**BrightFuture Academy: Building a Secure Digital Campus with Tailored Access Control**

**Problem Statement:**

BrightFuture Academy needs a secure and efficient way to manage access to its digital resources for various groups like teachers, students, and IT staff. Currently, access is unstructured, leading to data security issues. The academy plans to develop an application using cloud services to create user groups with specific permissions, ensuring that each group only accesses the data and features relevant to their roles (e.g., teachers access student records, students access their own information, IT has full control).



**Pre-requisites:**

### 1. AWS Account Setup: [https://youtu.be/CjKhQoYeR4Q?si=ui8Bvk\_M4FfVM-D](https://youtu.be/CjKhQoYeR4Q?si=ui8Bvk_M4FfVM-Dh)h

### 2. Understanding of IAM: <https://youtu.be/gsgdAyGhV0o?si=3qg-bULgkD4LXNvR>

3. Region Selection :<https://youtu.be/NQhH2kcKI5U?si=GwDI8Gx7oUot8PiT>

4. Basic Knowledge of Amazon S3: <https://youtu.be/tfU0JEZjcsg?si=F1QLN_QKvy753Zg8>

**Objective:**

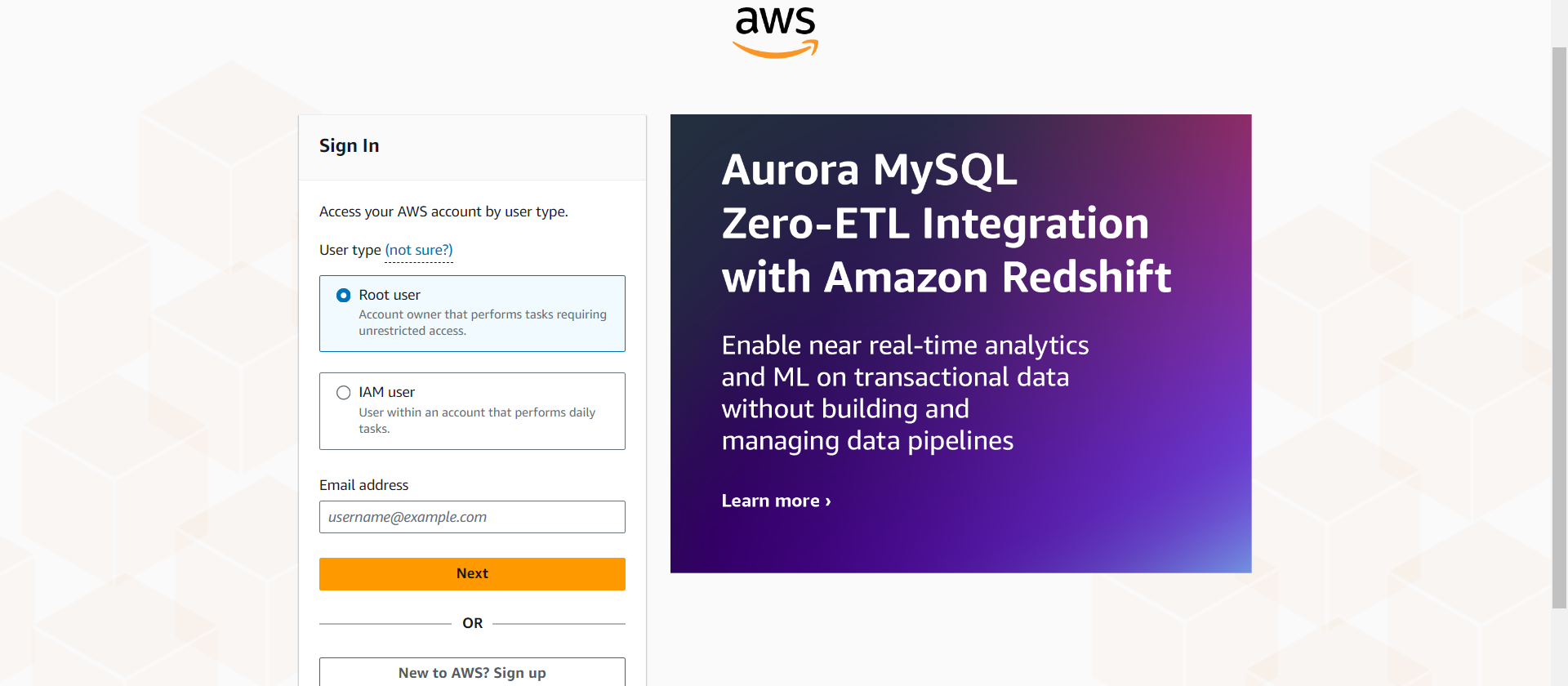
The primary objective of BrightFuture Academy is to establish a secure and efficient access management framework for its digital resources by leveraging AWS Identity and Access Management (IAM) services. This involves creating IAM groups that categorize users—such as teachers, students, and IT staff—based on their roles and responsibilities. Each group will be assigned predefined permissions tailored to their specific access needs, particularly regarding Amazon S3. By implementing this structured approach, the academy aims to enforce the principle of least privilege to minimize unauthorized access, streamline resource management through inherited permissions, enhance security protocols to protect sensitive data, and facilitate operational efficiency and scalability as its digital resource requirements evolve. This comprehensive access management strategy will ensure that the academy can safeguard its educational environment while effectively managing its cloud resources.

