¡Excelente! Prosigamos con el Examen 210 de LPIC-2. Después de la configuración de servidores DHCP, nos centramos en cómo integrar sistemas Linux con servicios de directorio centralizados. El objetivo 210.3 trata sobre la configuración de un cliente LDAP.

LDAP (Lightweight Directory Access Protocol) se utiliza para acceder y mantener información en un servicio de directorio. Configurar un cliente Linux para usar LDAP permite centralizar la gestión de usuarios, grupos y otra información, de modo que los usuarios pueden iniciar sesión en múltiples máquinas Linux utilizando las mismas credenciales administradas centralmente. Analizaremos las herramientas y archivos necesarios para configurar un cliente LDAP, destacando las diferencias en los métodos de integración entre las ramas Debian y Red Hat.

Comencemos con el objetivo 210.3.

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

210.3 Configuración de cliente LDAP

Teoría

Configurar un sistema Linux como cliente LDAP significa permitirle obtener información de usuarios y grupos, y autenticar usuarios, contra un servidor LDAP remoto en lugar (o además) de utilizar las bases de datos locales (`/etc/passwd`, `/etc/shadow`, `/etc/group`).

Componentes de un Cliente LDAP en Linux:

1. **Librerías Cliente LDAP y Herramientas:** El sistema necesita librerías para comunicarse con servidores LDAP. También existen herramientas de línea de comandos para consultar directorios LDAP.
    - **Paquete Principal:** `openldap-clients` (estándar en ambas ramas Debian/Red Hat, aunque puede tener dependencias adicionales). Incluye comandos como `ldapsearch`, `ldapwhoami`, `ldapadd`, `ldapdelete`.
    - `ldapsearch`: Herramienta esencial para realizar consultas a un servidor LDAP.
2. **NSS (Name Service Switch):** (Revisado de 109.4) El mecanismo del sistema para determinar dónde buscar información de nombres (usuarios, grupos, hosts, etc.). El archivo clave es `/etc/nsswitch.conf`. Para que el sistema busque usuarios y grupos en LDAP, debes añadir `ldap` o `sss` (si usas SSSD) a las líneas `passwd:`, `group:`, y `shadow:` en este archivo.
    - Ejemplo (usando `ldap` directamente): `passwd: files ldap`, `group: files ldap`, `shadow: files ldap`.
    - Ejemplo (usando `sss`): `passwd: files sss`, `group: files sss`, `shadow: files sss`.
3. **PAM (Pluggable Authentication Modules):** (Revisado de 210.2) Controla el proceso de autenticación, gestión de cuentas, contraseñas y sesiones. Para que PAM utilice LDAP para la autenticación, debes configurar los módulos PAM apropiados en los archivos de

configuración de los servicios relevantes (ej: `/etc/pam.d/login`, `/etc/pam.d/sshd`, o archivos comunes como `common-auth`).

4. **Archivos de Configuración de Cliente LDAP (Diferencias y Métodos):** Aquí reside una de las mayores diferencias entre los métodos tradicionales y SSSD. Estos archivos le dicen a las librerías y módulos *cómo* contactar y buscar en el servidor LDAP.
    - **Método Tradicional (NSS/PAM directos):** Se configuran las librerías `libnss-ldap` y `pam-ldap` directamente. El archivo de configuración puede variar significativamente en nombre y ubicación:
        - **Debian/Ubuntu:** A menudo usan `/etc/ldap.conf` (para `libnss-ldap`) o archivos de configuración para los módulos PAM (`pam-ldap`) que pueden estar en `/etc/pam_ldap.conf` o gestionados por `pam-auth-update`. A veces usan `nss-pam-ldapd` con su propio archivo `/etc/libnss-ldapd.conf`.
        - **Red Hat/CentOS/Fedora:** A menudo usan `/etc/ldap.conf` para las configuraciones generales del cliente LDAP, y la configuración para los módulos PAM (`pam_ldap`) puede integrarse de forma diferente (a menudo a través de `authconfig` o `authselect`).
        - **Directivas Comunes en estos archivos:** `uri ldap://<servidor_ldap>:<puerto>`, `base <base_dn_busqueda>`, `ldap_version 3`, `binddn <dn_usuario_bind>`, `bindpw <contraseña_bind>`, `tls_reqcert never/allow/try/demand`.
    - **Método Moderno (SSSD - System Security Services Daemon):** SSSD es el enfoque preferido y más robusto para integrar Linux con varios servicios de directorio (LDAP, Active Directory, FreeIPA). Proporciona caché (para logins offline), mejor manejo de fallos y unificación de diferentes backends.
        - **Paquete:** `sssd` (estándar en ambas ramas).
        - **Funcionamiento:** SSSD actúa como un proxy local. NSS y PAM se configuran para usar SSSD (`sss`) en lugar de hablar directamente con LDAP. SSSD es el que maneja la comunicación con el servidor LDAP.
        - **Archivo de Configuración SSSD:** `/etc/sssd/sssd.conf` (estándar). Formato INI con secciones como `[sssd]`, `[domain/<nombre_dominio>]`, `[nss]`, `[pam]`.
        - **Directivas Clave en `sssd.conf` (`[domain/...]`):** `id_provider=ldap`, `auth_provider=ldap`, `access_provider=ldap` (o `simple`, etc.), `ldap_uri`, `ldap_search_base`, `ldap_tls_reqcert`, `ldap_id_use_starttls`, `ldap_sasl_mech`, `ldap_default_bind_dn`, `ldap_default_bind_dn_password`, etc.

