**IAM Tasks**

1. Create five IAM users.

2. Generate programmatic access keys for the users.

3. Create an IAM user group.

4. Add the five IAM users to the user group.

5. Attach one policy (EC2 Full Access) to a single IAM user.

6. Log in as the user using the AWS Management Console URL, username, and

password.

7. Verify the EC2 Full Access permissions assigned to the user.

8. Attach one policy (S3 Full Access) to the user group.

9. Verify that all users in the group can access the S3 service based on the

assigned policy.

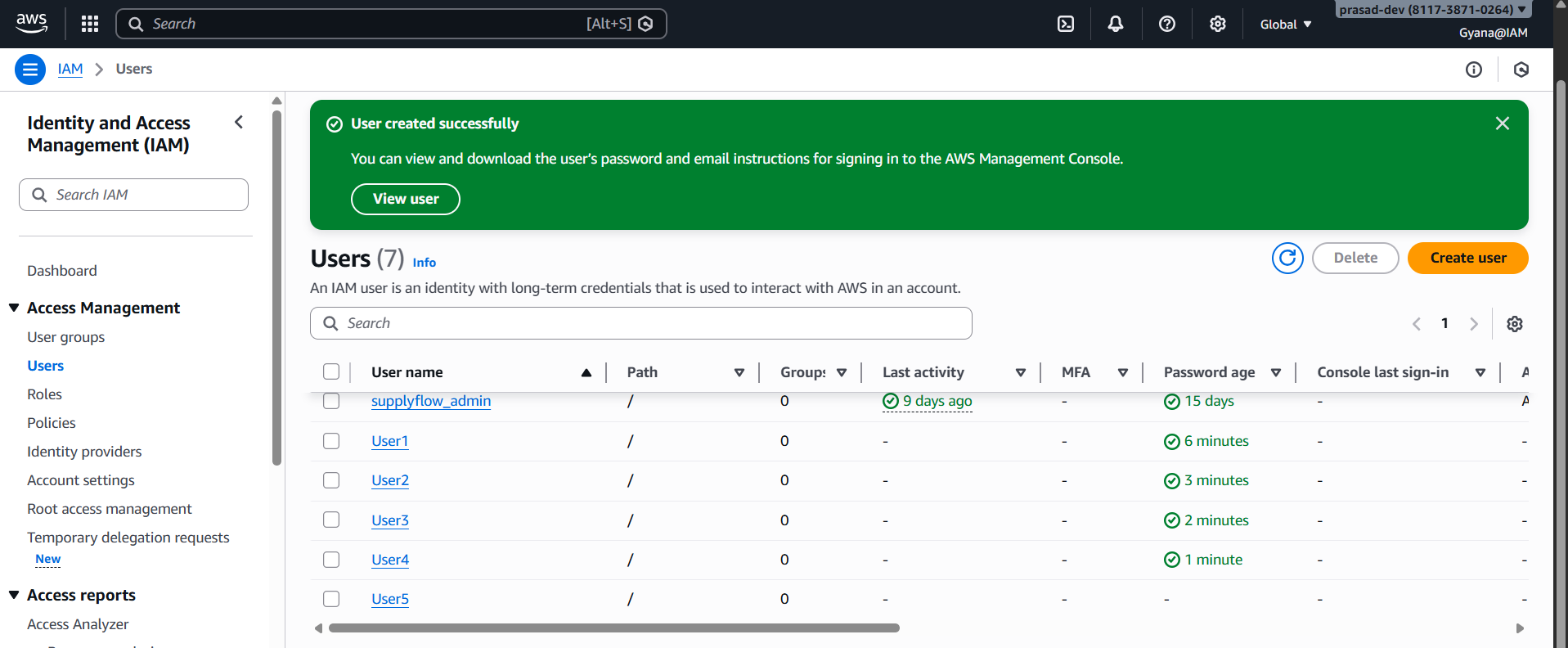
10. Create a customer-managed inline policy.