**Tasks:**

1. Log in to the AWS Management Console and navigate to the IAM service.
2. Select the existing IAM user that requires access to AWS services.
3. Attach the necessary permissions for both Amazon S3 and Amazon EC2 directly to the IAM user.
4. Verify that the IAM user has appropriate access to S3 buckets and EC2 instances by testing the permissions.
5. Ensure that security best practices are followed, including applying the principle of least privilege.

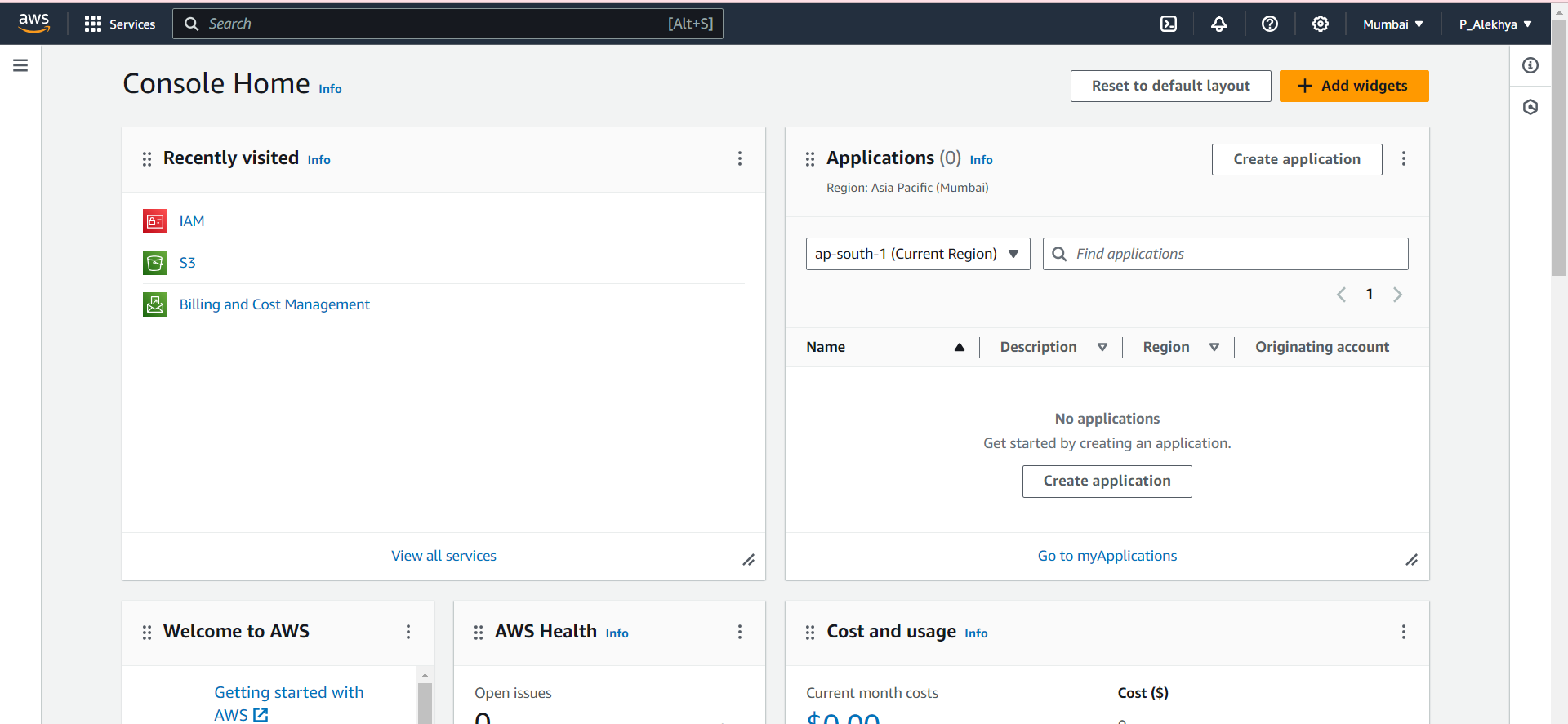
**Solution Development Procedure:**

1. Log in to the AWS Management Console and navigate to the IAM service.



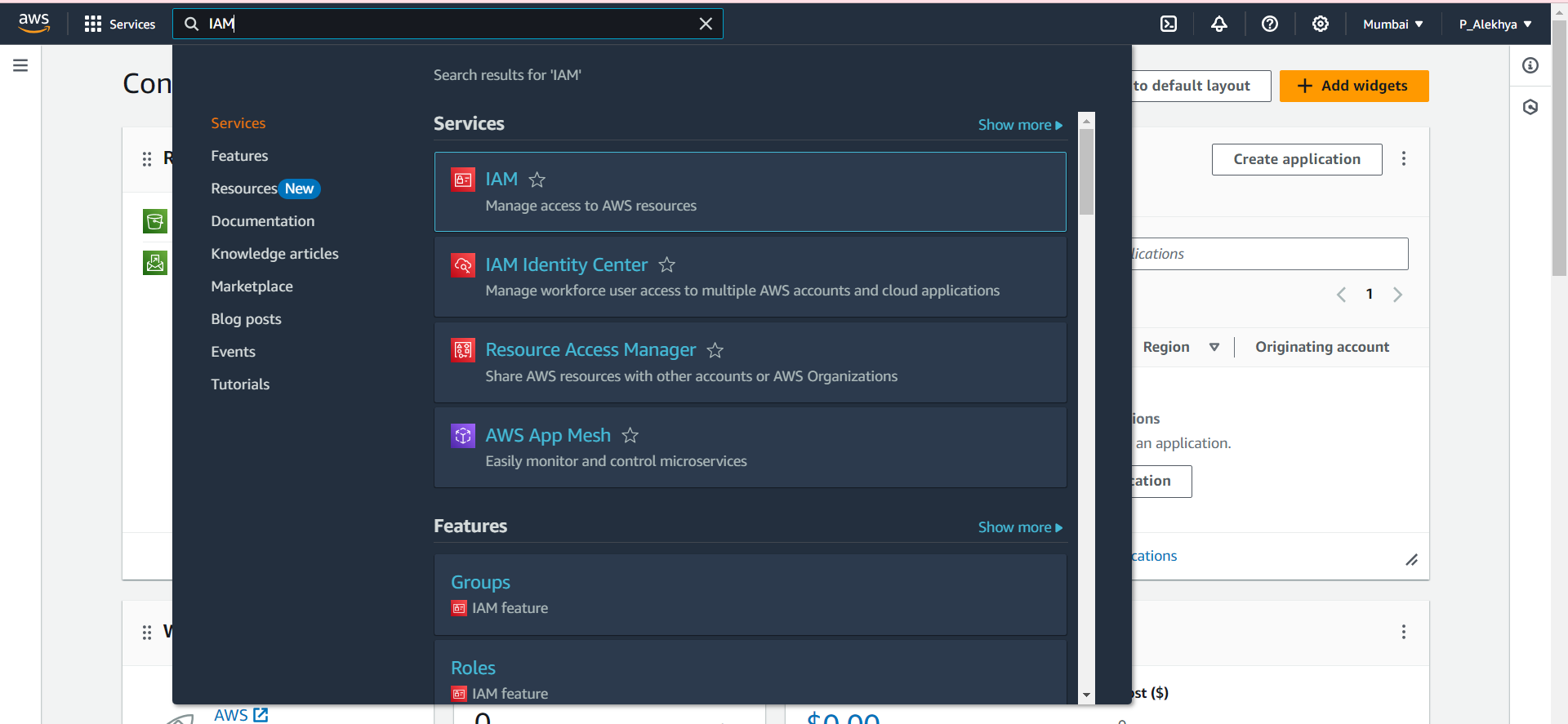
AWS sign-in page where the user selects between signing in as a **Root user** or an **IAM user**. This is the initial step for accessing the AWS Management Console.

