ping debian.aula11.local

LDAP: Protocolo, Utilidad, Puertos y Herramientas de Implementación en Linux

¿Qué es LDAP?

LDAP (Lightweight Directory Access Protocol) es un protocolo de comunicaciones ligero y estándar abierto que se utiliza para acceder a servicios de información de directorio distribuidos y mantenerlos. En términos sencillos, es como una base de datos optimizada para operaciones de lectura intensivas que almacena información estructurada y jerárquica sobre recursos de red y usuarios.

La información en un directorio LDAP se organiza en una estructura de árbol, donde cada nodo es una entrada. Cada entrada tiene un nombre distintivo (DN - Distinguished Name) que la identifica de forma única dentro del directorio, y contiene una colección de atributos, cada uno con un nombre (tipo de atributo) y uno o más valores.

Ejemplo de estructura jerárquica (simil-DNS):

- `dc=ejemplo,dc=com` (Dominio de Componentes: https://www.google.com/url?sa=E&source=gmail&q=ejemplo.com)
- `ou=usuarios,dc=ejemplo,dc=com` (Unidad Organizativa: usuarios)
- `cn=Juan Perez,ou=usuarios,dc=ejemplo,dc=com` (Nombre Común: Juan Perez)
- `ou=grupos,dc=ejemplo,dc=com` (Unidad Organizativa: grupos)
- `cn=administradores,ou=grupos,dc=ejemplo,dc=com` (Nombre Común: administradores)

Utilidad de LDAP

La utilidad principal de LDAP radica en la centralización de la gestión de identidades y la información de recursos. Sus aplicaciones más comunes incluyen:

1. Autenticación Centralizada: Permite que múltiples aplicaciones y servicios (servidores web, SSH, VPNs, sistemas de correo electrónico) autentiquen a los usuarios contra un único repositorio central (el servidor LDAP). Esto simplifica la gestión de contraseñas y mejora la seguridad al evitar la dispersión de credenciales.
2. Autorización (Basada en Grupos y Atributos): Una vez que un usuario es autenticado, LDAP puede proporcionar información sobre la pertenencia a grupos o atributos específicos del usuario, lo que permite a las aplicaciones determinar qué recursos o permisos tiene ese usuario.
3. Gestión de Usuarios y Grupos: Facilita la creación, modificación, eliminación y gestión de usuarios y grupos de forma centralizada, lo que es crucial en entornos con un gran número de usuarios.

4. Libreta de Direcciones Global (GAL): Almacena información de contacto de los empleados (nombres, direcciones de correo electrónico, números de teléfono, etc.) de manera que sea fácilmente consultable por aplicaciones de correo electrónico y otros sistemas.
5. Gestión de Recursos de Red: Puede almacenar información sobre impresoras, servidores, aplicaciones, y otros dispositivos de red, facilitando su descubrimiento y acceso.
6. Sincronización de Directorios: Permite la replicación y sincronización de información entre diferentes servidores LDAP o con otros tipos de directorios.

Puertos Utilizados por LDAP

LDAP opera sobre TCP/IP y utiliza los siguientes puertos estándar:

- Puerto 389/TCP: Es el puerto predeterminado para las comunicaciones LDAP no cifradas.
- Puerto 636/TCP (LDAPS): Se utiliza para comunicaciones LDAP cifradas mediante SSL/TLS (Secure Sockets Layer/Transport Layer Security). Es la forma recomendada de comunicación para proteger la privacidad y la integridad de los datos transmitidos, especialmente credenciales de usuario.

Herramientas de Implementación en Linux

La implementación más popular y utilizada de un servidor LDAP en Linux es OpenLDAP. Para interactuar con él y gestionarlo, existen diversas herramientas:

- OpenLDAP (slapd): Es el demonio del servidor LDAP (`slapd` significa Stand-alone LDAP Daemon). Es el corazón de la implementación, encargado de gestionar el directorio y atender las solicitudes de los clientes.
- `openldap-clients` (Paquete): Contiene un conjunto de utilidades de línea de comandos para interactuar con el servidor LDAP:
- `ldapsearch`: Para buscar y consultar entradas en el directorio.
- `ldapadd`: Para añadir nuevas entradas al directorio.
- `ldapmodify`: Para modificar entradas existentes.
- `ldapdelete`: Para eliminar entradas del directorio.
- `ldappasswd`: Para cambiar contraseñas de usuarios LDAP.
- phpLDAPadmin: Una interfaz web muy popular para la administración gráfica de servidores OpenLDAP. Simplifica tareas como la creación y gestión de usuarios, grupos y objetos, así como la configuración del esquema.
- Apache Directory Studio: Una aplicación de escritorio multiplataforma (basada en Eclipse) que proporciona una suite completa de herramientas para interactuar con servidores LDAP. Incluye un navegador de directorio, un editor LDIF, un analizador de esquemas, y otras funcionalidades avanzadas. Es muy útil para desarrollo y depuración.
- LDAP Account Manager (LAM): Otra interfaz web robusta para la gestión de usuarios y grupos en OpenLDAP, que a menudo se integra con otras funcionalidades como Samba, Postfix, etc.

Cómo Configurar un Servidor LDAP (OpenLDAP)

La configuración de un servidor OpenLDAP ha evolucionado significativamente a lo largo de las versiones. En Ubuntu 14.04, la configuración principal se realizaba a través del archivo `/etc/ldap/slapd.conf`. En versiones más modernas, como Rocky 9.5, OpenLDAP utiliza un sistema de configuración en tiempo real (OLC - Online Configuration), donde la configuración se almacena en el propio directorio LDAP y se gestiona mediante archivos LDIF en el directorio `/etc/openldap/slapd.d/`.

A continuación, se presenta una tabla con comandos y descripciones generales para la configuración de un servidor OpenLDAP, enfocándose en la configuración moderna (OLC) cuando es relevante.

Paso	Comando/Acción	Descripción
1. Instalación de OpenLDAP	`sudo apt-get install slapd ldap-utils` (Debian/Ubuntu) `sudo dnf install openldap-servers openldap-clients` (RHEL/CentOS/Rocky)	Instala el paquete del servidor OpenLDAP (`slapd`) y las utilidades cliente (`ldap-utils` o `openldap-clients`) para interactuar con el servidor.
2. Configuración Inicial (durante la instalación o manual)	Durante la instalación, se te pedirá establecer la contraseña de administrador (`admin` o `cn=admin,cn=config`). `sudo dpkg-reconfigure slapd` (Ubuntu)	En sistemas basados en Debian/Ubuntu, `dpkg-reconfigure slapd` permite configurar rápidamente el dominio base (ej. `dc=ejemplo,dc=com`), el nombre de la organización, la contraseña de administrador, y si se eliminará la base de datos antigua.
3. Carga de Esquemas Estándar	(Configuración dinámica - OLC) Copiar/crear archivos LDIF para los esquemas en `/etc/openldap/slapd.d/cn=config/cn=schema/` y reiniciar `slapd` o usar `ldapadd`. Generalmente ya vienen cargados los básicos.	Los esquemas definen los tipos de objetos y atributos que se pueden almacenar en el directorio. Esquemas comunes incluyen `core`, `cosine`, `inetorgperson`, `nis` (para usuarios y grupos Unix/Linux). OpenLDAP moderno ya carga muchos por defecto.
4. Definición de la Base de Datos (Backend)	Modificar la configuración OLC (`cn=config`) para especificar el backend (por ejemplo, `mdb`), el	El backend determina cómo OpenLDAP almacena los datos (ej. `mdb` es el predeterminado y recomendado en versiones recientes,

