Practical-11

JK Enterprises wants to create a service in IBM Security Identity Manager to manage accounts and groups on the Tech Support LDAP (IBM Security Directory Server) system. The service communicates with LDAP (SDS) through the LDAP Profile. Organization wants provisioning policy to evaluate which entities are given access to a particular resource governed by a service. Provisioning policy should be checked for the accounts on Linux Service

**LDAP service**

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

A common use of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP server to validate users.

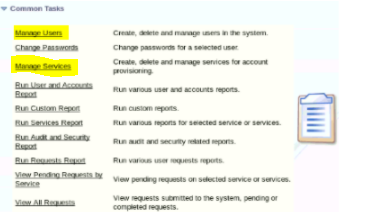
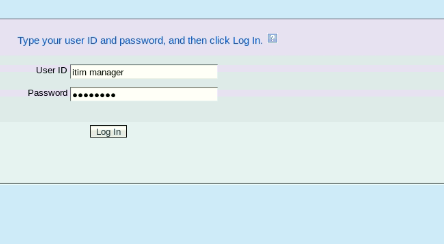
**Tasks to be done:**

1. Creating a LDAP Service.
2. Adding users to a static role.
3. Creating a provisioning policy.
4. Verifying account provisioning.

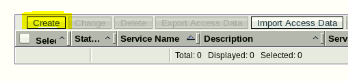
Implementation:

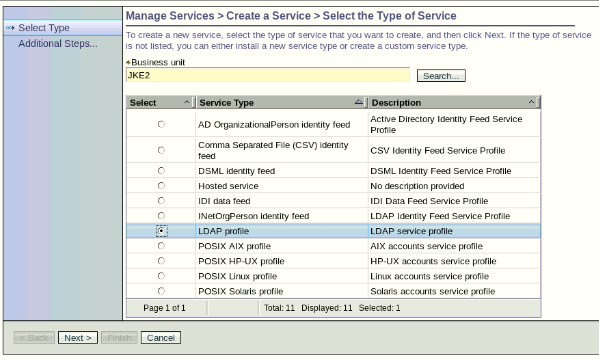
**Creating a LDAP Service.**

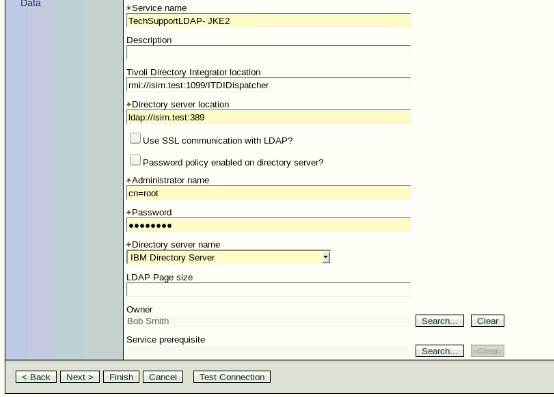
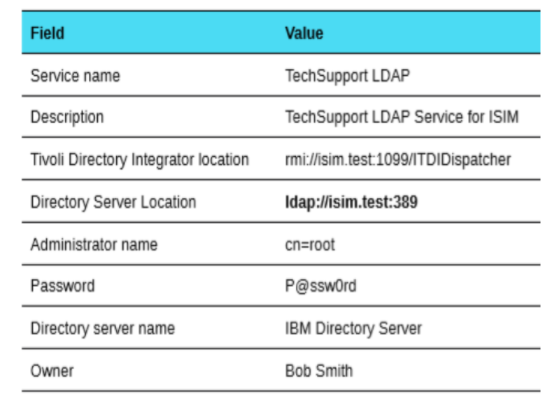
1. On the Home tab, you go to Manage Services.

