**St. Francis Institute of Technology**

**Department of Computer Engineering**

**Academic Year: 2021-2022 Semester: VIII**

**Subject: Cloud Computing Lab Class / Branch / Division: BE/CMPN/A**

Name :-Rebecca Dias Roll Number:18

**Experiment No: 06**

# Aim:

Study and implement Identity and Access Management (IAM)

# Theory:

## 1. Study Identity and Access Management

Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations.Systems used for IAM include single sign-on systems, [two-factor authentication](https://www.techtarget.com/searchsecurity/definition/two-factor-authentication), multifactor authentication and [privileged access management](https://www.techtarget.com/searchsecurity/definition/privileged-access-management-PAM). These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.



IAM is not just for employees anymore. Organizations must be able to provide secure access for contractors and business partners, remote and mobile users, and customers. With digital transformation, identities are also assigned to the Internet of Things (IoT) devices, robots and pieces of code such as APIs or microservices. Multicloud hybrid IT environments and software as a service (SaaS) solutions further complicate the IAM landscape.

## 2. Explain the need for Access Management Services in cloud computing.

* **Security.** Traditional security often has one point of failure - the password. If a user's password is breached - or worse yet, the email address for their password recoveries - your organization becomes vulnerable to attack. IAM services narrow the points of failure and backstop them with tools to catch mistakes when they're made.
* **Productivity.** Once you log on to your main IAM portal, your employee no longer has to worry about having the right password or right access level to perform their duties. Not only does every employee get access to the perfect suite of tools for their job, but their access can also be managed as a group or role instead of individually, reducing the workload on your IT professionals.
* **Enhanced Network Abilities**: Identity access management (IAM) makes it simple in sharing the network capabilities with a complete grid of users who were connected with it.
* **Support On-demand improvement**: 24\*7 hours support and monitoring can be provided based on need.
* **Increase Overall Productivity**: Cloud-based services are configured and hosted by service providers. As a result, many organizations can improve their overall productivity instead of worrying about the infrastructure.
* **Centralized Management System**: Clients can be able to manage all their services and programs in one place with cloud-based services. Identity access management can be done with one click on a single dashboard.

## 3. Explain Functional architecture and Component of IAM

We have the user; many users together form a group. Policies are the engines that allow or deny a connection based on policy. Roles are temporary credentials that can be assumed to an instance as needed.

* Users

An IAM user is an identity with an associated credential and permissions attached to it. This could be an actual person who is a user, or it could be an application that is a user. With IAM, you can securely manage access to AWS services by creating an IAM user name for each employee in your organization. Each IAM user is associated with only one AWS account. By default, a newly created user is not authorized to perform any action in AWS. The advantage of having one-to-one user specifications is that you can individually assign permissions to each user.

* Groups

A collection of IAM users is an IAM group. You can use IAM groups to specify permissions for multiple users so that any permissions applied to the group are applied to the individual users in that group as well. Managing groups is quite easy. You set permissions for the group, and those permissions are automatically applied to all the users in the group. If you add another user to the group, the new user will automatically inherit all the policies and the permissions already assigned to that group. This lessens the administrative burden.

* Policies

An IAM policy sets permission and controls access to AWS resources. Policies are stored in AWS as JSON documents. Permissions specify who has access to the resources and what actions they can perform. For example, a policy could allow an IAM user to access one of the buckets in [Amazon S3](https://www.simplilearn.com/tutorials/aws-tutorial/aws-s3).

* Roles

An IAM role is a set of permissions that define what actions are allowed and denied by an entity in the AWS console. It is similar to a user in that it can be accessed by any type of entity (an individual or AWS service). Role permissions are temporary credentials.