-To create an IAM user select Root User



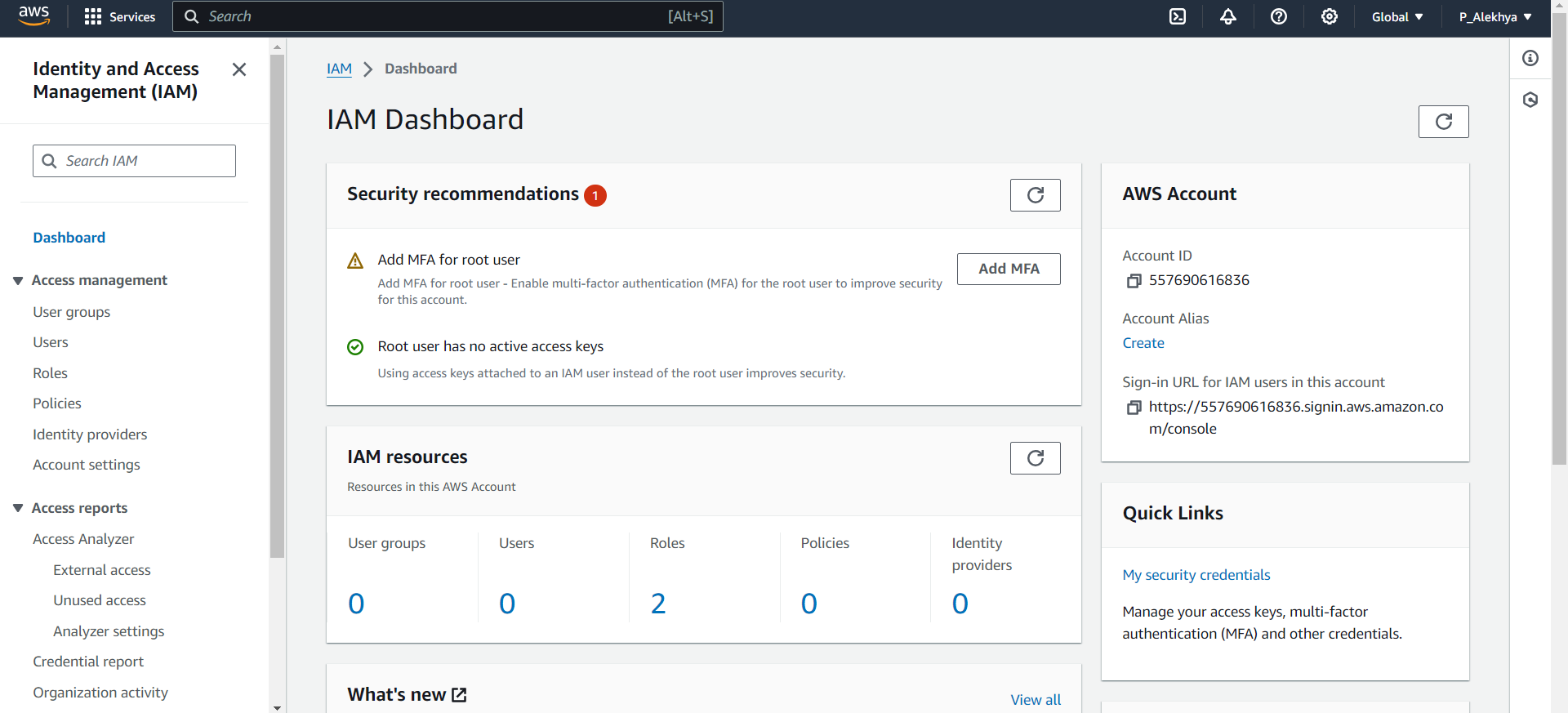
AWS Console Home page after login, displaying recently accessed services , along with an overview of the account’s activities.

* By navigating to the search bar ,we could find desired services.



AWS search bar being used to look for **IAM** (Identity and Access Management) services. This enables quick navigation to the IAM dashboard.

