📁 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.