Name: Nitin Madas

Roll no: A036

SapId: 86062300054

Msc SDS Batch 1

**Practical : 3 Identity Access Management (IAM)**

WRITE UPS

**Users and Groups in Cloud Computing**

In cloud computing, effective management of users and groups is crucial for maintaining security, efficiency, and organizational structure.

**Users**: A user is an individual or entity with credentials that access cloud services and resources. These credentials might be usernames and passwords, access keys, or tokens. Each user has specific permissions and roles that dictate what they can and cannot do within the cloud environment. Managing users involves creating accounts, assigning roles, and configuring permissions to ensure that each user has appropriate access based on their role and needs.

**Groups**: A group is a collection of users that share a common set of permissions. Instead of managing permissions for each user individually, groups allow administrators to manage permissions collectively. For instance, you might create a group for developers, one for administrators, and another for analysts. By assigning permissions to a group, you simplify the administration of access controls. Users added to a group inherit the permissions assigned to that group, which streamlines the management of large numbers of users.

Effective use of users and groups helps in organizing access control, enhancing security, and reducing administrative overhead.

**IAM (Identity and Access Management)**

Identity and Access Management (IAM) is a framework of policies and technologies for ensuring that the right individuals have access to the right resources at the right times and for the right reasons within a cloud environment. IAM encompasses the processes of identifying users, managing their roles and permissions, and ensuring secure access to resources.

**Components of IAM**:

* **Authentication**: Verifying the identity of users or systems through methods such as passwords, multi-factor authentication (MFA), or biometrics.
* **Authorization**: Determining what authenticated users are allowed to do. This involves defining and managing roles, permissions, and policies that control access to resources.
* **User Management**: Creating, updating, and deleting user accounts, along with managing user attributes and credentials.
* **Role Management**: Creating and managing roles, which are collections of permissions assigned to users or groups.
* **Policy Management**: Defining and enforcing policies that control access and permissions based on user roles, attributes, and other factors.

IAM systems are essential for securing cloud environments, ensuring compliance with regulations, and managing the complexity of user access.

**Role of IAM**

The role of IAM in cloud computing is pivotal for maintaining security, compliance, and operational efficiency. IAM systems help organizations control access to cloud resources by managing user identities, roles, and permissions effectively.

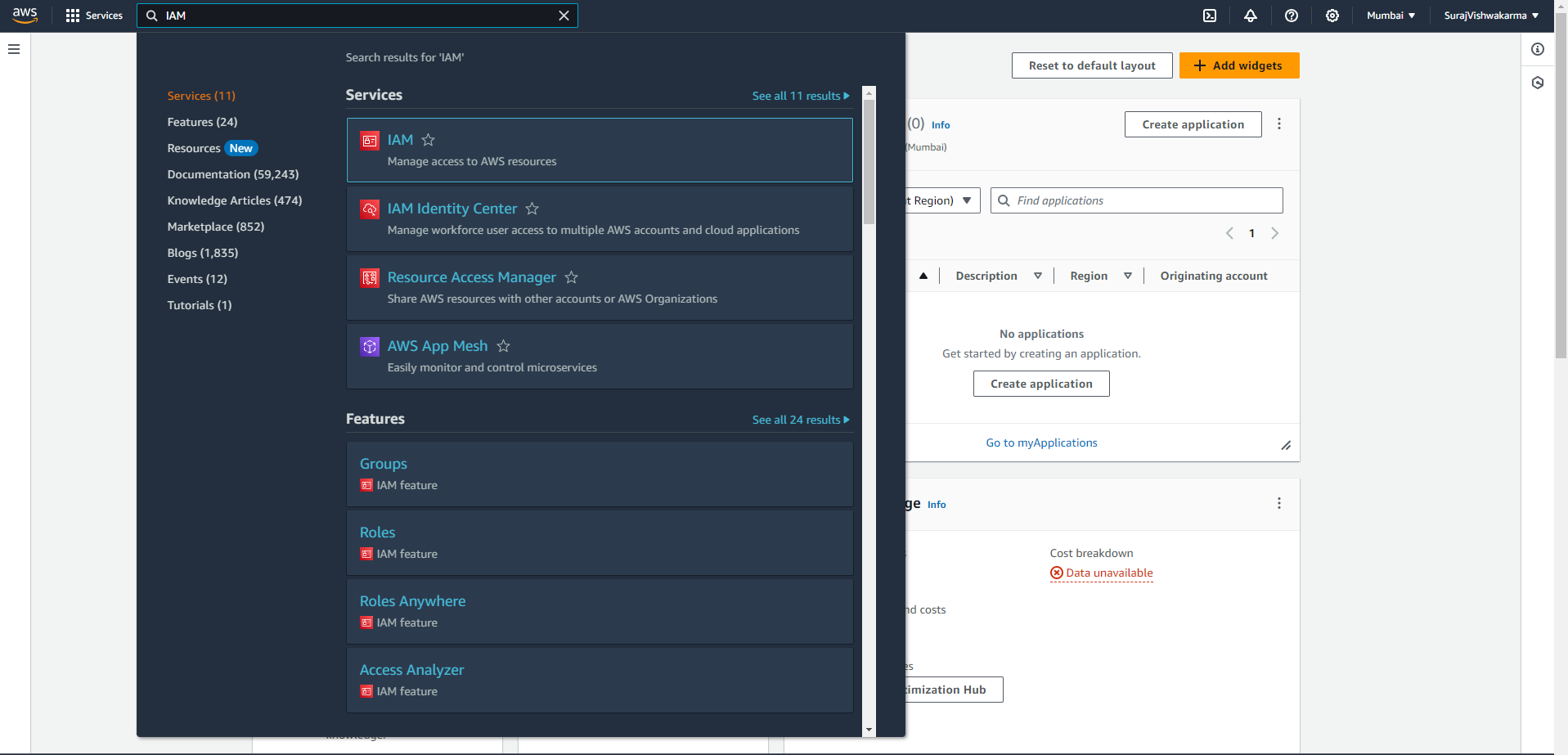
**Key Roles of IAM**:

1. **Security**: IAM systems enhance security by ensuring that only authorized users have access to sensitive resources. Through features like MFA, role-based access control (RBAC), and least privilege principles, IAM helps protect against unauthorized access and potential security breaches.
2. **Compliance**: IAM supports regulatory compliance by enabling detailed access controls and audit trails. Organizations can enforce policies that comply with standards such as GDPR, HIPAA, and others, and maintain records of access and changes for auditing purposes.
3. **Operational Efficiency**: By streamlining the management of user access through roles and groups, IAM reduces administrative overhead and minimizes the risk of errors. Automated processes for provisioning and de-provisioning users further enhance operational efficiency.
4. **User Experience**: IAM systems improve user experience by providing seamless access to resources. Single sign-on (SSO) capabilities, for instance, allow users to access multiple applications with a single set of credentials, simplifying access while maintaining security.
5. **Scalability**: IAM solutions scale with the growth of an organization. As new users and resources are added, IAM systems can dynamically adjust access controls and policies to accommodate changes without compromising security.