- **Configuración en `/etc/nsswitch.conf`:** Se cambia `ldap` por `sss` en las líneas `passwd`, `group`, `shadow`.
- **Configuración en `/etc/pam.d/`:** Se modifican los archivos para incluir módulos PAM de SSSD (ej: `pam_sss.so`) en lugar de `pam_ldap.so`.

Prueba de Configuración Cliente LDAP:

- **`ldapsearch`:** Permite verificar si puedes contactar al servidor LDAP y buscar información (requiere conocer la base DN, quizás credenciales bind). `ldapsearch -x -H ldap://<servidor> -b "<base_dn>" "uid=<usuario>"`.
- **`getent <base_de_datos> <clave>`:** Consulta las bases de datos configuradas en `/etc/nsswitch.conf`. Útil para verificar si el sistema puede encontrar usuarios/grupos LDAP.
  - `getent passwd <nombre_usuario_ldap>`: Busca un usuario en `/etc/passwd` y las fuentes configuradas (ej: ldap o sss).
  - `getent group <nombre_grupo_ldap>`: Busca un grupo.
- **`id <nombre_usuario_ldap>`:** Verifica si el sistema reconoce el usuario LDAP y sus membresías de grupo.
- **Intento de Login:** Intentar iniciar sesión (SSH o consola) como un usuario LDAP para probar la autenticación PAM.

Consideraciones de Seguridad y UID/GID:

- La comunicación entre el cliente y el servidor LDAP debe ser segura (TLS/LDAPS). Usa `ldap_tls_reqcert allow/demand` o `ldap_uri` con `ldaps://`.
- El mapeo de UID/GID es un desafío. Los usuarios y grupos deben tener los mismos IDs en el servidor LDAP que se esperan en los sistemas cliente, o debes confiar en `nfs-idmapd` (para NFS) o la funcionalidad de mapeo de SSSD.

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

*Nota: Estos ejercicios implican configurar el sistema para comunicarse con un servicio de directorio externo. Realízalos **SIEMPRE en una VM de prueba dedicada**. Necesitarás acceso a un servidor LDAP funcional para probar. Necesitarás privilegios de superusuario (`sudo`). Configurar un cliente LDAP puede bloquearte si se hace incorrectamente, ten un plan de recuperación.*

Ejercicio 10.3.1: Instalando Herramientas Cliente LDAP

- **Objetivo:** Instalar las utilidades básicas de línea de comandos para interactuar con servidores LDAP.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet.
- **Desarrollo Paso a Paso:**
  1. Abre una terminal.

2. **Instala el paquete:** `sudo apt update && sudo apt install openldap-clients` (Debian/Ubuntu) o `sudo dnf install openldap-clients` (Red Hat/CentOS/Fedora).
3. **Verifica que `ldapsearch` está disponible:** Ejecuta `which ldapsearch`.