# Activity:

Demonstrate the case study based on Identity and Access Management (IAM) on AWS

Go to the IAM Dashboad-> User-> Add user

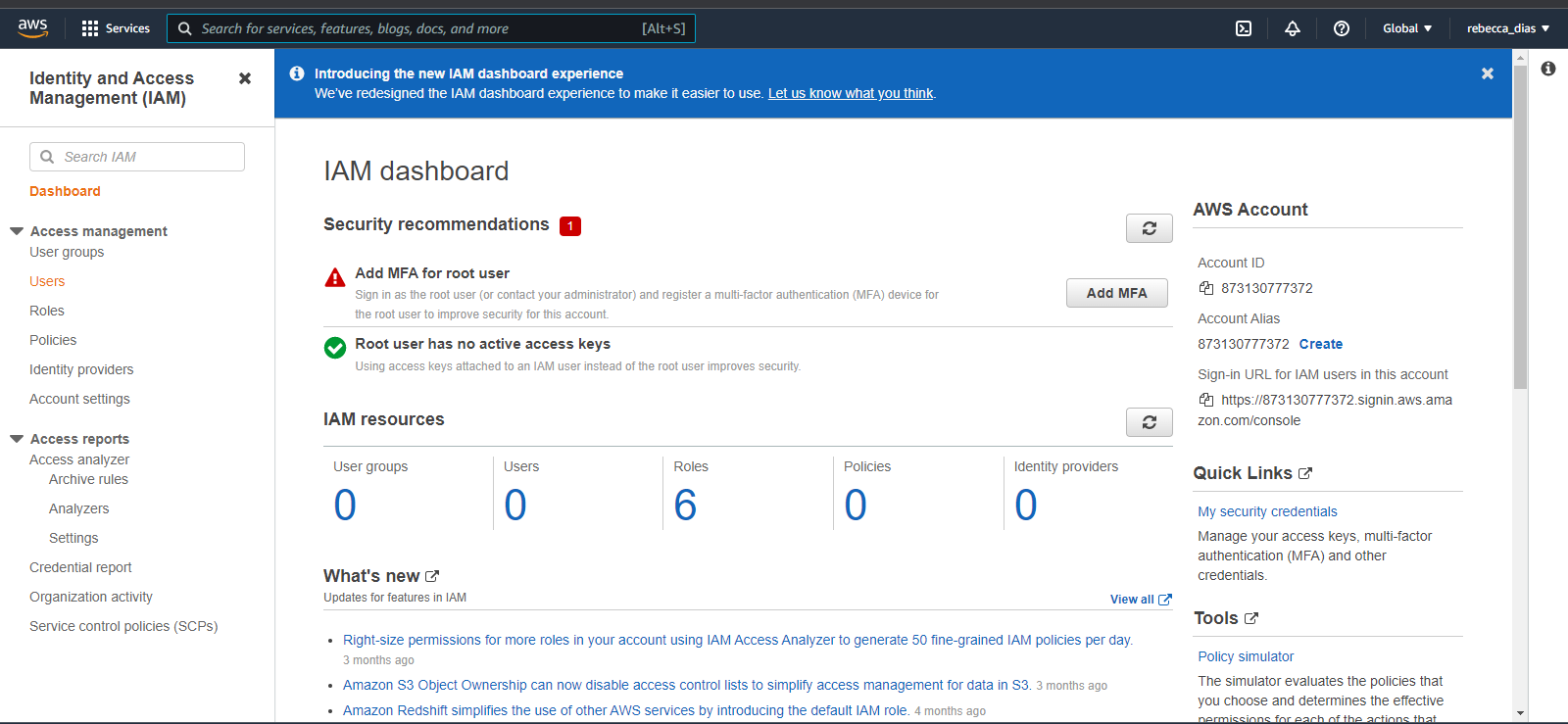


Fig 1

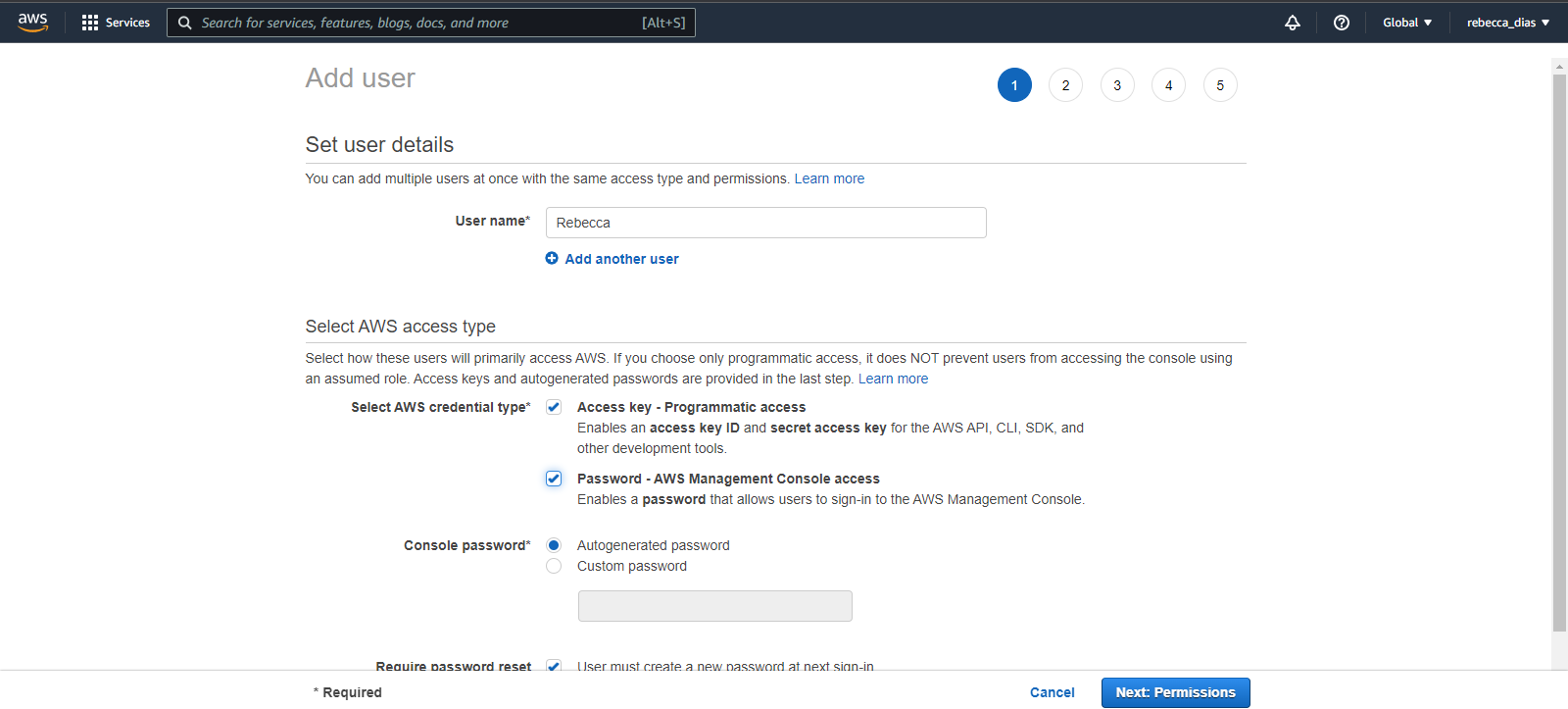


Fig 2

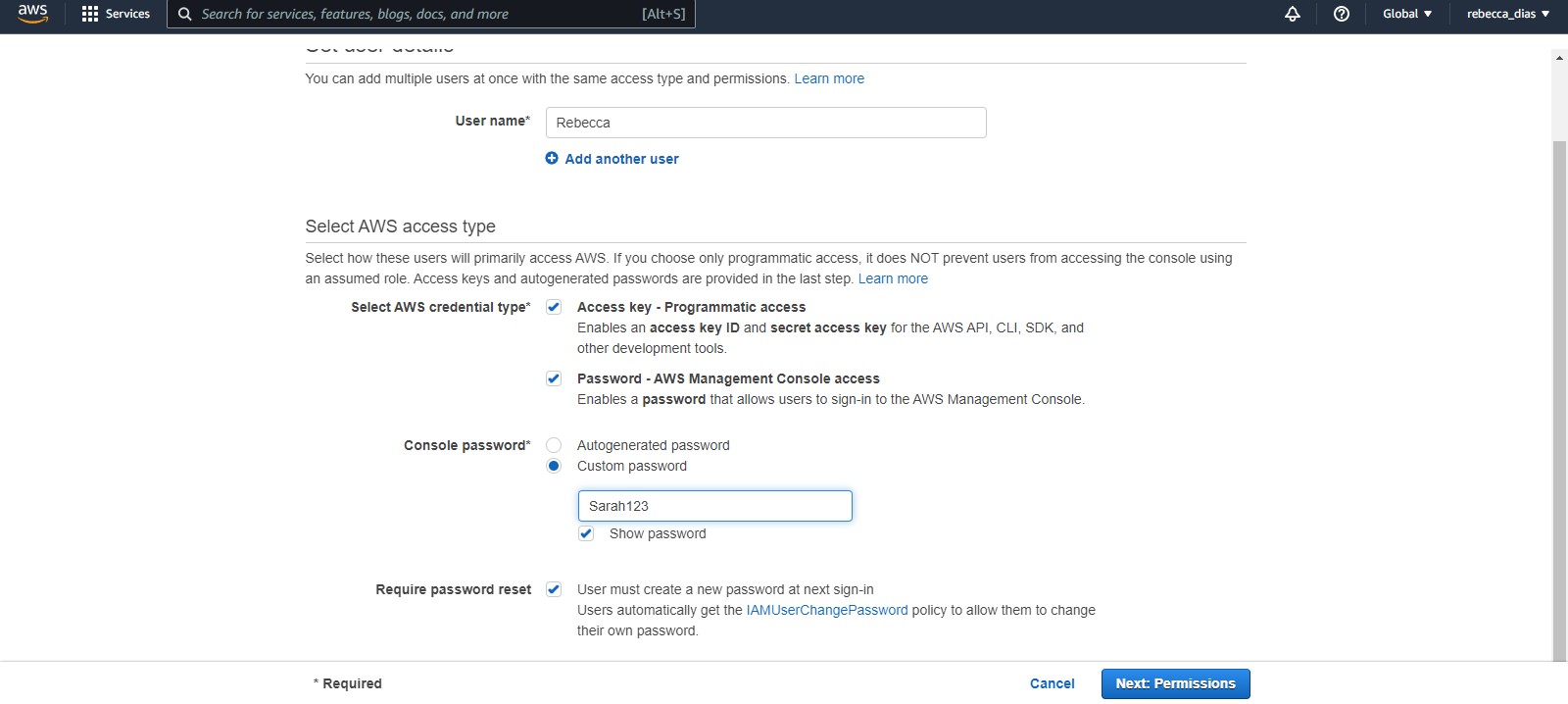


Fig 3