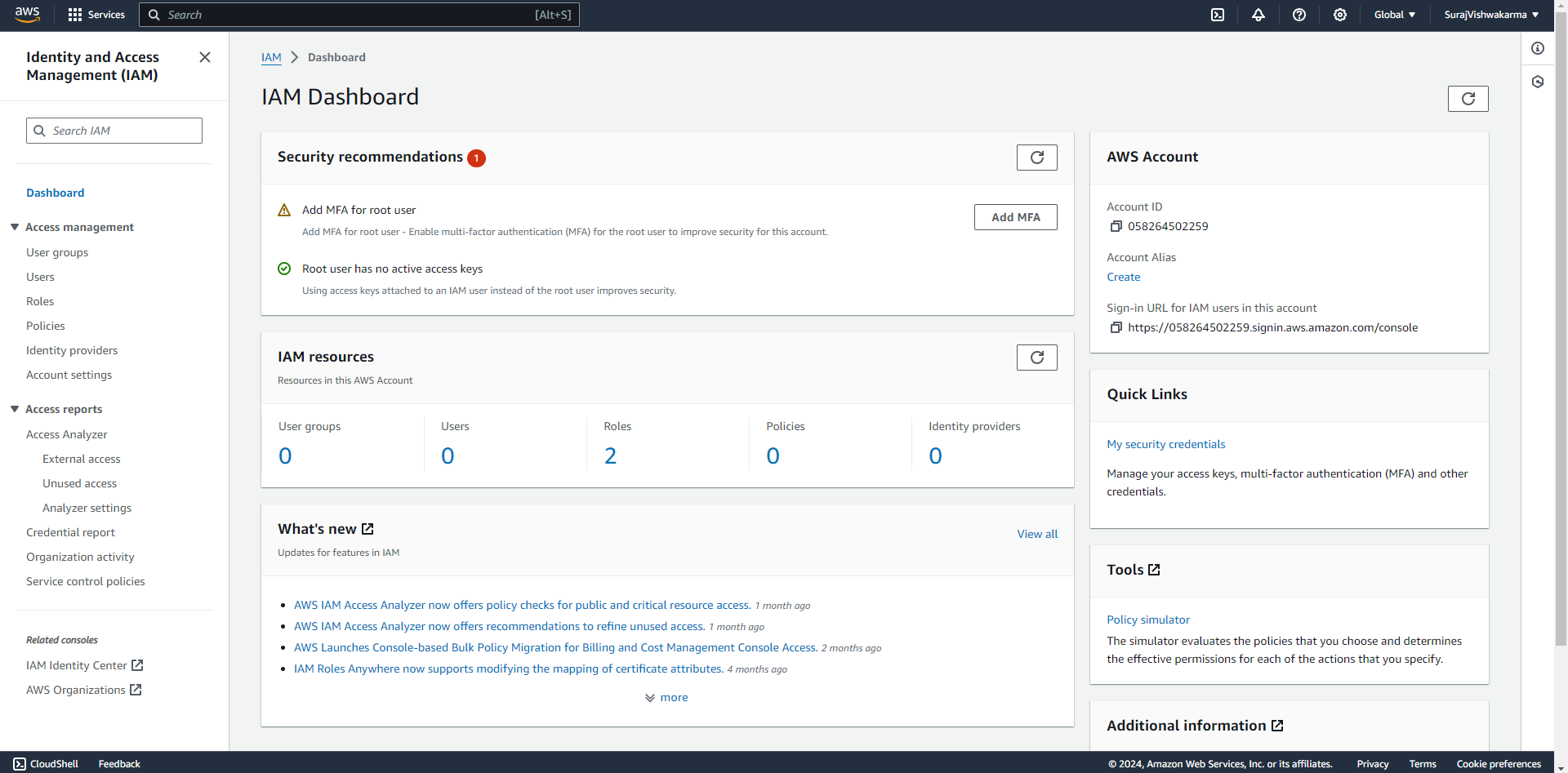
In summary, IAM plays a crucial role in managing access, ensuring security, and supporting compliance within cloud computing environments. It provides the tools and frameworks necessary for controlling who can access what resources and under what conditions, thereby safeguarding the integrity and confidentiality of cloud-based systems.

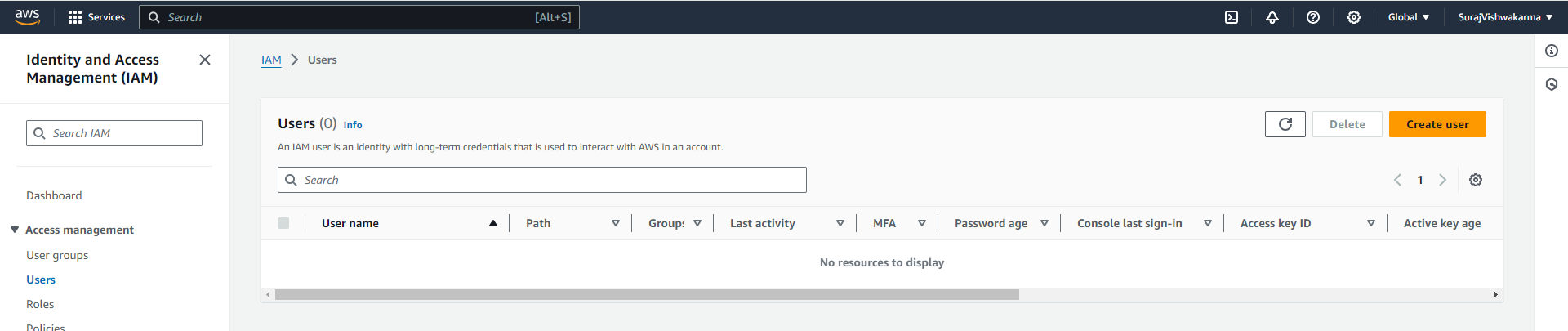
Step1: Log in to your AWS account and log in.