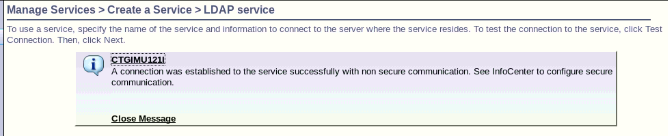
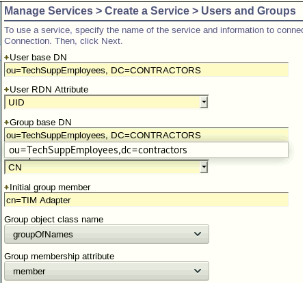
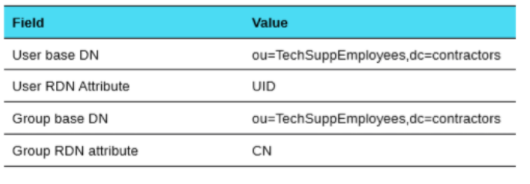
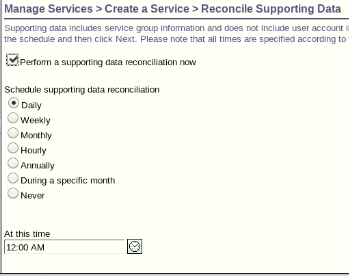
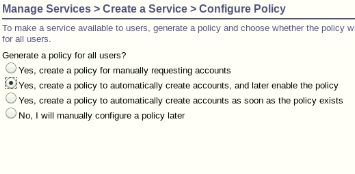
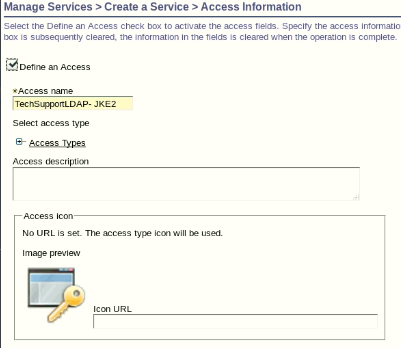
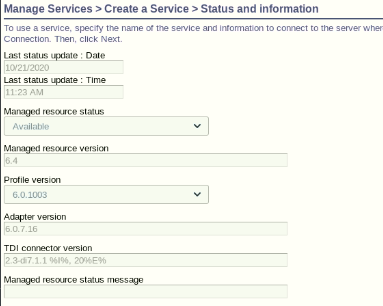
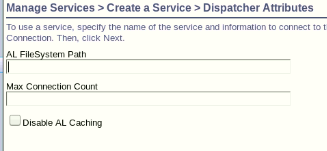


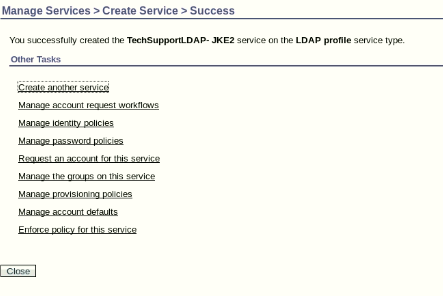
1. Click Create.

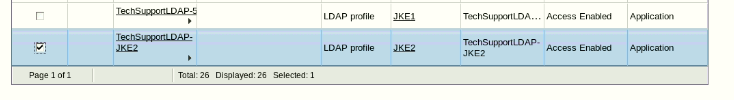
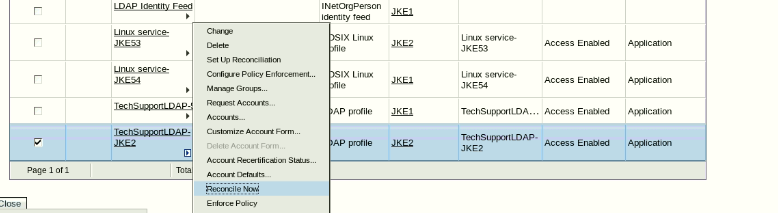
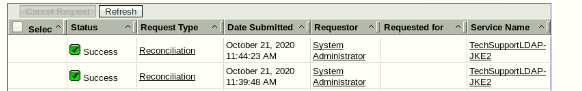
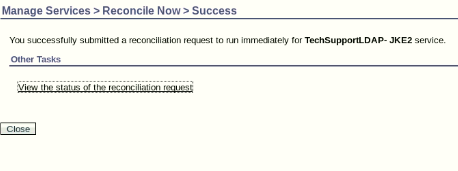
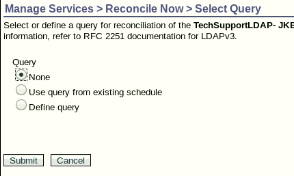
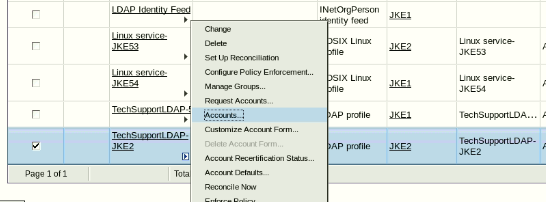
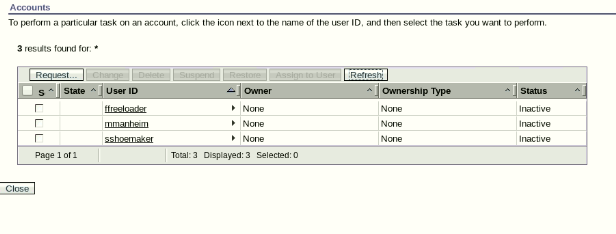


