6 Services and policies exercises

The exercises in this chapter teach the following topics:

- Creating the Linux Service
- Creating an identity policy
- Creating a password policy
- Running a reconciliation on Linux
- Creating a system person
- Adopting accounts manually
- Adopting accounts automatically
- Creating the LDAP service

6.1 Exercise 1 – Creating a Linux Service

In this exercise, you create a service in IBM Security Identity Manager to manage accounts and groups on a Linux system. You also create a default provisioning policy as part of the service creation process.

1. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager.**

2. On the Home tab, navigate to **Manage Services.**

3. Click **Create**.

4. Wait for the list of services to appear. Ensure that Business unit is set to **JK Enterprises.**

5. Select **POSIX Linux profile** and click **Next**.

6. Use the information in the following table to complete the Create a Service form (Keep other settings as it is) :

Field	Value
Service name	Linux Service
Description	Linux Service on ISIM
Tivoli Directory Integrator location	rmi://isim.test:1099/ITDIDispatcher
Managed resource location	isim.test
Owner	Bob Smith
Service Prerequisite	[Leave blank]
Use Shadow File (Additional Configuration Section)	Checked
Command used to query failed logins (Additional Configuration Section)	pam_tally2
Administrator name (Authentication	root

Section)	
Is Sudo User? (Authentication Section)	Checked
Password(Authentication Section)	P@ssw0rd
Configure Policy(Section)	Yes, create a policy for manually requesting account
Perform a supporting data reconciliation now	[Leave cleared]

Hint : After you enter authentication information, you can click **Test Connection** to verify that communication to the adapter is operational. If the test is not successful, confirm that you entered the correct value for the Tivoli Directory Integrator Location field and correctly filled out the Authentication section of the **Create Service** form. If the test still is not successful, confirm that the Tivoli Directory Integrator Adapter service is **running**. Type in the following commands to stop and start the service:

```
/opt/IBM/TDI/V7.2/timsol/ITIMAd stop
/opt/IBM/TDI/V7.2/timsol/ITIMAd start
```

After the test connection is successful, you can use the Status and Information section of the create service form to see details about the adapter and managed resource.

7. Click **Finish** to create the service.

8. Verify that the Linux Service was added.

6.2 Exercise 2 – Creating an identity policy

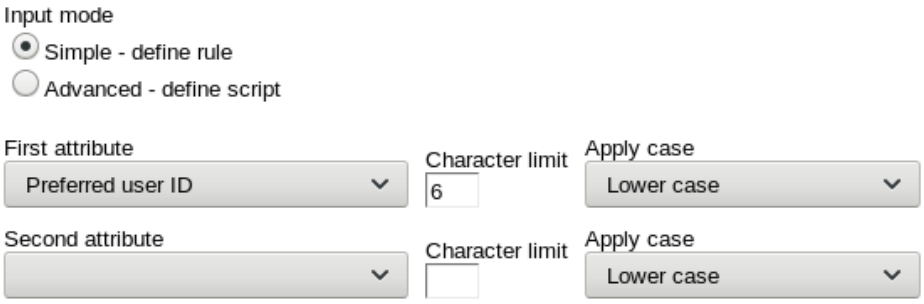
The default identity policy for IBM Security Identity Manager returns login account names that are based on the user's preferred user ID. If the login account name is already in use, the default policy appends a number in order to make the login account name unique.
In this exercise, you create a new identity policy that returns a user name that only uses the first 6 characters of the preferred user ID. Your new identity policy is associated with the Service you created.

1. On the **Home** tab, navigate to **Manage Policies > Manage Identity Policies**.

2. **Create** a new identity policy with the following information:

Field	Value
Name	Linux Identity Policy
Description	Identity Policy for Linux Service
Status	Enabled
User type	Person
Make policy available to services in	This business unit and its subunits
Business unit	JK Enterprises
Targets (Section)	Click **Add** → Linux Service (Service)

3. In the Rule section, select the first attribute to be **Preferred user ID.** Set the **Character limit** to **6** and set Apply case to **Lower case.**



4. Click **Apply**.

Hint : After creating a rule in **Simple** mode, you can switch to **Advanced** mode and IBM Security Identity Manager generates JavaScript that carries out your simple rule. You can use the generated script as a starting point for further customization.