Step2: On the search bar search IAM and Click on the IAM

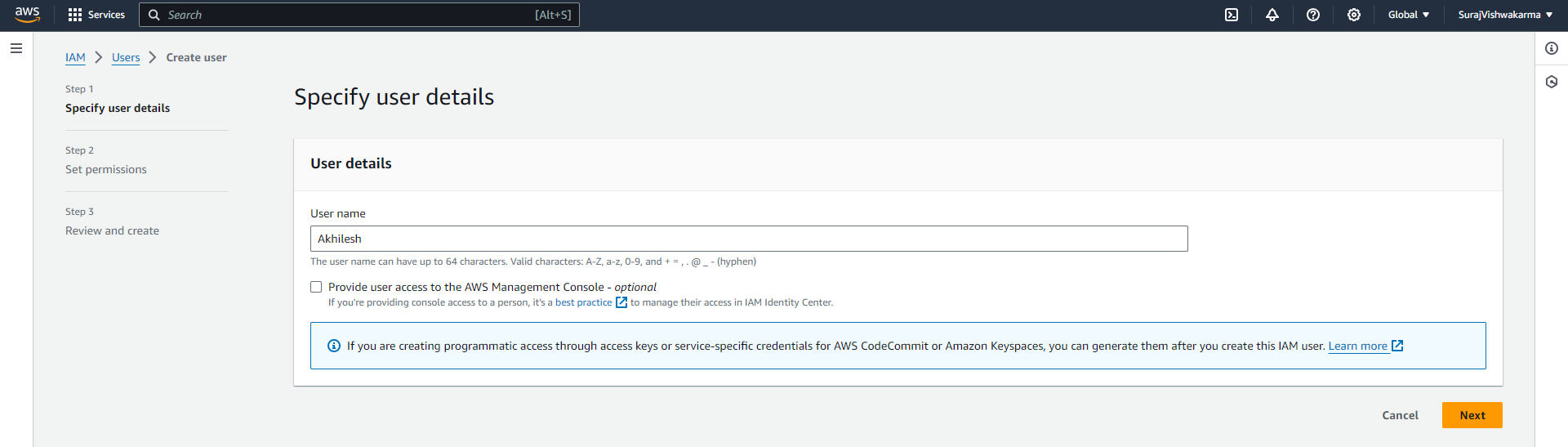


Step3: Click on the user

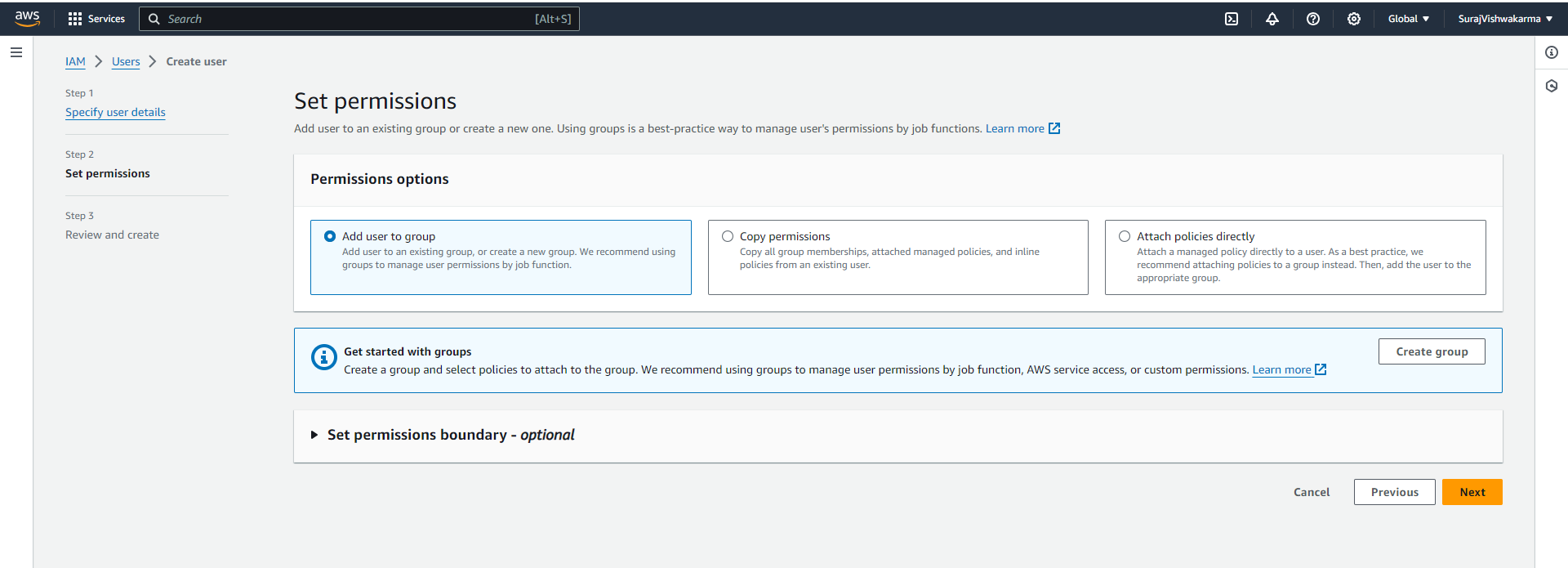