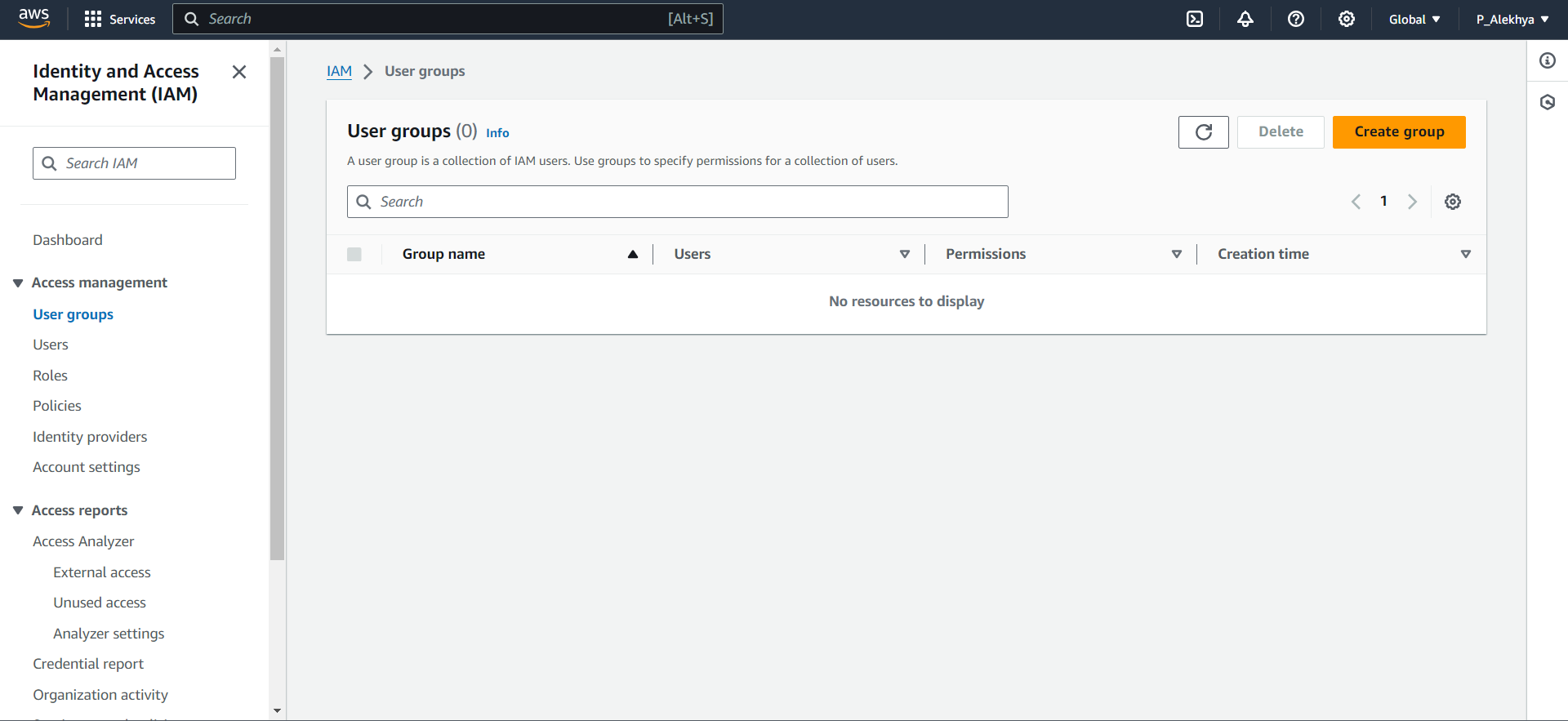
* Select IAM Service ,which is at the top.



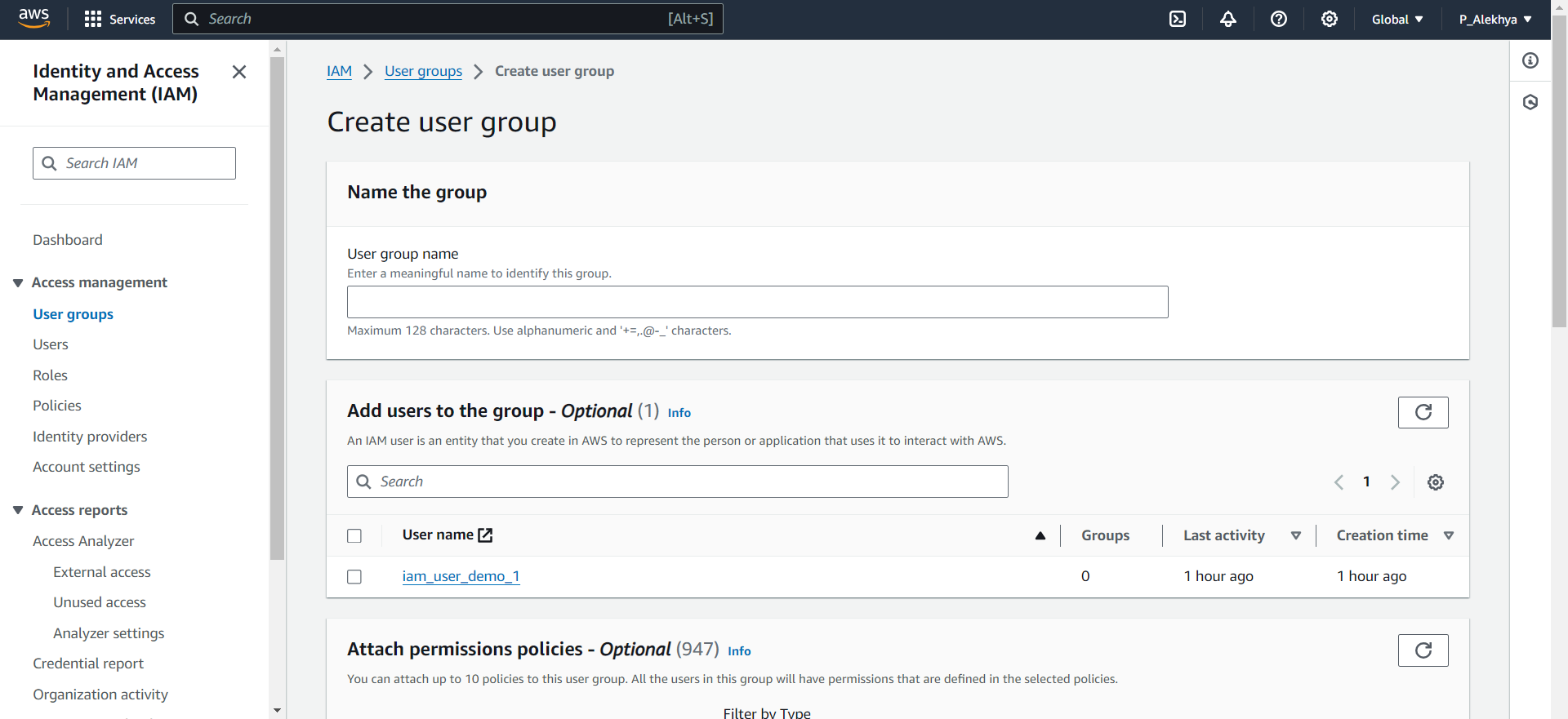
The **IAM Dashboard**, showing important security recommendations, such as enabling MFA for the root user, and displaying an overview of existing IAM resources like users, roles, and policies.