Paso	Comando/Acción	Descripción
	DN base (`suffix`), y el DN del administrador (`rootdn`). Se hace mediante archivos LDIF y `ldapmodify`.	antes `bdb`). El `suffix` define la raíz de tu directorio (ej. `dc=ejemplo,dc=com`). El `rootdn` es la cuenta con permisos administrativos para esa base de datos.
5. Configuración de la Contraseña de Administrador	`slappasswd` (para generar un hash de la contraseña) Luego, usar `ldapmodify` para actualizar el atributo `olcRootPW` en la entrada de configuración de la base de datos.	Es crucial establecer una contraseña segura para el administrador del directorio (`rootpw` o `olcRootPW`). Se recomienda generar un hash de la contraseña con `slappasswd` y luego usar ese hash.
6. Configuración de Permisos (ACLs)	Modificar la configuración OLC (`cn=config`) para agregar reglas ACL (`olcAccess`). Se hace mediante `ldapmodify` o creando archivos LDIF.	Las ACLs (Access Control Lists) determinan quién puede leer, escribir, añadir, eliminar o buscar información en el directorio. Son fundamentales para la seguridad.
7. Inicio y Habilitación del Servicio	`sudo systemctl start slapd` `sudo systemctl enable slapd`	Inicia el demonio del servidor OpenLDAP. `enable` asegura que el servicio se inicie automáticamente al arrancar el sistema.
8. Verificación del Servicio	`sudo systemctl status slapd` `ldapsearch -x -LLL -H ldap://localhost -b "dc=ejemplo,dc=com"` (reemplaza el DN base)	Verifica que el servicio `slapd` esté en ejecución. `ldapsearch` permite realizar una consulta para ver si el directorio responde correctamente.
9. Añadir Entradas Iniciales (LDIF)	Crear un archivo `.ldif` con las entradas a añadir (ej. unidad organizativa `ou=usuarios`, `ou=grupos`, un usuario inicial). `ldapadd -x -D "cn=admin,dc=ejemplo,dc=com" -W -f mi_inicial.ldif`	Una vez que el servidor está funcionando, se añaden las estructuras básicas y los usuarios iniciales utilizando archivos LDIF.
10. Configuración	Generar certificados SSL/TLS.	Para comunicaciones seguras, es esencial configurar SSL/TLS. Esto

Paso	Comando/Acción	Descripción
de SSL/TLS (Opcional pero Recomendado)	Modificar la configuración OLC para habilitar LDAPS (puerto 636) y especificar las rutas de los certificados.	implica obtener o generar certificados y configurar OpenLDAP para usarlos.

Cómo Configurar un Cliente LDAP

Configurar un cliente LDAP implica decirle al sistema dónde encontrar el servidor LDAP y cómo autenticarse contra él para servicios como SSH, inicio de sesión de usuario, etc. Esto generalmente se logra mediante la configuración de PAM (Pluggable Authentication Modules) y NSS (Name Service Switch).

Paso	Comando/Acción	Descripción
1. Instalación de Paquetes Cliente	`sudo apt-get install libnss-ldap libpam-ldap ldap-utils nscd` (Debian/Ubuntu) `sudo dnf install nss-pam-ldapd pam_ldap openldap-clients` (RHEL/CentOS/Rocky)	Instala las librerías y utilidades necesarias para que el sistema opere como cliente LDAP. `libnss-ldap`/`nss-pam-ldapd` para NSS, `libpam-ldap`/`pam_ldap` para PAM, y `nscd` para caching.

2. Configuración de NSS (Name Service Switch)	Editar `/etc/nsswitch.conf` para añadir `ldap` a las líneas de `passwd`, `group`, y `shadow`.
	 `passwd: files systemd compat ldap`
	 `group: files systemd compat ldap`
	 `shadow: files systemd compat ldap`
		NSS determina el orden en que el sistema resuelve la información de usuarios y grupos. Añadir `ldap` indica al sistema que también consulte el servidor LDAP.

3. Configuración de PAM (Pluggable Authentication Modules)	Configurar `/etc/pam.d/common-auth`, `common-account`, `common-password`, `common-session` (Debian/Ubuntu) Usar `authconfig` o `authselect` (RHEL/CentOS/Rocky)	PAM gestiona cómo se autentican los usuarios. Se deben añadir líneas para el módulo `pam_ldap.so` o `pam_sss.so` (si usas SSSD) para que las autenticaciones pasen por LDAP.
4.	Editar `/etc/ldap.conf` o	Este es el archivo de

Paso	Comando/Acción	Descripción

Configuración del Cliente LDAP	`/etc/sssd/sssd.conf` (si usas SSSD) o las configuraciones generadas por `authconfig`/`authselect`.
	 Especificar:
	 `base dc=ejemplo,dc=com`
	 `uri ldap://ip_servidor_ldap/`
	 `ldap_version 3`
	 `binddn cn=admin,dc=ejemplo,dc=com` (o un usuario no-admin con permisos de lectura)
	 `bindpw tu_password_admin`
	 `ssl start_tls` o `tls_cacert /ruta/al/ca.crt`
		configuración principal del cliente. Se especifica la base de búsqueda del directorio (`base`), la URI del servidor LDAP (`uri`), la versión del protocolo, el DN del usuario para realizar consultas (si es necesario un bind autenticado) y la configuración de TLS/SSL.