1. Wait for the list of services to appear.Ensure that the Business unit is set to JKE-2.Select LDAP Profile and click Next.
2. Create a new service of type LDAP Profile with the information in the following table:



1. Click Test Connection.
2. If the connection is successful, click Next. If it is not, check that you correctly entered the URL, user ID, and Password.
3. Complete the form the information in the below table :
4. 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.

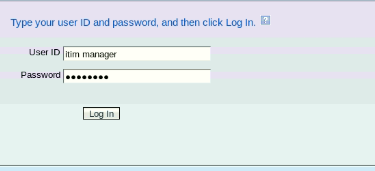
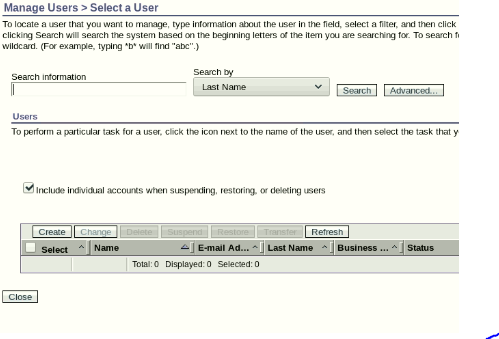


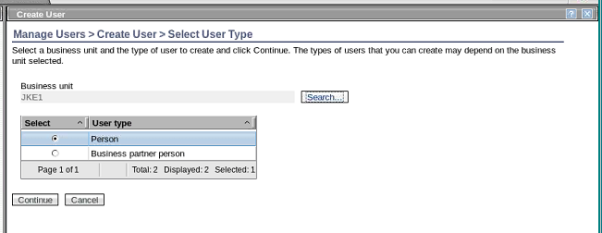
1. Return to Manage Services and verify TechSupport LDAP service is added.
2. Click the small arrow to the right of TechSupport LDAP service and click Reconcile Now. Do not use a query. Submit the reconcile request.
3. View the status of the reconciliation request. Refresh the list after a few moments if the status is pending.
4. Return to Manage Services. Click the small arrow to the right of TechSupport LDAP service and click Accounts.
5. Click Refresh to display all the accounts on the TechSupport LDAP service

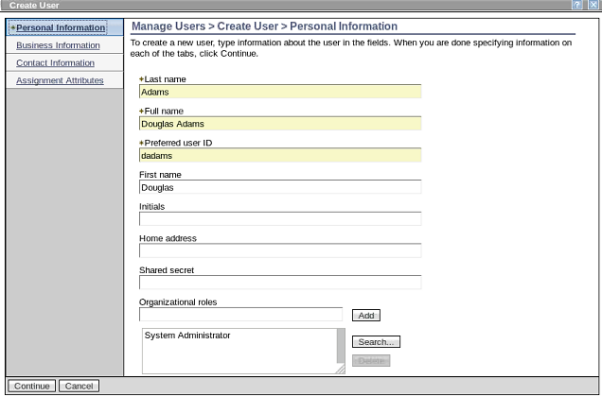
NOTE:The red X icon in the State column indicates that the account is not permitted. Click the red X for details. The account is not permitted because there is currently no active provisioning policy that allows the account on the service. Recall that when you created the TechSupport LDAP service, you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

1. Close the Reconcile Now Tab.

**Adding users to a static role.**

1. Adding users to the JKE-2 System Admin role.
2. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID itim manager.
3. In the Home tab, go to Manage Users.
4. Repeat steps 1-5 for Douglas Adams and Edwin Abbott.

