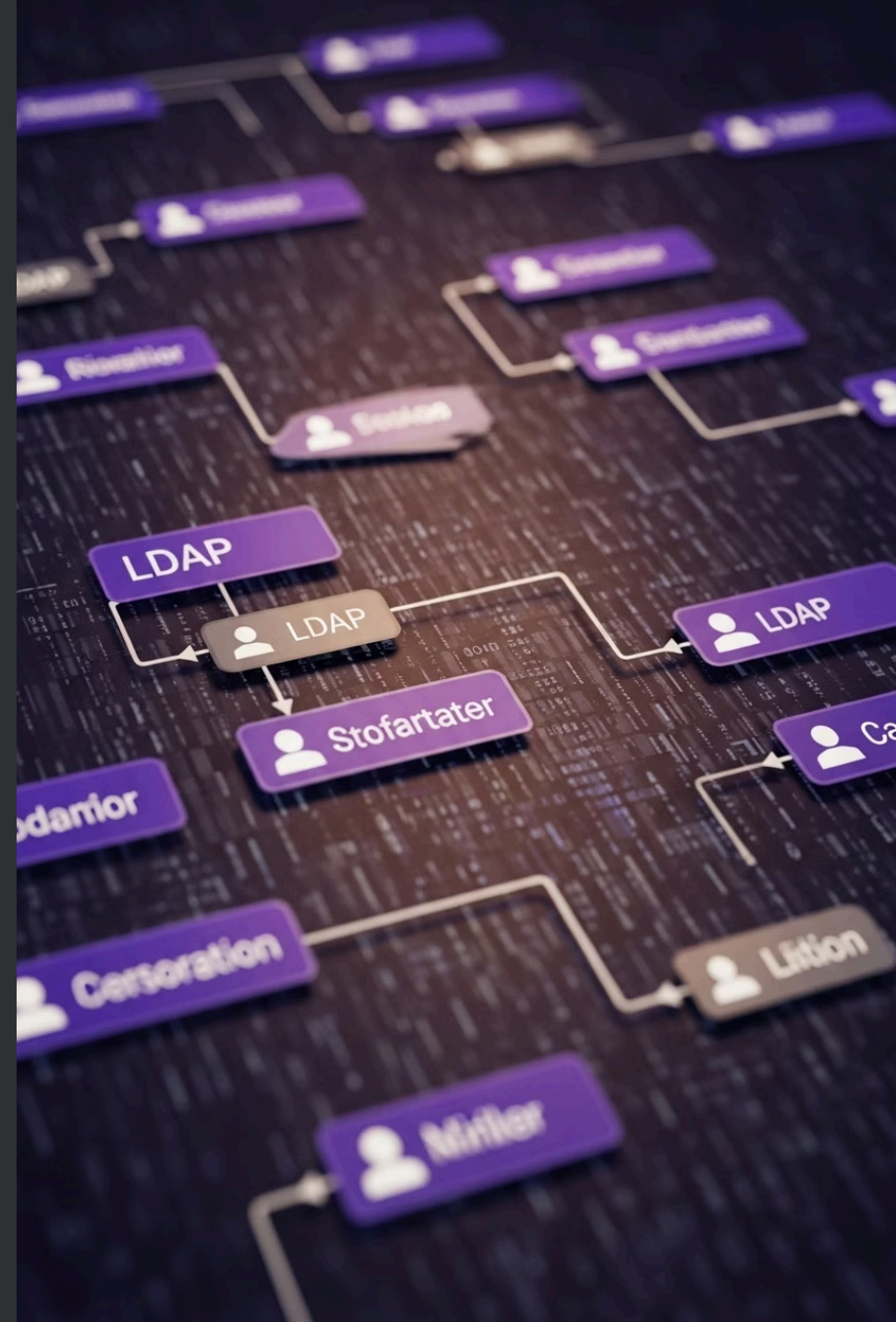


OpenLDAP Basics & Important Configuration

A comprehensive guide to understanding, implementing, and configuring OpenLDAP for centralised authentication and directory services in enterprise environments.