5. Configuración del NSS Cache Daemon (NSCD)	`sudo systemctl start nscd`
	 `sudo systemctl enable nscd`
	 `sudo systemctl restart nscd`
		NSCD (Name Service Cache Daemon) cachea las consultas de nombres (incluidas las de LDAP) para mejorar el rendimiento y reducir la carga en el servidor LDAP. Es recomendable reiniciarlo después de cambios en NSS.

6. Prueba de Acceso	`getent passwd nombre_usuario_ldap` `ssh nombre_usuario_ldap@localhost` (si SSH está configurado para usar LDAP)	Verifica si el sistema puede resolver usuarios y grupos de LDAP. Intenta iniciar sesión con un usuario LDAP para confirmar la autenticación.

Parte 1: Configurar el Servidor LDAP en Debian 12

Paso 1: Instalar OpenLDAP

Explicación: OpenLDAP es el software para implementar el servidor LDAP. El paquete slapd proporciona el demonio LDAP, y ldap-utils incluye herramientas para gestionar la base de datos LDAP.

1. Actualiza el sistema:
   sudo apt update && sudo apt upgrade -y
2. Instala OpenLDAP y las herramientas necesarias:
   sudo apt install slapd ldap-utils -y
3. Durante la instalación, se te pedirá configurar una contraseña para el administrador LDAP. Usa una contraseña segura (por ejemplo, "qwerty" para este ejemplo). Esta contraseña es para la cuenta de administrador LDAP, no para los usuarios.

Paso 2: Configurar OpenLDAP

Explicación: OpenLDAP debe configurarse para el dominio aula11.local. Esto implica definir el DN base (Distinguished Name) como dc=aula11,dc=local y asegurarse de que el servidor esté listo para aceptar conexiones.

1. Reconfigura slapd para asegurarte de que el dominio esté correctamente definido:
   sudo dpkg-reconfigure slapd
   - Responde a las preguntas:
     - **Omitir configuración inicial**: No (selecciona configurar).
     - **Nombre del dominio DNS**: Introduce aula11.local.
     - **Nombre de la organización**: Puede ser "Aula11" o cualquier nombre.
     - **Contraseña de administrador**: Confirma o cambia la contraseña (por ejemplo, "qwerty").
     - **Backend de la base de datos**: Selecciona MDB (recomendado).
     - **Eliminar base de datos al purgar**: No.
     - **Mover base de datos antigua**: Sí, si aplica.
2. Verifica que el servidor LDAP esté funcionando:
   sudo systemctl status slapd
   Asegúrate de que esté activo y en ejecución. Si no, inicia el servicio:
   sudo systemctl start slapd
   sudo systemctl enable slapd
3. Prueba la conexión LDAP:
   ldapsearch -x -b "dc=aula11,dc=local" -H ldap://debian.aula11.local
   Esto debería devolver la estructura básica del dominio. Usa -x para autenticación simple y -H para especificar el servidor.

Paso 3: Crear Archivos LDIF para los Usuarios

Explicación: Los archivos LDIF (LDAP Data Interchange Format) definen la estructura de los datos a añadir al servidor LDAP. Crearemos un archivo LDIF para la unidad organizativa (OU) y los 14 usuarios (user01 a user14) con la contraseña "qwerty".