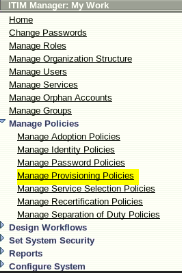


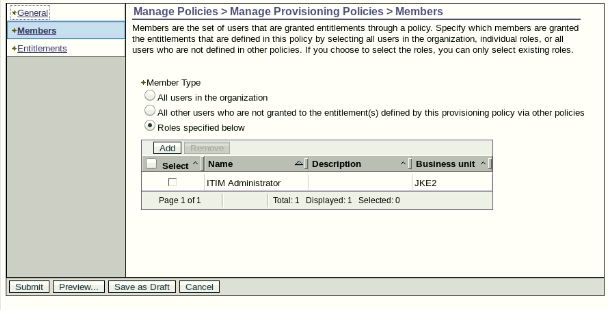
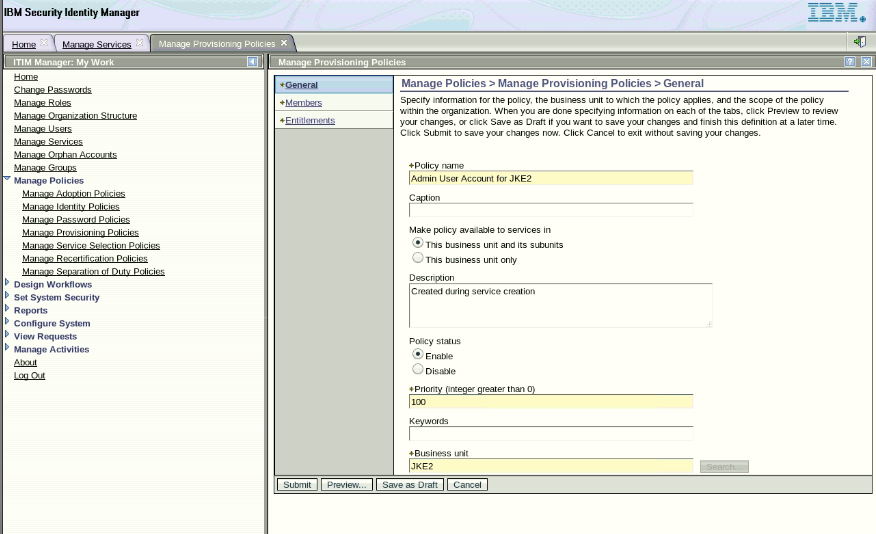
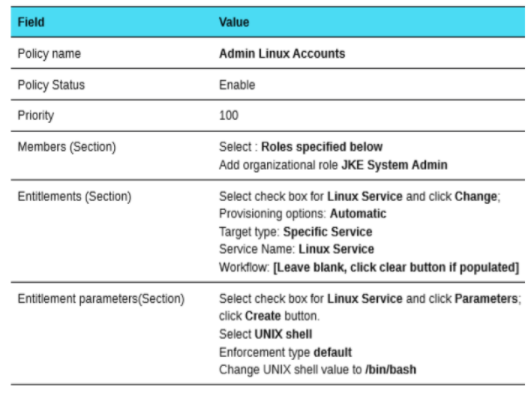


