Name- Tushar Bisht
Subject - Cloud Based Application Development and Management
subject Code - PCS-552
Date - 04/10/21
Roll no - 19011267/19187711/52

Q-1- What is the use of SSO? Show the implementation of SSO.

Ans-1- Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple application and websites by using just one set of credentials.

1- It improves security capabilities.
2- It reduces password fatigue.
3- It increases employee and IT productivity.
4- It combines with Risk-Based Authentication (RBA).
5- It increaseases software adoption rates
6- It prevents shadow IT.
7- It streamlines the user experience.

Implementation of SSO:

1- Navigate to the AWS SSO console, and choose AWS accounts from the navigation pane choose which account from Marketing BU or Organizational Unit. Then choose Assign users.
2- choose user, short typing to search for users, and then choose Search connected directory. This is Search will return a list of user from connected directory. You can also search for groups.

3- To Select permission sets, you first have to create one choose create, new permission set.

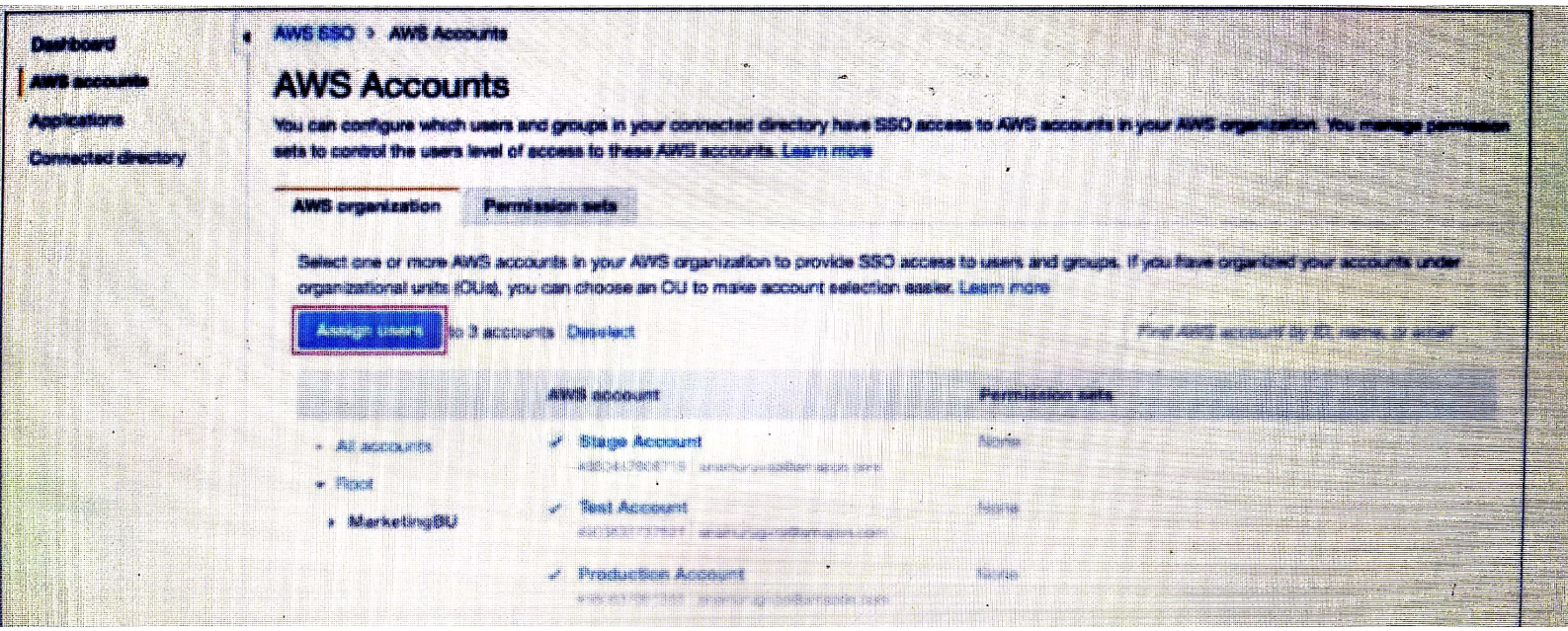
4- You can use an existing job function policy to create a permission set. This type of policy allows you to apply predefined AWS managed policies to a permission set that are based on common job functions in the IT industry. Alternatively, you can create a custom permission set based on custom policies.

