📁 LPIC-2 / 🖥️ Examen 210 - Gestión de Clientes de Red - Ejercicios

*Nota: Estos ejercicios implican instalar software y modificar configuraciones sensibles de un servidor de directorio. Realízalos **SIEMPRE en una VM de prueba dedicada** con al menos otra VM como cliente. Asegúrate de que tu VM tiene acceso a internet para la instalación de paquetes y de que tu firewall permite tráfico en los puertos LDAP (389, 636). Necesitarás privilegios de superusuario (`sudo`). La configuración de un servidor LDAP es compleja; estos ejercicios son básicos y conceptuales.*

Ejercicio 10.4.1: Instalando el Software del Servidor LDAP

- **Objetivo:** Instalar el paquete del servidor OpenLDAP.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet. **VM de prueba.**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Instala el paquete (Diferencias):** `sudo apt update && sudo apt install slapd ldap-utils` (Debian/Ubuntu - `ldap-utils` incluye herramientas cliente como `ldapadd`). `sudo dnf install openldap-servers openldap-clients` (Red Hat/CentOS/Fedora).
    3. **Durante la instalación en Debian/Ubuntu, se te pedirá configurar lo básico (sufijo DN y contraseña de admin).** Proporciona un sufijo (ej: `dc=mycompany,dc=local`) y una contraseña de administrador. Anótalos. En Red Hat, la configuración inicial es manual o a través de scripts.
    4. **Verifica el estado del servicio:** `systemctl status slapd.service`. Debería estar `active (running)`.

Ejercicio 10.4.2: Verificando Reglas de Firewall para Puertos LDAP

- **Objetivo:** Asegurarse de que el firewall permite el tráfico necesario para LDAP.
- **Requisitos:** Privilegios de superusuario (`sudo`). Identificar la herramienta de firewall activa (Ej. 5.2.5). Puertos LDAP (389 TCP/UDP, 636 TCP).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Si usas `firewalld`:** Ejecuta `sudo firewall-cmd --zone=<zona> --list-services` o `sudo firewall-cmd --zone=<zona> --list-ports`. Busca los servicios `ldap` (389) y `ldaps` (636). Si no están, añádelos: `sudo firewall-cmd --zone=<zona> --add-service={ldap,ldaps} --permanent` y `sudo firewall-cmd --reload`.
    3. **Si usas `ufw`:** Ejecuta `sudo ufw status`. Busca reglas para los puertos 389 TCP/UDP y 636 TCP. Si no están, añádelas: `sudo ufw allow ldap` y `sudo ufw allow ldaps`.

4. **Si usas `iptables` directamente:** Ejecuta `sudo iptables -L -v -n`. Busca reglas que permitan el tráfico relevante.

Ejercicio 10.4.3: Identificando el Método de Configuración y Archivos Relevantes

- **Objetivo:** Determinar si el servidor usa `slapd.conf` o `cn=config`.
- **Requisitos:** Servidor LDAP instalado. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Verifica si existe `slapd.conf` y su contenido:** Ejecuta `sudo less /etc/ldap/slapd.conf` (Debian) o `sudo less /etc/openldap/slapd.conf` (Red Hat). Si este archivo existe y contiene configuración (no solo comentarios), el servidor *podría* usar este método.
    3. **Verifica si existe el directorio de configuración `cn=config` (basado en backend):** Ejecuta `ls -l /etc/ldap/slapd.d/` (Debian) o `ls -l /etc/openldap/slapd.d/` (Red Hat). Si este directorio contiene archivos `.ldif`, el servidor *probablemente* usa el método `cn=config`. **En sistemas modernos, aunque `slapd.conf` exista, a menudo solo contiene una directiva para incluir la configuración `cn=config`.**
    4. **(Conceptual):** Si la instalación te pidió un sufijo y contraseña de admin, ya se creó una configuración básica (probablemente en `cn=config`). Puedes intentar consultarla.

Ejercicio 10.4.4: (Conceptual) Configuración Básica de la Base de Datos (`cn=config` vía LDIF)

- **Objetivo:** Entender cómo se definen el sufijo, rootdn y rootpw en el método `cn=config`.
- *Requisitos:* Servidor LDAP instalado usando `cn=config`. Privilegios de superusuario (`sudo`). Conocer el sufijo DN y la contraseña de administrador (si configuraste en instalación) o estar preparado para establecerlos. **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual - Manipulando `cn=config` vía LDIF):**
    1. Abre una terminal.
    2. **Entiende que la configuración está en LDAP:** La configuración de la base de datos (`mdb`) está en una entrada bajo `olcDatabase={1}mdb,cn=config`.
    3. **Genera un hash de contraseña para el rootdn (si no lo tienes):** Ejecuta `slappasswd`. Introduce la contraseña. Te dará un hash como `{SSHA}xxxxxxxx`. Anótalo.
    4. **Crea un archivo LDIF para modificar la configuración de la base de datos (ej: modify_mdb.ldif - requiere sudo):**
       LDIF

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSuffix
olcSuffix: <Tu_Sufijo_DN> # Ej: dc=mycompany,dc=local
```