11. Attach the inline policy to the user group and verify access to the service.

12. Attach the inline policy to an individual user and verify access to the service.

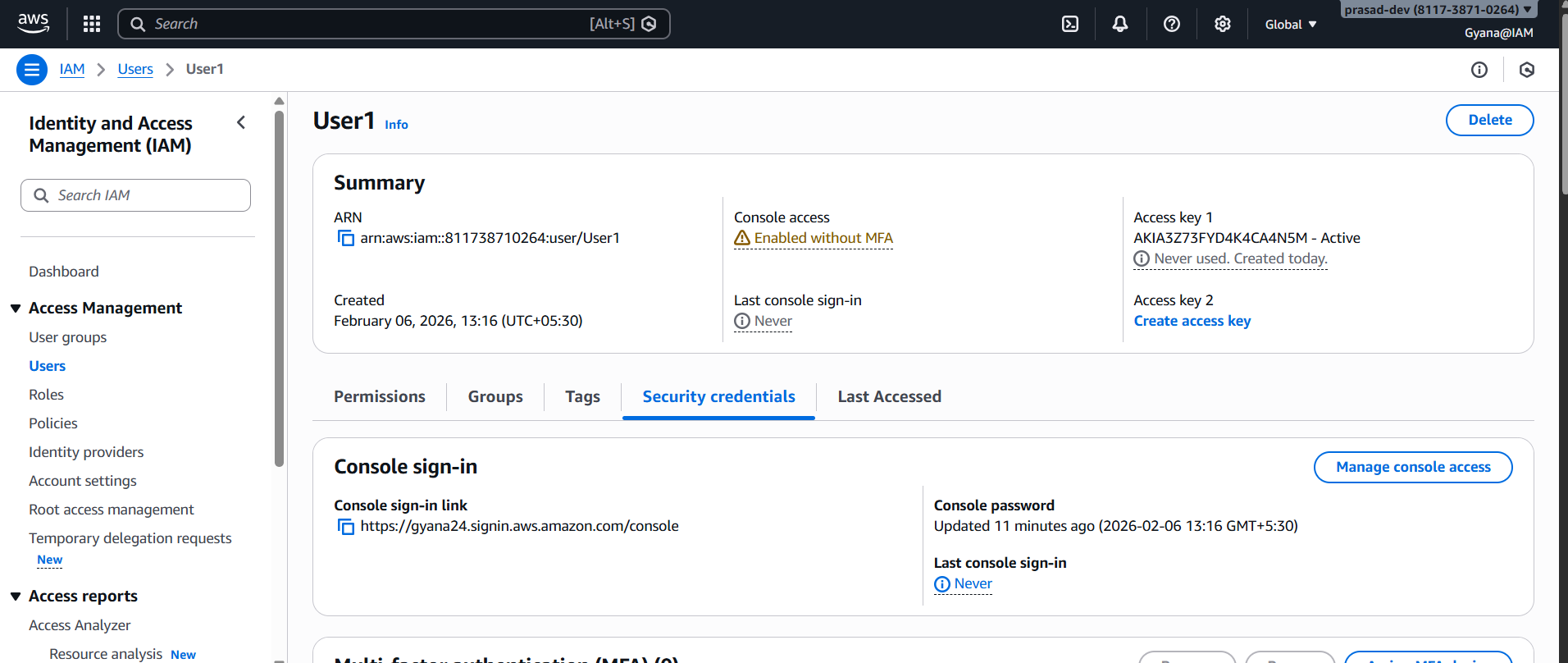