Ejercicio 10.3.2: Usando `ldapsearch` para Consultar un Servidor LDAP

- **Objetivo:** Realizar una consulta básica a un servidor LDAP para verificar la conectividad y el funcionamiento.
- **Requisitos:** Herramientas cliente LDAP instaladas. Acceso a un servidor LDAP funcional (IP/nombre, puerto, base DN). Puedes usar un servidor de prueba si no tienes uno propio.
- **Desarrollo Paso a Paso:**
  1. Abre una terminal.
  2. **Realiza una consulta anónima básica (si el servidor lo permite):** Ejecuta `ldapsearch -x -H ldap://<IP_servidor_LDAP> -b "<Base_DN_de_Busqueda>" "(objectClass=*)"`.
     - `-x`: Usar autenticación simple (anónima si no se especifica binddn/bindpw).
     - `-H <URI_LDAP>`: Especifica la URI del servidor LDAP (ldap:// o ldaps://).
     - `-b "<Base_DN>"`: Especifica la base de la búsqueda (el punto de partida en el árbol DIT). Ej: `"dc=example,dc=com"`.
     - `"(objectClass=*)"`: El filtro de búsqueda (busca todos los objetos).
  3. **Realiza una consulta para un usuario específico (si el servidor permite consultas anónimas):** Ejecuta `ldapsearch -x -H ldap://<IP_servidor_LDAP> -b "<Base_DN_de_Usuarios>" "uid=<nombre_usuario_ldap>"`.
  4. **Si el servidor requiere autenticación bind:** Necesitas las credenciales de un usuario con permisos de lectura.
     Bash

     ```
     ldapsearch -x \
       -D "cn=admin,dc=example,dc=com" \
       -w "su_contraseña_bind" \
       -H ldap://<IP_servidor_LDAP> \
       -b "<Base_DN_de_Busqueda>" \
       "(objectClass=*)"
     ```

     - `-D <DN_bind>`: Especifica el Distinguished Name (DN) del usuario para autenticarse.
     - `-w <contraseña>`: Especifica la contraseña. (Evita esto en scripts, usa `-W` para que la pida).
  5. **Observa la salida:** Si la consulta tiene éxito, verás los atributos de los objetos encontrados en formato LDIF. Si falla, revisa la IP/puerto del servidor, el firewall, la base DN, las credenciales bind o si el servidor permite consultas anónimas.

Ejercicio 10.3.3: (Conceptual) Modificando `/etc/nsswitch.conf`

- **Objetivo:** Entender cómo indicar al sistema que busque usuarios y grupos en LDAP (o SSSD).
- *Requisitos:* Privilegios de superusuario (`sudo`). **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Haz una copia de seguridad:** `sudo cp /etc/nsswitch.conf /etc/nsswitch.conf.orig`.
    3. **Edita `/etc/nsswitch.conf` (requiere sudo):** `sudo vi /etc/nsswitch.conf`.
    4. **Busca las líneas `passwd:`, `group:`, `shadow:`:**
        - Buscarán primero en los archivos locales (`files`).
        - Añade `ldap` *después* de `files` si vas a usar los módulos `nss-ldap`/`pam-ldap` directos.
        - Añade `sss` *después* de `files` si vas a usar SSSD.
    5. **Ejemplos:**

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap

# O si usas SSSD
# passwd:         files sss
# group:          files sss
# shadow:         files sss
```

    6. **Guarda y sal.**
    7. **Los cambios en `nsswitch.conf` se aplican inmediatamente a las nuevas llamadas a la librería getpwent/getgrent (usadas por `getent`, `id`).** No suelen requerir reinicio.

Ejercicio 10.3.4: (Conceptual) Explorando Archivos de Configuración Cliente LDAP (no SSSD)

- **Objetivo:** Localizar y ver la configuración de los módulos NSS/PAM directos.
- *Requisitos:* Privilegios de superusuario (`sudo`). **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Busca posibles archivos de configuración (varían mucho por distribución y método):**
        - `sudo less /etc/ldap.conf` (puede ser para `libnss-ldap` o `pam-ldap`).
        - `sudo less /etc/libnss-ldap.conf` (si usas `libnss-ldap`).
        - `sudo less /etc/pam_ldap.conf` (si usas `pam-ldap`).
        - `sudo less /etc/nss-ldapd.conf` o `/etc/libnss-ldapd.conf` (si usas `nss-pam-ldapd`).

3. **Busca las directivas clave:** `uri`, `base`, `ldap_version`, `binddn`, `bindpw`, `tls_reqcert`.
4. **(Contexto):** Estos archivos le dicen a las librerías `libnss-ldap.so` y `pam_ldap.so` cómo conectar al servidor.

Ejercicio 10.3.5: (Conceptual) Configurando SSSD para Integración LDAP

- **Objetivo:** Entender cómo configurar SSSD como cliente LDAP.
- *Requisitos:* Paquete `sssd` instalado. Privilegios de superusuario (`sudo`). Acceso a un servidor LDAP. **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
  1. Abre una terminal.
  2. **Haz una copia de seguridad del archivo de configuración SSSD (suele crearse con permisos restrictivos, solo root):** `sudo cp /etc/sssd/sssd.conf /etc/sssd/sssd.conf.orig`. Asegúrate de que solo root puede leer/escribir (`sudo chmod 600 /etc/sssd/sssd.conf`).
  3. **Edita el archivo (requiere sudo):** `sudo vi /etc/sssd/sssd.conf`. Puede estar vacío o con una configuración de ejemplo.
  4. **Configura la sección `[sssd]` y define un dominio:**
     Ini, TOML

