Practical 11: Services, Policies, and Reconciliation

Subject: Identity and Access Management (ISIM)

This practical covers connecting ISIM to a managed resource (Linux), defining how accounts are created (Policies), and linking existing accounts to users (Reconciliation/Adoption).

Part 1: Service Creation

Exercise 1: Creating a Linux Service

You are connecting ISIM to a Linux server to manage its users.

1. **Navigate:** Home -> **Manage Services** -> **Create**.
2. **Select Business Unit:** `JK Enterprises` . Click **Next**.
3. **Service Type:** Select `POSIX Linux profile` . Click **Next**.
4. **General Information:**
   - **Service Name:** `Linux Service`
   - **Tivoli Directory Integrator location:** `rmi://isim.test:1099/ITDIDispatcher`
   - **Managed resource location:** `isim.test`
   - **Owner:** Search and select `Bob Smith` .
5. **Additional Configuration:**
   - **Use a shadow file?** Check this box.
   - **Path to sudoers:** `/etc/sudoers`
   - **Command for failed logins:** `pam_tally2`
6. **Authentication:**
   - **Administrator name:** `root`
   - **Is sudo user?** Checked.
   - **Password:** `P@ssword` (or your lab password).
   - *Click **Test Connection**.* If successful, click Next.
7. **Configure Policy:** Select **"Yes, create a policy to automatically create accounts..."**.
8. **Reconcile Supporting Data:** Leave default (Daily).
9. **Finish.**

Part 2: Policy Management

Exercise 2: Creating an Identity Policy

This policy decides what the User ID (Login ID) will look like for new accounts.

1. **Navigate:** Home -> **Manage Policies** -> **Manage Identity Policies**.
2. **Create:**
   - **Name:** `Linux Identity Policy`.
   - **Business Unit:** `JK Enterprises`.
3. **Targets:** Add `Linux Service`.
4. **Rule:**
   - **First attribute:** `Preferred user ID`.
   - **Character limit:** `6`.
   - **Apply case:** `Lower case`.
5. Click **OK**.

Exercise 3: Creating a Password Policy

This sets the rules for passwords on the Linux system.

1. **Navigate:** Home -> **Manage Policies** -> **Manage Password Policies**.
2. **Create:**
   - **Name:** `Linux Password Policy`.
   - **Business Unit:** `JK Enterprises`.
3. **Targets:** Add `Linux Service`.
4. **Rules:**
   - **Minimum length:** `4` (as per the screenshot).
5. Click **OK**.

Part 3: Reconciliation (Reading Data)

Exercise 4: Running Reconciliation

Now we pull data from the Linux server into ISIM.

1. **Navigate:** Home -> **Manage Services**.
2. Find `Linux Service`.
3. **Schedule:** Click arrow -> **Set Up Reconciliation**.
   - Click the existing schedule. Change it to **Daily** at **4:00 PM**. Click OK.
4. **Run Now:** Click arrow -> **Reconcile Now**.
   - Query: `None`. Click Submit.
5. **Verify:**
   - Go to **View Requests** to confirm success.
   - Go to **Manage Services** -> `Linux Service` -> **Accounts**.

- You will see accounts like `root`, `bin`, `daemon`, etc. Their status is "Active" but Owner is "None" (Orphan accounts).

Part 4: Account Adoption (Fixing Orphans)

Exercise 5: Creating a System Person

We need a "fake" user to own all the technical accounts (like root) so they aren't orphans.

1. **Navigate:** Home -> **Manage Users** -> **Create**.
2. **Type:** `Person`. **Unit:** `JK Enterprises`.
3. **Details:**
   - **First Name:** `Linux`
   - **Last Name:** `System-Accounts`
   - **User ID:** `linuxsystemaccounts`
4. **Submit.**

Exercise 6: Manual Adoption

Manually link one specific account to the user we just created.

1. **Navigate:** Home -> **Manage Services** -> `Linux Service` -> **Accounts**.
2. Find the account named `nobody`.
3. Click arrow -> **Assign to User**.
4. Search and select `Linux System-Accounts`.
5. Click **Assign**.

Exercise 7: Automatic Adoption (Adoption Policy)

Write a script to automatically grab all system accounts (UID < 500) and give them to our system user.

1. **Navigate:** Home -> **Manage Policies** -> **Manage Adoption Policies**.
2. **Create:**
   - **Name:** `Linux Service Adoption Policy`.
   - **Service Type:** `POSIX Linux profile`.
3. **Services:** Add `Linux Service`.
4. **Rule (Script):** Select "Providing a Script".
   - *Type exactly:*

```
if (subject.erposixuid <= 499) {
   var ps = new PersonSearch();
   return ps.searchByFilter("Person", "(cn=Linux System-Accounts)", 2);
```

```
}
```

5. Click **OK**.
6. **Apply Policy:**
   - Go to **Manage Services** -> `Linux Service` -> **Reconcile Now**.
   - Once finished, check **Accounts** again. Accounts like `root`, `bin`, `adm` should now be owned by `Linux System-Accounts`.

Part 5: LDAP Service (Extra Exercise)

Exercise 8: Creating an LDAP Service

Connecting to another directory server (TechSupport).

1. **Navigate:** **Manage Services** -> **Create**.
2. **Type:** `LDAP profile`.
3. **Details:**
   - **Name:** `TechSupport LDAP`.
   - **URL:** `ldap://isim.test:389`.
   - **User:** `cn=root` / **Password:** `P@ssword` (or lab default).
4. **Users and Groups:**
   - **User base DN:** `ou=TechSuppEmployees,dc=contractors`.
   - **User RDN:** `UID`.
   - **Group base DN:** `ou=TechSuppEmployees,dc=contractors`.
5. **Reconcile:** Run **Reconcile Now**.
6. **Verify:** Check Accounts. You might see red "X" icons because we haven't created a Provisioning Policy to allow them yet.

Exam Prep Strategy: "S-P-R-A"

To remember this practical, use the acronym **S-P-R-A**.

1. Service (The Connection)

- **What:** You are creating a pipe to the outside world (Linux or LDAP).
- **Key Params:** You *must* know the URL (`rmi://...` for Linux/TDI, `ldap://...` for LDAP) and the credentials (`root` / `cn=root`).
- *Tip:* Linux uses a "Profile" and usually needs the TDI dispatcher running on port 1099.

2. Policy (The Rules)

- **Identity Policy:** "How do I name you?" (Max 6 chars, lowercase).

- **Password Policy:** "How safe is your key?" (Min 4 chars).
- *Tip:* Policies must be linked to a **Target** (The Service) to work.

3. Reconciliation (The Fetch)

- **What:** Pulling data in.
- **Critical Step:** If you create a service but don't Reconcile, ISIM knows nothing. Always **Reconcile Now** after creation.

4. Adoption (The Cleaning)

- **The Problem:** Reconciled accounts have no owner ("Orphans").
- **The Fix:**
  - **Manual:** Right-click account -> Assign.
  - **Automatic:** Adoption Policy -> Script.
- **The Script Logic:** "If the user ID number is small (system account), give it to the System Admin user."

Summary Checklist for Exam

1. **Create Service:** Did you Test Connection?
2. **Reconcile:** Did you wait for "Success"?
3. **Adoption:** Did you create the `Linux System-Accounts` user *before* trying to assign accounts to it? (You can't assign to a user that doesn't exist).
4. **Script Syntax:** Memorize `ps.searchByFilter("Person", "(cn=Name)", 2);` . This