1. Crea un directorio para trabajar con los archivos LDIF:

mkdir ~/ldap-config
cd ~/ldap-config

2. Crea un archivo LDIF para la unidad organizativa (ou=users,dc=aula11,dc=local):
   nano ou_users.ldif #(o usad vi si os sentís cómodo con él)
   Contenido del archivo:
   dn: ou=users,dc=aula11,dc=local
   objectClass: organizationalUnit
   ou: users
   Guarda y cierra el archivo.
3. Añade la OU al servidor LDAP:
   ldapadd -x -D "cn=admin,dc=aula11,dc=local" -W -f ou_users.ldif
   Ingresa la contraseña de administrador LDAP ("qwerty" en este ejemplo).
4. Genera la contraseña cifrada para "qwerty":
   slappasswd -s qwerty
   Esto genera un hash, por ejemplo: {SSHA}8fXz3i4j5k6l7m8n9o0p1q2r3s4t5u6v. Copia este hash. (OJO!!!! ejecutad el comando y mostrará el hash correcto)
5. Crea un archivo LDIF para los 14 usuarios:
   vi users.ldif
   dn: uid=user01,ou=users,dc=aula11,dc=local
   objectClass: inetOrgPerson
   objectClass: posixAccount
   objectClass: shadowAccount
   uid: user01
   cn: User One
   sn: User01
   uidNumber: 10001
   gidNumber: 10001
   homeDirectory: /home/user01
   loginShell: /bin/bash
   userPassword: {SSHA}8fXz3i4j5k6l7m8n9o0p1q2r3s4t5u6v

   dn: uid=user02,ou=users,dc=aula11,dc=local
   objectClass: inetOrgPerson
   objectClass: posixAccount
   objectClass: shadowAccount
   uid: user02
   cn: User Two
   sn: User02
   uidNumber: 10002
   gidNumber: 10002
   homeDirectory: /home/user02
   loginShell: /bin/bash
   userPassword: {SSHA}8fXz3i4j5k6l7m8n9o0p1q2r3s4t5u6v
   Contenido del archivo (repite la estructura para cada usuario, ajustando uid y cn):

Continúa hasta user14, incrementando uidNumber y gidNumber (10001 a 10014) y ajustando uid, cn, y homeDirectory. Usa el mismo hash de contraseña para todos.

6. Añade los usuarios al servidor LDAP:
   ldapadd -x -D "cn=admin,dc=aula11,dc=local" -W -f users.ldif
   Ingresa la contraseña de administrador LDAP.
7. Verifica que los usuarios se hayan añadido:
   ldapsearch -x -b "ou=users,dc=aula11,dc=local" -H ldap://debian.aula11.local
   Deberías ver los 14 usuarios listados.

Paso 4: Configurar el Servidor para Permitir Autenticación

Explicación: Para que los clientes puedan autenticarse, el servidor LDAP debe permitir consultas anónimas o autenticadas y estar accesible en la red.

1. Asegúrate de que el servidor esté escuchando en la interfaz de red (no solo localhost):
   Edita /etc/ldap/slapd.d/cn=config.ldif o /etc/openldap/slapd.conf (dependiendo de tu configuración):
   sudo nano /etc/ldap/slapd.d/cn=config/olcDatabase={1}mdb.ldif
   Asegúrate de que olcAccess permita acceso a los usuarios:
   olcAccess: to attrs=userPassword by self write by anonymous auth by * none
   olcAccess: to * by * read
2. Reinicia el servicio LDAP:
   sudo systemctl restart slapd
3. Configura el firewall para permitir conexiones LDAP (puerto 389):
   sudo ufw allow 389