```
[sssd]
config_file_version = 2
services = nss, pam # Habilitar servicios NSS y PAM
domains = myldap.local # Nombre de tu dominio o conector

[domain/myldap.local] # Definir el dominio
id_provider = ldap    # Usar LDAP para informacion de ID
(usuarios/grupos)
auth_provider = ldap  # Usar LDAP para autenticacion
access_provider = permit # Permitir acceso a todos los usuarios
encontrados (o usar 'ldap' para control via atributos LDAP)
ldap_uri = ldap://<IP_servidor_LDAP> # URI del servidor LDAP
ldap_search_base = "<Base_DN_de_Busqueda>" # Base de busqueda (ej:
dc=example,dc=com)
ldap_id_use_starttls = true # Usar StartTLS para cifrar la conexion
(si el servidor lo soporta)
ldap_tls_reqcert = demand # Requerir certificado valido del servidor
LDAP

# Opcional: Si necesitas bind con un usuario para buscar
# ldap_default_bind_dn = "cn=binduser,dc=example,dc=com"
# ldap_default_bind_dn_password = "bindpassword"
```

     - Adapta los valores a tu entorno LDAP.
  5. **Guarda y sal.**
  6. **Verifica permisos (CRUCIAL):** `sudo chmod 600 /etc/sssd/sssd.conf`. Si los permisos son incorrectos, SSSD no se iniciará por seguridad.

7. **Modifica `/etc/nsswitch.conf` para usar `sss` (Ej. 10.3.3).**
8. **Habilita e inicia el servicio SSSD:** `sudo systemctl enable sssd && sudo systemctl start sssd`.
9. **Verifica el estado y los logs:** `systemctl status sssd` y `journalctl -u sssd -f`. Busca errores de conexión o configuración.

Ejercicio 10.3.6: Probando la Configuración Cliente (getent, id)

- **Objetivo:** Verificar si el sistema ahora puede encontrar usuarios y grupos definidos en LDAP.
- **Requisitos:** Configuración cliente LDAP aplicada (ya sea método tradicional o SSSD). Servidor LDAP accesible. Un usuario definido en LDAP.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Intenta buscar un usuario LDAP usando `getent`:** Ejecuta `getent passwd <nombre_usuario_ldap>`. Si la configuración es correcta, debería mostrar la línea de `/etc/passwd` para ese usuario, obtenida del servidor LDAP.
    3. **Intenta buscar un grupo LDAP:** Ejecuta `getent group <nombre_grupo_ldap>`.
    4. **Intenta obtener información detallada del usuario:** Ejecuta `id <nombre_usuario_ldap>`. Debería mostrar el UID, GID principal y los grupos secundarios del usuario LDAP.

Ejercicio 10.3.7: (Conceptual) Probando Autenticación PAM con Usuario LDAP

- **Objetivo:** Verificar si puedes iniciar sesión con credenciales LDAP.
- *Requisitos:* Configuración cliente LDAP funcional (Ej. 10.3.6). Configuración PAM modificada para usar LDAP/SSSD (Conceptual Ej. 10.3.5 o usando herramientas como `authconfig`/`authselect` que lo hacen por ti). Un usuario LDAP con contraseña. **VM de prueba. Plan de recuperación si falla.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Intenta usar `su` como el usuario LDAP:** Ejecuta `su - <nombre_usuario_ldap>`. Te pedirá la contraseña del usuario LDAP. Si la configuración PAM es correcta, deberías autenticarte y obtener un shell como ese usuario.
    3. **Intenta iniciar sesión por SSH como el usuario LDAP (desde otra VM o haciendo SSH a localhost):** Ejecuta `ssh <nombre_usuario_ldap>@localhost`. Te pedirá la contraseña LDAP. Deberías poder iniciar sesión.
    4. **Si falla, revisa los logs de PAM** (`auth.log`, `secure`, o journalctl) para ver por qué la autenticación falló.