

INSTITUTE OF COMPUTER TECHNOLOGY
B-TECH COMPUTER SCIENCE ENGINEERING 2025-26
SUBJECT: IDENTITY ACCESS MANAGEMENT

NAME: Rahul Prajapati

ENRLL NO: 23162171020

BRANCH: CYBER SECURITY

BATCH: 52

Lab 11: Services and policies exercises

6.1 Creating a Linux Service

Objective: To create a **POSIX Linux service** in ISIM and configure its provisioning policy.

Steps:

1. **Service Creation:** Log in to the ISIM Administrative Console and navigate to **Home → Manage Services → Create**.
2. **Service Type:** Selected **POSIX Linux Profile** under the Business Unit **JK Enterprises**.
3. **Configuration:** Filled in the service details:
 - **Service Name:** Linux Service
 - **TDI Location:** rmi://isim.test:1099/ITDIDDispatcher
 - **Managed Resource Location:** isim.test
 - **Owner:** Bob Smith
 - **Use Shadow File:** Checked
 - **Query Failed Logins Command:** pam_tally2
 - **Is Sudo User?:** Checked
 - **Password:** P@ssw0rd

		Service Name	Description	Service T...	Business ...
<input type="checkbox"/>		<u>CSV Identity Feed</u>	CSV Feed for Finance Users	Comma Separated File (CSV) identity feed	<u>Finance</u>
<input type="checkbox"/>		<u>DSML Identity Feed</u>	Load Dev team through DSML Feed	DSML identity feed	<u>Development</u>
<input type="checkbox"/>		<u>ITIM Service</u>		ITIM	<u>JK Enterprises</u>
<input type="checkbox"/>		<u>LDAP inetOrgPerson identity feed</u>	LDAP identity feed	INetOrgPerson identity feed	<u>JK Enterprises</u>
<input type="checkbox"/>		<u>Linux Service</u>	Linux Service to ISIM	POSIX Linux profile	<u>JK Enterprises</u>
<input type="checkbox"/>		<u>TDI feed</u>		IDI data feed	<u>JK Enterprises</u>

Page 1 of 1 | Total: 6 Displayed: 6 Selected: 0

- 4. **Policy Configuration:** Selected Yes, create policy for manual account request before clicking Finish.

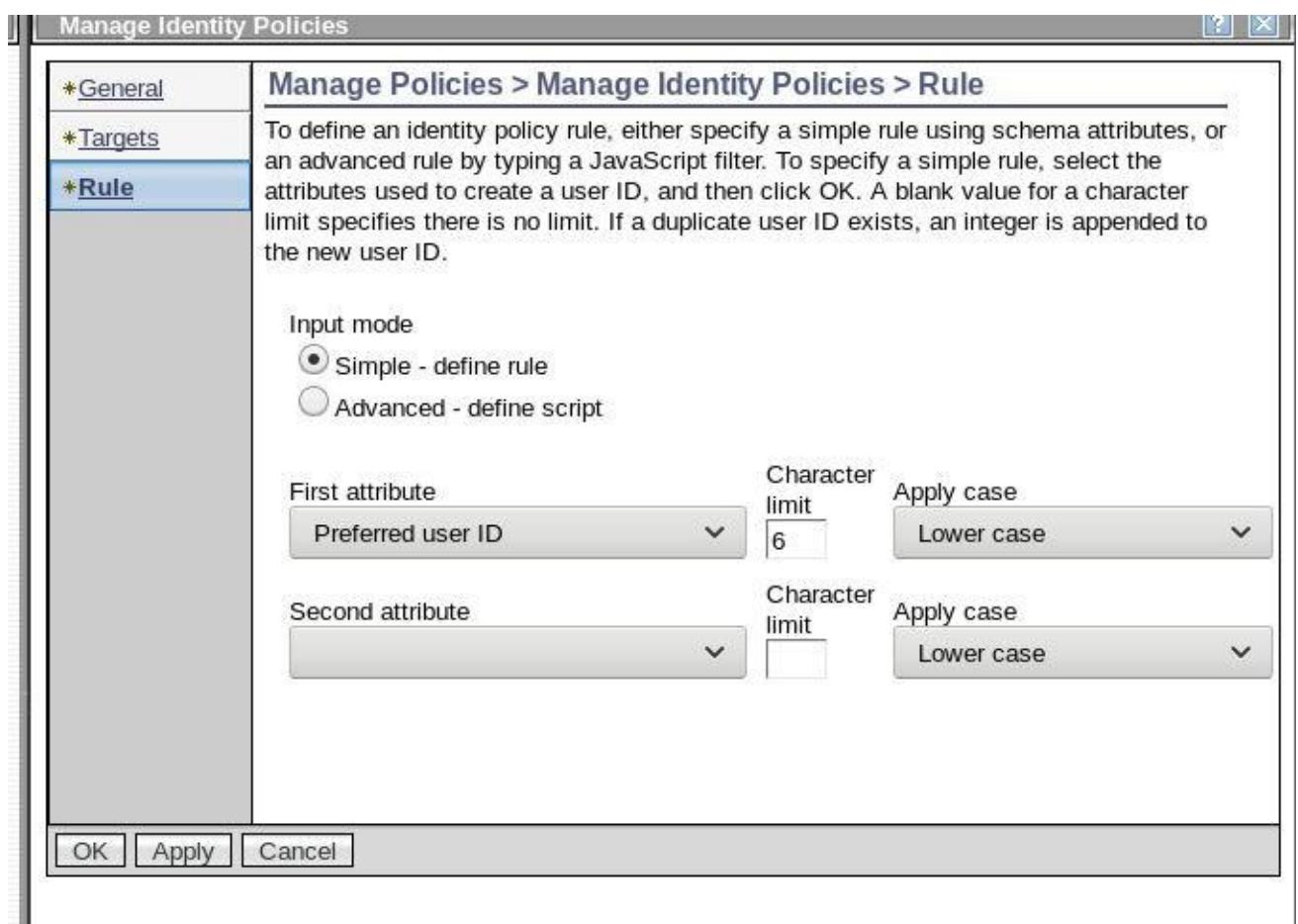
Output: The Linux Service was successfully created and appeared under Manage Services.

