Practical 7: ISIM LDAP Setup and Configuration

Subject: Identity and Access Management (ISIM)

This guide details the steps to configure IBM Security Directory Server (LDAP), set up two instances, populate them with data, and establish replication between them.

Part 1: Initial Setup and Instance Creation

Exercise 1: List Existing Instances

Before starting, check what is currently running to avoid conflicts.

- **Command:**

```
/opt/ibm/ldap/V6.4/sbin/idsilist -a
```

- **Explanation:** Lists all configured LDAP instances. `-a` displays detailed info (ports, IP, version).

Exercise 2: Create Operating System Users

You need OS users to "own" the LDAP instances. We will create two users: `nisarg1` and `nisarg2`.

- **Commands:**

```
./idsadduser -u nisarg1 -w P@ssword -l /home/nisarg1 -g idsldap -n
./idsadduser -u nisarg2 -w P@ssword -l /home/nisarg2 -g idsldap -n
```

- **Key Flags:**
  - `-u` : Username
  - `-w` : Password
  - `-g` : Primary Group (must be `idsldap`)
  - `-l` : Home directory location

Exercise 3: Create LDAP Instances

Now, create the actual Directory Server instances linked to the users created above.

- **Commands:**

```
./idsicrt -I nisarg1 -e encryptionseed -l /home/nisarg1 -n
./idsicrt -I nisarg2 -e encryptionseed -l /home/nisarg2 -n
```

- Key Flags:
  - `-I` : Instance name (usually matches the OS user)
  - `-e` : Encryption seed (internal random seed for crypto)

Exercise 4: Configure DB2 Database

LDAP needs a backend database (DB2) to store the data.

- Commands:

```
./idscfgdb -I nisarg1 -w P@ssword -a nisarg1 -t nisarg1 -l /home/nisarg1 -n
./idscfgdb -I nisarg2 -w P@ssword -a nisarg2 -t nisarg2 -l /home/nisarg2 -n
```

- Key Flags:
  - `-a` : DB2 administrator ID (matches instance name)
  - `-t` : Database name
  - `-w` : DB administrator password

Exercise 5: Set Administrator Password

Set the password for the LDAP superuser (`cn=root`).

- Commands:

```
./idsdnpw -I nisarg1 -u cn=root -p P@ssword -n
./idsdnpw -I nisarg2 -u cn=root -p P@ssword -n
```

- Key Flags:
  - `-u` : Admin DN (Distinguished Name)
  - `-p` : Password

Part 2: Configuration and Data Population

Exercise 6: Start/Stop Instances & Check Configuration

Always test if the configuration works before proceeding.

1. Test Start (Configuration Check):

```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I nisarg1 -n -t
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I nisarg2 -n -t
```

(The `-t` flag tests the config file without actually keeping the server running).

2. Stop Instances (Gracefully):

```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I nisarg1 -k
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I nisarg2 -k
```

(The `-k` flag kills/terminates the server process).

Exercise 7: Add Suffixes

A "suffix" is the root of your directory tree (e.g., `o=jke`).

- Commands:

```
/opt/ibm/ldap/V6.4/sbin/idscfgsuf -I nisarg1 -s "o=jke" -n
/opt/ibm/ldap/V6.4/sbin/idscfgsuf -I nisarg2 -s "o=jke" -n
```

Exercise 8: Start Instances (For Real)

Now that suffixes are added, start the servers to accept data.

- Commands:

```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I nisarg1 -n
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I nisarg2 -n
```

(Note: The practical guide uses `-t` again in the screenshots, but usually, you remove `-t` to keep it running. If `-t` is used, the server stops immediately after checking. Ensure servers are running for the next steps).

Exercise 9: Add Organization Entry

Add the top-level organization entry (`o=jke`) to the directory.

- Command (Interactive Mode):

```
/opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssword -p 1389
```

- Input Data:

```
dn: o=jke
objectclass: organization
objectclass: top
o: jke
```

(Repeat for `nisarg2` on port `2389`).

Exercise 10: Import LDIF Data (Bulk Add)

Instead of typing manually, create a file and import it.

1. **Create File** `User1.ldif`:

```
dn: cn=joe, o=jke
objectclass: person
objectclass: top
sn: walter

dn: cn=carry, o=jke
objectclass: person
objectclass: top
sn: jones
```

2. **Import Command:**

```
/opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssword -p 1389 -i /classfil
```

(Repeat for `nisarg2` on port `2389`).