5. Click **OK** to submit the new identity policy.
   You test this identity policy in a later exercise.

6.3 Exercise 3 – Creating a password policy

In this exercise, you create a password policy that requires passwords for the Linux Service to be at least **four** characters long.

1. On the **Home** tab, navigate to **Manage Policies > Manage Password Policies.**
2. Create a new password policy with the following information.

Field	Value
Name	Linux Password Policy
Description	Password policy for Linux Service
Business unit	JK Enterprises
Make policy available to services in	This business unit and its subunits
Status	Enabled
Targets (Section)	Click **Add** → Linux Service (Service)
Rules (Section)	**Minimum length** of 4

3. Click **OK** to submit the new password policy.
   You test this password policy in a future exercise.

6.4 Exercise 4 – Running a reconciliation on Linux

In this exercise, you set up a reconciliation schedule and run a reconciliation for the Linux Service. After the reconciliation is completed, you see the Linux service accounts in IBM Security Identity Manager. You do not see accounts provisioned to users because the default provisioning policy for Linux was created in disabled mode. In a later unit, you attach roles to this policy and provision users.

Task 1. Setting up a reconciliation schedule

1. On the **Home** tab, you go to **Manage Services.**
2. Click **Search** to refresh the list. Click the small **arrow** to the right of **Linux Service** and click **Set Up Reconciliation.**
3. A reconciliation schedule is automatically created by the **Create Service** wizard. Click the link for **Reconciliation Schedule for Linux Service** to edit it.
4. Modify the schedule for this reconciliation to run **Daily** at **4:00 p.m**.
5. Click **OK** to submit this change.

Task 2. Running an initial reconciliation

1. Return to **Manage Services**.
2. Click the small **arrow** to the right of **Linux Service** and click **Reconcile Now.** Select **None** for Query when prompted, and **submit** the request.
3. View the **status** of the reconciliation request. **Refresh** the list after a few moments if the status is pending.
4. **Close** Reconcile Now Tab.

Task 3. Review Account list

1. Return to **Manage Services**
2. Click the small **arrow** to the right of **Linux Service** and click **Accounts**.
3. Click **Search** to display all the accounts that are found by the reconciliation.
4. **Close** the Manage Accounts tab.

6.5 Exercise 5 – Creating a system person

IBM Security Identity Manager discovered many existing system accounts during reconciliation. In this exercise, you create a system user to own all the system accounts on the Linux Service.

1. On the **Home** tab, you go to **Manage Users**.
2. Click **Create** to add a new **Person** entry to the **JK Enterprises** business unit:

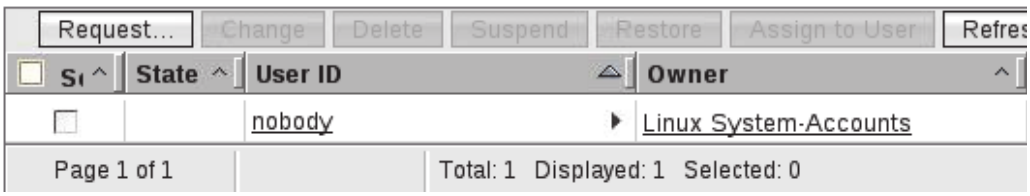
User	Data
Linux System-Accounts	Last Name: **System-Accounts** Full Name: **Linux System-Accounts** Preferred user ID: **linuxsystemaccounts** First Name: **Linux** Password: **P@ssw0rd**

6.6 Exercise 6 – Adopting accounts manually

In this exercise, you grant ownership of an account to the Linux System-Accounts person.

1. Return to the **Manage Services** tab.
2. Click the small **arrow** to the right of **Linux Service** and click **Accounts**.
3. **Refresh** the list. Click the small **arrow** to the right of the **nobody** account and click **Assign to User.** Assign nobody to the **Linux System-Accounts** user you created in the previous exercise.

4. **Refresh** the accounts list and verify that **Linux System-Accounts** is now the owner of **nobody**. **Close** Manage Accounts Tab.



6.7 Exercise 7 – Adopting accounts automatically

In this exercise, you specify that any account whose uid <= 499 is owned by Linux System-Accounts.

