FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Department of Computer Engineering

Course, Subject & Experiment Details

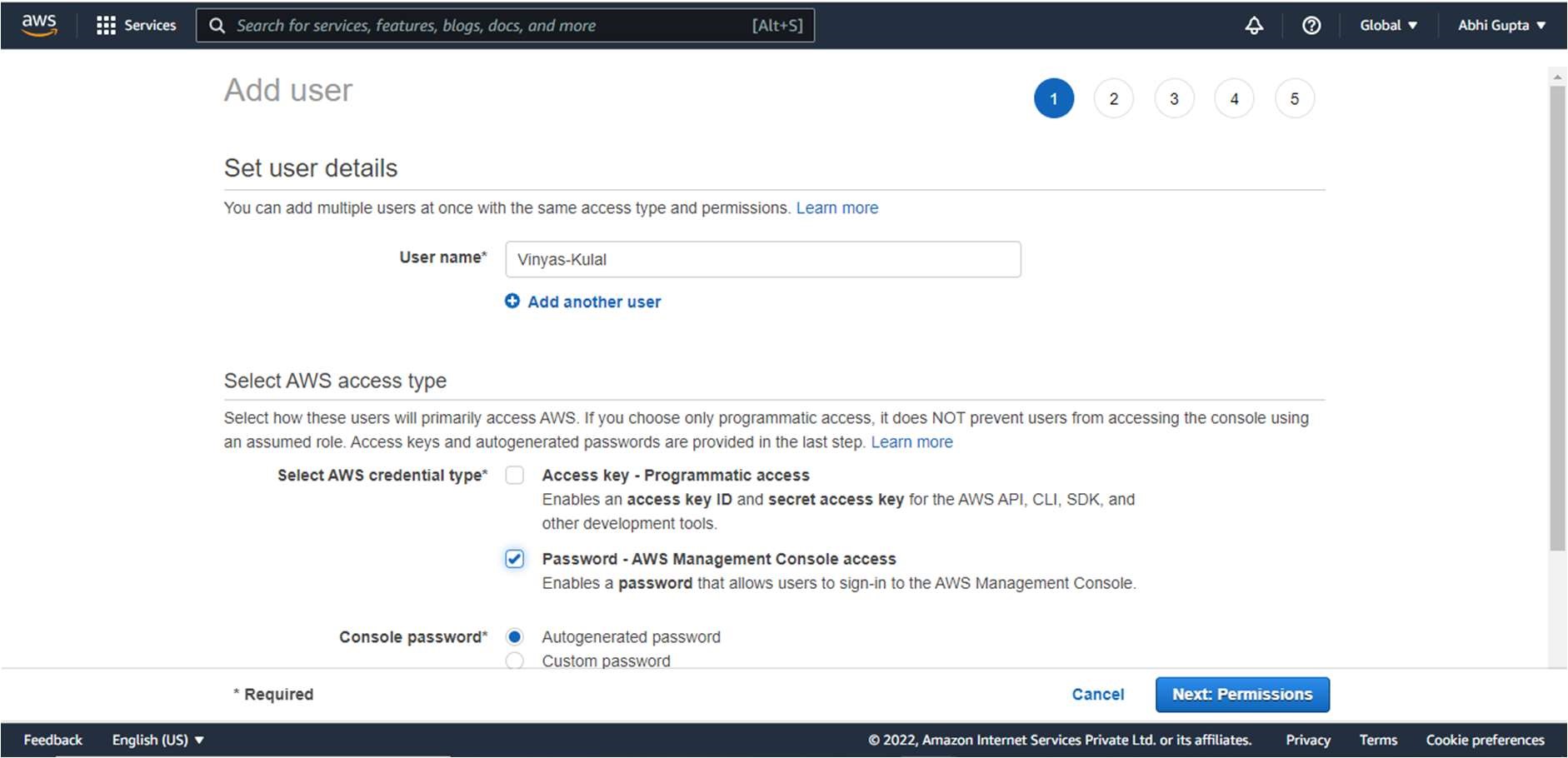