Pasos para crear el usuario proxyuser en el servidor Debian 12

1. **Crea un archivo LDIF para proxyuser**: En el servidor Debian 12 (debian), crea un archivo LDIF para el usuario sin privilegios:
   nano ~/ldap-config/proxyuser.ldif
   Contenido del archivo:
   dn: cn=proxyuser,ou=users,dc=aula11,dc=local
   objectClass: simpleSecurityObject
   objectClass: organizationalRole
   cn: proxyuser
   userPassword: {SSHA}8fXz3i4j5k6l7m8n9o0p1q2r3s4t5u6v #(OJO!!!!! el hash)
   description: LDAP proxy user for client queries
   Usa el mismo hash de contraseña generado anteriormente para "qwerty" (o genera uno nuevo con slappasswd -s <contraseña>).
2. **Añade el usuario al servidor LDAP**:
   ldapadd -x -D "cn=admin,dc=aula11,dc=local" -W -f ~/ldap-config/proxyuser.ldif
   Ingresa la contraseña del administrador LDAP (qwerty en el ejemplo).
3. **Configura permisos en el servidor LDAP**: Asegúrate de que proxyuser pueda realizar consultas. Edita las reglas de acceso en el servidor LDAP si es necesario. Por ejemplo, en /etc/ldap/slapd.d/cn=config/olcDatabase={1}mdb.ldif:
   olcAccess: to * by dn="cn=proxyuser,ou=users,dc=aula11,dc=local" read by * none
   Esto permite que proxyuser lea la base de datos. Aplica los cambios:
   sudo systemctl restart slapd
4. **Vuelve al cliente y responde**: En el cliente (Ubuntu o Rocky), introduce:
   cn=proxyuser,ou=users,dc=aula11,dc=local
5. **Configura la contraseña de proxyuser en el cliente**: Edita /etc/ldap.conf (o /etc/ldap/ldap.conf) en el cliente para incluir la credencial de proxyuser:
   sudo nano /etc/ldap.conf
   Añade o modifica:
   binddn cn=proxyuser,ou=users,dc=aula11,dc=local
   bindpw qwerty
6. **Prueba la conexión**: En el cliente, verifica que puedes consultar el servidor LDAP con proxyuser:
   ldapsearch -x -D "cn=proxyuser,ou=users,dc=aula11,dc=local" -W -b "dc=aula11,dc=local"
   Ingresa la contraseña "qwerty". Deberías ver la estructura del dominio.

Alternativa: Usar autenticación anónima

Si no quieres crear un proxyuser y el servidor permite consultas anónimas (como configurado en el paso 4 de la Parte 1), puedes dejar el campo en blanco o configurar el cliente para autenticación anónima. En /etc/ldap.conf, asegúrate de que no haya binddn ni bindpw, y verifica que el servidor permita acceso anónimo:

olcAccess: to * by anonymous read by * none

Parte 2: Configurar los Clientes (Ubuntu 24.04, Rocky 9.5, Rocky 10)

Paso 5: Configurar el Cliente Ubuntu 24.04

Explicación: Configuraremos el cliente para autenticar contra el servidor LDAP y crear directorios home automáticamente usando PAM y pam_mkhomedir.

1. Instala los paquetes necesarios:
   sudo apt update
   sudo apt install libnss-ldap libpam-ldap ldap-utils -y
2. Durante la instalación, configura:
   - **URI del servidor LDAP**: ldap://debian.aula11.local
   - **DN base**: dc=aula11,dc=local
   - **Versión de LDAP**: 3
   - **Hacer root administrador LDAP**: No
   - **Autenticación local**: Sí (para usuarios locales como root)
3. Edita /etc/nsswitch.conf para usar LDAP:
   sudo nano /etc/nsswitch.conf
   Modifica las siguientes líneas:
   passwd: compat ldap
   group: compat ldap
   shadow: compat ldap
4. Configura PAM para crear directorios home automáticamente:
   sudo nano /etc/pam.d/common-session
   Añade al final:
   session required pam_mkhomedir.so skel=/etc/skel umask=0022
5. Configura /etc/pam.d/common-session-noninteractive de la misma manera:
   sudo nano /etc/pam.d/common-session-noninteractive
   Añade:
   session required pam_mkhomedir.so skel=/etc/skel umask=0022
6. Configura el cliente LDAP: Edita /etc/ldap.conf o /etc/ldap/ldap.conf:
   sudo nano /etc/ldap.conf
   Asegúrate de que contenga:
   base dc=aula11,dc=local
   uri ldap://debian.aula11.local
   ldap_version 3
7. Habilita autenticación SSH para usuarios LDAP: Edita /etc/ssh/sshd_config:
   sudo nano /etc/ssh/sshd_config
   Asegúrate de que PasswordAuthentication yes esté habilitado.
8. Reinicia los servicios:
   sudo systemctl restart nslcd sshd
9. Prueba la autenticación SSH: Desde otro equipo o el mismo, intenta:
   ssh user01@<IP_del_cliente_ubuntu>
   Usa la contraseña "qwerty". El directorio /home/user01 se creará automáticamente.