**Doing**

1. Create five IAM users.

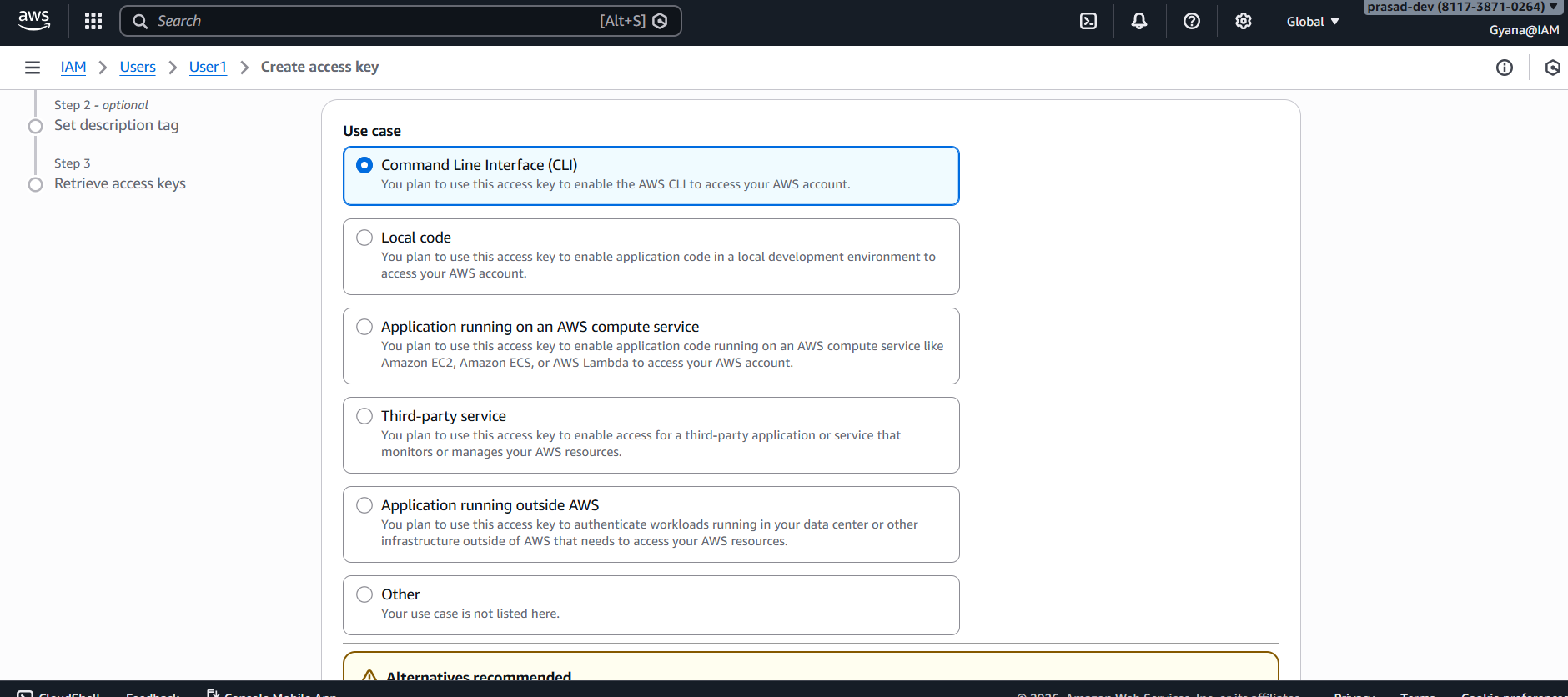
****

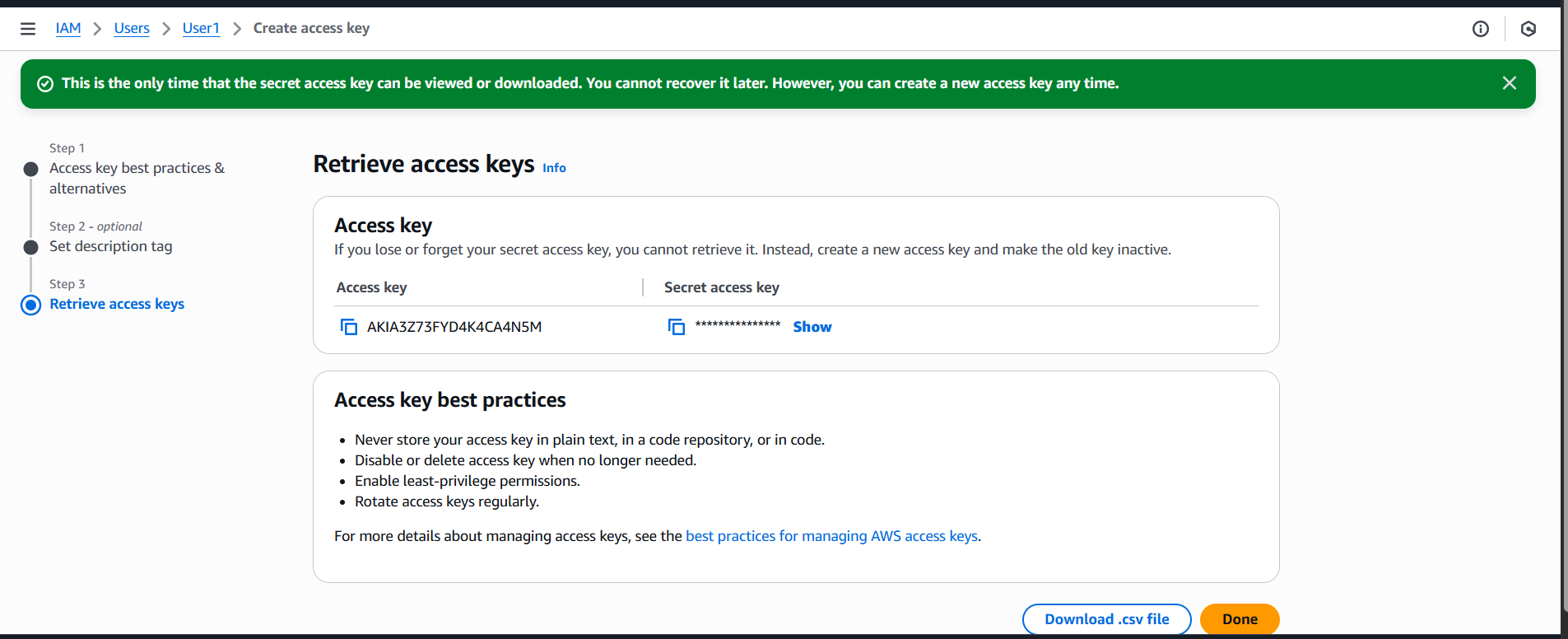
**Five users has been created User1, User2, User3, User4, User5**