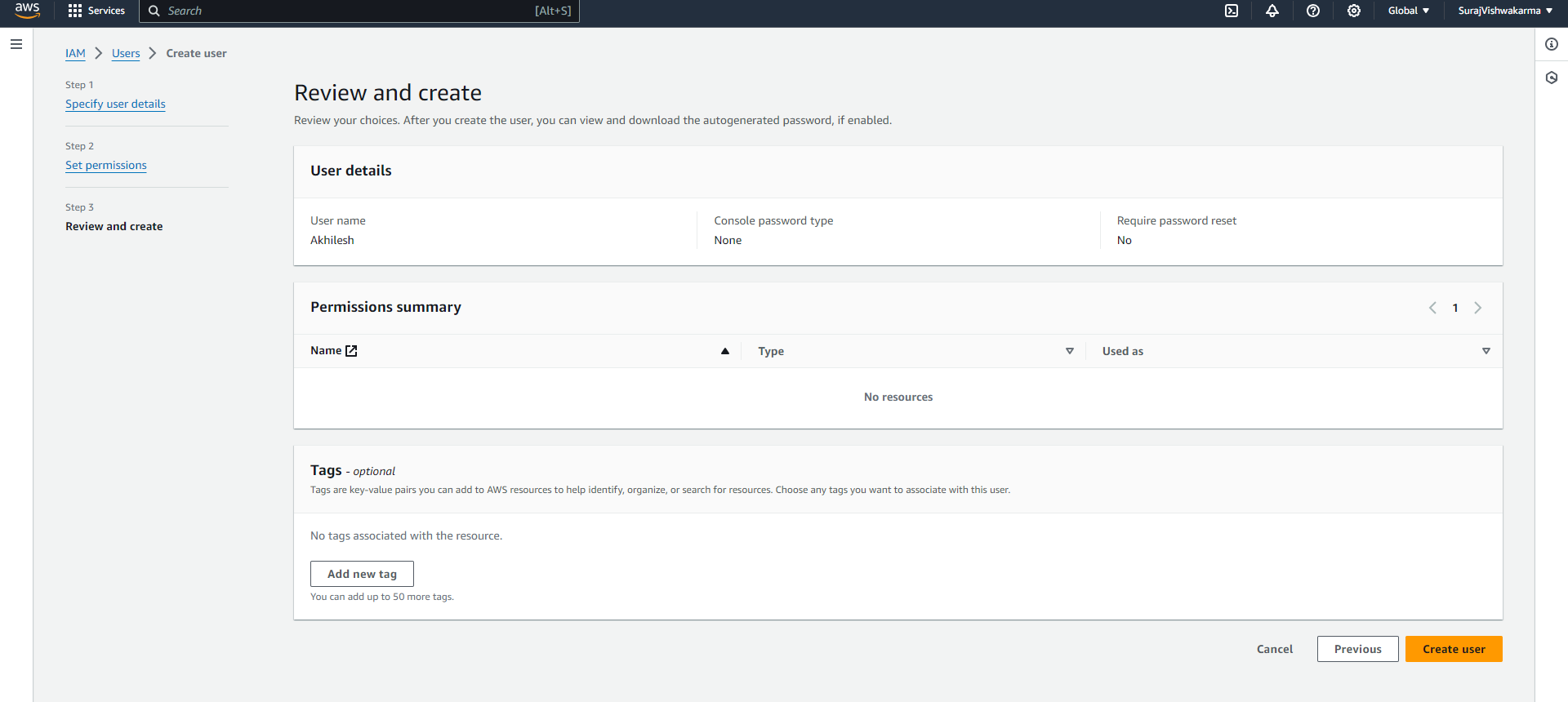


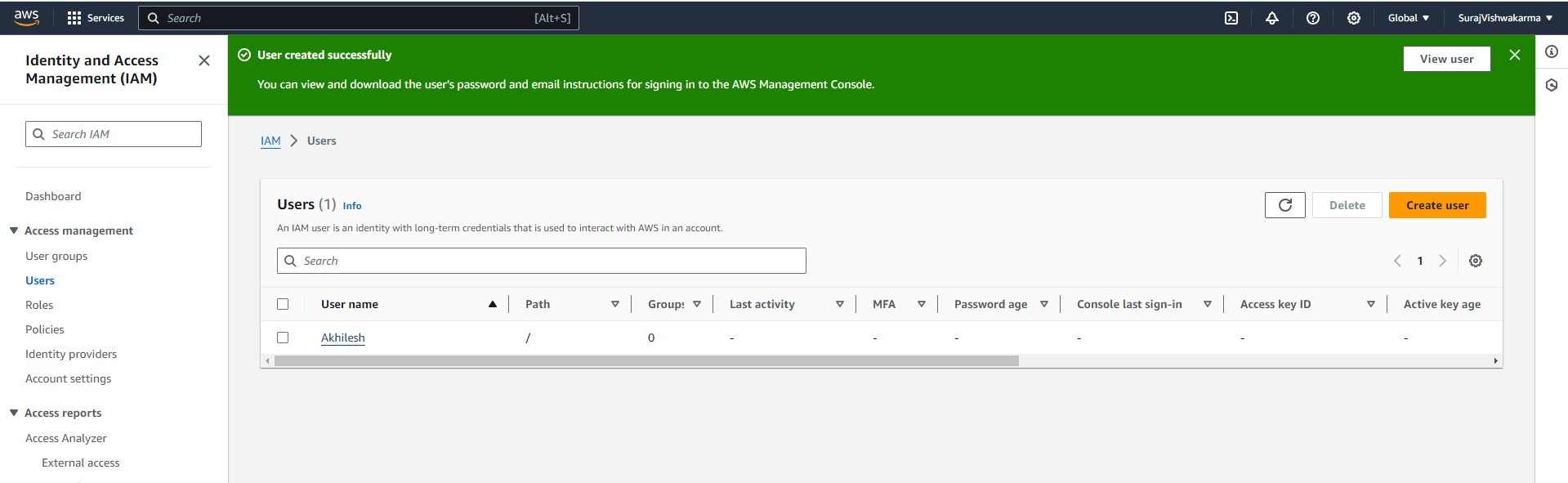
Step4: Give the name of user and do not select the ‘Provide user access to the AWS Management Console - *optional*’