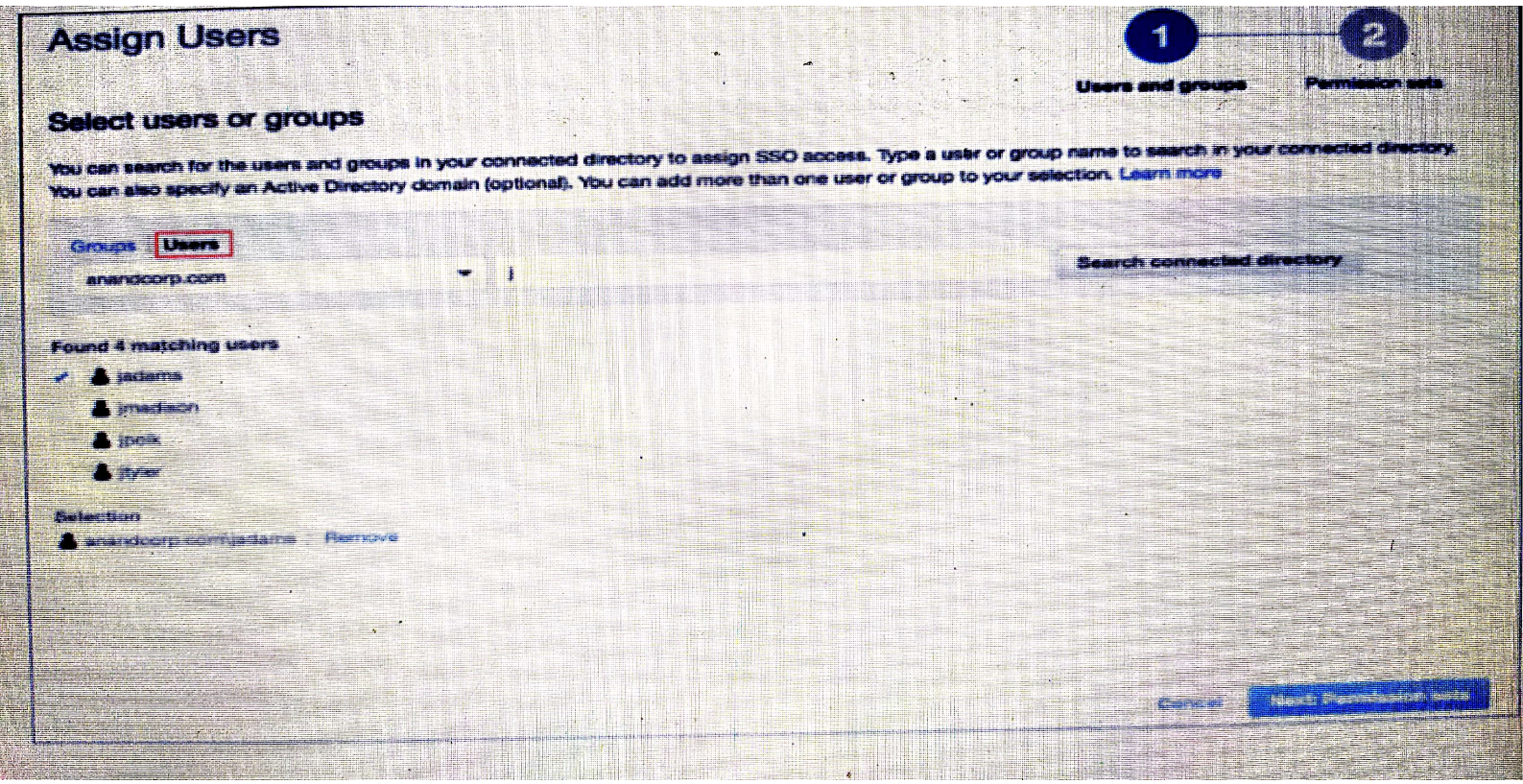
5- For this example, choose the Security Audit job function policy and then choose Create. As a result, this permission set will be available to pick on the next screen.