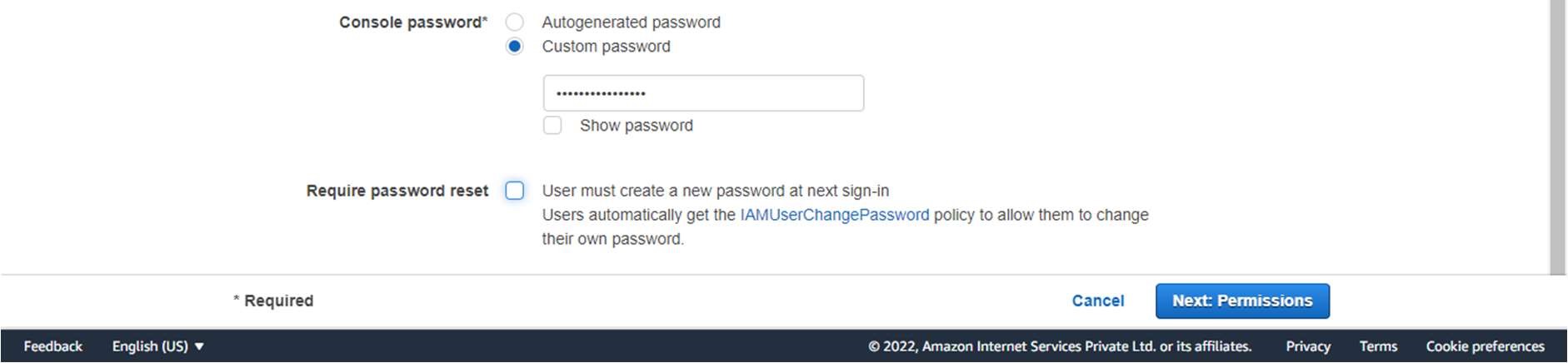
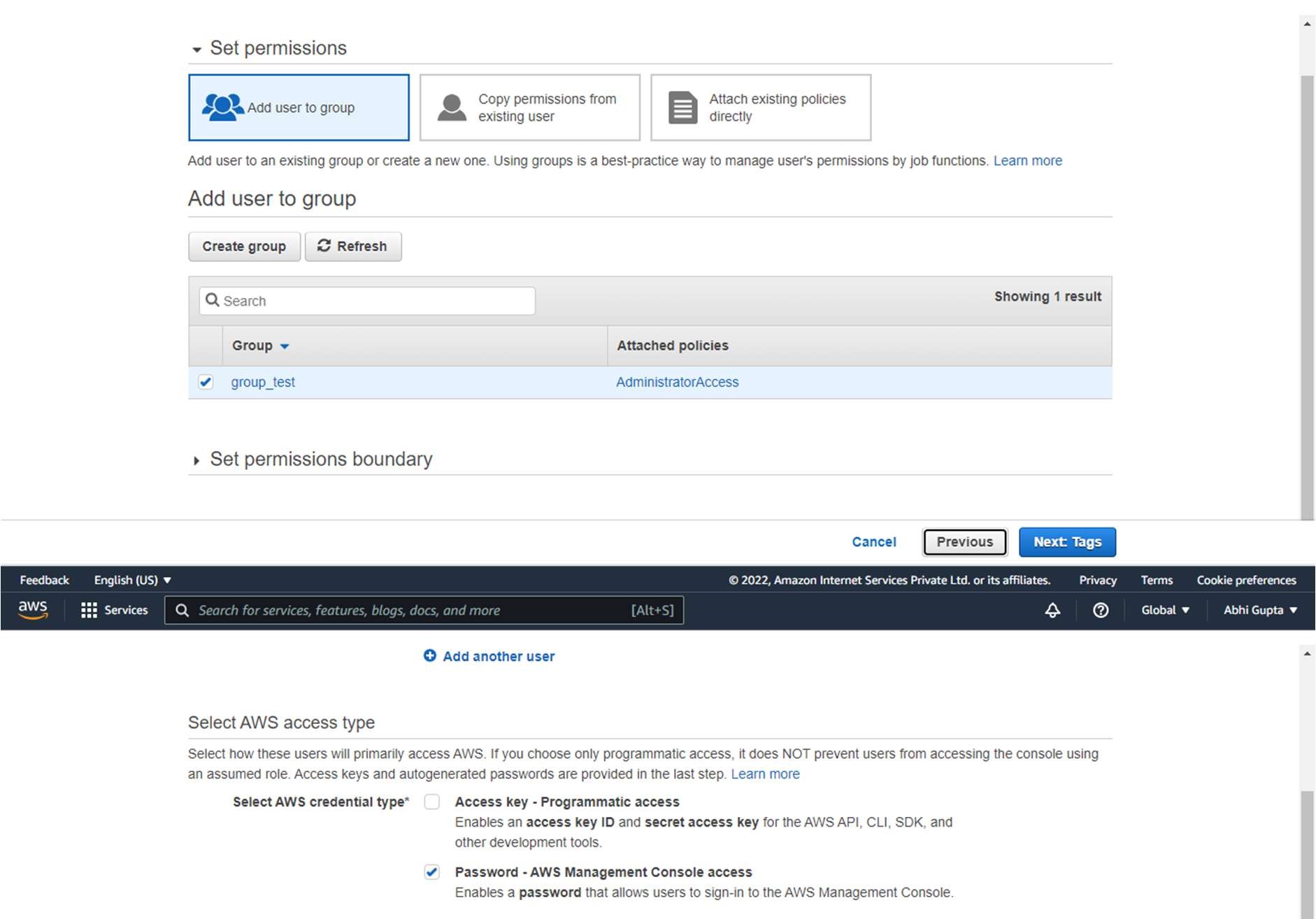
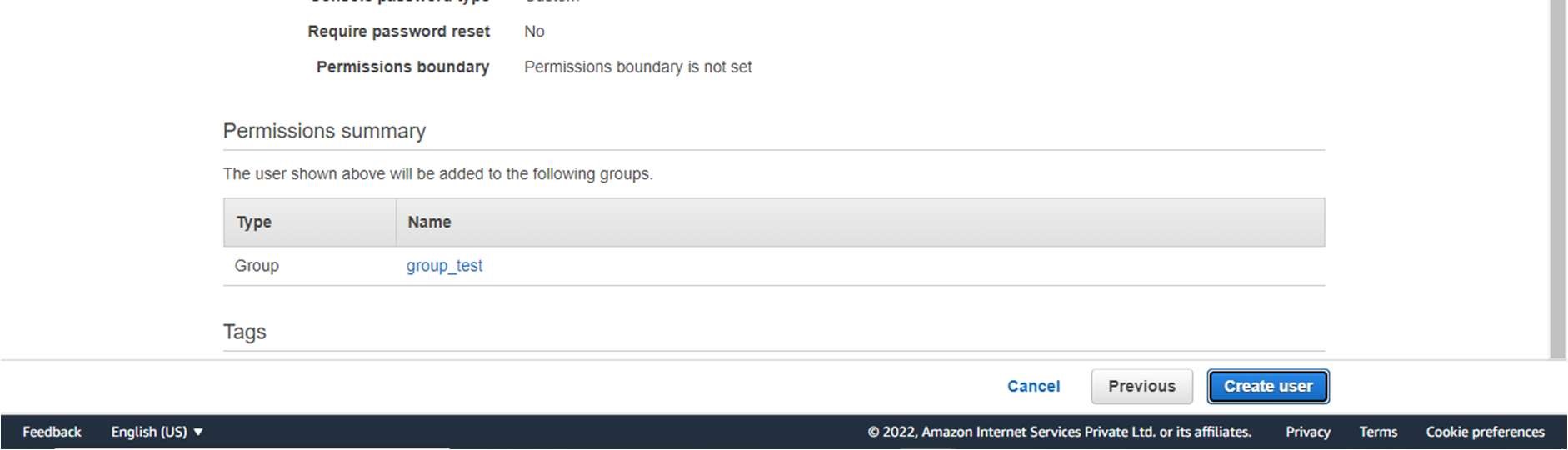
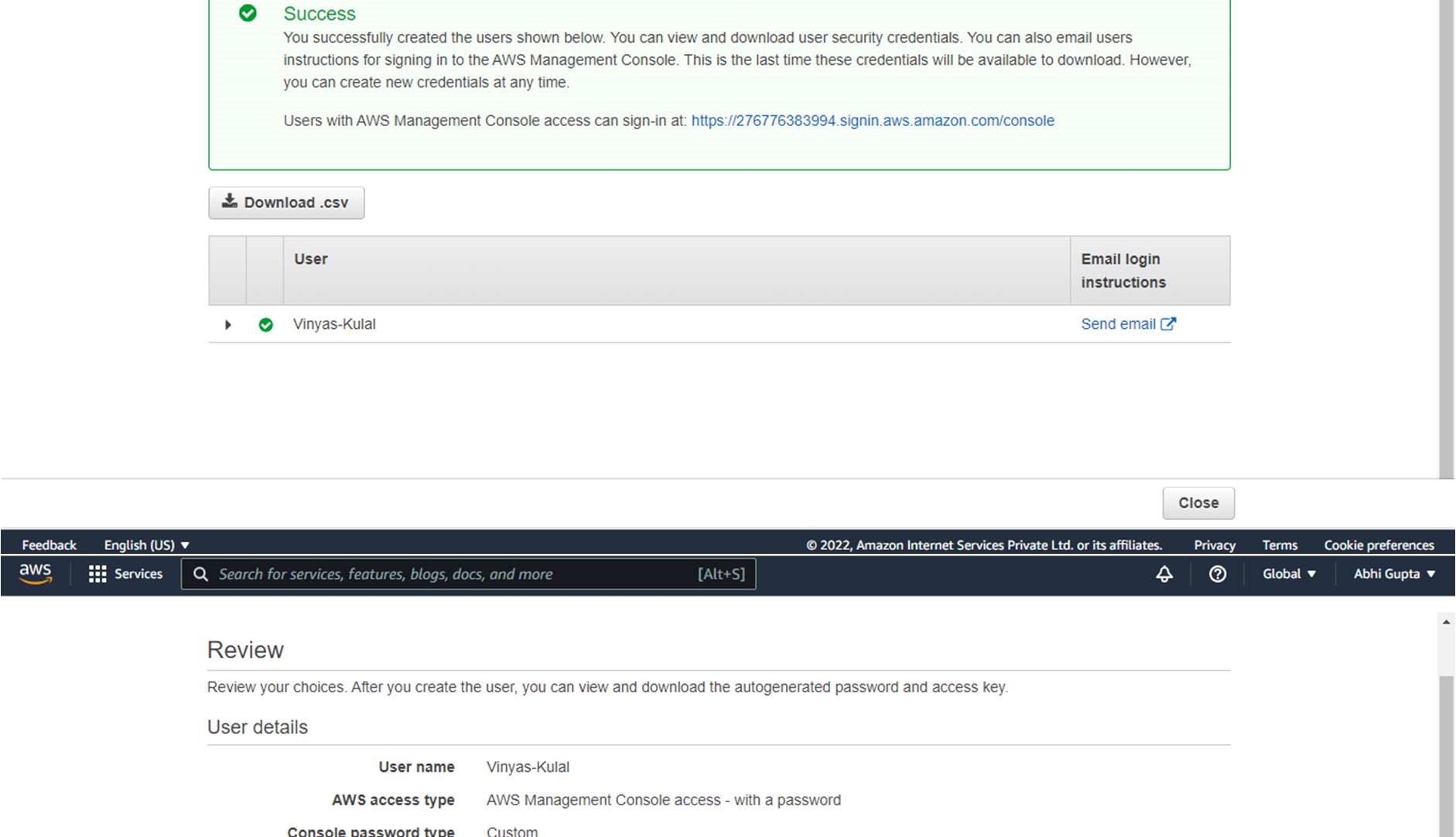