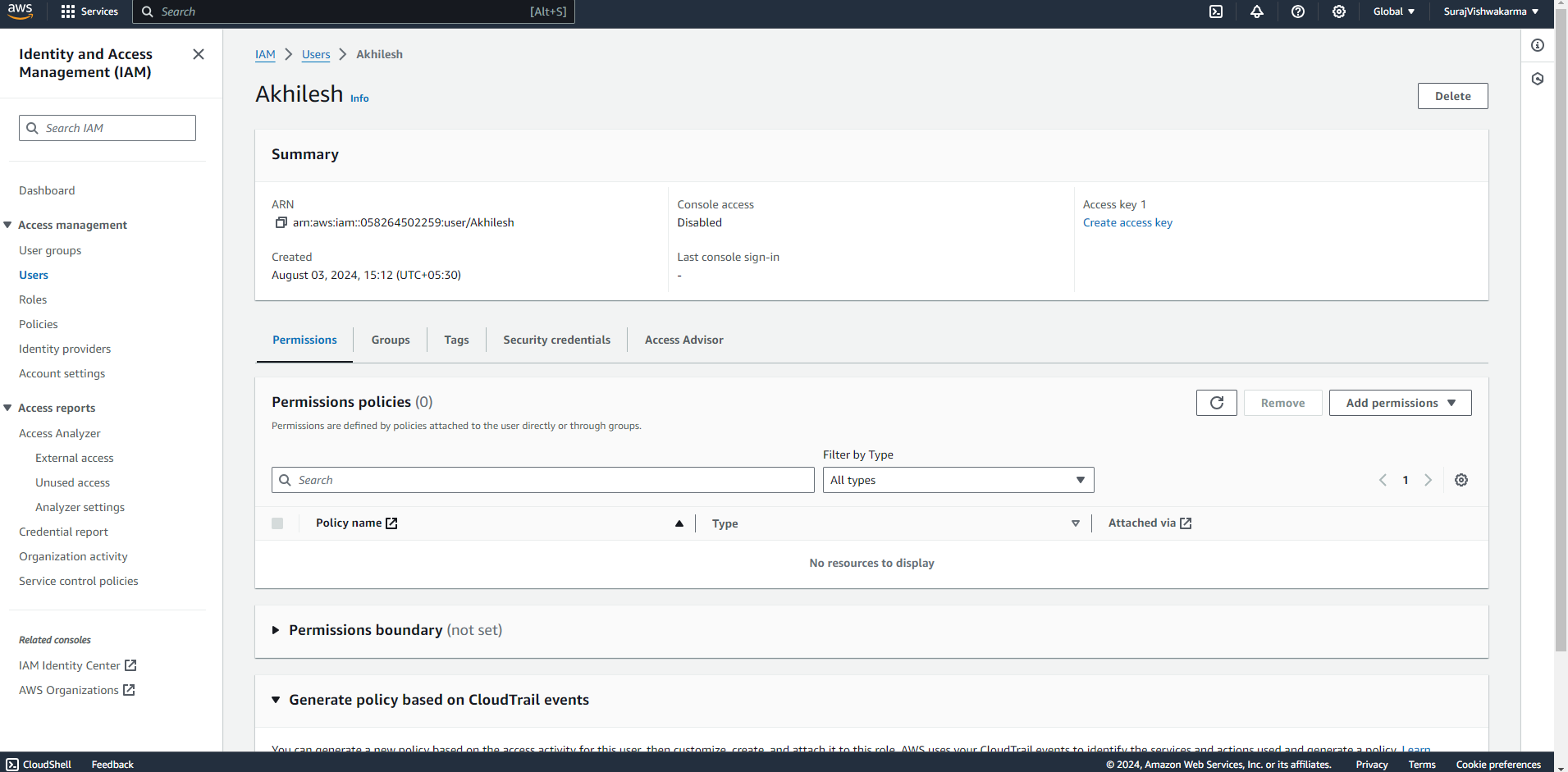
Step5: Then click on the next button



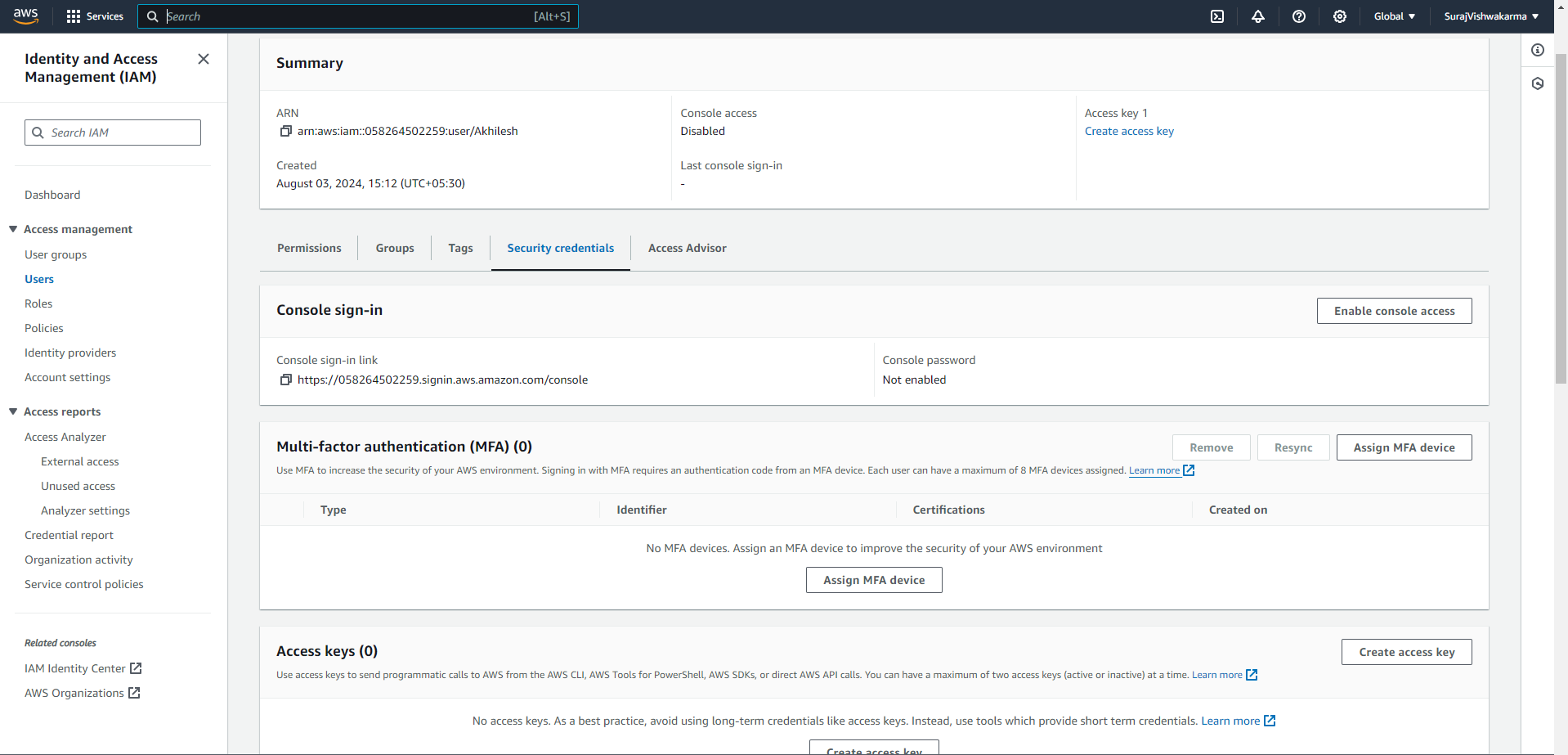


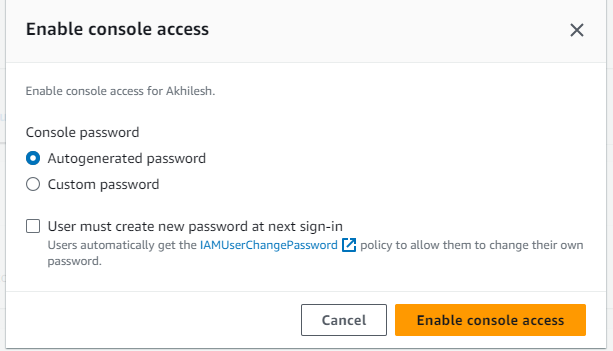


Step6: Then click on the user name i.e “Akhilesh”

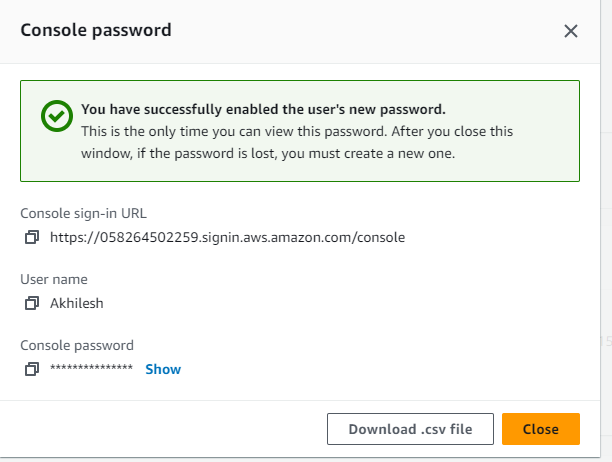


Step7: Click on the Security Credentials and then click on the enable console access