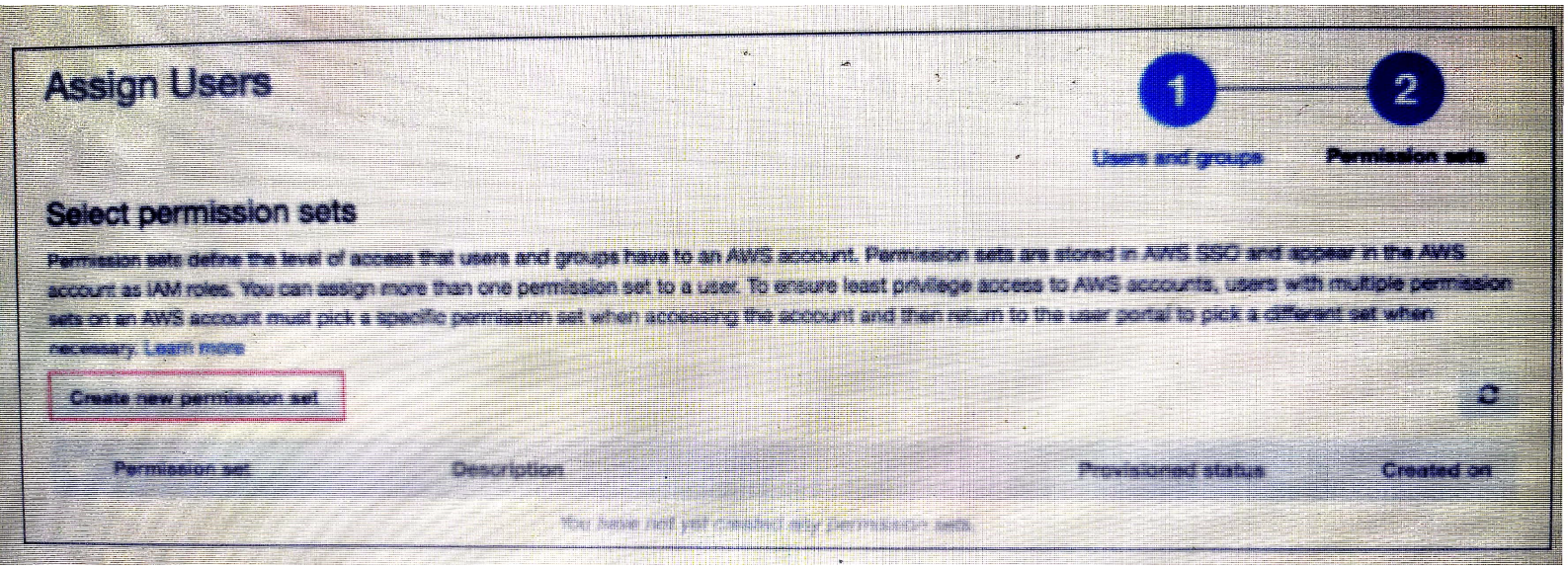
6- Choose a permission set to indicate what level of access you want to grant your users. For this example, assign the Security Audit Permission set its created in the Previous step to the users choose. Then choose Finish.