* Click on User groups, to create an IAM group.

1. Create a new IAM group to manage S3 access.

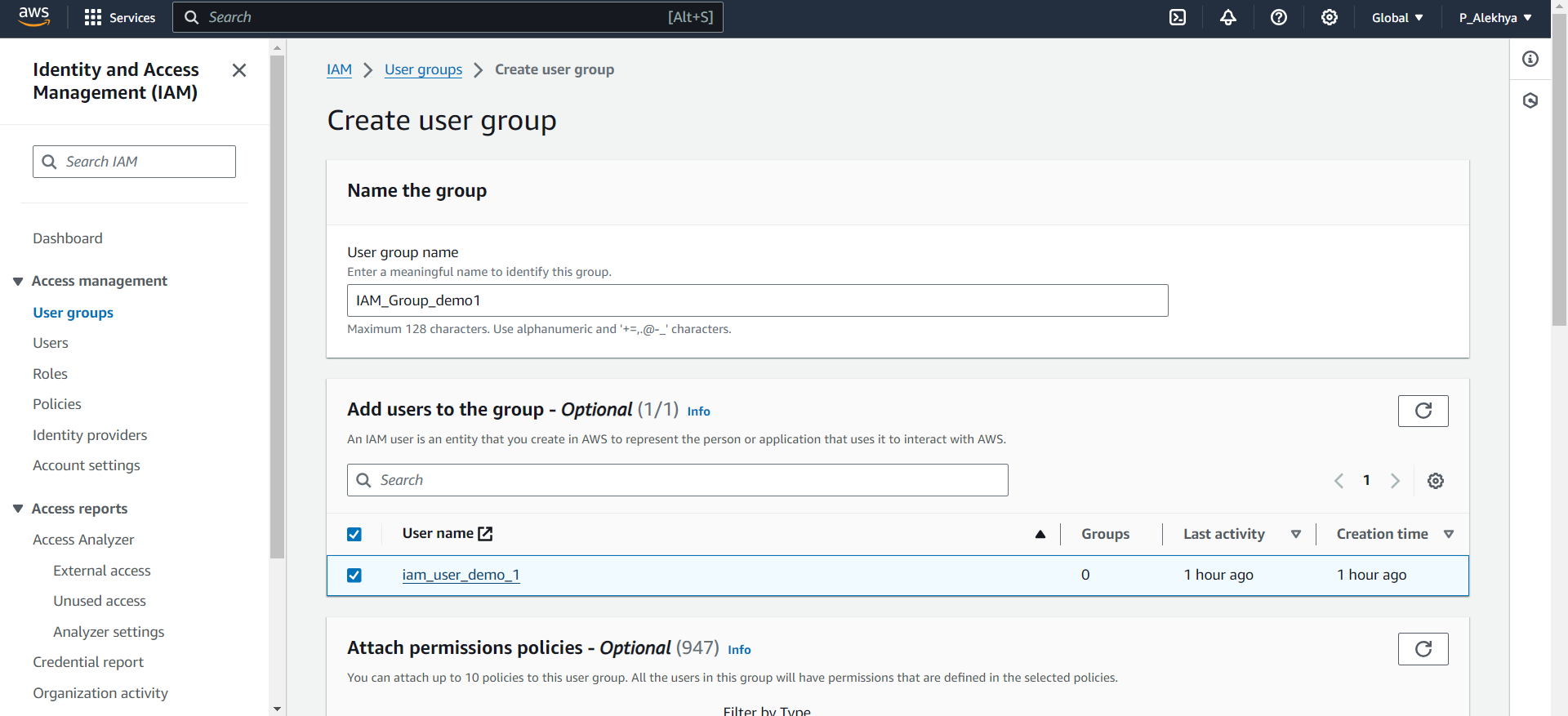


-The IAM User groups dashboard, click on ‘create group’ to create an IAM group.