1. **Generate programmatic access keys for the users.**

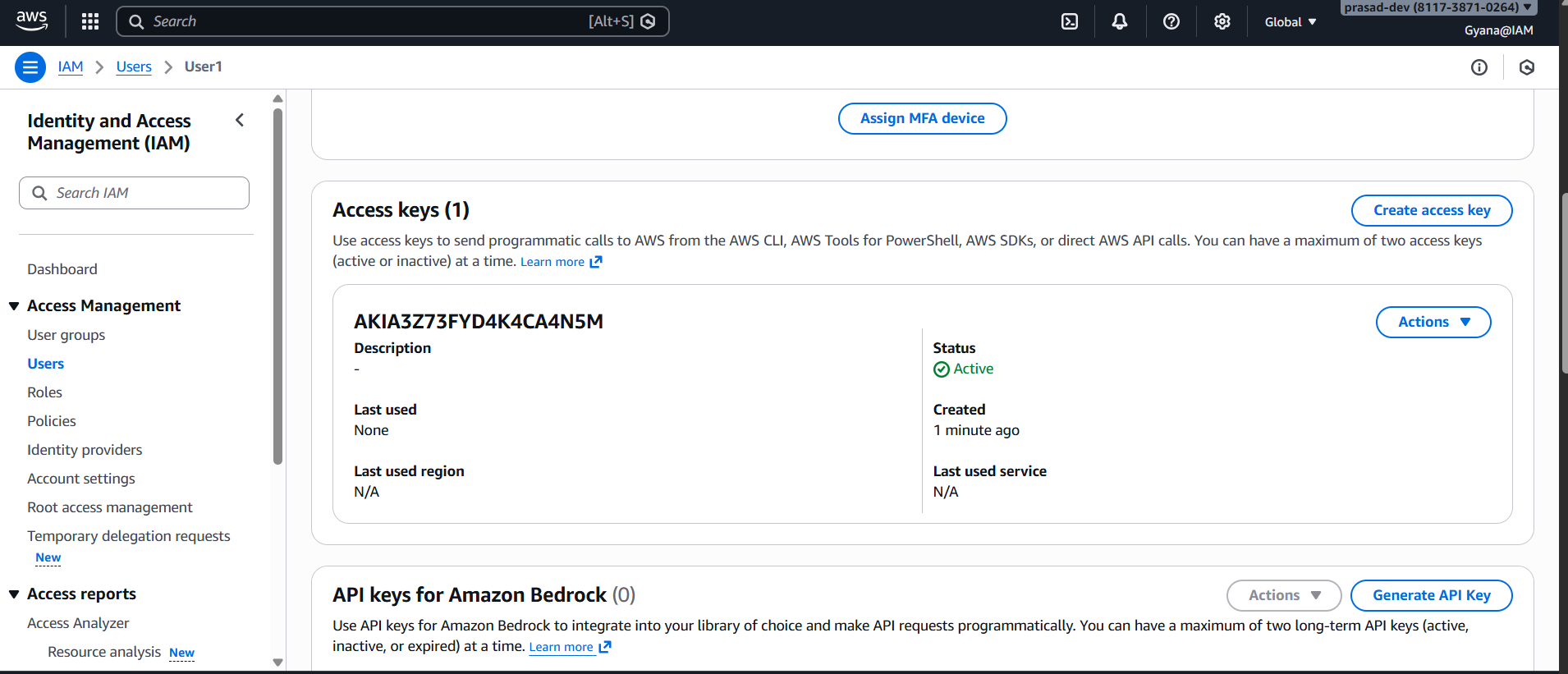
****

**User the Security Credentials we can generate programmatical access keys.**

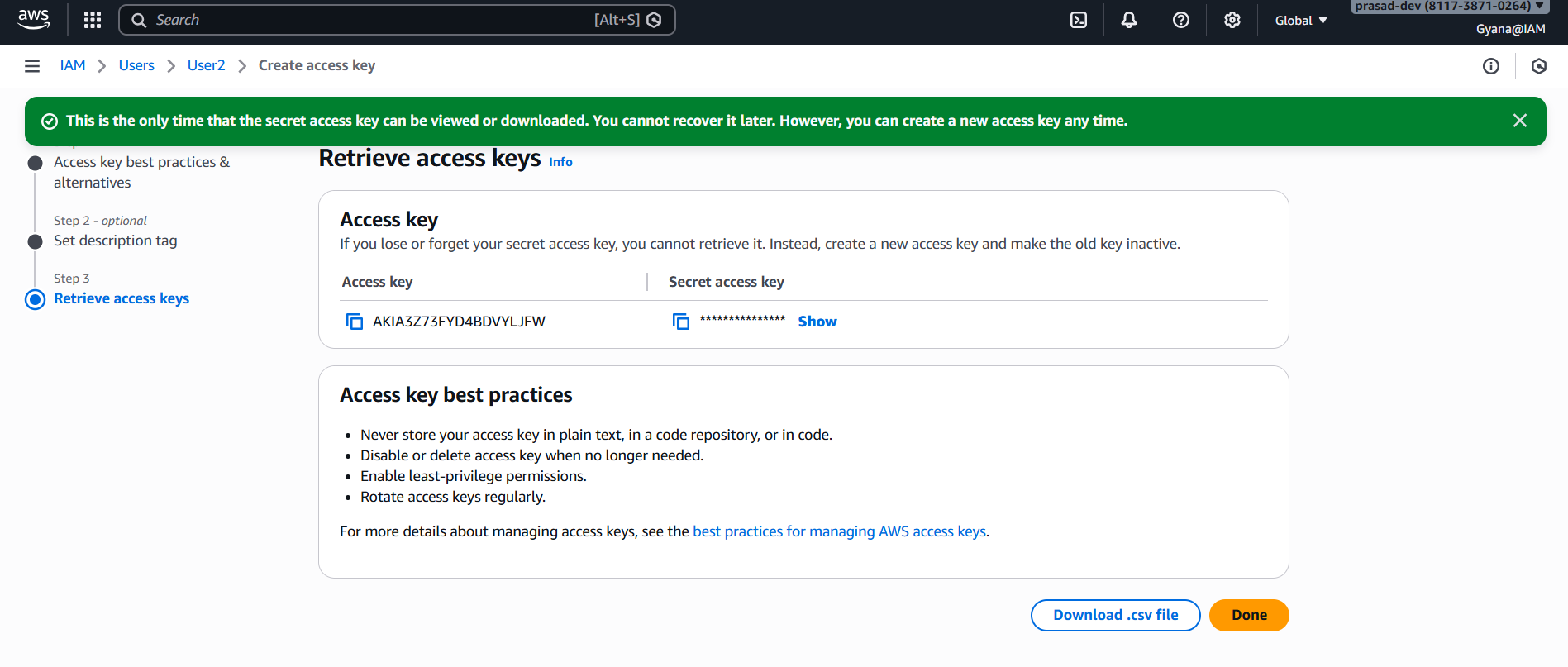