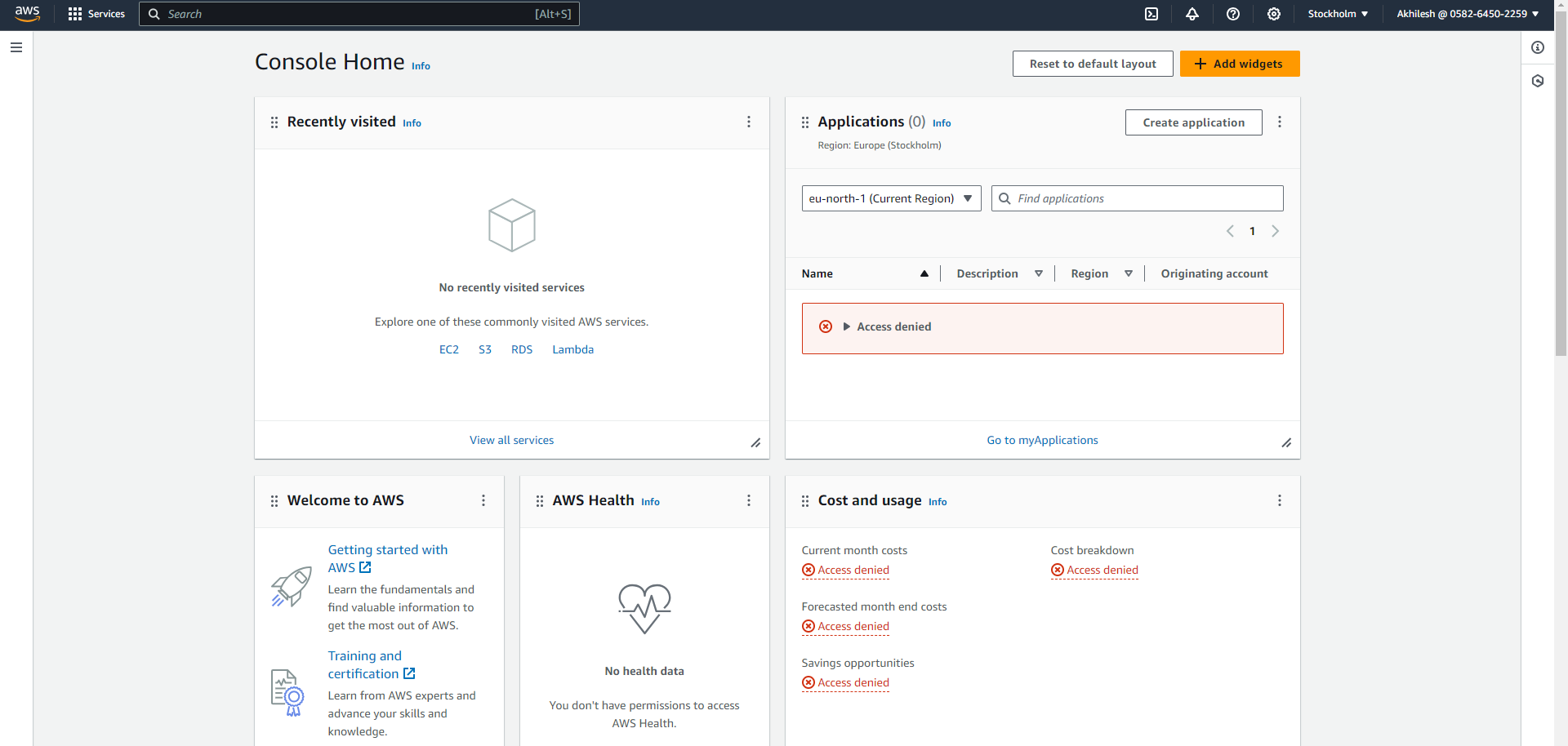




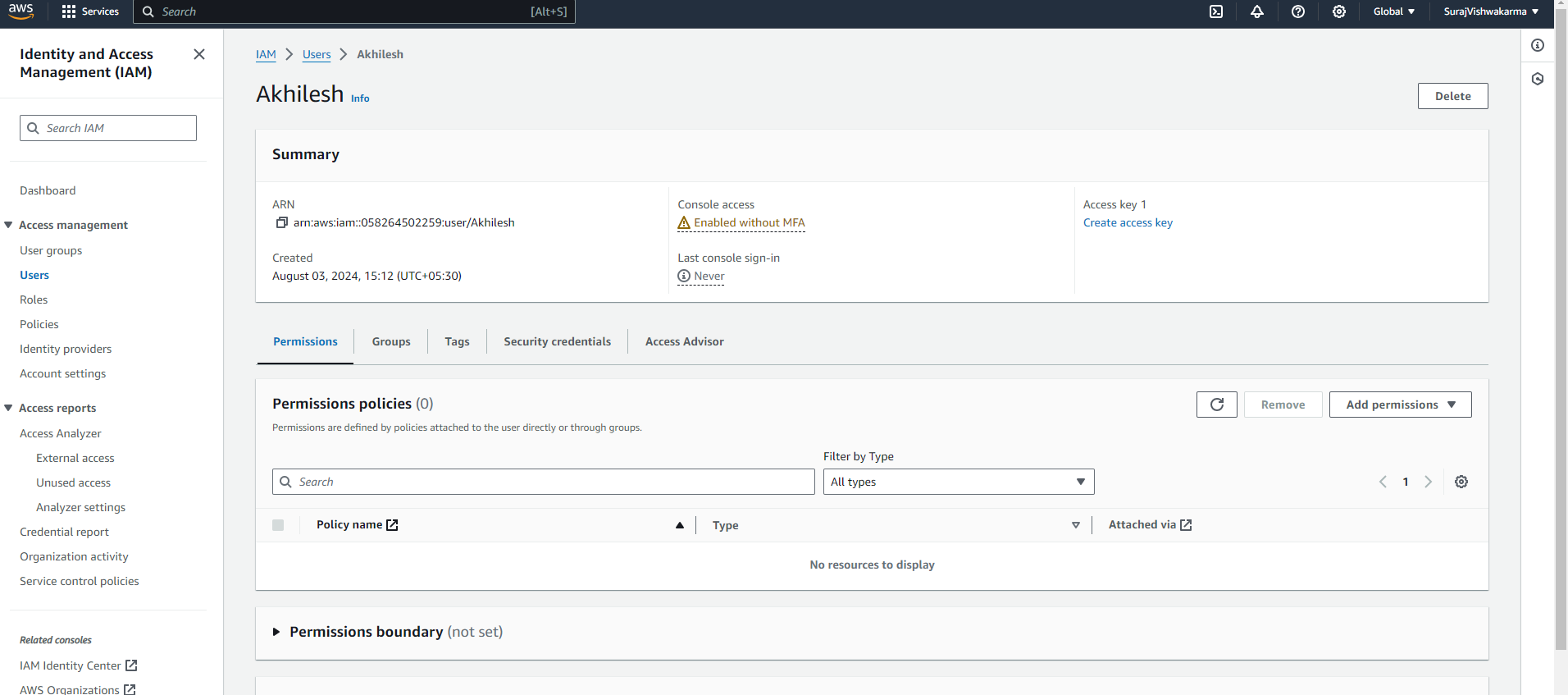
Step8: Then click on the Enable Console Access by default setting and it will show the screen Then download the csv file