6.2 Creating an Identity Policy

Objective: To create a new identity policy for the Linux Service that standardizes the account name using the first 6 lowercase characters of the user's preferred ID.

Steps:

1. Go to Home → Manage Policies → Manage Identity Policies and click Create.
2. **Policy Details:** Set the Name to Linux Identity Policy, Status to Enabled, and Business Unit to JK Enterprises (with availability to subunits).
3. **Targets:** Added the newly created Linux Service.
4. **Add Rule:** Configured the account naming rule:
 - **First Attribute:** Preferred User ID
 - **Character Limit:** 6
 - **Apply Case:** Lowercase



5. Clicked **Apply** and then **OK** to submit.

<input type="button" value="Create"/>	<input type="button" value="Change"/>	<input type="button" value="Delete"/>			
<input type="checkbox"/> Select	Identity Policy Name	Description	User Type	Status	
<input type="checkbox"/>	Default identity policy for ITIM (BPPerson)	Default identity policy for all services and for BPPerson class.	Business partner person	Enable	
<input type="checkbox"/>	Default identity policy for ITIM (Person)	Default identity policy for all services and for Person class.	Person	Enable	
<input type="checkbox"/>	Linux Identity Policy	Identity Policy for Linux Service	Person	Enable	

Page 1 of 1 | Total: 3 Displayed: 3 Selected: 0

6.3 Creating a Password Policy

Objective: To create a password policy requiring a minimum of 4 characters for Linux accounts.

Steps:

1. Go to Home → Manage Policies → Manage Password Policies and click Create.
2. **Policy Details:** Set the Name to Linux Password Policy, Status to Enabled, and Business Unit to JK Enterprises (with availability to subunits).
3. **Targets:** Added the Linux Service.
4. **Rules:** Set the Minimum length = 4.
5. Clicked OK to submit.

2 results found for: *

<input type="button" value="Create"/>	<input type="button" value="Change"/>	<input type="button" value="Delete"/>			
<input type="checkbox"/> Select	Password policy ...	Description	Status	Targets	Business
<input type="checkbox"/>	Default password policy for ITIM service	Disallow empty password for ITIM service	Enabled	ITIM Service	JK Enterpri
<input type="checkbox"/>	Linux Password Policy	Password Policy for Linux Service	Enabled	Linux Service	JK Enterpri