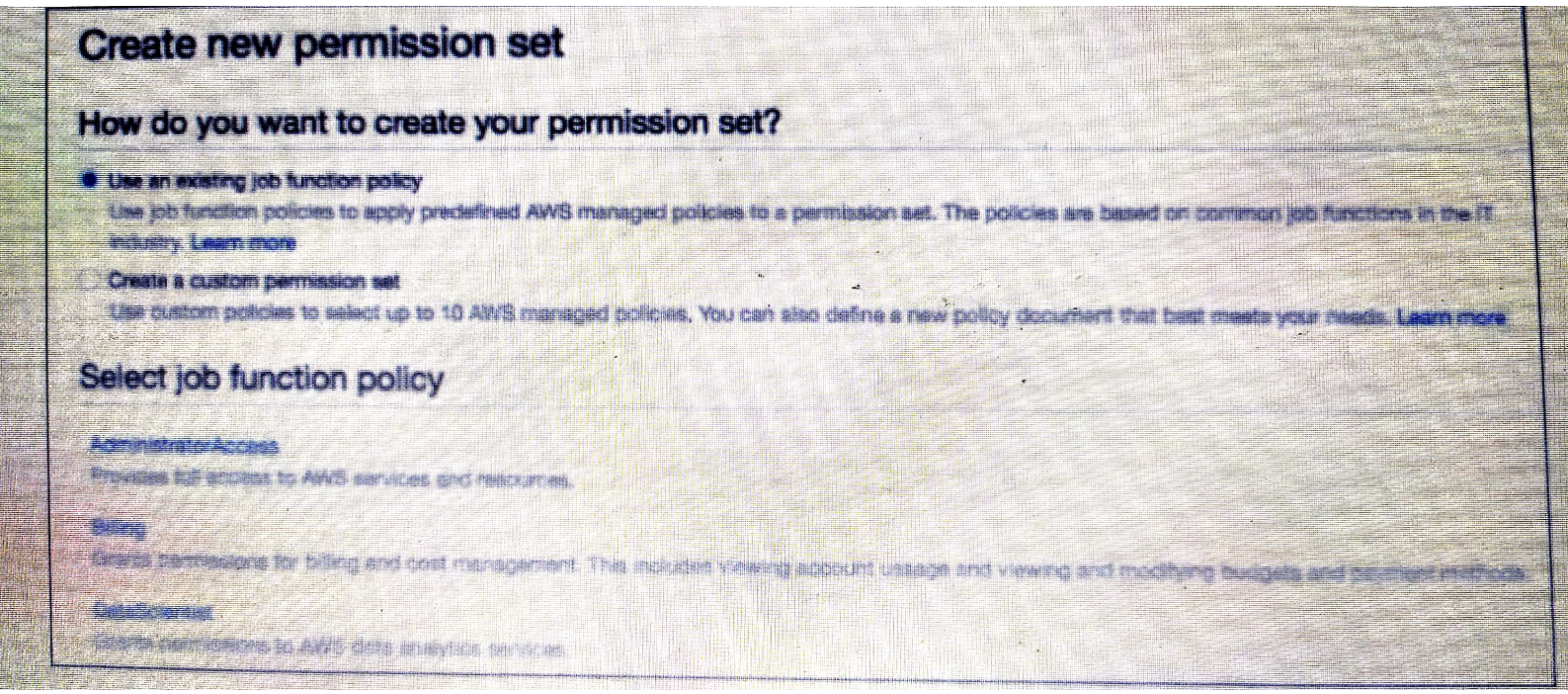
7- Your users can sign to the user portal and access the accounts to which you gave them access. AWS SSO automatically set up the necessary trust b/w accounts to enable SSO. This helps you scale your administrative tasks across multiple AWS accounts.