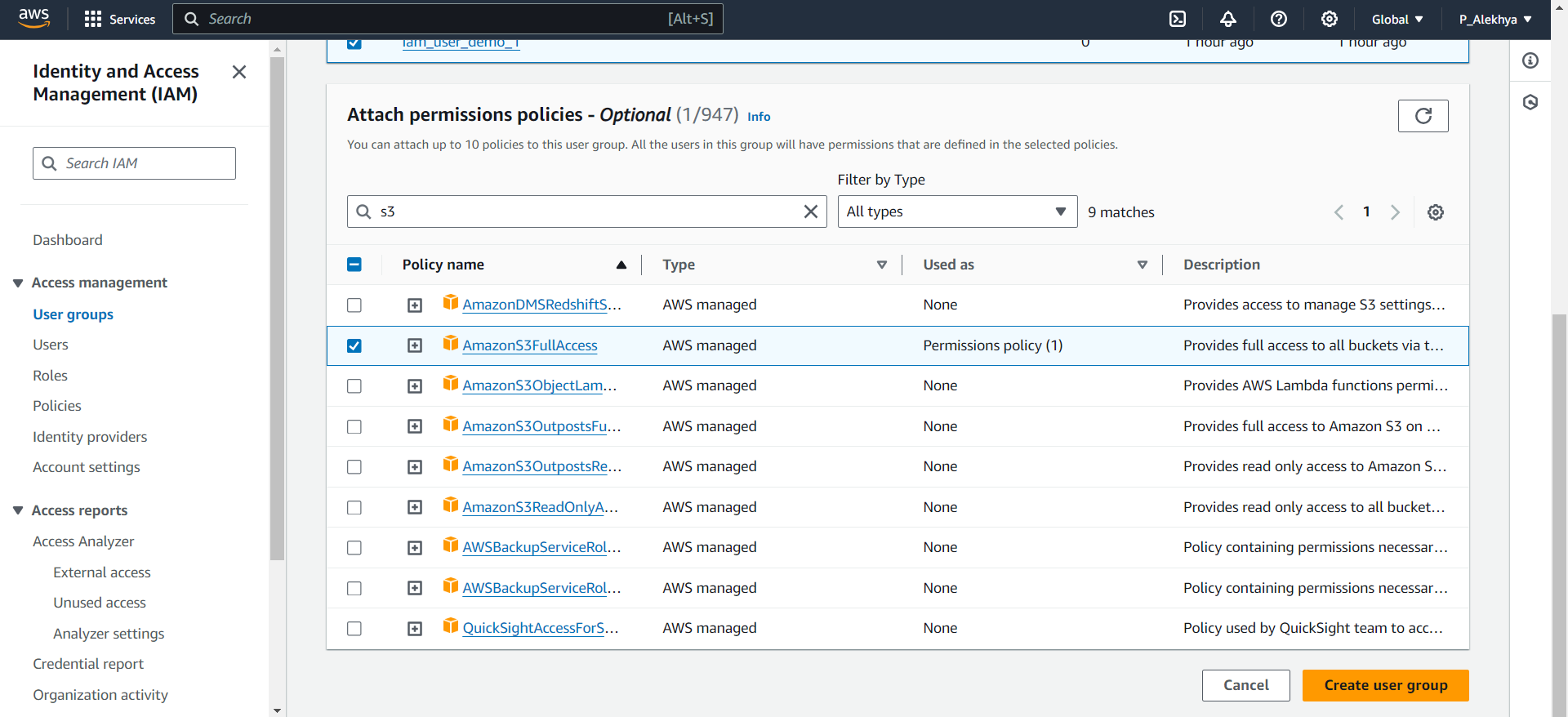
* IAM User group creation dashboard

1. Add an existing IAM user to the newly created group.

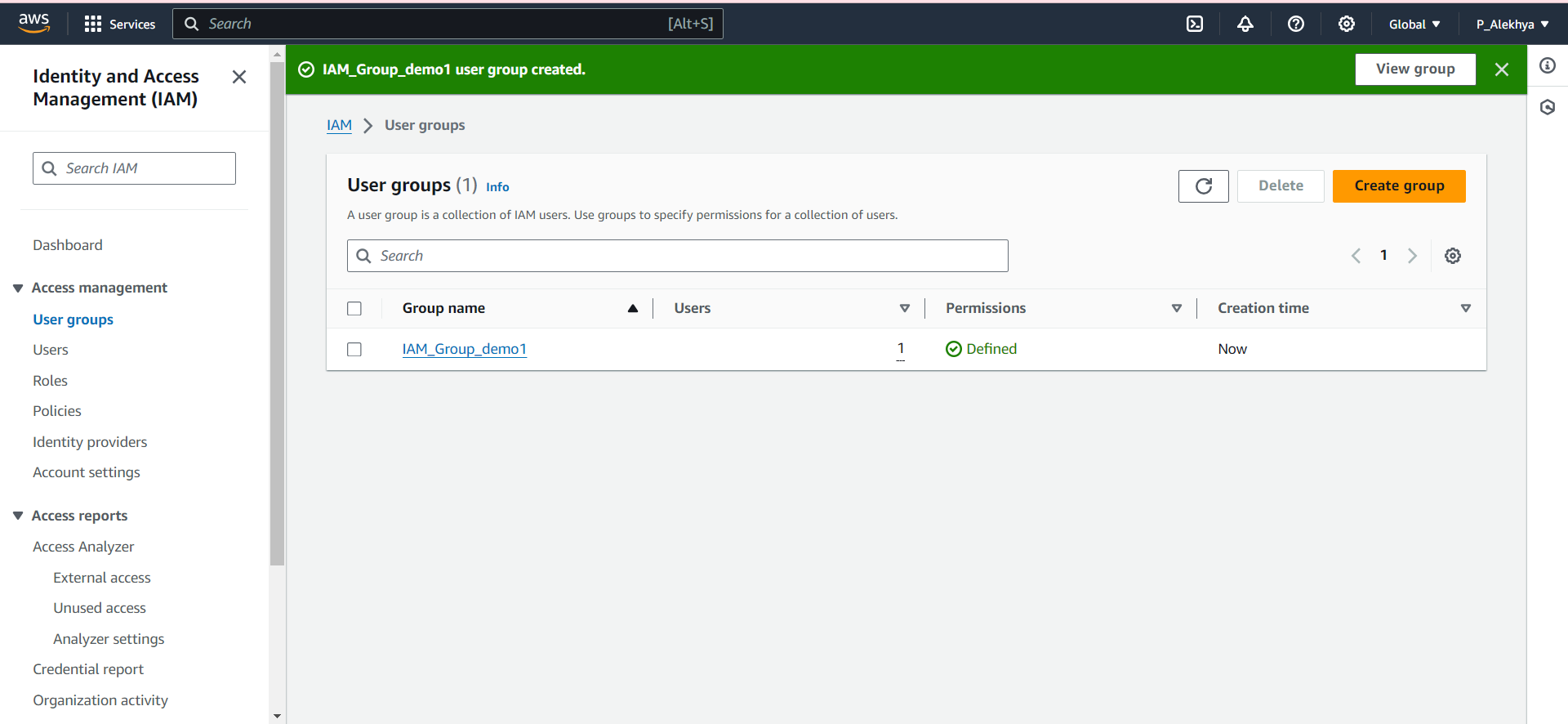


* The process begins by navigating to the IAM service and selecting the option to create a new user group. You provide a name for the group in the "Name the group" section. Then, in the "Add users to the group" section, you can select an existing user, such as "iam\_user\_demo\_1." Finally, you can optionally attach permissions policies from a list of available options before finalizing the group creation.

1. Attach the necessary permissions for Amazon S3 access to the IAM group.



* In this step, you are attaching permission policies to the newly created IAM group. You’ve filtered and selected the **AmazonS3FullAccess** policy, which grants full access to all S3 resources. After selecting the necessary policies, you can finalize the process by clicking **"Create user group"** to apply the permissions to the group.



The IAM group creation has been completed. The green confirmation bar indicates that the **IAM\_Group\_demo1 for education institutions** has been successfully created. The group now appears under the "User groups" section, with one user assigned to it and permissions successfully defined. You can view or manage the group further by selecting the **"View group"** button or continue creating additional groups if needed.

**Conclusion:**

By implementing a structured IAM group-based access management system within AWS, BrightFuture Academy can significantly enhance its security posture and control over digital resources. This method ensures that users are granted appropriate permissions, thereby reducing the risk of unauthorized access to sensitive information. Adhering to AWS security best practices, the academy can efficiently manage its S3 resources while supporting future growth and compliance needs. Furthermore, the flexibility of IAM groups enables the institution to adapt permissions as necessary, ensuring a responsive approach to evolving educational and operational requirements. This strategic implementation ultimately fosters a secure and efficient digital learning environment.