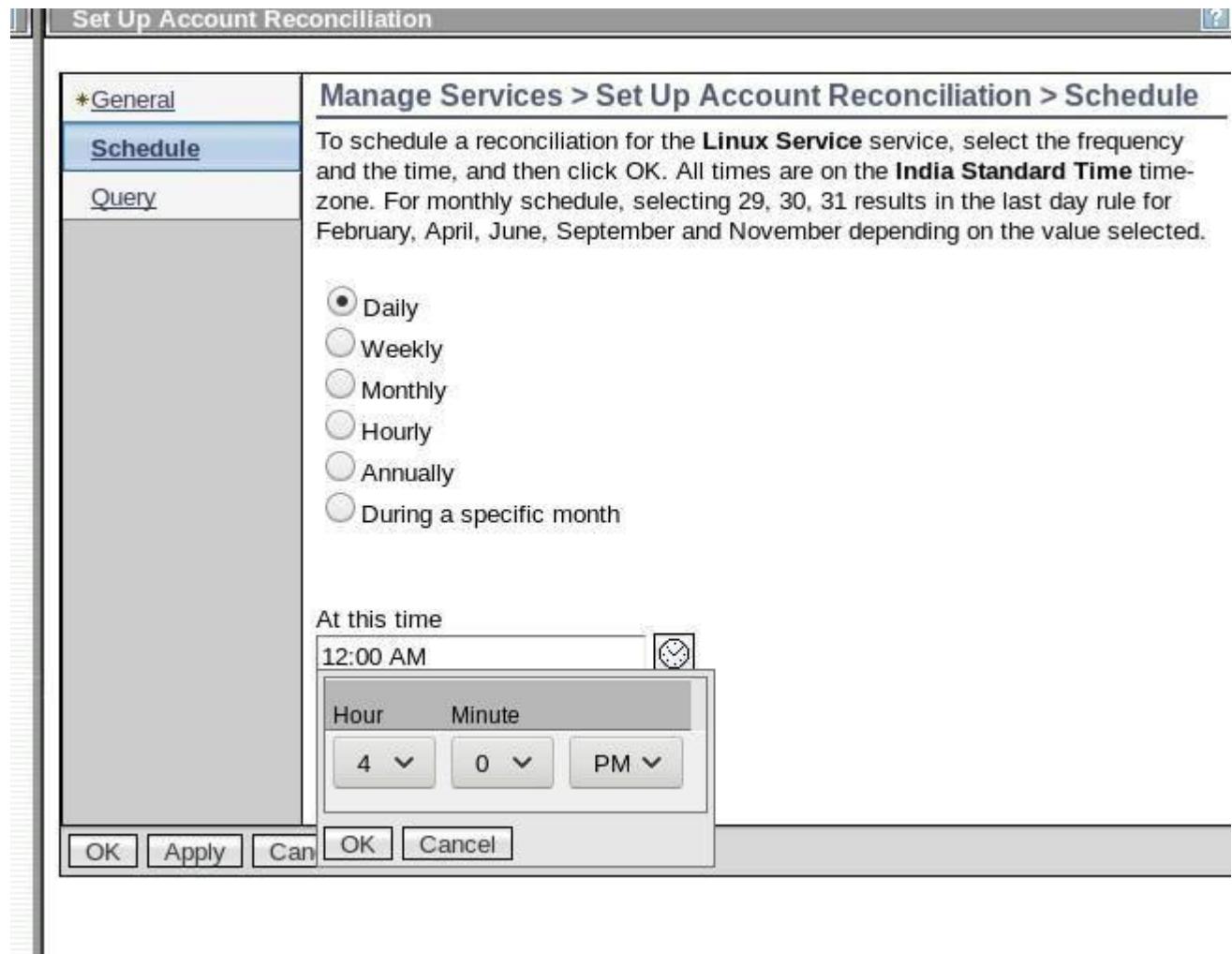
Page 1 of 1 | Total: 2 Displayed: 2 Selected: 0

6.4 Running a Reconciliation on Linux

Objective: To schedule and execute the first reconciliation against the Linux system to discover existing accounts.

Task 1: Setup Reconciliation Schedule

1. In **Manage Services**, clicked the arrow next to Linux Service and selected **Set Up Reconciliation**.
2. Modified the schedule to **Daily at 4:00 PM**.



Task 2: Run Initial Reconciliation

1. Selected the Linux Service **Reconcile Now**.
2. Ran the reconciliation with **Query = None**.

Requests

To view the details for a request, click the request type.

13 requests were submitted by **ITIM Manager** between **November 17, 2025** and **November 17, 2025**.

<input type="button" value="Cancel Request"/> <input type="button" value="Refresh"/>					
<input type="checkbox"/> Select ^	Status ^	Request Type ^	Date Submitted ^	Requestor ^	Requested
	<input checked="" type="checkbox"/> Success	<u>Reconciliation</u>	November 17, 2025 9:08:06 PM	<u>System Administrator</u>	

Task 3: Review Accounts

1. Navigated to **Linux Service Accounts**.
2. Clicked **Search** to list the discovered Linux system accounts (e.g., root, nobody, gdm).