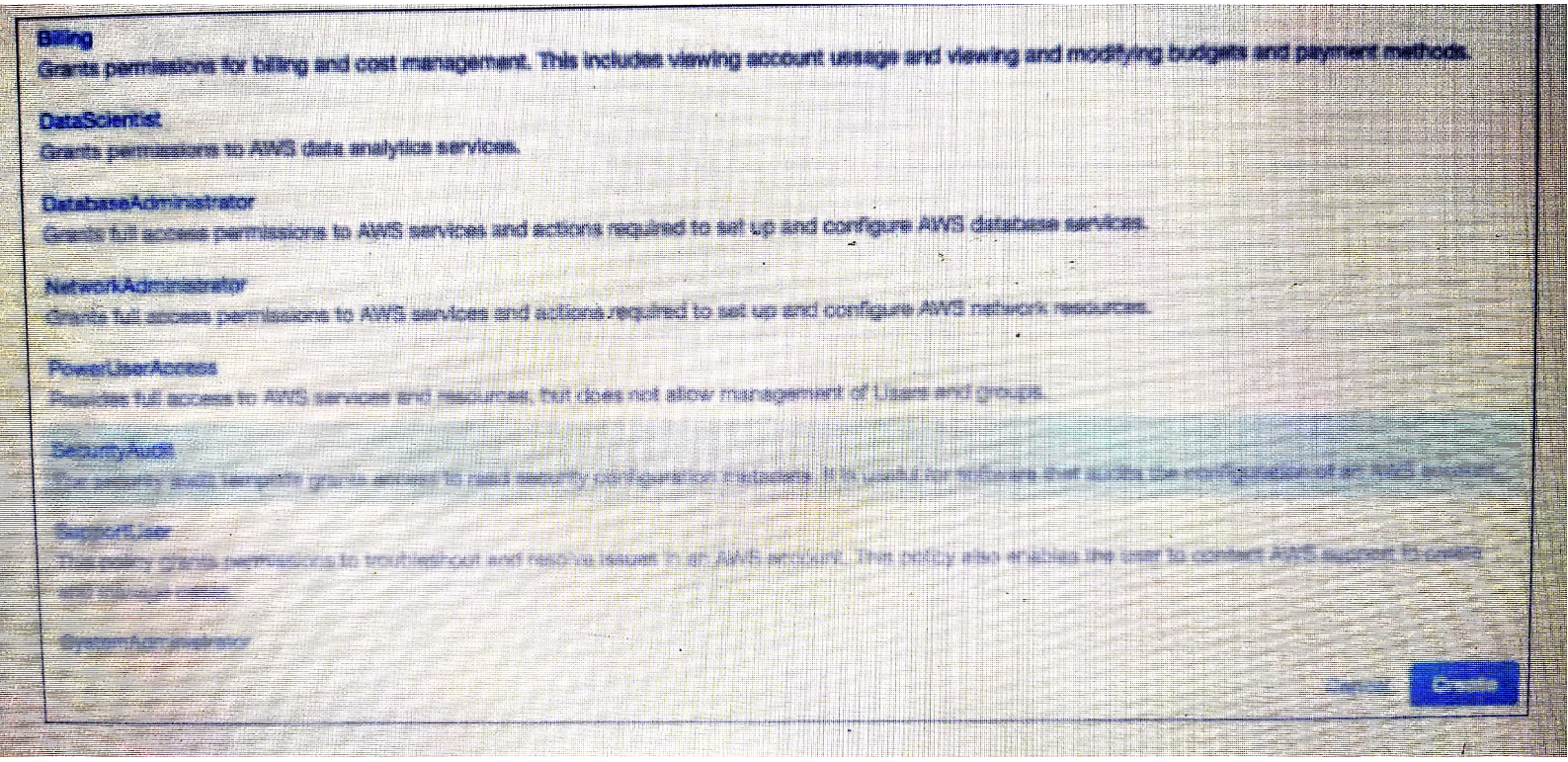
8- The users can choose an account and a permission set to sign in to that account without needing to provide a password again.