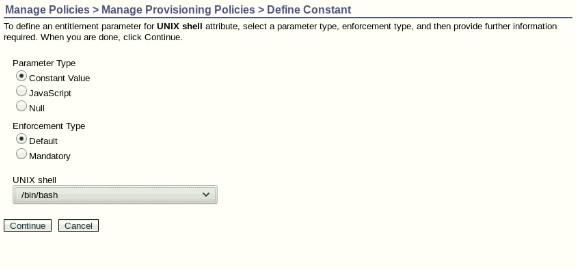
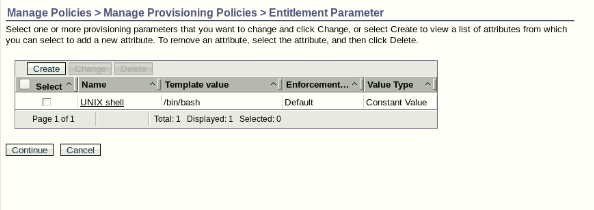
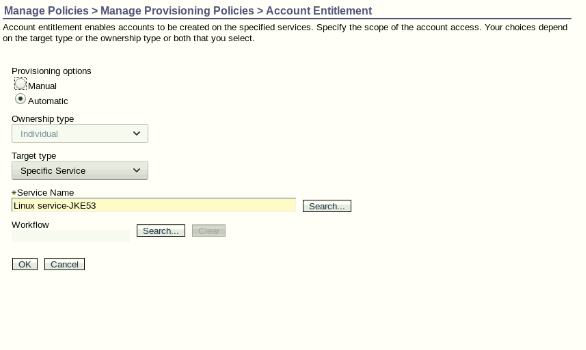


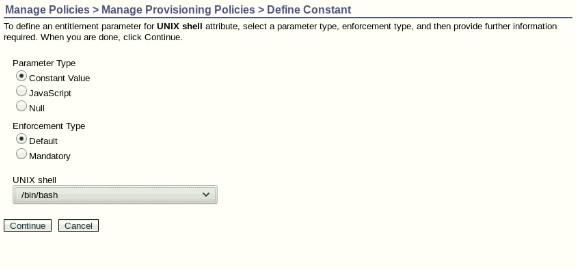
**Creating a provisioning policy.**

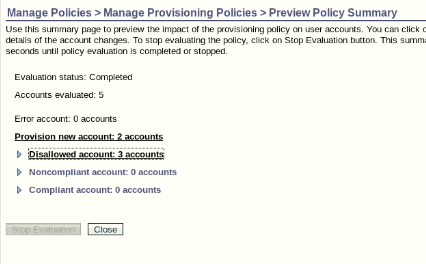
1. On the Home tab, you go to Manage Policies > Manage Provisioning Policies.



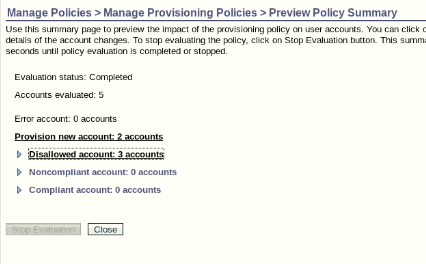
1. Click Refresh. Click the policy named Default Provisioning Policy for service Linux Service.
2. Modify the provisioning policy to match the following information:



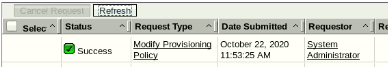
1. Click Preview to see the effects of the new policy, choosing the option to enforce the entire policy. Click Continue. Wait until the Evaluation Status shows completed.
2. Click the Provision New Accounts link to see the users who are provisioned new accounts for the users (Douglas, and Edwin) who you added to the JKE System Admin organization role in the previous exercise. One is for Erica, who you added to the JKE System Admin role when you initially created it.



1. You also see a number of disallowed accounts (the accounts that were adopted by Linux SystemAccounts) because there is no provisioning policy in place that allows those accounts. Since the enforcement action is set to Mark account, no concrete action is taken by IBM Security Identity Manager regarding these violations. If you set the enforcement action to Correct, the system would de-provision the accounts.

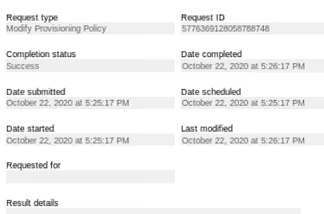


1. Close the preview screen and submit the policy, enforcing the entire policy.



**Verifying account provisioning.**

1. On the Home tab, you go to View Requests > View All Requests by User.



1. Click Search Requests to find the Modify Provisioning Policy request.
2. Click the link under the column Request Type to open and review the request details. Expand Clicking the plus sign (+) and you can see 4 new accounts are added.
3. In a terminal window, view /etc/passwd. Verify that the accounts are provisioned with the correct shell of /bin/bash:
4. cat /etc/passwd