<input type="text"/> Owner <input type="button" value="All"/>					
Accounts					
To perform a particular task on an account, click the icon next to the name of the user ID, and then select the					
49 results found for: *					
<input type="button" value="Request..."/> <input type="button" value="Change"/> <input type="button" value="Delete"/> <input type="button" value="Suspend"/> <input type="button" value="Restore"/> <input type="button" value="Assign to User"/> <input type="button" value="Refresh"/>					
<input type="checkbox"/> S ^	State ^	User ID	Owner		Ownership Ty
<input type="checkbox"/>		abrt	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		adm	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		avahi	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		bin	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		chrony	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		colord	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		daemon	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		db2admin	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		db2fenc1	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		dbus	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		ftp	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		games	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		gdm	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		geoclue	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		gluster	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		gnome-initial-setup	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		halt	<input type="button" value="▶"/> None		None
<input type="checkbox"/>		idsIdan	<input type="button" value="▶"/> None		None

6.5 Creating a System Person

Objective: To create a designated ISIM user (System Person) who will be assigned ownership of non- user accounts discovered on the managed resource.

Steps:

1. Go to **Home** → **Manage Users** → **Create Person**.
2. Entered the following details:
 - **Full Name:** Linux System-Accounts
 - **Preferred User ID:** linuxsystemaccounts
 - **Password:** P@ssw0rd
3. Submitted the user.

Create User

Manage Users > Create User > Success

You successfully submitted a request for **November 17, 2025 at 9:12 PM** to create user **Linux System-Accounts** .

Other Tasks

[View my request](#)

[Create another user](#)

[Close](#)

6.6 Adopting Accounts Manually

Objective: To manually assign existing Linux system accounts to the designated system user.

Steps:

1. Go to **Manage Services** → **Linux Service** → **Accounts**.
2. For the account **nobody**, clicked the arrow and selected **Assign to User**.
3. Searched for and assigned the account to **Linux System-Accounts**.
4. Refreshed the account list to confirm the nobody account now shows the new ownership.

Manage Services > Assign Account > Select a User

To assign the **nobody** account on the **Linux Service** service to a user, type information about the user in the field, and then click Search. By default, clicking Search will search the system based on the beginning letters of the item you are searching for. To search for a textual pattern in the middle of an item, use the "*" symbol on the keyboard to indicate a wildcard. (For example, typing "b*" will find "abc".)

Search information Search by

Users

To assign the **nobody** account to a user, select the user, and then click Continue.

1 results found for: linu

Select	Name	E-mail Ad...	Last Name	Business ...	Status
<input checked="" type="radio"/>	Linux System-Accounts		System-Accounts	JK Enterprises	Active

Page 1 of 1 | Total: 1 | Displayed: 1 | Selected: 1

<input type="checkbox"/>	nfsnobody	▶ None	None	Inactive
<input type="checkbox"/>	nobody	▶ Linux System-Accounts	Individual	Active
<input type="checkbox"/>	ntp	▶ None	None	Inactive
<input type="checkbox"/>	operator	▶ None	None	Active

6.7 Adopting Accounts Automatically

Objective: To automatically adopt Linux accounts with UID to the system user during reconciliation.

Task 1: Create Adoption Policy

If the account does not have an owner, then the account wil

Specify rule by

- Defining Matches
 Providing a Script

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

1. Go to Home → Manage Policies → Manage Adoption Policies and click Create.
2. **Policy Details:** Set the Name to Linux Service Adoption Policy.
3. **Services:** Added the Linux Service (POSIX Linux Profile).

- Rule: The adoption rule script was configured to check if the discovered account's UID is less than or equal to 499, which typically identifies system accounts.

Task 2: Run Reconciliation Again

- Go to Manage Services → Linux Service → Reconcile Now.

Requests

To view the details for a request, click the request type.

16 requests were submitted by **ITIM Manager** between **November 17, 2025** and **November 17, 2025**.

<input type="checkbox"/> Select	Status	Request Type	Date Submitted	Requestor	Requested for	Service Na
<input checked="" type="checkbox"/>	Success	Reconciliation	November 17, 2025 9:25:44 PM	System Administrator		Linux Servic

- After the reconciliation completed, checked the **Accounts** list.
- Confirmed that system accounts like gdm and ntp (which have UIDs) were automatically assigned ownership to the **Linux System-Accounts** user.