****

****

**Keys have been created successfully.**

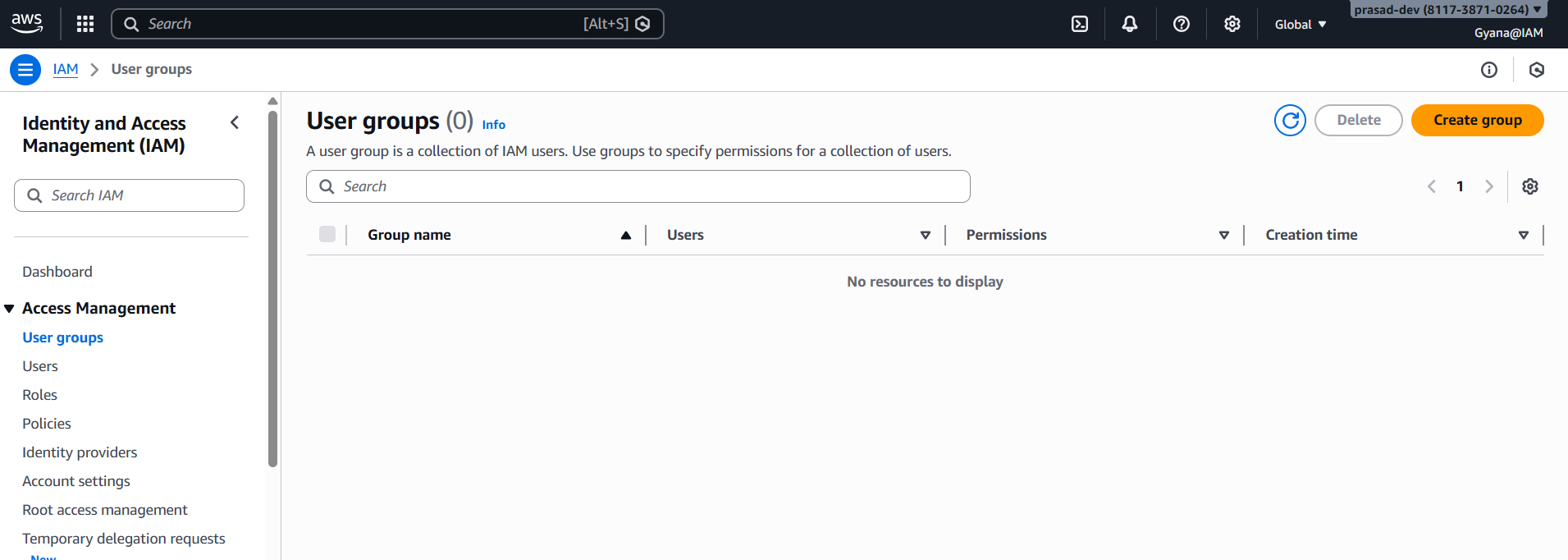
****

**Created keys for all the other users.**

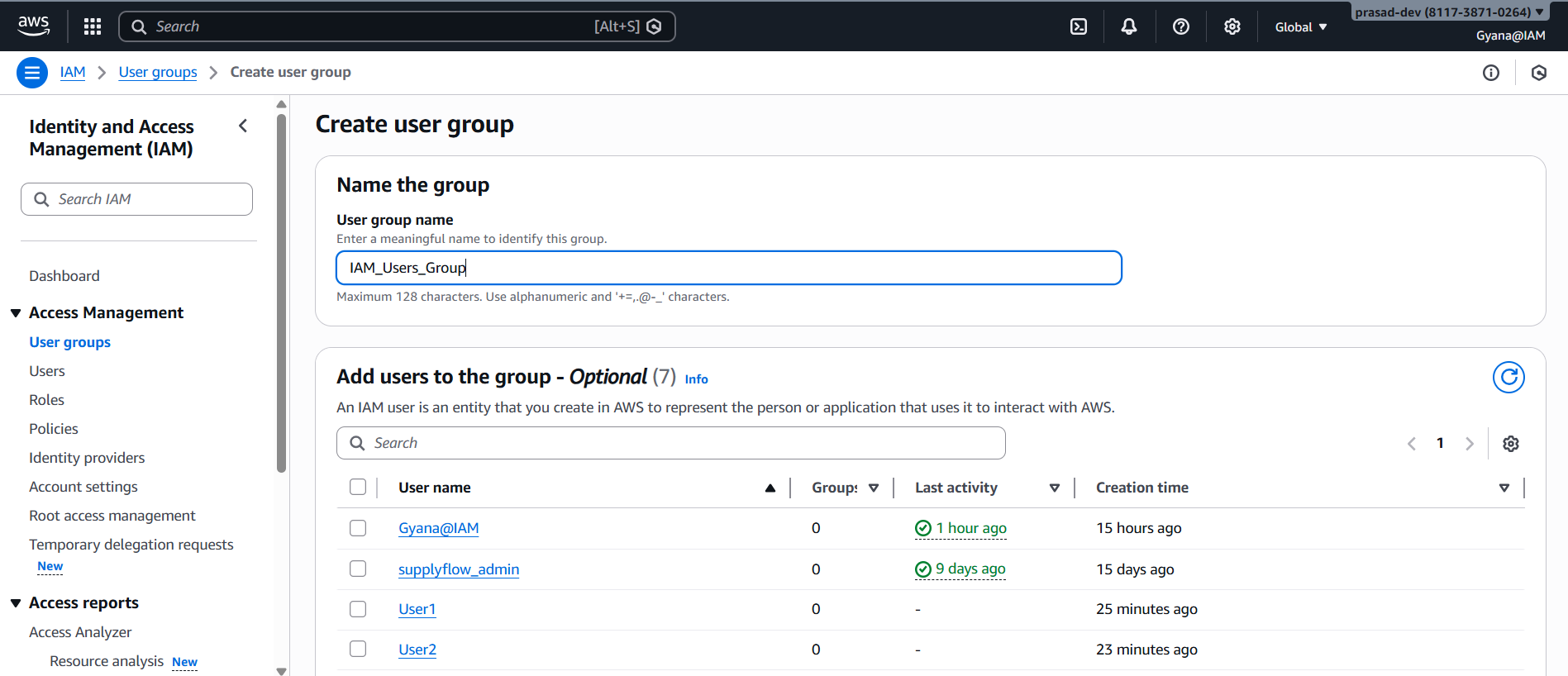


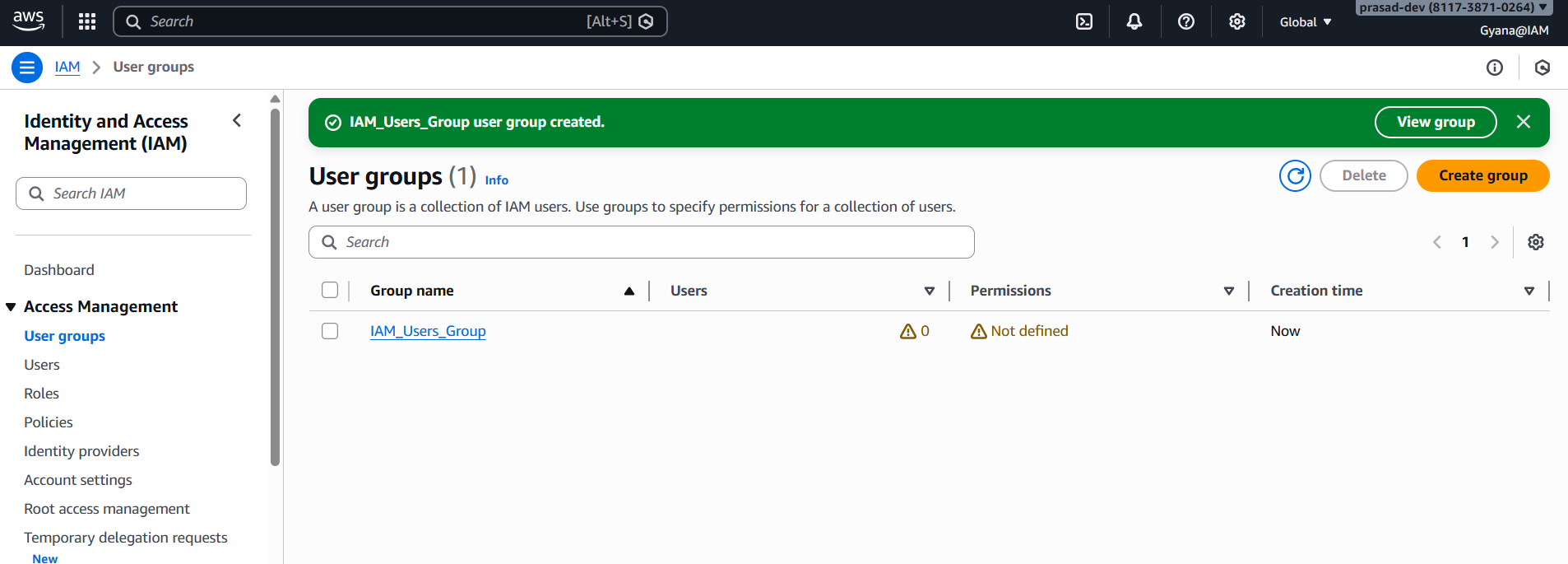