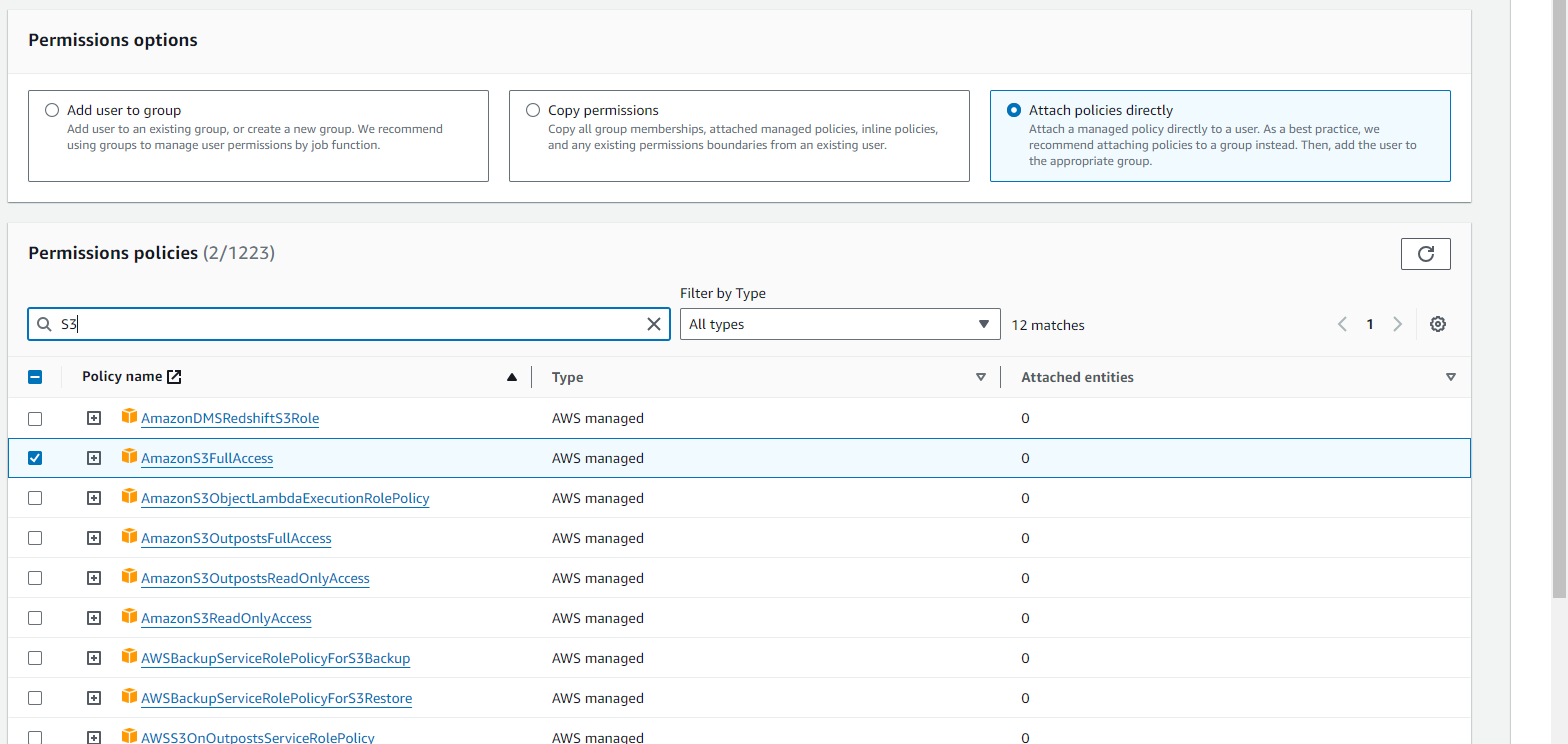
Step9: Then go to incognitive and then search AWS and click on AWS services and login with the user and password

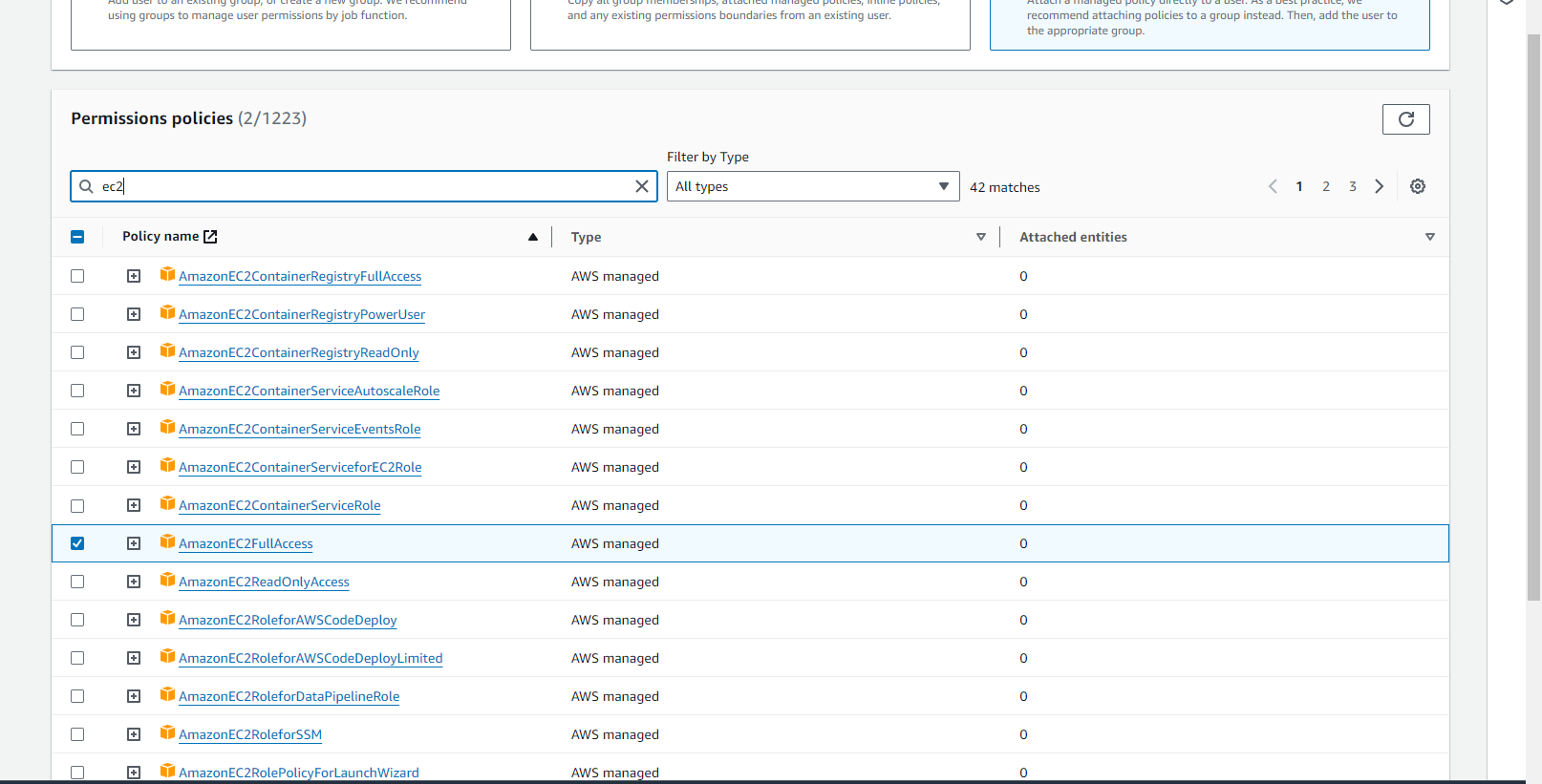


Step10: Give the permission to user of S3 and EC2



Step11: Click on the attach policies





Step12: Then click on the next button and click on the add permission