Getting Started

Table of Contents

Directory Concepts 2
Your First Directory 3
- Prepare the Environment 3
- Set Up and Start the Server 3
- Add a Person 4
- Search and Change the Entry 4
- Restart and Remove the Sample Data 5
- Next Steps 6

Learn the directory concepts used by OpenDJ, then install a local *evaluation server and add, find, change and delete an LDAP entry.*

Directory Concepts

OpenDJ stores directory entries and makes them available to applications through LDAP. A directory is commonly used to hold users, groups and application configuration. Applications bind to the server to authenticate, then search or update entries according to their access rights.

Entry

A record containing named attributes. A person entry can have `cn` (common name), `sn` (surname) and `mail` attributes. Some attributes can have multiple values.

Distinguished name (DN)

The name identifying an entry in the directory tree. For example, `uid=alice,ou=People,dc=example,dc=com` identifies Alice beneath the People organizational unit. Its parent is `ou=People,dc=example,dc=com`.

Base DN

The starting point of a search or the root of a directory suffix. The tutorial creates a suffix with base DN `dc=example,dc=com`.

Object class and schema

An entry's `objectClass` values determine which attributes are required or permitted. For example, `inetOrgPerson` permits `mail` and requires the inherited `cn` and `sn` attributes. The server checks changes against its schema.

Bind

Authentication of a client connection. The tutorial binds as `cn=Directory Manager`, an administrative account created by setup. Applications should use accounts with only the access they need.

Search

A request with a base DN, scope and filter. The filter `(uid=alice)` finds entries whose `uid` is `alice`; the attributes requested determine which values are returned. Access controls still apply to matching entries.

LDIF

LDAP Data Interchange Format, a text format for entries and changes. Each attribute appears as `name: value`, and a blank line separates entries. Change records also specify an operation, such as `changetype: modify`.

A server stores a suffix in a backend. Replication can synchronize directory data between servers; it does not replace backups. This tutorial uses one server and one backend.

Continue with Your First Directory. For a fuller explanation, see Understanding Directory Services.

Your First Directory

This exercise uses the published OpenDJ 5.2.0 ZIP distribution on Linux or macOS with Bash. It creates a new evaluation instance, uses a self-signed certificate for LDAPS, and leaves existing installations alone. For Windows, native packages or Docker, use the Installation Guide.

Prepare the Environment

Install Java 11 or later, `curl` and `unzip`. Run `java -version` to check the Java runtime. If several runtimes are installed, set `OPENDJ_JAVA_HOME` to the Java installation you want OpenDJ to use. Run the commands below in Bash; on macOS, enter `bash` first if your terminal uses another shell, such as zsh.

Use a host reserved for local evaluation and keep the listener ports inaccessible from other hosts. Ports 1389 (LDAP), 1636 (LDAPS) and 4444 (administration) must be free. The example connects to `localhost`; the setup host name does not restrict listeners to the loopback interface.

Download and unpack the server in a new directory:

```
mkdir opendj-quickstart
cd opendj-quickstart
curl --fail --location --output opendj.zip \
  https://github.com/OpenIdentityPlatform/OpenDJ/releases/download/5.2.0/opendj-
5.2.0.zip
unzip -q opendj.zip
```

Set Up and Start the Server

Read the license before accepting it with the setup command below. Choose a nonempty administrator password. Save it in a file readable only by your account so it does not appear in command arguments or shell history:

```
read -r -s -p 'Directory Manager password: ' quickstart_password
printf '\n'
(umask 077; printf '%s\n' "$quickstart_password" > quickstart-password.txt)
unset quickstart_password
cd opendj
./setup --cli --no-prompt --acceptLicense \
  --hostname localhost --ldapPort 1389 --ldapsPort 1636 \
  --adminConnectorPort 4444 --generateSelfSignedCertificate \
  --rootUserDN 'cn=Directory Manager' \
  --rootUserPasswordFile ../quickstart-password.txt \
  --baseDN 'dc=example,dc=com' --addBaseEntry
```

Setup creates the base entry and starts the server. Keep this terminal in the `opendj` directory for the remaining commands.

Verify that the base entry exists:

```
./bin/ldapsearch --hostname localhost --port 1636 --useSSL --trustAll \
  --bindDN 'cn=Directory Manager' --bindPasswordFile ../quickstart-password.txt \
  --baseDN 'dc=example,dc=com' --searchScope base '(objectClass=*)' dn
```

The output should contain `dn: dc=example,dc=com`. The `--trustAll` option accepts the evaluation certificate without validating its identity. For a deployed service, configure a trusted certificate and client trust instead; see Preparing For Secure Communications.

Add a Person

Create a People organizational unit and Alice's entry in an LDIF file. The parent entry must precede its child:

```
cat > people.ldif <<'LDIF'
dn: ou=People,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People

dn: uid=alice,ou=People,dc=example,dc=com
objectClass: top
objectClass: inetOrgPerson
uid: alice
cn: Alice Jensen
sn: Jensen
mail: alice@example.com
LDIF
./bin/ldapmodify --hostname localhost --port 1636 --useSSL --trustAll \
  --bindDN 'cn=Directory Manager' --bindPasswordFile ../quickstart-password.txt \
  --defaultAdd --filename people.ldif
```

Both additions should succeed. Alice is a directory record here; this example does not assign her a password or configure application access.

Search and Change the Entry

Search below the base DN for Alice, requesting only her name and email address:

```
./bin/ldapsearch --hostname localhost --port 1636 --useSSL --trustAll \
  --bindDN 'cn=Directory Manager' --bindPasswordFile ../quickstart-password.txt \
  --baseDN 'dc=example,dc=com' '(uid=alice)' cn mail
```

The result includes Alice's DN, `cn: Alice Jensen` and `mail: alice@example.com`.

Replace the email address using an LDIF change record:

```
cat > update-alice.ldif <<'LDIF'
dn: uid=alice,ou=People,dc=example,dc=com
changetype: modify
replace: mail
mail: alice.jensen@example.com
LDIF
./bin/ldapmodify --hostname localhost --port 1636 --useSSL --trustAll \
  --bindDN 'cn=Directory Manager' --bindPasswordFile ../quickstart-password.txt \
  --filename update-alice.ldif
```

Repeat the search. It should now return `mail: alice.jensen@example.com`.

Restart and Remove the Sample Data

Stop and restart the server as the same operating-system user who ran setup:

```
./bin/stop-ds
./bin/start-ds
```

Repeat the search to verify that Alice's changed email address survives the restart.

Delete the child entry before its parent:

```
for dn in 'uid=alice,ou=People,dc=example,dc=com' 'ou=People,dc=example,dc=com'; do
  ./bin/ldapdelete --hostname localhost --port 1636 --useSSL --trustAll \
    --bindDN 'cn=Directory Manager' --bindPasswordFile ../quickstart-password.txt \
    "$dn"
done
```

Repeat the search once more. It should return no entries. The base entry remains available for another exercise.

Stop the evaluation server and remove the temporary password and LDIF files when finished:

```
./bin/stop-ds
rm ../quickstart-password.txt people.ldif update-alice.ldif
```

The installation and its database remain on disk. To use it again, run `./bin/start-ds` and re-create `../quickstart-password.txt` with the same administrator password and restrictive permissions before repeating the client commands. To remove it, follow Removing OpenDJ Servers.

Next Steps

- Configuring Privileges and Access Control explains how to give application accounts the access they need.
- Backing Up and Restoring Data and Monitoring cover routine operations.
- Managing Data Replication covers multiple servers.
- Find a Procedure links deployment and integration recipes.
- OpenDJ 5.2.0 Release Notes describes this release and links the complete change list.