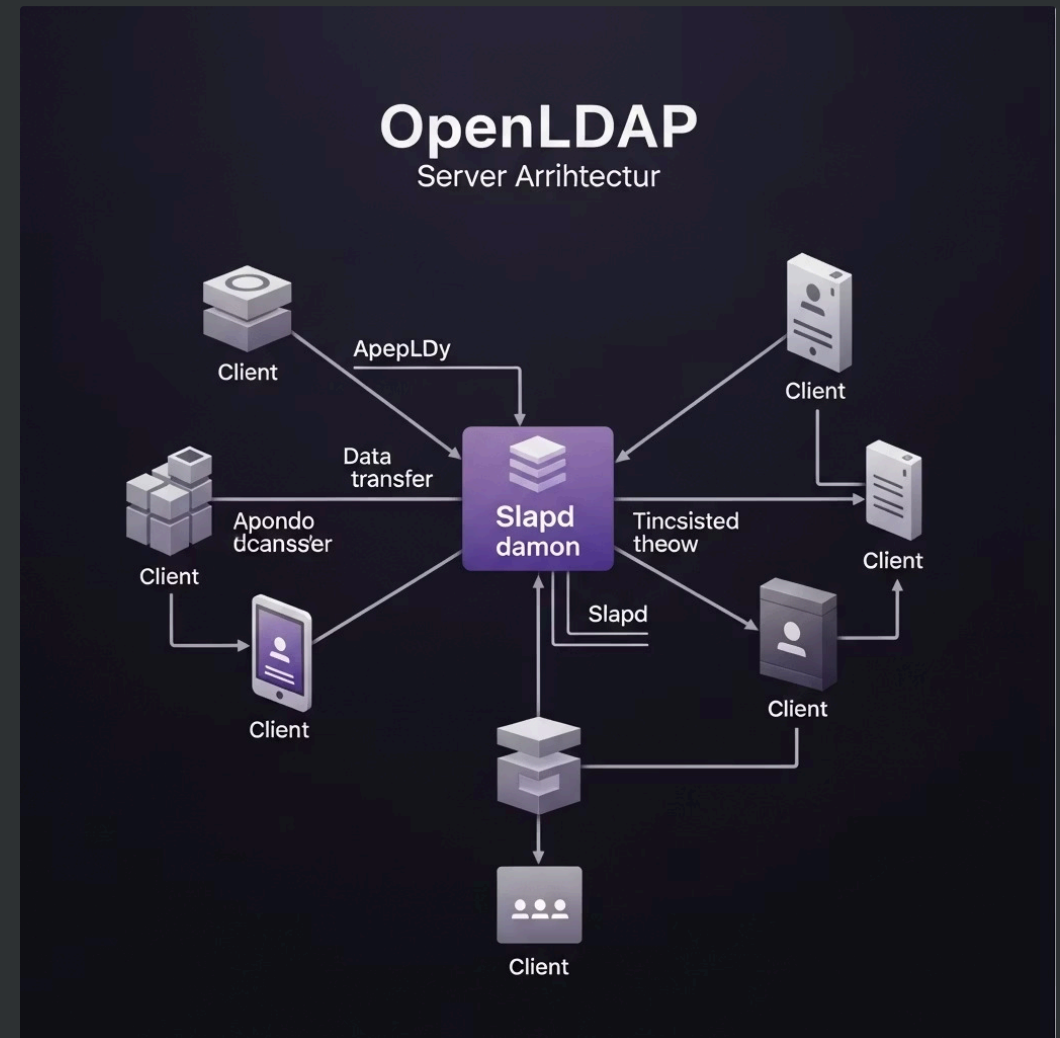


What is OpenLDAP?

OpenLDAP is an open-source implementation of the Lightweight Directory Access Protocol (LDAP), providing robust directory services for enterprise environments. It serves as a centralised repository for organisational data, user credentials, and access permissions.

The LDAP protocol excels at querying and modifying hierarchical directory data, making it the preferred choice for:

- Centralised authentication and authorisation
- User and group management
- Application configuration storage
- Organisational data management



At the core of OpenLDAP is the **slapd** daemon (Standalone LDAP Daemon), which listens for and processes LDAP requests over the network, serving directory data to authenticated clients.