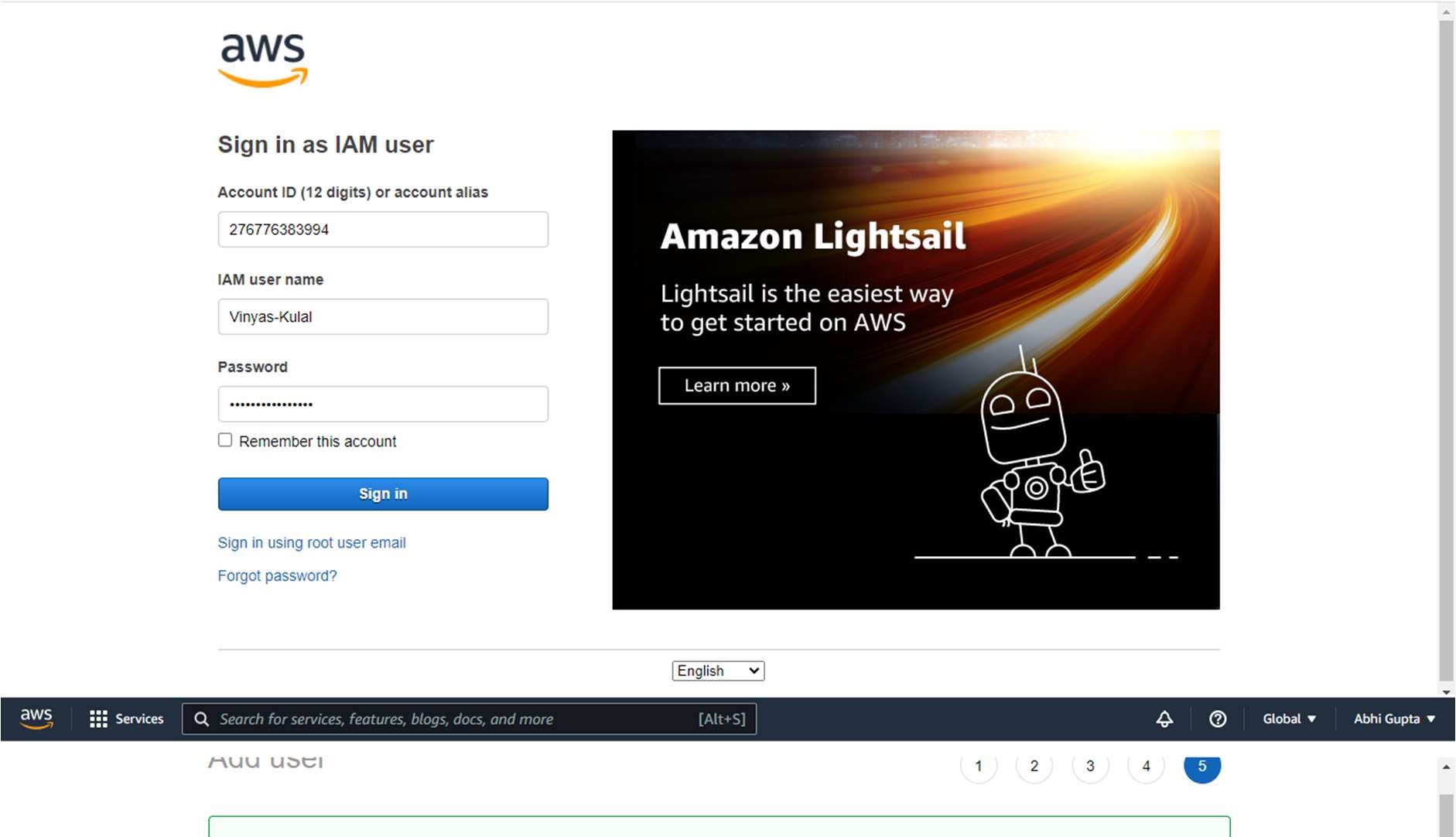
|  |  |
| --- | --- |
| Practical No: |  |
| Title: | To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud |
| Name of the Student: | Warren Fernandes |
| Roll No: | 8940 |
| Date of Performance: | 11/04/2022 |
| Date of Submission: | 11/04/2022 |