1. **Create an IAM user group.**

**Under user group section creating a IAM user group.**

****

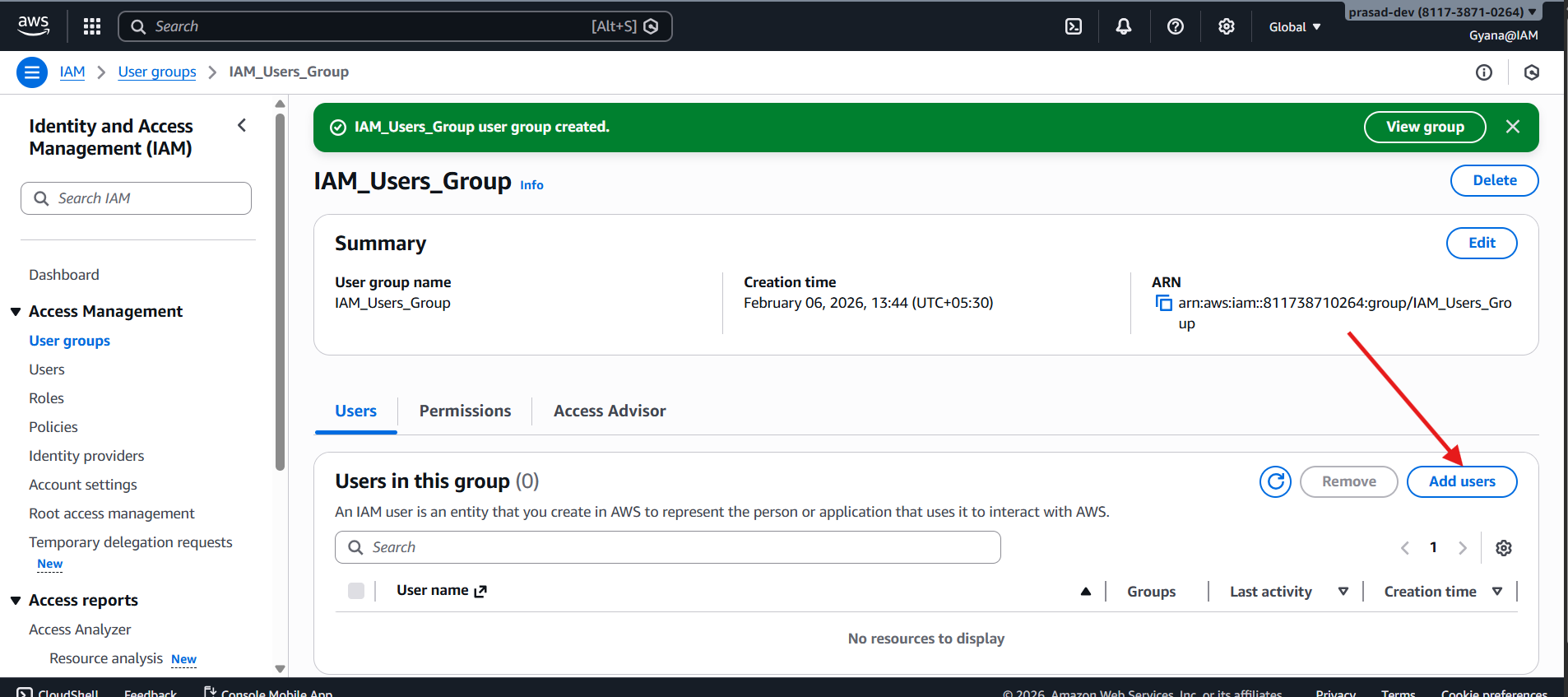
**Creating a group name as IAM\_Users\_Group we can add the user directly from here or can add later.**