Task 1. Creating an adoption policy

1. On the **Home** tab, you go to **Manage Policies > Manage Adoption Policies.**

2. **Create** a new adoption policy with the information in the following table:

Field	Value
Name	Linux Service Adoption Policy
Description	Adoption policy for Linux Service
Services (Section)	Linux Service (Change Service type to : **POSIX Linux Profile service type,** Click **Search**)

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

Note: There are system-defined JavaScript objects that you use in adoption rules. For more information, refer to the on-line help. In this example, you are using the **searchByFilter** method on the **PersonSearch object.** The syntax is:

searchByFilter(String profileName, String filter, [int scope])

where **scope=1** is a single-level search and **scope=2 i**s a SubTree search.

3. Click **OK** to save the adoption policy.

Task 2. Reconciling again to invoke new adoption policy

4. Return to the **Manage Services** tab. Click the small arrow to the right of **Linux Service** and click **Reconcile Now**. Do not use a query.

5. Verify that the status of the reconciliation is **completed**.

6. Return to the **Manage Services** tab. Click the small **arrow** to the right of **Linux Service** and click **Accounts**. Verify that Linux System-Accounts now owns many accounts, such as **gdm** and **ntp**. **Close** the Reconcile Now Tab.

dbus	Linux System-Accounts	Individual	Inactive
ftp	Linux System-Accounts	Individual	Active
games	Linux System-Accounts	Individual	Active
gdm	Linux System-Accounts	Individual	Inactive
halt	Linux System-Accounts	Individual	Active
lp	Linux System-Accounts	Individual	Active
mail	Linux System-Accounts	Individual	Active
nobody	Linux System-Accounts	Individual	Active
ntp	Linux System-Accounts	Individual	Inactive

Note: If you click one of these accounts to view the attributes, you might see the following warning message:

```
The following attributes contain invalid values. Please correct the values before submitting the form: UNIX shell
```

This error is occurring because **/sbin/nologin** is not a valid choice for the UNIX Shell on the erLinuxAccount form. You can safely **ignore** this error.

6.8 Exercise 8 – Creating an LDAP service

In this exercise, you create another service. This one manages accounts and groups on an Tech Support LDAP(IBM Security Directory Server) system. The service communicates with LDAP(SDS) through the LDAP Profile that is already installed in ISIM by default at installation time.

1. On the **Home** tab, you go to **Manage Services**.

2. Click **Create**.

3. Wait for the list of services to appear. Ensure that Business unit is set to **JK Enterprises.**

4. Select **LDAP Profile** and click **Next**.

5. Create a new service of type LDAP Profile with the information in the following table:

Field	Value
Service name	TechSupport LDAP
Description	TechSupport LDAP Service for ISIM
Tivoli Directory Integrator location	rmi://isim.test:1099/ITDIDispatcher
Directory Server Location	**ldap://isim.test:389**
Administrator name	cn=root
Password	P@ssw0rd
Directory server name	IBM Directory Server
Owner	Bob Smith

6. Click **Test Connection.**

7. If the connection is **successful**, click **Next**. If it is not, check that you correctly entered the URL, user ID, and Password.

8. Complete the form the information in the below table :

Field	Value
User base DN	ou=TechSuppEmployees,dc=contractors
User RDN Attribute	UID
Group base DN	ou=TechSuppEmployees,dc=contractors
Group RDN attribute	CN

9. Keep other values as default and Click **Next** → **Next** → **Next** → **Next** and at **Configure Policy**, Select **Yes, create a policy to automatically create accounts, and later enable the policy** and Click **Finish**.

10. Return to **Manage Services** and verify **TechSupport LDAP** service is added.

11. Click the small arrow to the right of **TechSupport LDAP** service and click **Reconcile Now**. Do not use a query. **Submit** the reconcile request.

12. View the status of the reconciliation request. **Refresh** the list after a few moments if the status is pending.

13. Return to Manage Services. Click the small arrow to the right of **TechSupport LDAP** service and click **Accounts**.

14. Click **Refresh** to display all the accounts on the **TechSupport LDAP** service

15. The red X icon in the State column indicates that the account is not permitted. Click the red X for details. The account is not permitted because there is currently no active provisioning policy that allows the account on the service. Recall that when you created the **TechSupport LDAP service**, you indicated you would **enable the provisioning policy later.** The next chapter teaches provisioning.

16. **Close** the Reconcile Now Tab.