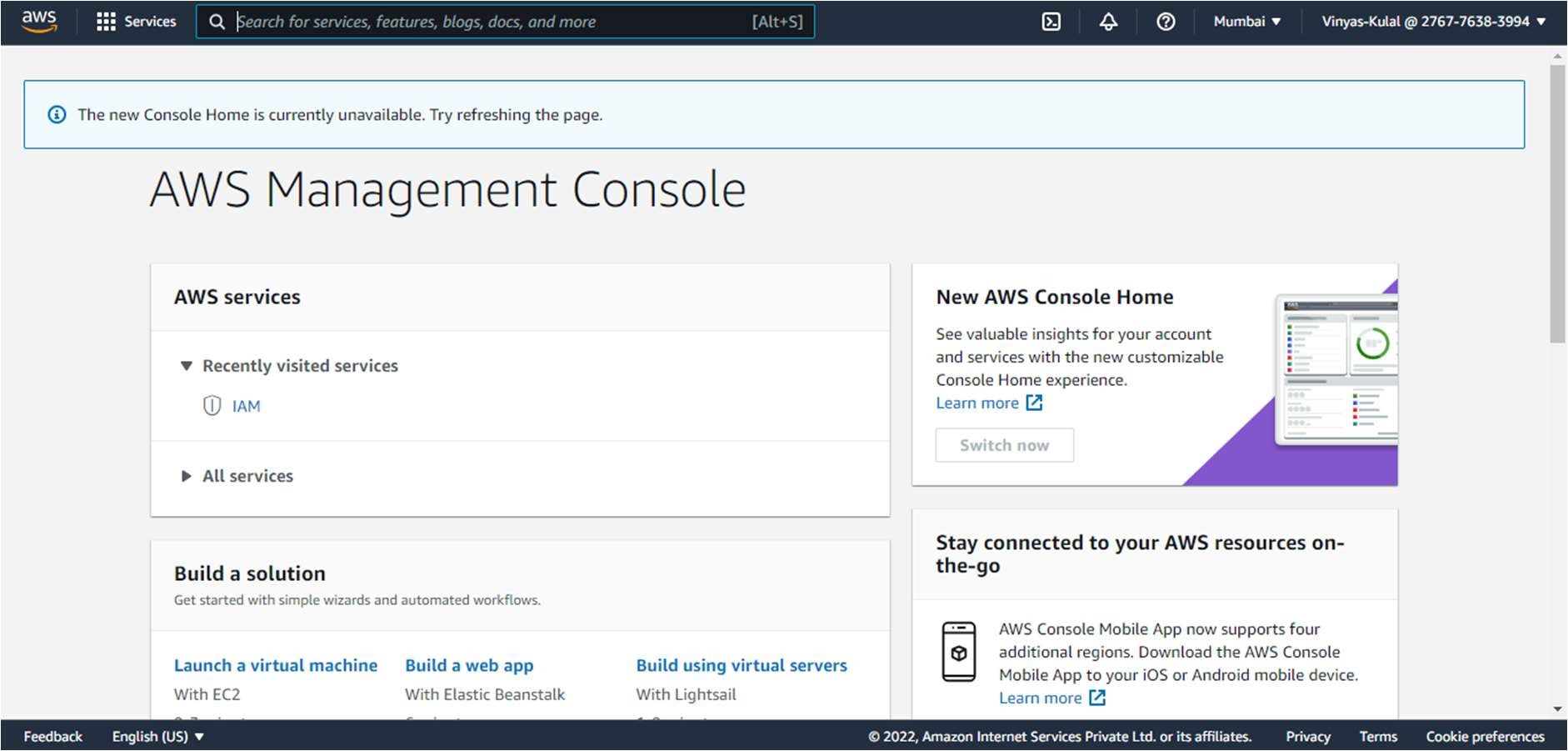
Evaluation:

|  |  |  |
| --- | --- | --- |
| Sr. No. | Rubric | Grade |
| 1 | On time submission/completion (2) |  |
| 2 | Preparedness (2) |  |
| 3 | Skill (4) |  |
| 4 | Output (2) |  |

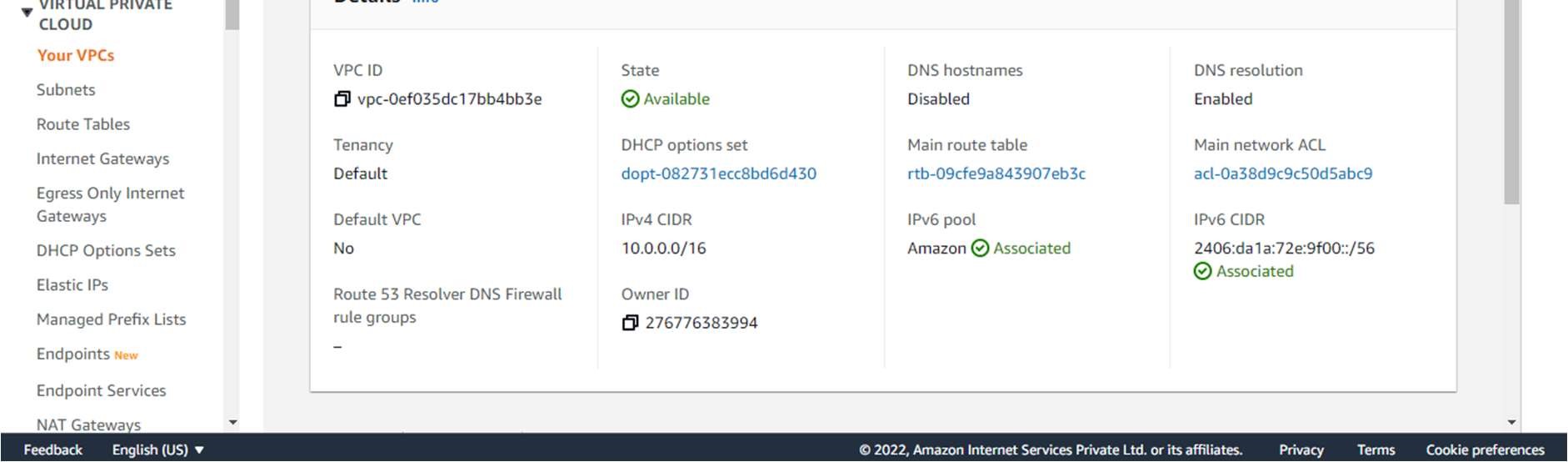
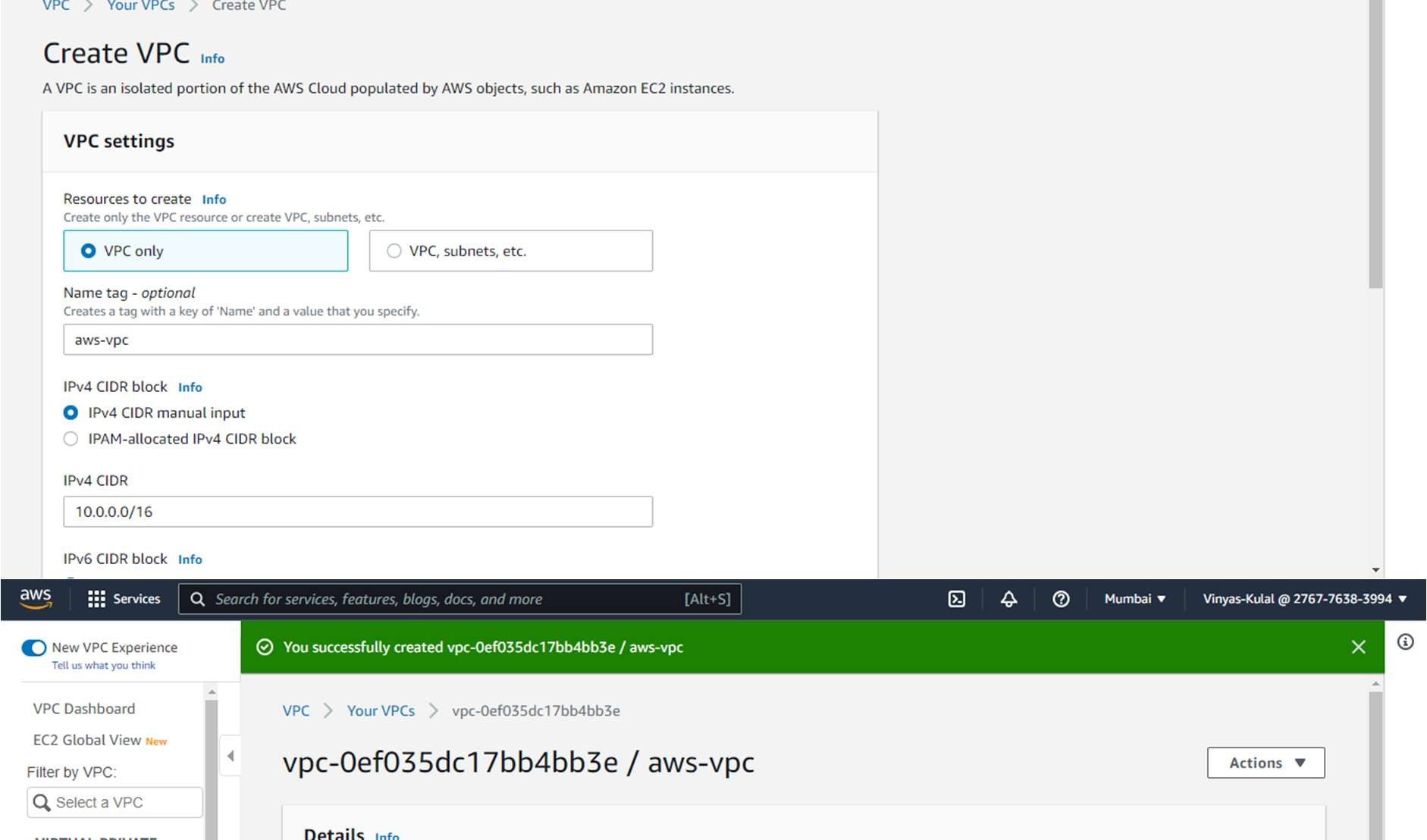
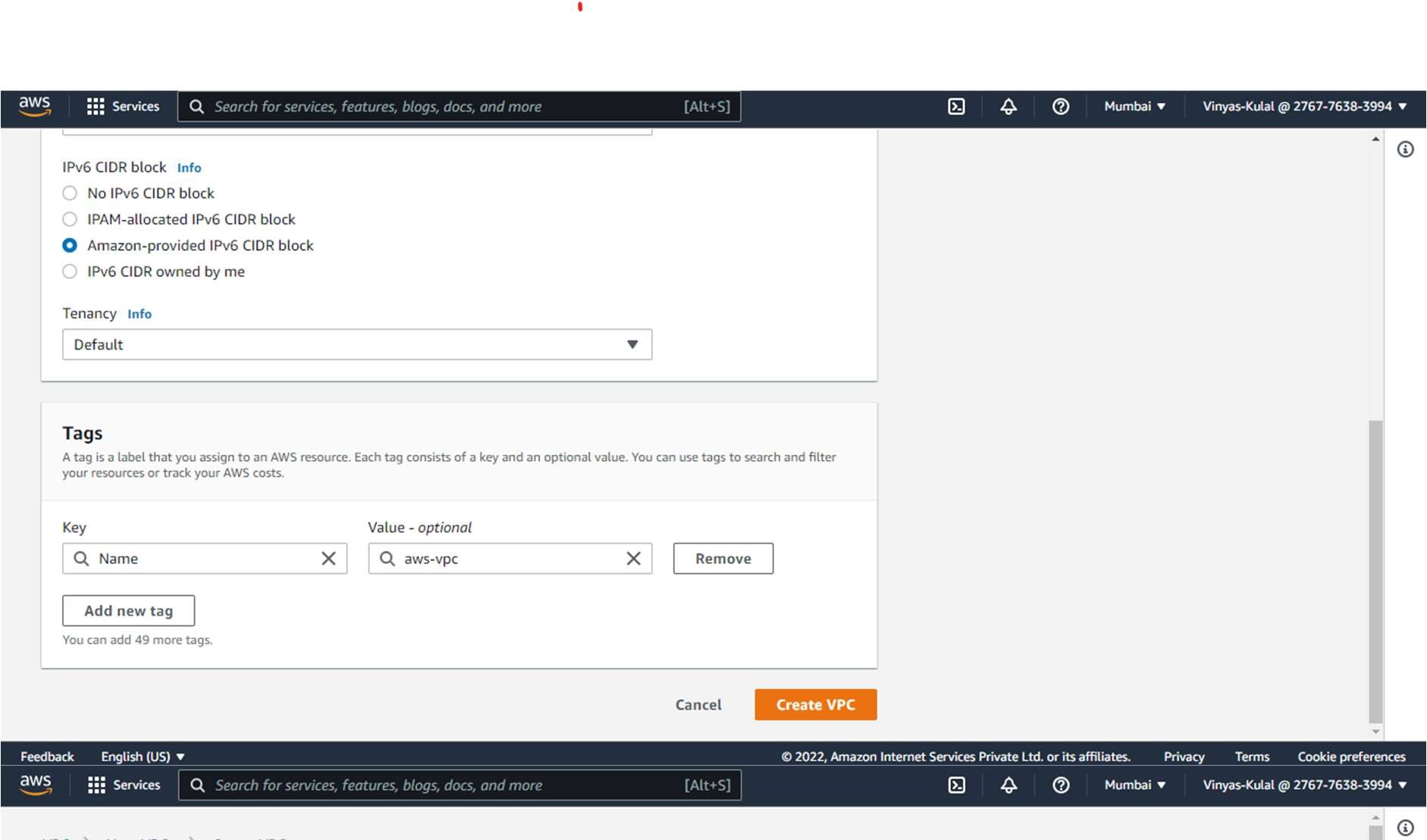
Signature of the Teacher