Part 3: GUI & Replication Setup (Web Admin Tool - WAT)

Exercise 11: Configure Web Admin Tool

1. Open Firefox: `https://isim.test:9444/IDSWebApp/`
2. Login as `superadmin` / `secret`.
3. **Manage Console Servers** -> **Add**:
   - **Server 1:** Name: `nisarg1`, Port: `1389`, Admin Port: `3538`.
   - **Server 2:** Name: `nisarg2`, Port: `2389`, Admin Port: `3540`.
4. Logout and Login to `nisarg1` (LDAP Login) using `cn=root`.

Exercise 12: Configure Replication (Master-Slave Topology)

We will make `nisarg1` the **Master** and `nisarg2` the **Replica**.

Steps on Master (`nisarg1`):

1. **Replication Management** -> **Manage Topology**.
2. **Add Subtree:** Select `o=jke`.
3. **Manage Credentials:**
   - Select `o=jke`.

- Add Credential Name: `cn=replicamanager` .
- Method: `Simple Bind` .
- DN: `cn=replicamanager,o=jke` .
- Password: `P@ssword` .

4. **Define Topology:**
   - Click **Show Topology**.
   - Click **Add Master** (This defines the destination/replica).
   - Hostname: `localhost:2389` (This points to `nisarg2`).
   - **Credentials:** Select the `replicamanager` credential created above.
   - **Additional Tab:** Check "Add credential information on consumer".
     - Consumer Admin DN: `cn=root` .
     - Consumer Admin Password: `P@ssword` .
5. Click **Finish** and synchronize if prompted.

Exercise 13: Start Replication Queue

1. Go to **Manage Queues** (on `nisarg1`).
2. If status is Suspended, click **Suspend/Resume** to start it.
3. Ensure status becomes **Ready**.

Part 4: Verification

Exercise 14: Verify Replication

1. Login to `nisarg1` (Master).
2. **Directory Management** -> **Manage Entries**.
3. Edit user `cn=joe` . Change `sn` (Surname) from `walter` to `hayden` .
4. Logout.
5. Login to `nisarg2` (Replica).
6. **Directory Management** -> **Manage Entries**.
7. Check `cn=joe` . The `sn` should automatically be `hayden` .

Exam Preparation Guide: How to Remember Everything

The practical seems long, but it follows a strict logic. Use the **"U-I-DB-PW-S"** flow for the command line part.

1. The "U-I-DB-PW-S" Mnemonic (Command Line)

Memorize this sequence. You cannot do the next step without the previous one.

1. **User** (`idsadduser`): You need an OS user first.

2. Instance (`idsicrt`): Create the LDAP instance for that user.
3. DB (`idscfgdb`): Give that instance a database.
4. PW (`idsdnpw`): Secure that instance with a password.
5. Suffix (`idscfgsuf`): Give the instance a name/domain (`o=jke`).

2. Understanding the Flags

Don't memorize full command strings; memorize the **flags**. They are consistent across commands.

- `-I` (Capital i) = **Instance** Name (e.g., `nisarg1`).
- `-n` = **No** interaction (Just do it, don't ask me questions).
- `-l` (Lowercase L) = **Location** (e.g., `/home/nisarg1`).
- `-w` = **Password** (e.g., `P@ssword`).
- `-p` = **Port** (Used when adding data, `1389` vs `2389`).

3. Port Number Logic

- **Standard LDAP:** 389
- **Instance 1 (** `nisarg1` **):** `1389` (1 + 389)
- **Instance 2 (** `nisarg2` **):** `2389` (2 + 389)
- **Secure Ports:** `636 -> 1636 -> 2636`
- *Tip:* If the exam asks for Instance 3, the port will likely be `3389` .

4. Replication Logic (The "Push" Concept)

Remember: You are configuring everything on the **Master (** `nisarg1` **)**. You are telling the Master:

1. "Here is the data tree I want to copy" (`Add Subtree`).
2. "Here is the ID/Password needed to talk" (`Manage Credentials`).
3. "Here is the guy I am copying to" (`Add Master` -> enter `nisarg2` port `2389`).
4. "Push the credentials to him so he knows me" (`Add credential info on consumer`).

5. Common Exam Pitfalls (Checklist)

- **Forgot to stop server?** You cannot add a suffix (`idscfgsuf`) if the server is running. Stop it with `-k` .
- **Wrong Port?** If `idsldapadd` fails, check if you typed `-p 1389` or left it default (which fails if you aren't root).
- **Replication not working?** check **Manage Queues**. If it says "Suspended", nothing will happen. You must click "Resume".