Paso 6: Configurar los Clientes Rocky Linux 9.5 y 10

Explicación: Rocky Linux usa authselect y sssd para la integración con LDAP, que es más moderno que libnss-ldap. Configuraremos ambos sistemas de manera similar.

1. Instala los paquetes necesarios:
   sudo dnf install sssd sssd-ldap -y
2. Configura sssd: Crea o edita /etc/sssd/sssd.conf:
   sudo nano /etc/sssd/sssd.conf
   Contenido:
   [sssd]
   config_file_version = 2
   services = nss, pam
   domains = aula11.local

   [domain/aula11.local]
   id_provider = ldap
   auth_provider = ldap
   ldap_uri = ldap://debian.aula11.local
   ldap_search_base = dc=aula11,dc=local
   ldap_user_search_base = ou=users,dc=aula11,dc=local
   ldap_id_use_start_tls = false
   cache_credentials = true
   enumerate = true
3. Ajusta los permisos del archivo:
   sudo chmod 600 /etc/sssd/sssd.conf
4. Configura authselect para usar LDAP:
   sudo authselect select sssd with-mkhomedir --force
5. Edita /etc/nsswitch.conf:
   sudo nano /etc/nsswitch.conf
   passwd: sss files
   group: sss files
   shadow: sss files
6. Configura SSH: Edita /etc/ssh/sshd_config:
   sudo nano /etc/ssh/sshd_config
   Asegúrate de que PasswordAuthentication yes esté habilitado.
7. Habilita e inicia sssd:
   sudo systemctl enable sssd --now
   sudo systemctl restart sshd

8. Prueba la autenticación SSH:
   ssh user01@<IP_del_cliente_rocky>
   Usa la contraseña "qwerty". El directorio home se creará automáticamente.
9. **Configura el cliente LDAP si es necesario**:
   Si usas un usuario sin privilegios como cn=proxyuser,ou=users,dc=aula11,dc=local (como se explicó antes), configura /etc/openldap/ldap.conf:

sudo nano /etc/openldap/ldap.conf
Contenido:

```
BASE dc=aula11,dc=local
URI ldap://debian.aula11.local
BIND_DN cn=proxyuser,ou=users,dc=aula11,dc=local
BIND_PW qwerty
```

1. **Prueba la conexión LDAP**:

   ldapsearch -x -D "cn=proxyuser,ou=users,dc=aula11,dc=local" -W -b "dc=aula11,dc=local"
   Ingresa la contraseña "qwerty" para verificar que el cliente puede consultar el servidor LDAP.

Verificación adicional

Si encuentras problemas con la autenticación:

- Revisa los logs en el cliente:
  sudo tail -f /var/log/sssd/*.log
  sudo tail -f /var/log/auth.log
- En el servidor LDAP, verifica:
  sudo tail -f /var/log/slapd.log
- Asegúrate de que el firewall en el servidor (debian) permita el puerto 389:
  sudo ufw status
- Confirma que el DNS resuelve correctamente debian.aula11.local desde el cliente:
  ping debian.aula11.local

Nota sobre MigrationTools

Explicación: MigrationTools es un conjunto de scripts en Perl que pueden simplificar la creación de archivos LDIF a partir de archivos de sistema como /etc/passwd. Aunque en este caso creamos los archivos LDIF manualmente, MigrationTools puede ser útil para migrar usuarios existentes o generar LDIF automáticamente.

1. Instala MigrationTools en el servidor Debian:
   sudo apt install migrationtools -y
2. Configura /etc/migrationtools.conf:
   sudo nano /etc/migrationtools.conf
   Ajusta:
   DEFAULT_BASE="dc=aula11,dc=local"
3. Usa MigrationTools para generar LDIF a partir de un archivo de usuarios (si tienes uno):
   /usr/share/migrationtools/migrate_passwd.pl /etc/passwd users.ldif
   Esto generaría un archivo LDIF que luego puedes modificar y añadir con ldapadd.

MigrationTools es especialmente útil para migraciones masivas, pero para este caso con 14 usuarios, crear los LDIF manualmente es más controlado y suficiente.