Key LDAP Concepts



Directory Information Tree (DIT)

The hierarchical structure that organises all entries in the directory. Similar to a file system, the DIT arranges entries in a tree-like structure, with broader categories at the top and more specific entries below.



Entry

A collection of attributes uniquely identified by a Distinguished Name (DN). Each entry represents an object (e.g., person, organisation, device) and contains related information as attributes.



Attributes

Key-value pairs defined by schemas. Common examples include:

- cn: Common Name (e.g., "John Doe")
- mail: Email address
- uid: User identifier

Example Distinguished Name (DN): `cn=John Doe,ou=People,dc=example,dc=com`

This DN uniquely identifies John Doe in the People organisational unit within the example.com domain.

Installing OpenLDAP



Install Packages

```
sudo apt install slapd ldap-utils
```

This installs the OpenLDAP server (slapd) and client utilities for Ubuntu/Debian systems.

Initial Configuration

During installation, you'll be prompted to:

- Set administrator password
- Configure domain name (e.g., example.com → dc=example,dc=com)
- Choose backend database (MDB is recommended)

Verify Installation

```
sudo systemctl status slapd
```

Ensure the service is running correctly before proceeding with further configuration.

❏ For Windows users: Run OpenLDAP via Windows Subsystem for Linux (WSL) or compile from source code. Alternative Windows-native LDAP servers like Active Directory or Apache Directory Server may be easier to manage.

Need to change initial settings? Reconfigure anytime with: `sudo dpkg-reconfigure slapd`

OpenLDAP Configuration Methods

OpenLDAP offers two distinct configuration approaches, with the newer method providing significant advantages for enterprise deployments:

slapd-config (cn=config)

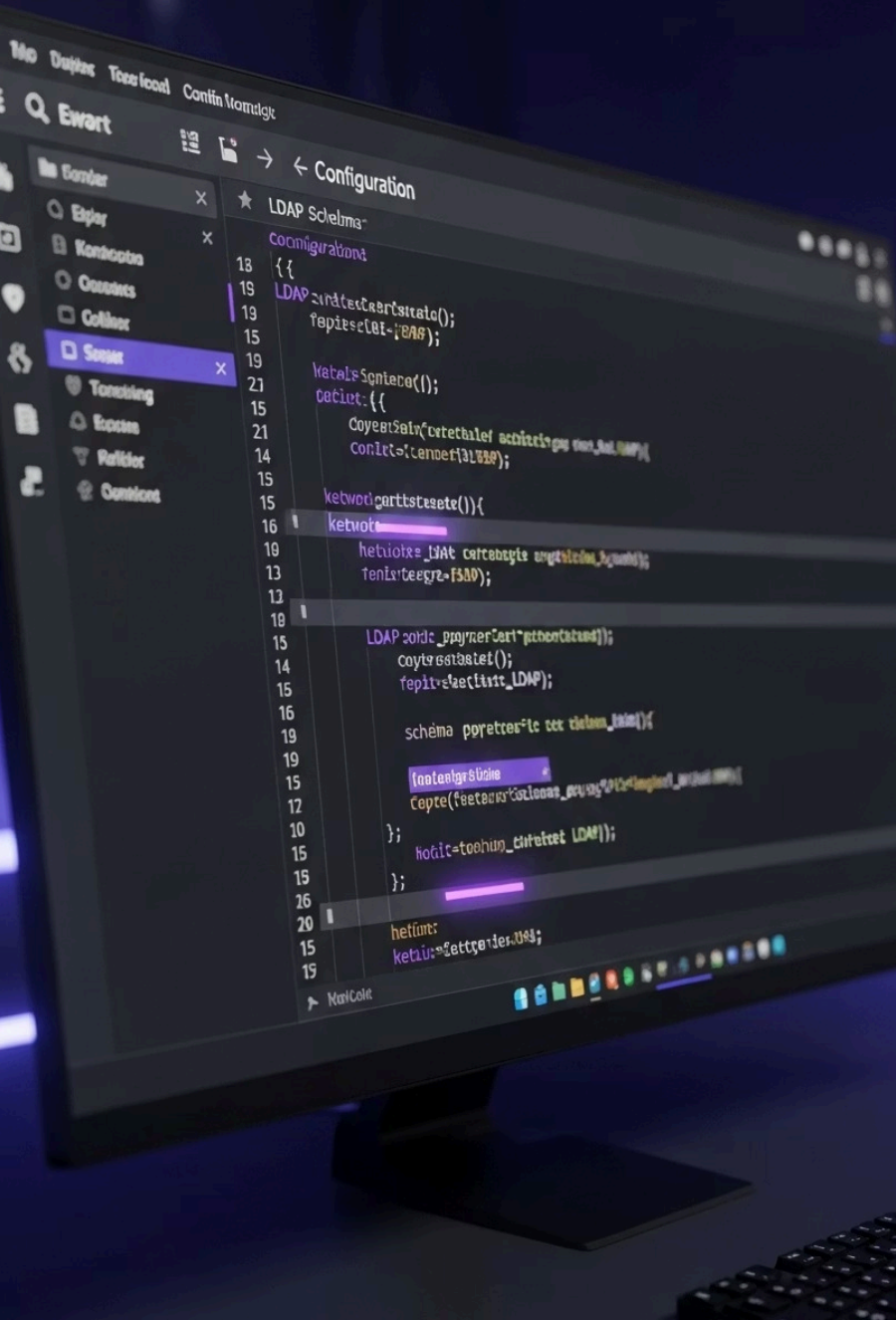
The modern, recommended approach that stores configuration as LDAP entries within a special DIT under `cn=config`. Key benefits:

- Dynamic runtime configuration without server restarts
- Changes managed via standard LDAP operations (`ldapadd`, `ldapmodify`)
- Configuration changes automatically persisted to disk
- Granular access control for configuration management

slapd.conf

The traditional flat file configuration method:

- Single text file with all configuration directives
- Deprecated but still supported for backward compatibility
- Requires server restart after changes
- Simpler for basic deployments



slapd-config Structure Overview

The `cn=config` configuration system organises settings hierarchically in a DIT structure that can be queried and modified using standard LDAP operations.

Major Configuration Components

Global Settings

`cn=config` - Server-wide parameters including security settings, network options, and logging configuration.

Schema Definitions

`cn=schema,cn=config` - Object classes and attribute types defining valid data structures.

Module Configuration

`cn=module{0},cn=config` - Loadable modules providing additional functionality.

Database Configuration

`olcDatabase={1}mdb,cn=config` - Settings for specific database instances.



⚠ Important: Never edit the LDIF files in `/etc/ldap/slapd.d/` directly. Always use LDAP tools like `ldapmodify` to make changes to the configuration.

```
# View current config
ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=config
```

Example slapd.conf Snippet (Legacy Config)

While modern OpenLDAP deployments use the `cn=config` method, understanding the legacy `slapd.conf` format is valuable for maintaining older systems or migrating to the new configuration approach.

```
# Global configuration
include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/inetorgperson.schema

# TLS configuration
TLSCACertificateFile /etc/ldap/certs/ca.crt
TLSCertificateFile /etc/ldap/certs/server.crt
TLSCertificateKeyFile /etc/ldap/certs/server.key


# Database configuration
database     mdb
suffix       "dc=example,dc=com"
rootdn       "cn=admin,dc=example,dc=com"
rootpw       {SSHA}hashed_password_here
directory    /var/lib/ldap

# Indices for performance
index        objectClass eq
index        uid eq
index        mail eq
index        cn eq,sub
```

Converting to Modern Configuration

You can convert a legacy `slapd.conf` file to the new `cn=config` format with:

```
sudo slaptest -f /path/to/slapd.conf -F /etc/ldap/slapd.d
```

 The migration process creates a new directory structure under `/etc/ldap/slapd.d/` containing LDIF files that represent the configuration as LDAP entries.

After conversion, validate the new configuration and restart the server to apply changes:

```
sudo slaptest -F /etc/ldap/slapd.d
sudo systemctl restart slapd
```