AWS IAM





AWS VPC



Experiment 4: Amazon Web Services IAM Post Lab Questions Q1. What is AWS Identity and Access Management (IAM)?

AWS Identity and Access Management (IAM) provides fine-grained access control across all of AWS. With IAM, you can specify who can access which services and resources, and under which conditions. With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.

Q2. What problems does IAM solve?

A robust IAM solution can ease management pains, streamline provisioning and deprovisioning, and boost user productivity, while lowering costs, reducing demands on IT, and providing the enterprise with comprehensive data to assist in complying with regulatory standards. In addition, enterprises can ensure security by deploying solutions with strong multifactor authentication, while eliminating user frustration by delivering seamless access to cloud-based applications through SSO. Furthermore, as identity and access management become increasingly complex, the ability to create policies based on granular, contextual information will become more and more important. IAM solutions that can collect and make decisions based on user identity, location, device, and the requested resource will allow enterprises to deliver quick access to bona fide employees, partners, contractors, or guests—and easily revoke or deny privileges to unauthorized users.

Q3. How are IAM users managed?

Manage IAM users and their access—You can create users in IAM, assign them individual security credentials (such as access keys, passwords, and multi-factor authentication devices), or request temporary security credentials to provide users access to AWS services and resources.

Q4. What kinds of security credentials can IAM users have?

AWS Identity and Access Management (IAM) lets you manage several types of long-term security credentials for IAM users:

* Passwords – Used to sign in to secure AWS pages, such as the AWS Management Console and the AWS Discussion Forums.
* Access keys – Used to make programmatic calls to AWS from the AWS APIs, AWS CLI, AWS SDKs, or AWS Tools for Windows PowerShell.
* Amazon CloudFront key pairs – Used for CloudFront to create signed URLs.
* SSH public keys – Used to authenticate to AWS CodeCommit repositories. IAM also lets you grant users temporary security credentials with a defined expiration for access to your AWS resources. For example, temporary access is useful when:
* Creating a mobile app with third-party sign-in.
* Creating a mobile app with custom authentication.
* Using your organization's authentication system to grant access to AWS resources.
* Using your organization's authentication system and SAML to grant access to AWS resources.
* Using web-based Single Sign-On (SSO) to the AWS Management Console.
* Delegating API access to third parties to access resources in your account or in another account you own.