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

210.4 Configurar un servidor LDAP básico

Teoría

Un servidor LDAP ejecuta un servicio de directorio que almacena información de forma estructurada y jerárquica, optimizada para lecturas rápidas. Es un componente clave en infraestructuras de red para centralizar información de usuarios, grupos, dispositivos, etc.

Software de Servidor LDAP (OpenLDAP):

OpenLDAP es la implementación de servidor LDAP de código abierto más común en Linux. El demonio principal es `slapd` (Standalone LDAP Daemon).

Implementación Básica de OpenLDAP Server:

1. **Instalación del Software:**
    - **Paquete (Diferencias):**
        - **Debian/Ubuntu:** `slapd` (instala el demonio y utilidades básicas).
        - **Red Hat/CentOS/Fedora:** `openldap-servers` (incluye `slapd` y otras utilidades).
    - **Comando:** `sudo apt install <paquete>` o `sudo dnf install <paquete>`. Durante la instalación, Debian/Ubuntu a menudo te guiará por una configuración básica interactiva (DN sufijo, contraseña de administrador).
2. **Gestión del Servicio:**
    - **Nombre del Servicio:** `slapd.service` (estándar en ambas ramas).
    - **Comandos Systemd:** `sudo systemctl enable slapd`, `sudo systemctl start slapd`, `sudo systemctl status slapd`, `sudo systemctl restart slapd`, `sudo systemctl reload slapd` (la recarga solo funciona con el método de configuración `cn=config`).
3. **Métodos de Configuración (`slapd`):** Aquí hay una diferencia importante entre los enfoques tradicionales y modernos.
    - **Método Tradicional (`slapd.conf`):** La configuración se define en un archivo de texto plano.
        - **Ubicación (Diferencias):** `/etc/ldap/slapd.conf` (Debian/Ubuntu), `/etc/openldap/slapd.conf` (Red Hat/CentOS/Fedora).
        - **Necesita Reinicio:** Los cambios en `slapd.conf` generalmente requieren reiniciar el servicio `slapd` para aplicarse.
    - **Método Moderno (`cn=config` - Online Configuration):** La configuración se almacena *dentro* del propio directorio LDAP, bajo el DN especial `cn=config`. La configuración se gestiona manipulando entradas LDAP usando herramientas estándar (`ldapadd`, `ldapmodify`, etc.).

    - **Ubicación Física (archivos backend):** Los archivos que representan la configuración `cn=config` se encuentran en un directorio específico, pero no debes editarlos directamente. Ej: `/etc/ldap/slapd.d/` (Debian/Ubuntu), `/etc/openldap/slapd.d/` (Red Hat/CentOS/Fedora).
    - **Cambios Online:** La mayoría de los cambios se pueden aplicar dinámicamente sin reiniciar `slapd`.
    - **Preferido:** Este es el método preferido en distribuciones modernas por su flexibilidad.
4. **Base de Datos Backend (`database`):** `slapd` necesita un motor de base de datos para almacenar los datos del directorio.
    - **Configuración:** Se define en `slapd.conf` o bajo `cn=config`. Se especifica el tipo de base de datos y los parámetros asociados.
    - **Tipos Comunes:**
        - `mdb`: Memory-Mapped Database. El backend por defecto moderno, reemplazó a `bdb` y `hdb`. Es robusto y eficiente.
    - **Parámetros de Base de Datos:**
        - `suffix "<base_dn>"`: Define el sufijo (la base DN) para esta base de datos. Es el punto más alto de la jerarquía de datos que esta base de datos gestionará (ej: `dc=example,dc=com`).
        - `rootdn "<root_dn>"`: El Distinguished Name (DN) del "superusuario" administrativo para esta base de datos (ej: `cn=admin,dc=example,dc=com`).
        - `rootpw "<contraseña>"`: La contraseña para el `rootdn`. Debe ser un hash (se puede generar con `slappasswd`).
5. **Estructura del Directorio (DIT - Directory Information Tree):**
    - Los datos en LDAP se organizan en una jerarquía similar a un árbol.
    - **DN (Distinguished Name):** La ruta única completa a una entrada dentro del DIT (ej: `uid=jdoe,ou=users,dc=example,dc=com`).
    - **RDN (Relative Distinguished Name):** El componente más específico del DN (ej: `uid=jdoe` es el RDN de `uid=jdoe,ou=users,...`).
    - **Entradas (Entries):** Nodos en el árbol del DIT que contienen información. Cada entrada tiene un RDN y una lista de atributos y clases de objeto.
    - **Clases de Objeto (Object Classes):** Definen los tipos de entradas (ej: `organizationalUnit`, `person`, `posixAccount`). Cada clase de objeto requiere ciertos atributos y permite otros opcionales.
    - **Atributos:** Pares clave=valor que almacenan los datos reales (ej: `cn=John Doe`, `uid=jdoe`, `gidNumber=1000`, `homeDirectory=/home/jdoe`).
6. **Carga de Datos Iniciales (LDIF):**
    - Después de configurar la base de datos, el directorio está vacío. Debes añadir las entradas iniciales, comenzando por la base DN.

- **LDIF (LDAP Data Interchange Format):** Formato de texto estándar para representar entradas LDAP y realizar operaciones (add, modify, delete).
- **Herramienta:** `ldapadd -x -D "<root_dn>" -W -f <archivo.ldif>` (para añadir entradas desde un archivo LDIF).

Conceptos Adicionales:

- **Schemas:** Definen las clases de objeto y atributos permitidos en el directorio. Los schemas estándar (ej: `core`, `inetorgperson`, `nis`) vienen preinstalados. Puedes añadir schemas personalizados.
- **ACLs (Access Control Lists):** Definen quién tiene permiso para leer, escribir, etc., partes del directorio. Cruciales por seguridad. Se configuran en `slapd.conf` o `cn=config`.
- **TLS/SSL (LDAPS):** Cifrar la comunicación entre clientes y servidor (puerto 636 por defecto) es esencial para proteger las credenciales y los datos. Requiere configurar certificados en `slapd`.
- **Replicación:** Configurar múltiples servidores LDAP para redundancia y distribución de carga.