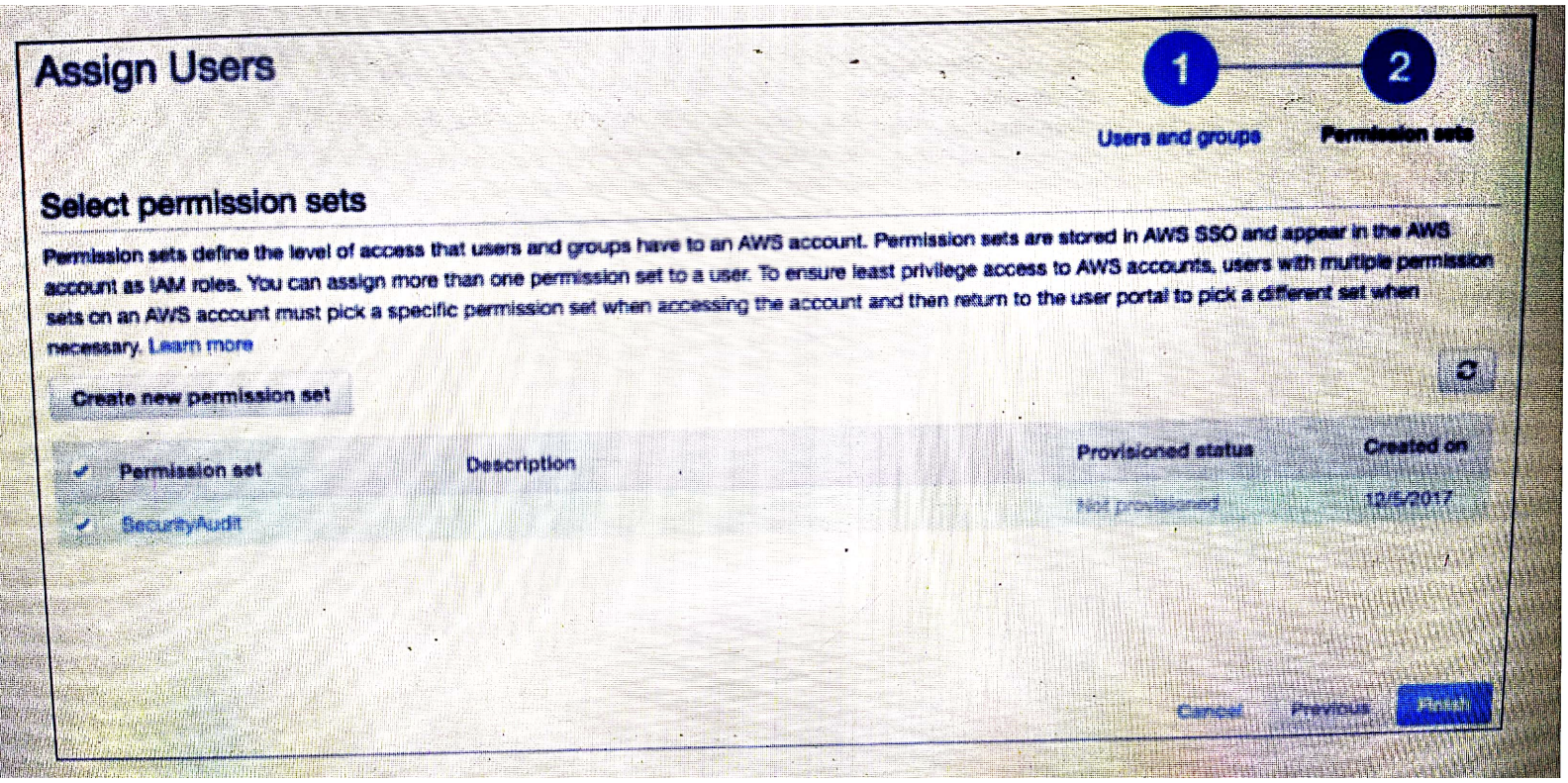


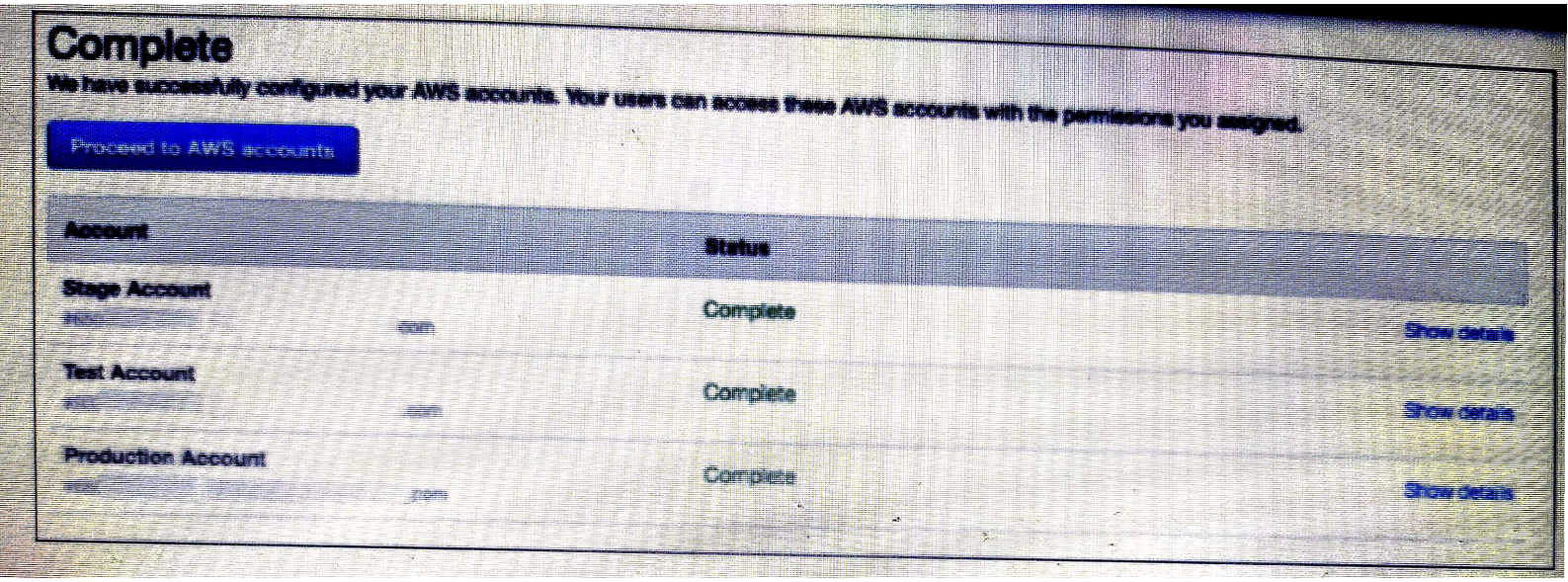


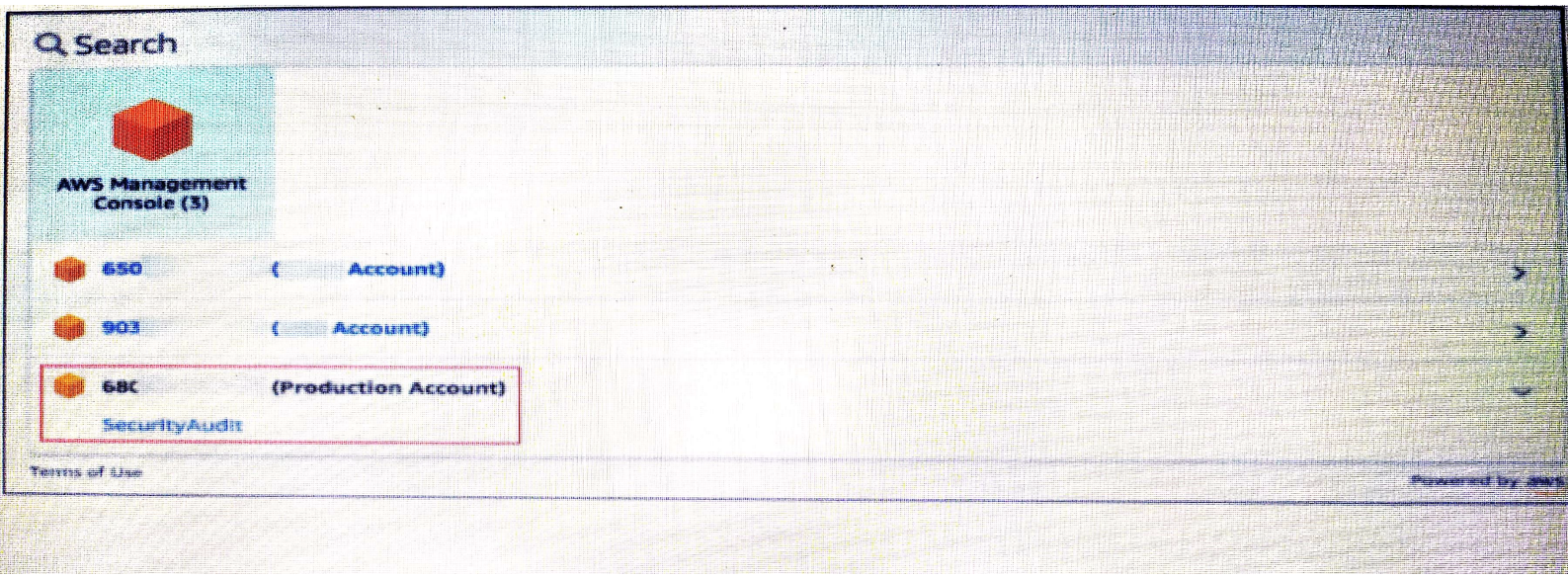












Name - Tushar Bisht
Section - K
Subject - Cloud Based Application Development and Management
Subject Code - PCS-552
Date - 04/10/21
Roll no - 1901267/1918771/52

Q-3 - Show the working in Github for Fork and Pull Request.

Ans-3 - 1- Navigate to the original repository where you created your fork.
2- In the 'Branch' menu, choose the branch that contains your commits.
3- Above the list of files, click pull request.
4- Use the base branch dropdown menu to select the branch you'd like to merge your changes into, then use the compare branch drop-down menu to choose the to pic branch you made changes in.
5- Type a title and description for your pull request.
6- To create pull request ready for review, click create pull Request to create a draft pull request, use the drop down and select create Draft Pull request then click Draft Pull Request.
7- After your Pull Request has been reviewed. It can be merged into repository.