**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

[**FECHA DE INICIO:** 16/01/2025 **FECHA DE FINALIZACIÓN ESPERADA:** 21/01/2025 1](#_Toc187912105)

[**OBJETIVOS** 1](#_Toc187912106)

[**ENUNCIADO** 2](#_Toc187912107)

[1. Añadir entidades 2](#_Toc187912108)

[2. Búsquedas 4](#_Toc187912109)

[3. Modificar entidades 4](#_Toc187912110)

[4. Eliminar entidades 5](#_Toc187912111)

[DOCUMENTACIÓN 6](#_Toc187912112)

[Añadir entradas 6](#_Toc187912113)

[Búsquedas 8](#_Toc187912114)

[Modificar Entidades 11](#_Toc187912115)

[Eliminar Entidades 13](#_Toc187912116)

# **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.

# 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 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

**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. o 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:**

o Contraseña del usuario en formato de texto plano o encriptado. o 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.

# 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"

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

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

# 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).

1. Ejecutar el siguiente comando para aplicar las modificaciones:

ldapmodify -x -D cn=admin,dc=daw,dc=com -W -f modify\_entradas.ldif

1. Verificar los cambios realizando una búsqueda:

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

# 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

1. 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:**

o Elimina las entradas especificadas en el archivo LDIF. o 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)

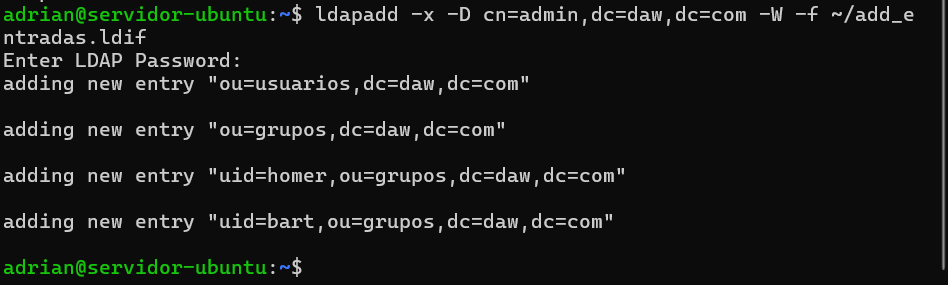
añadimos el siguiente contenido:

Texto

Descripción generada automáticamente

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**



## Búsquedas

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

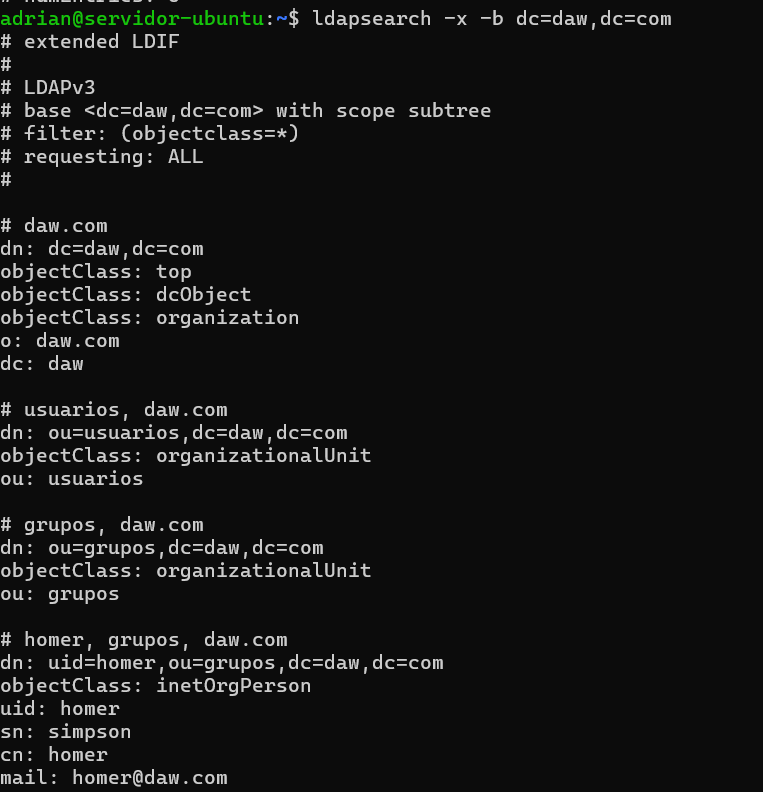
Texto

Descripción generada automáticamente

**Realizar Búsquedas**

Mostrar todas las entradas del DIT:

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



Mostrar sólo los correos electrónicos:

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

Texto

Descripción generada automáticamente

Mostrar las entidades de clase inetOrgPerson:

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

Texto

Descripción generada automáticamente

Mostrar las entidades con cn=homer:

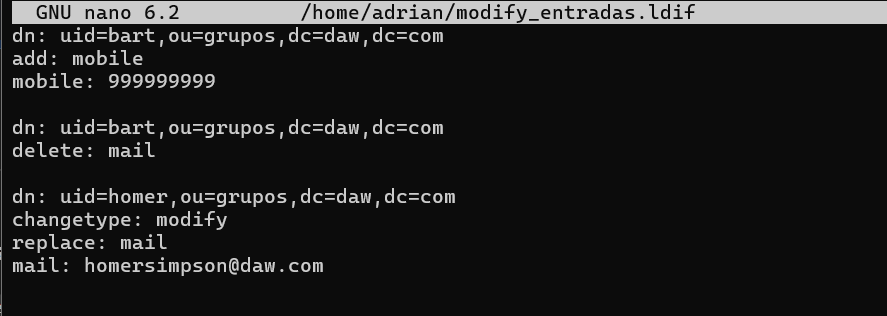
Texto

Descripción generada automáticamente

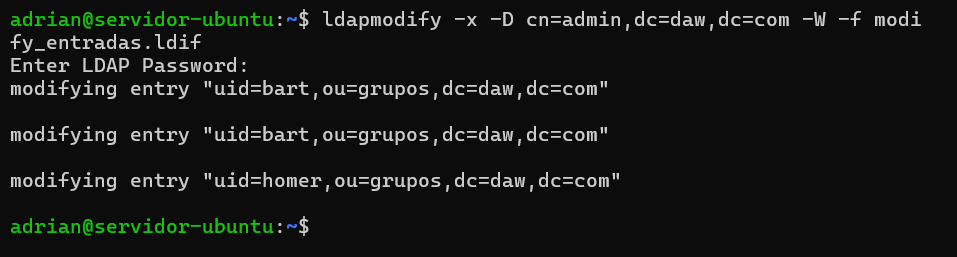
## Modificar Entidades

Creamos el archivo modify\_entradas.ldif con el siguiente comando:

**nano ~/modify\_entradas.ldif** (en mi caso en la raíz)



**ldapmodify -x -D cn=admin,dc=daw,dc=com -W -f modify\_entradas.ldif**



Texto

Descripción generada automáticamente

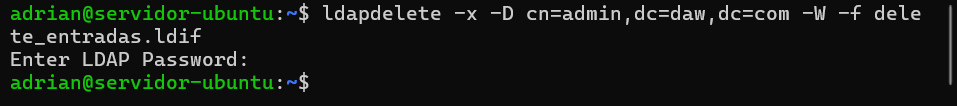
## Eliminar Entidades

**nano ~/delete\_entradas.ldif**



Ejecutar el comando para eliminar:

**ldapdelete -x -D cn=admin,dc=daw,dc=com -W -f delete\_entradas.ldif**



**Verificamos**

Texto

Descripción generada automáticamente

(Solución 2)