****

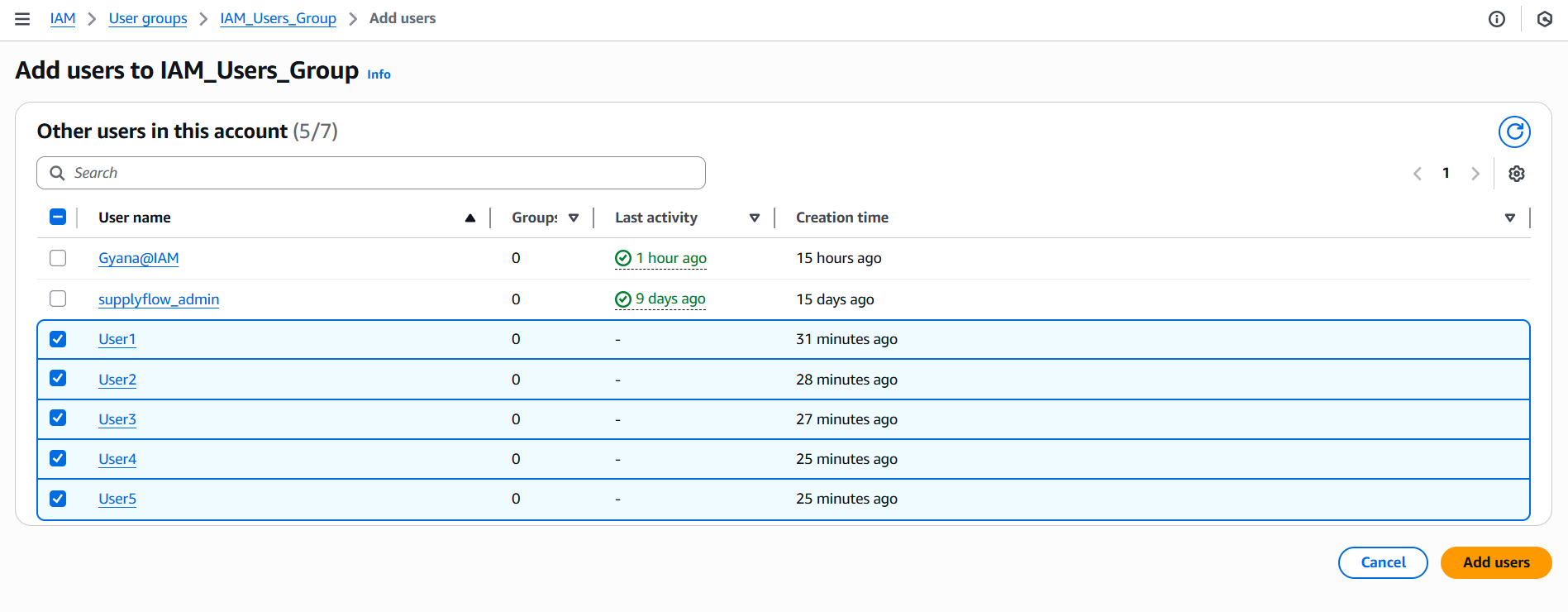
****

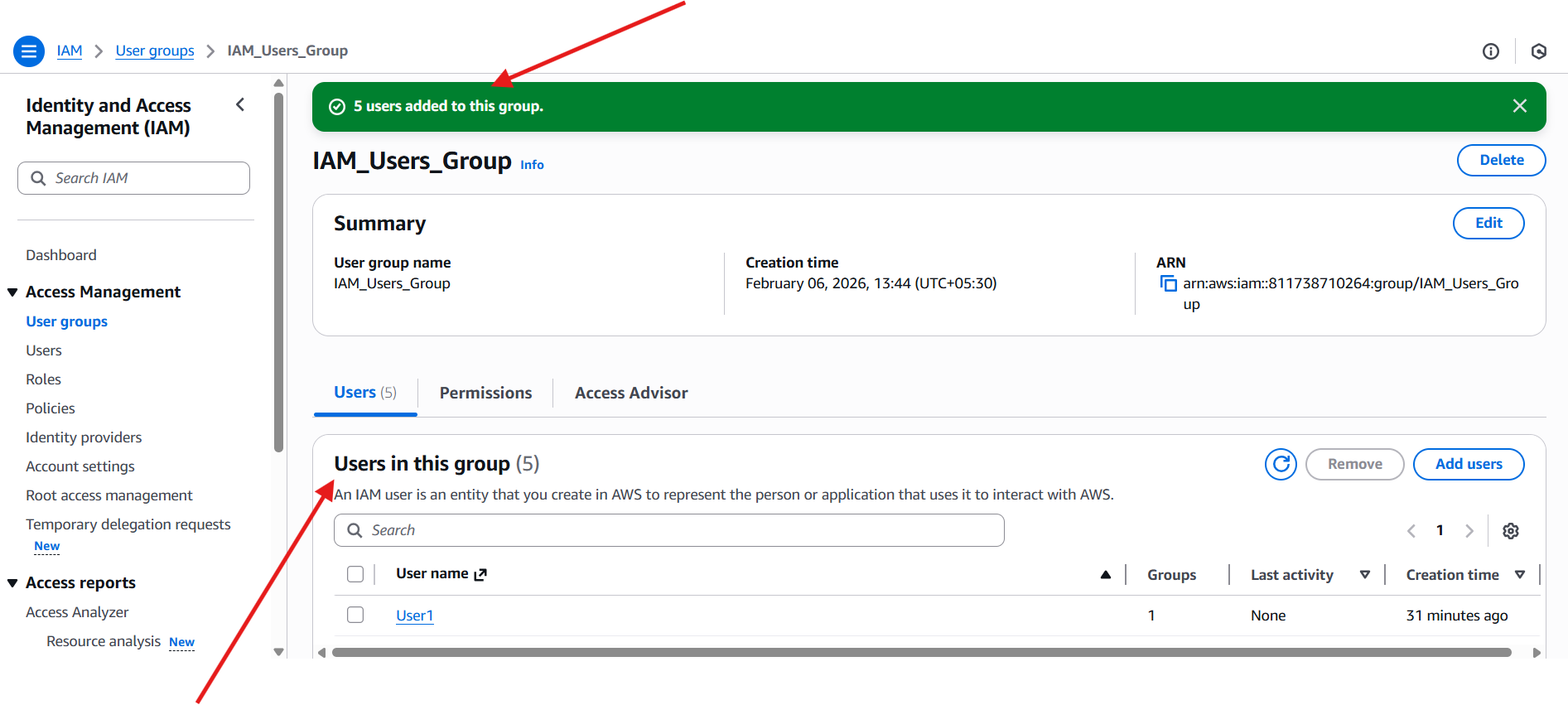
**Group created.**

1. **Add the five IAM users to the user group.**