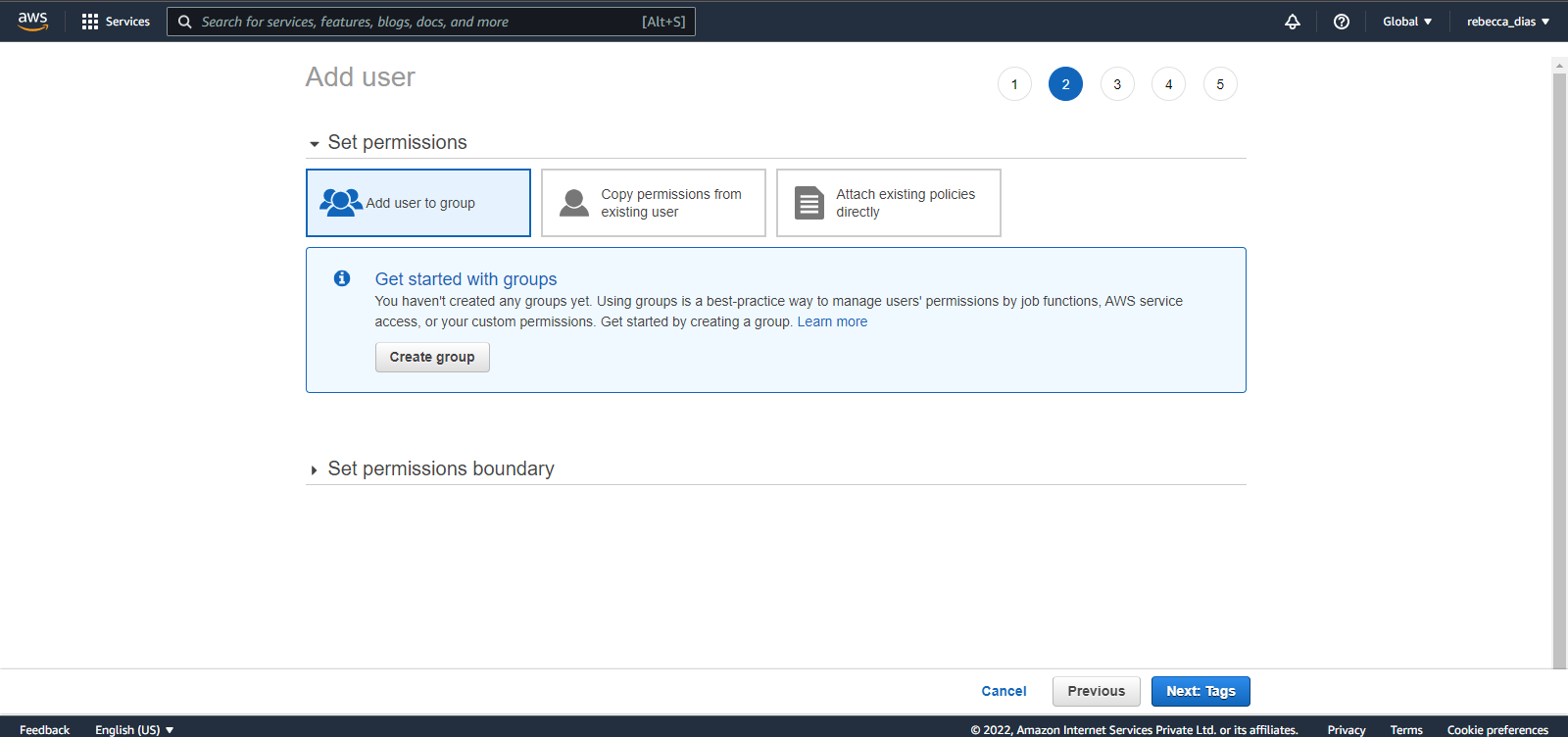


Fig 4

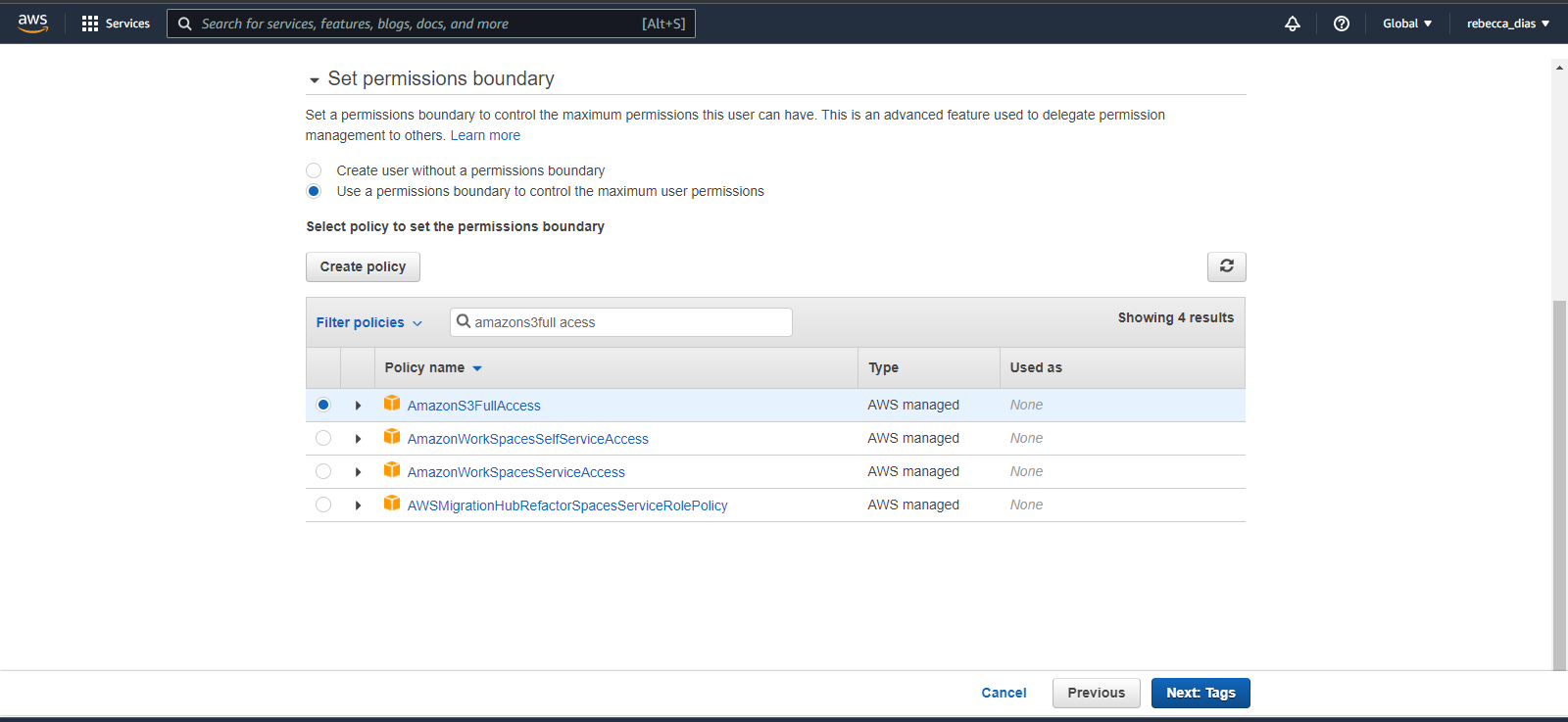


Fig 5

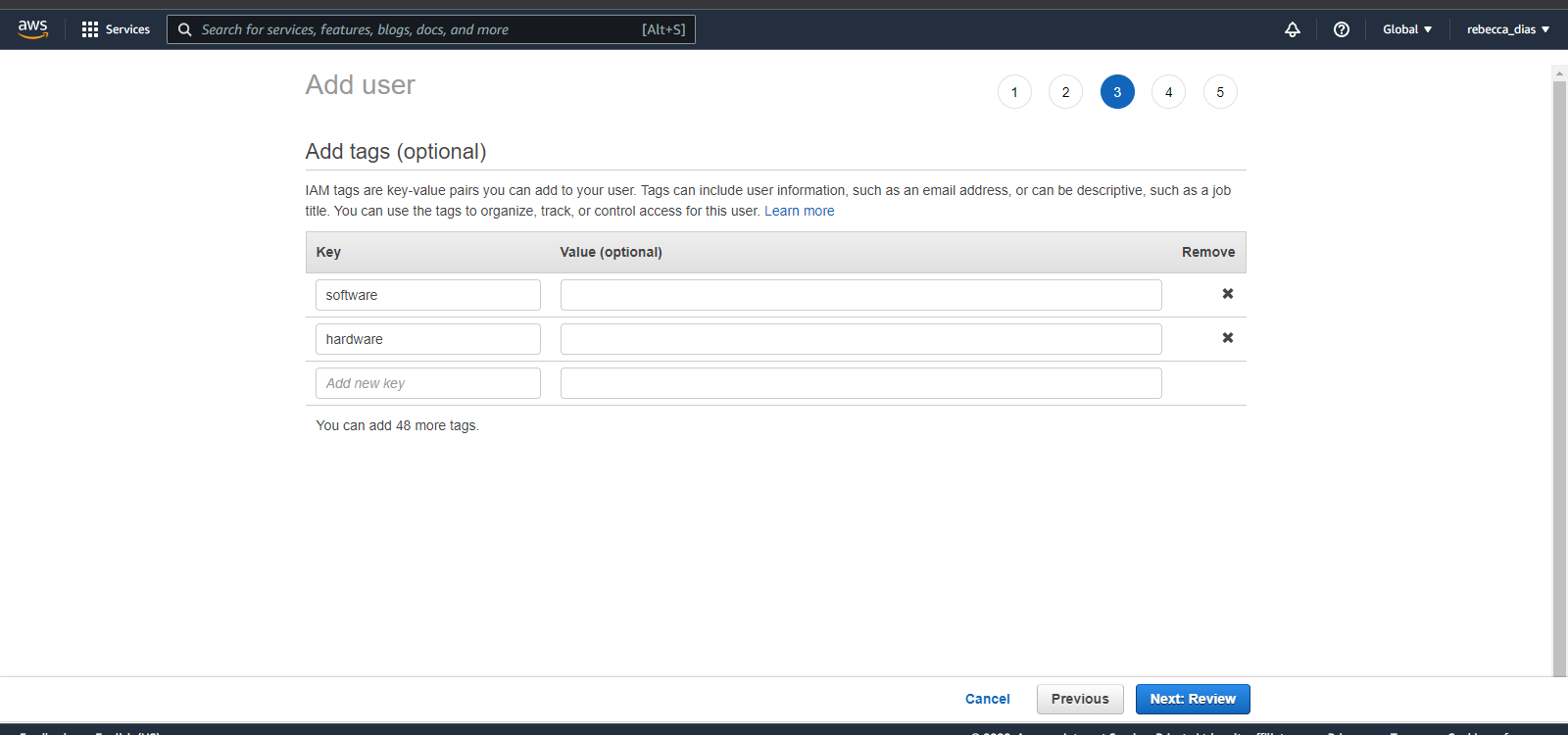


Fig 6

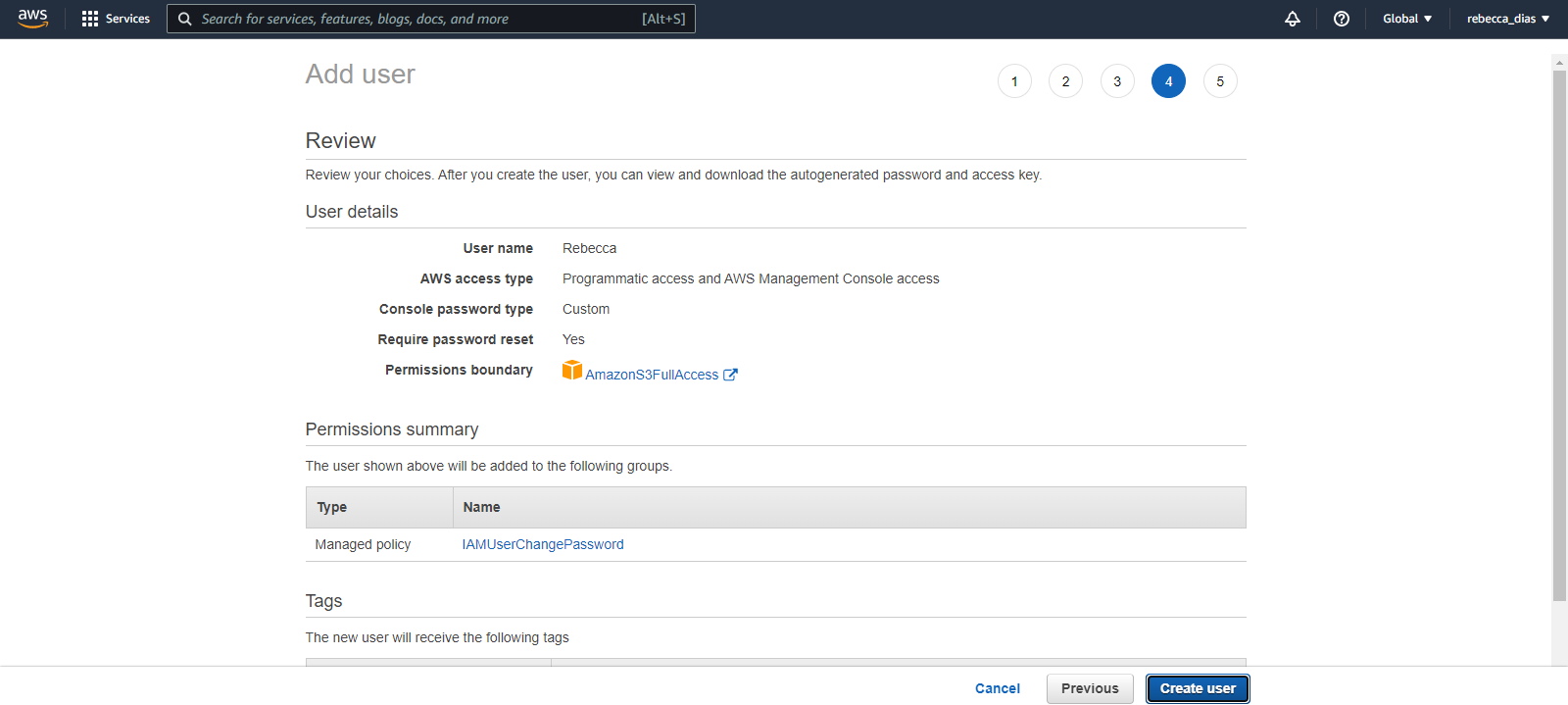


Fig 7

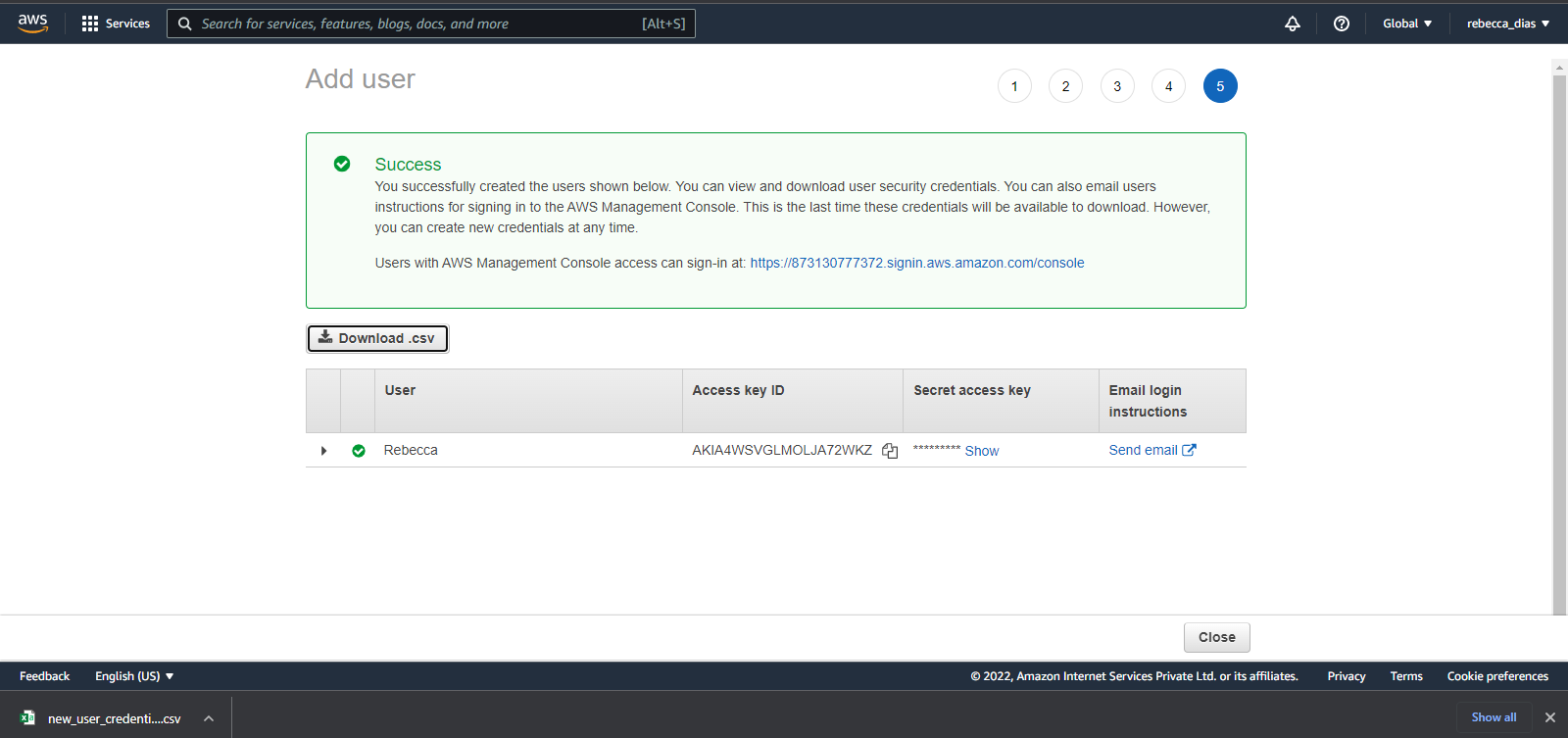


Fig 8

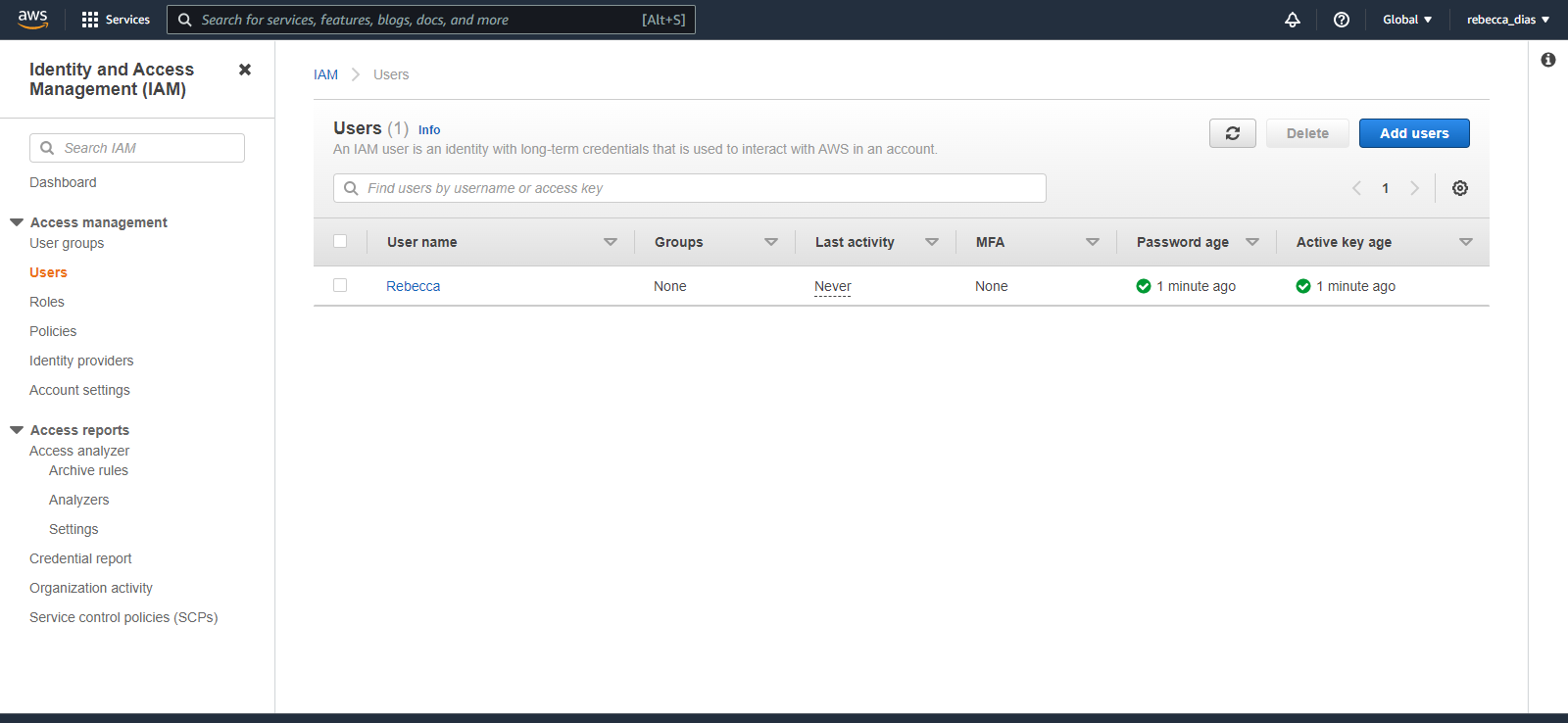


Fig 10

# Conclusion:

1. What are the benefits of IAM

* Shared access to the AWS account. The main feature of IAM is that it allows you to create separate usernames and passwords for individual users or resources and delegate access.
* Granular permissions. Restrictions can be applied to requests. For example, you can allow the user to download information, but deny the user the ability to update information through the policies.
* Multifactor authentication (MFA). IAM supports MFA, in which users provide their username and password plus a one-time password from their phone—a randomly generated number used as an additional authentication factor.
* Identity Federation. If the user is already authenticated, such as through a Facebook or Google account, IAM can be made to trust that authentication method and then allow access based on it. This can also be used to allow users to maintain just one password for both on-premises and cloud environment work.
* Free to use. There is no additional charge for IAM security. There is no additional charge for creating additional users, groups or policies.
* PCI DSS compliance. The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. IAM complies with this standard.
* Password policy. The IAM password policy allows you to reset a password or rotate passwords remotely. You can also set rules, such as how a user should pick a password or how many attempts a user may make to provide a password before being denied access.