios,dc=daw,dc=com
Enter LDAP Password:
adrian@servidor-ubuntu:~$ ldapdelete -x -D cn=admin,dc=daw,dc=com -W ou=grup
os,dc=daw,dc=com
Enter LDAP Password:
adrian@servidor-ubuntu:~$ ldapsearch -x -LLL -b dc=daw,dc=com
dn: dc=daw,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw.com
dc: daw

adrian@servidor-ubuntu:~$
```