Practical 8: Organization Management Exercises

Subject: Identity and Access Management (ISIM)

This guide covers creating an organization structure, managing users, setting up administrative domains, and navigating the LDAP directory using both command-line tools and a GUI browser.

Part 1: Organization & User Management (ISIM Console)

Login:

- **URL:** `https://isim.test:9444/itim/console/`
- **User:** `itim manager`
- **Password:** `P@ssword`

Exercise 1: Creating the Organization Tree

You are building the skeleton of your company, "JK Enterprises".

1. Create Organizational Units (Departments):

1. Go to **Manage Organization Structure**.
2. Click the arrow next to `JK Enterprises` to expand it.
3. Click the arrow/triangle next to `JK Enterprises` -> Select **Create Organizational Unit.**
4. Enter Name: `Sales` . Click **OK**.
5. **Repeat** for `Finance` and `Development` .

2. Create Locations (Regions):

1. Click the arrow next to `JK Enterprises -> Sales` (You are creating these *under* Sales).
2. Select **Create Location.**
3. Enter Name: `WW` (Worldwide). Click **OK**.
4. **Repeat** for `Americas` , `EMEA` , and `AP` .

3. Create Business Partner Unit (External):

1. Click the arrow next to `JK Enterprises` .
2. Select **Create Business Partner Unit.**
3. Enter Name: `TechSupport` . Click **OK**.

Exercise 2: Creating Users manually

Now populate the organization with employees.

1. Go to **Manage Users** on the Home tab.
2. Click **Create.**

3. **Select User Type:** Choose `Person` and Business Unit `Finance` (or `JK Enterprises` as required). Click **Continue**.

4. **Fill in Tabs:**

   - **Personal Information:** Last Name (`Smith`), Full Name (`Alice Smith`), User ID (`asmith`).

   - **Contact Information:** Email (`asmith@jke.test`).

   - **Password:** Select "Allow me to type a password" -> `P@ssword` .

5. Click **Submit**.

   - *Repeat for other users like Bob Smith, Sue Thomas, etc., as listed in your lab manual.*

Exercise 3: Creating an Admin Domain

Admin domains are used to separate administrative powers (e.g., giving TechSupport their own admin area).

1. Go to **Manage Organization Structure**.

2. Expand to find `TechSupport` (created in Ex 1).

3. Click the arrow next to `TechSupport` -> Select **Create Admin Domain**.

4. **Details:**

   - **Name:** `TechSupport Business Security` .

   - **Administrator:** Search and select `John Davis` .

5. Click **OK**.

Exercise 4: Adding a System Administrator

You will create a new user (your own ID) and give them full system power.

1. **Create the User:**

   - Go to **Manage Users** -> **Create**.

   - Create a user with **your name** (e.g., `Nisarg Prajapati` , ID: `NPrajapati`).

   - Set password to `P@ssword` . Submit.

2. **Assign Admin Role:**

   - Go to **Manage Groups**.

   - Search for Service: `ITIM Service` . Click **Continue**.

   - Find the Group: `System Administrator` .

   - Click arrow next to it -> **Add Members**.

   - Search for your user (`NPrajapati`), select it, and click **OK**.

3. **Verify:** Log out and log back in with `NPrajapati` to ensure you have admin access.

Exercise 5: Enabling Automatic Group Membership

This setting automatically adds new users to default groups like "Manager" or "Service Owner".

1. Log in as `NPrajapati` (or `itim manager`).

2. Go to **Set System Security** -> **Set Security Properties**.

3. Scroll to **Group Settings**.

4. Check the box: "Automatically populate identity manager groups".

5. Click **OK**.

Part 2: LDAP Navigation (Backend)

Exercise 6: Navigating LDAP (CLI & GUI)

A. Using CLI (`idsldapsearch` **)**

- **Path:** `cd /opt/ibm/ldap/V6.4/bin`

- **Syntax:** `./idsldapsearch -b "basedn" "filter" attribute`

- **Task 1: Find all attributes for Bob Smith**

  ```
  ./idsldapsearch -s sub -b "dc=com" "cn=Bob Smith"
  ```

- **Task 2: Find email for Sue Thomas**

  ```
  ./idsldapsearch -b "dc=com" "cn=Sue Thomas" mail
  ```

- **Task 3: Find Managers (Filter by Title)**

  ```
  ./idsldapsearch -b "dc=com" "title=*manager*"
  ```

B. Using LDAP Browser (GUI Tool)

1. Open **LDAP Browser** from the desktop.

2. Connect to `ISIM_LDAP`.

3. Expand `dc=com` -> `ou=ibm` -> `ou=itim` ... to browse the tree manually.

4. **Searching:**

   - Right-click `ou=ibm` -> **Search**.

   - **Filter:** `(title=*manager*)`.

   - Click **Search**. You will see Sue Thomas.

   - Right-click her entry -> **View Entry** to see raw LDAP data.

Exam Preparation: How to Remember This

1. The "Tree Builder" Mental Model (Exercise 1 & 3)

Imagine you are an architect drawing a company chart.

- **Root:** JK Enterprises.

- **Branches (Depts):** Sales, Finance, Dev. (Created via "Create Org Unit").

- **Sub-Branches (Locations):** WW, AP, EMEA (Created *under* Sales via "Create Location").

- **External Branch:** TechSupport (Created via "Create Business Partner").

- **Security Fence:** Admin Domain (Created *under* TechSupport).

Exam Tip: Always check *where* you are clicking in the tree. If the question says "Create a location under Sales," you must click the arrow next to **Sales**, not JK Enterprises.

2. The User Lifecycle (Exercise 2 & 4)

Memorize the tab order for creating a user:

1. **Who?** (Personal Info: Name, ID).

2. **Where?** (Business Info: Employee #, Manager).

3. **How to contact?** (Contact Info: Email).

4. **Access?** (Password/Security).

3. The "Power Up" Sequence (Exercise 4)

To make someone a Super Admin, remember you don't do it in the "User" tab.

- **Step 1:** Create User (Normal person).

- **Step 2:** Go to **Groups** (Where the power lives).

- **Step 3:** Find **ITIM Service** (The system itself).

- **Step 4:** Add to **System Administrator** group.

4. LDAP Search Syntax (The "B-F-A" Rule)

For the CLI part, memorize **B-F-A**:

- **-b (Base):** Where to start? (`"dc=com"`).

- **Filter:** What are we looking for? (`"cn=Bob Smith"` or `"title=*manager*"`).

- **Attribute:** What specific info do we want? (`mail`). If empty, you get everything.

Command: `./idsldapsearch -b "..." "..." [attribute]`

5. Common Exam Pitfalls

- **Forgetting to Refresh:** After creating a user or unit, if you don't see it, look for the **Refresh** button or click the parent folder again.

- **Wrong Context:** When creating a Location, make sure you selected "Sales" first. If you create it under "Finance" by mistake, you lose points.

- **LDAP Filters:** Remember the wildcards. `title=manager` looks for exact match.