```
-
add: olcRootDN
olcRootDN: <Tu_Root_DN> # Ej: cn=admin,<Tu_Sufijo_DN>
-
add: olcRootPW
olcRootPW: <Hash_Contraseña_RootDN> # Pega el hash generado con
slappasswd
```

- Reemplaza los marcadores de posición. Las líneas con `-` indican fin de una operación de adición/modificación.

5. **Aplica el archivo LDIF (requiere autenticación en `cn=config`):** Ejecuta `sudo ldapmodify -x -D "cn=config" -W -f modify_mdb.ldif`. Te pedirá la contraseña del administrador de `cn=config` (esta es diferente a la del rootdn que estás configurando; la contraseña de `cn=config` se establece durante la instalación o inicialización de OpenLDAP y a menudo está en archivos en `slapd.d`).
6. **Verifica la configuración (difícil sin bind):** Puedes intentar `sudo slapcat -n 0 -l config.ldif` para exportar la configuración de `cn=config` a un archivo y revisarla (`-n 0` es la base de datos de configuración).

Ejercicio 10.4.5: (Conceptual) Creando el Archivo LDIF para la Base DN Inicial

- **Objetivo:** Entender cómo definir la entrada raíz de tu directorio.
- *Requisitos:* Servidor LDAP configurado con un sufijo. Acceso a la línea de comandos.
- **Desarrollo Paso a Paso (Conceptual):**
  1. Abre una terminal.
  2. **Crea un archivo LDIF para la entrada base (ej: base.ldif):**
     LDIF

```
dn: <Tu_Sufijo_DN> # Ej: dc=mycompany,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: <Tu_Organizacion> # Ej: My Company
dc: <Primer_Componente_Sufijo> # Ej: mycompany

dn: ou=users,<Tu_Sufijo_DN> # Una unidad organizacional para
usuarios
objectClass: top
objectClass: organizationalUnit
ou: users

dn: ou=groups,<Tu_Sufijo_DN> # Una unidad organizacional para grupos
objectClass: top
objectClass: organizationalUnit
ou: groups
```

     - Reemplaza los marcadores de posición. Asegúrate de que los `dc` en el sufijo DN coinciden con la estructura del dominio.
  3. **Guarda el archivo.**

Ejercicio 10.4.6: (Conceptual) Cargando Datos Iniciales con `ldapadd`

- **Objetivo:** Añadir entradas al directorio.
- *Requisitos:* Archivo LDIF de la base DN. Servidor LDAP corriendo con la base de datos configurada. Privilegios de superusuario (`sudo`) o conocer el rootdn y su contraseña. **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Añade la entrada base y las OUs usando el archivo LDIF (requiere autenticación como rootdn):** Ejecuta `ldapadd -x -D "<Tu_Root_DN>" -W -f base.ldif`. Te pedirá la contraseña del rootdn.
    3. **Verifica las entradas con `ldapsearch` (desde el cliente o el propio servidor):** Ejecuta `ldapsearch -x -H ldap://localhost -b "<Tu_Sufijo_DN>" "(objectClass=*)"`. Deberías ver las entradas que acabas de añadir. Si no las ves, revisa los logs de slapd y el comando `ldapadd`.

Ejercicio 10.4.7: (Conceptual) Creando y Añadiendo Entradas de Usuario/Grupo

- **Objetivo:** Entender cómo definir usuarios y grupos en formato LDIF.
- *Requisitos:* Directorio base creado. Acceso a la línea de comandos. **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Crea un archivo LDIF para un grupo (ej: group.ldif):**
       LDIF

```
dn: cn=sysadmins,ou=groups,<Tu_Sufijo_DN>
objectClass: top
objectClass: posixGroup # O groupOfNames
gidNumber: 2000 # Un GID unico
cn: sysadmins
# Si usas groupOfNames, añade miembros:
# member: uid=usuario1,ou=users,<Tu_Sufijo_DN>
# member: uid=usuario2,ou=users,<Tu_Sufijo_DN>
```

    3. **Crea un archivo LDIF para un usuario (ej: user.ldif):**
       LDIF

```
dn: uid=myuser,ou=users,<Tu_Sufijo_DN> # RDN es uid
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount # Para compatibilidad Unix/Linux
uid: myuser # Nombre de usuario
cn: My User # Nombre comun
sn: User # Apellido
uidNumber: 1001 # UID unico
gidNumber: 2000 # GID primario (ej: el GID del grupo sysadmins)
homeDirectory: /home/myuser # Directorio personal
loginShell: /bin/bash # Shell de login
# userPassword: {SSHA}hash_contraseña # Puedes añadir el hash aqui o
usar ldappasswd despues
```

4. **Añade las entradas usando `ldapadd` (requiere autenticación rootdn):** Ejecuta `ldapadd -x -D "<Tu_Root_DN>" -W -f group.ldif` y `ldapadd -x -D "<Tu_Root_DN>" -W -f user.ldif`.
5. **Establece la contraseña del usuario con `ldappasswd`:** Ejecuta `ldappasswd -x -D "<Tu_Root_DN>" -W -S "uid=myuser,ou=users,<Tu_Sufijo_DN>"`. Te pedirá la contraseña del rootdn y luego la nueva contraseña para `myuser`.
6. **Verifica las entradas con `ldapsearch`:** Busca el usuario o grupo que acabas de añadir.