<input type="checkbox"/>	<u>avahi</u>	► Linux System-Accounts	Individual	In
<input type="checkbox"/>	<u>bin</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>daemon</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>dbus</u>	► Linux System-Accounts	Individual	In
<input type="checkbox"/>	<u>ftp</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>games</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>gdm</u>	► Linux System-Accounts	Individual	In
<input type="checkbox"/>	<u>halt</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>lp</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>mail</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>nobody</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>ntp</u>	► Linux System-Accounts	Individual	In
<input type="checkbox"/>	<u>operator</u>	► Linux System-Accounts	Individual	A
<input type="checkbox"/>	<u>postfix</u>	► Linux System-Accounts	Individual	In
<input type="checkbox"/>	<u>pulse</u>	► Linux System-Accounts	Individual	In
<input type="checkbox"/>	<u>gemu</u>	► Linux System-Accounts	Individual	In
<input type="checkbox"/>	<u>radvd</u>	► Linux System-Accounts	Individual	In

6.8 Creating an LDAP Service

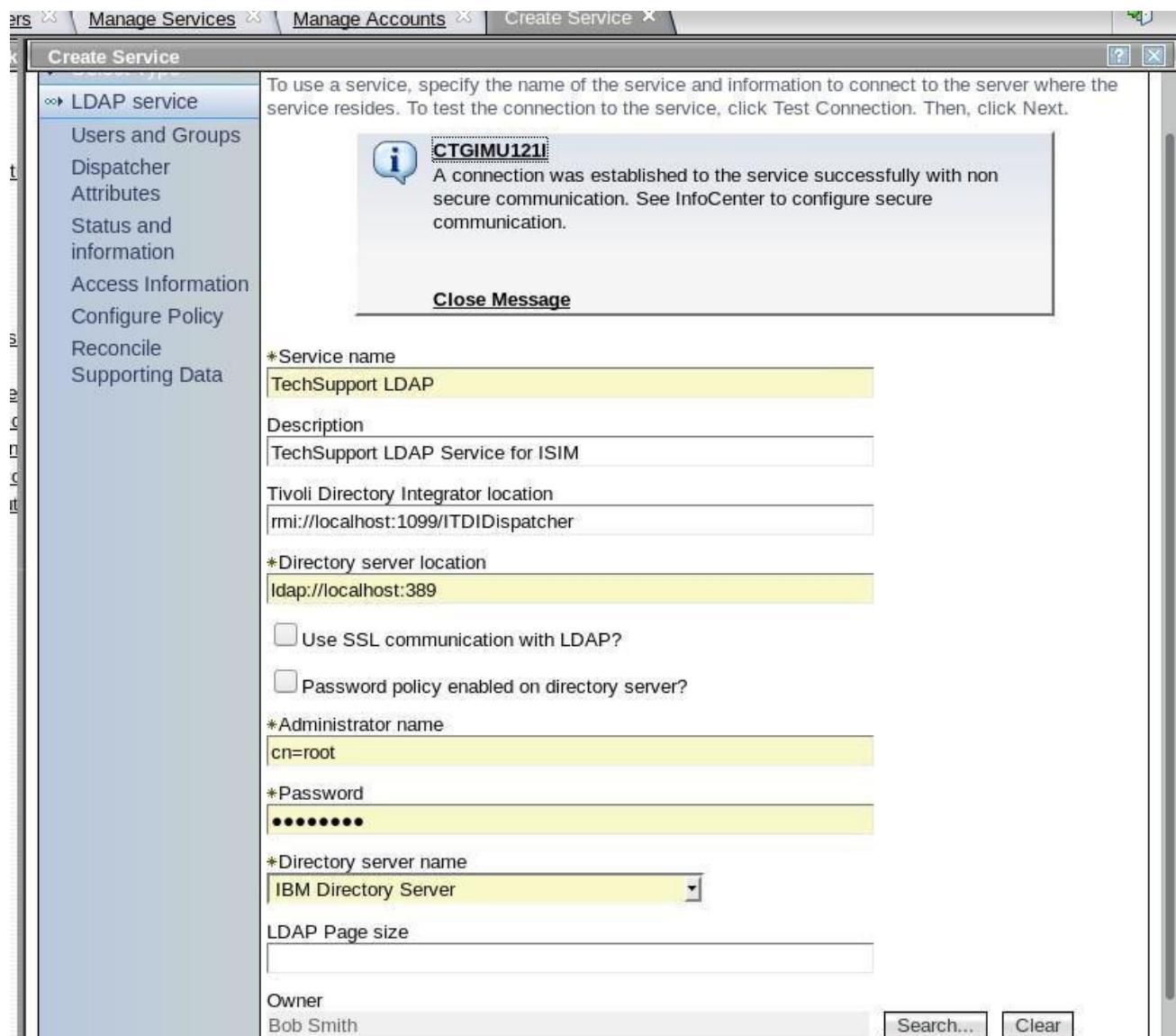
Objective: To create a service for provisioning and managing accounts and groups in an external LDAP directory.

Steps:

1. **Service Creation:** Go to Home → Manage Services → Create, selecting LDAP Profile under JK Enterprises.

2. **Connection Configuration:** Filled in the details:

- **Service Name:** TechSupport LDAP
- **TDI Location:** rmi://isim.test:1099/ITDIDDispatcher
- **Directory Server Location:** ldap://isim.test:389
- **Administrator Name/Password:** cn=root / P@ssw0rd
- **Owner:** Bob Smith



3. **Test Connection** and continued.

4. **DN Details:** Set the Base Distinguished Names (DNs):
 - **User Base DN:** ou=TechSuppEmployees,dc=contractors
 - **Group Base DN:** ou=TechSuppEmployees,dc=contractors
5. **Provisioning Policy:** Selected Yes, create policy for automatic accounts and clicked **Finish.**

[Create Service](#)

Manage Services > Create Service > Success

You successfully created the **TechSupport LDAP** service on the **LDAP profile** service type.

Other Tasks

[Create another service](#)

[Manage account request workflows](#)

[Manage identity policies](#)

[Manage password policies](#)

[Request an account for this service](#)

[Manage the groups on this service](#)

[Manage provisioning policies](#)

[Manage account defaults](#)

[Enforce policy for this service](#)

[Close](#)

6. **Reconciliation:** Executed **Reconcile Now** for the TechSupport LDAP service.

7. **View Accounts:** Viewing the accounts showed a Red “X” status, indicating that while the accounts were discovered, they were not fully provisioned because the automatic provisioning policy was not yet enabled (or configured for automatic account creation).

	IIM Service	IIM	JK Enterprises	Access Disabled
<input type="checkbox"/>	LDAP inetOrgPerson identity feed	LDAP identity feed	INetOrgPerson identity feed	JK Enterprises
<input type="checkbox"/>	Linux Service	Linux Service to ISIM	POSIX Linux profile	JK Enterprises
<input type="checkbox"/>	TDI feed		IDI data feed	JK Enterprises
<input type="checkbox"/>	TechSupport LDAP	TechSupport LDAP Service for ISIM	LDAP profile	JK Enterprises

Page 1 of 1 | Total: 7 | Displayed: 7 | Selected: 0

Requests

To view the details for a request, click the request type.

19 requests were submitted by ITIM Manager between November 17, 2025 and November 17, 2025.

Request Details						
Select		Status	Request Type	Date Submitted	Requestor	Requested for
<input type="checkbox"/>	Success	Reconciliation	November 17, 2025 9:42:15 PM	System Administrator		TechSupport
			November 17, 2025	Custom		

Conclusion

This lab successfully configured and tested provisioning services for both a **POSIX Linux system** and an **LDAP directory**. Key outcomes include:

- Policy Enforcement:** Established the **Identity Policy** (naming convention) and **Password Policy** (minimum length) for the Linux service.

Account information

Ownership type

Owner

All

Search

Accounts

To perform a particular task on an account, click the icon next to the name of the user ID, and then select the task you want to perform.

3 results found for: *

Actions		User ID	Owner	Ownership Type	Status
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ffreeloader	Freddy Freeloader	Individual	Inactive
<input type="checkbox"/>	<input checked="" type="checkbox"/>	mmanheim	Manny Manheim	Individual	Inactive
<input type="checkbox"/>	<input checked="" type="checkbox"/>	sshoemaker	Shelly Shoemaker	Individual	Inactive

Page 1 of 1 | Total: 3 | Displayed: 3 | Selected: 0

- Account Discovery:** Performed **reconciliation** to discover and bring existing system accounts into ISIM management.
- System Account Governance:** Created a dedicated system user and implemented **manual and automatic adoption policies** to assign ownership of system accounts (UID).
- Directory Integration:** Created and reconciled the **LDAP Service**, setting the foundation for managing external directory accounts and groups via ISIM.