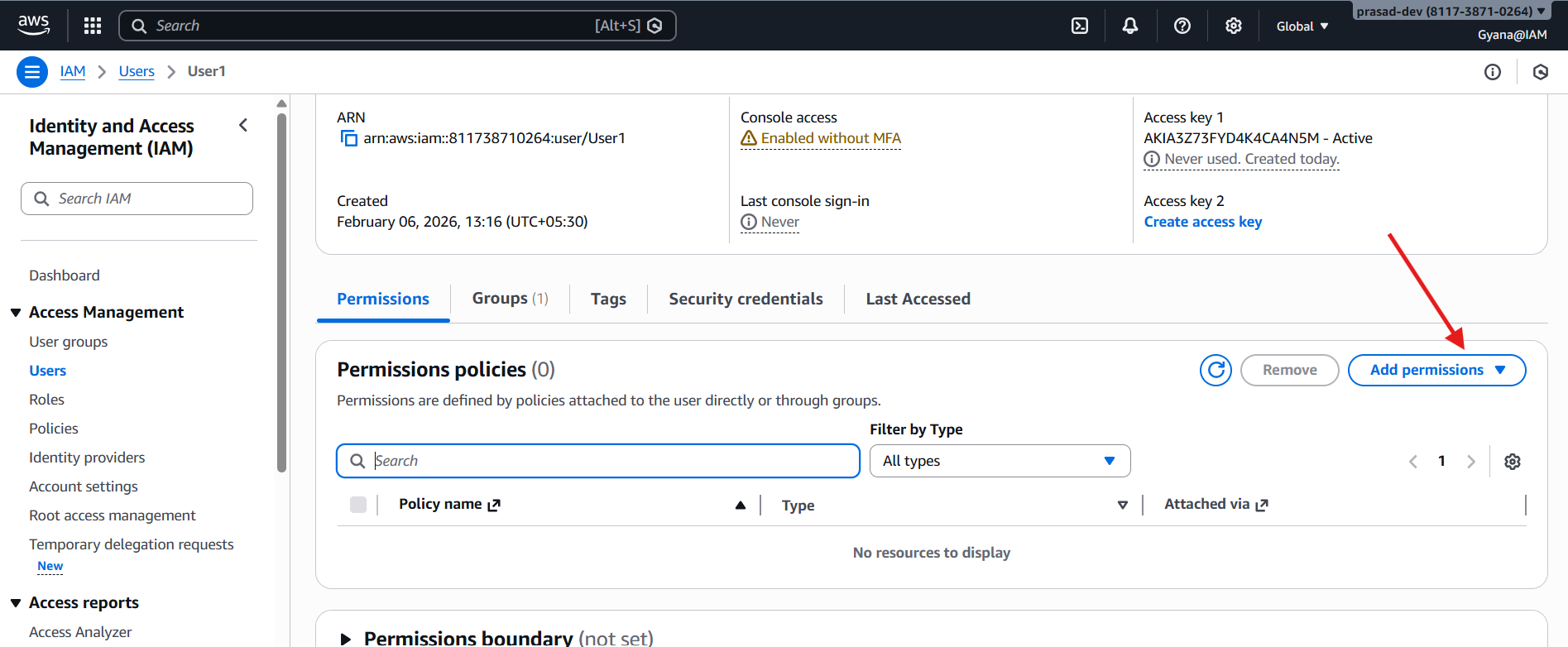
****

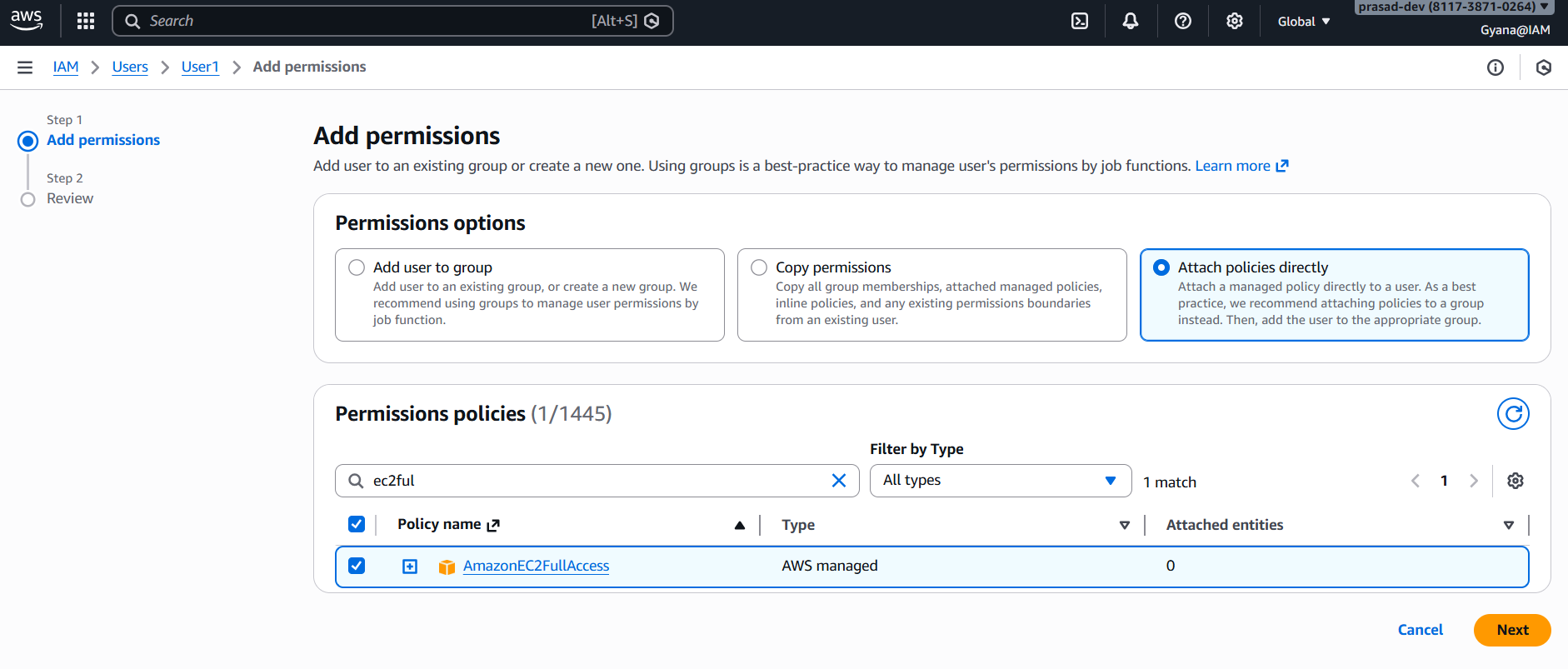
**In the group adding the 5 users using that Add users button.**

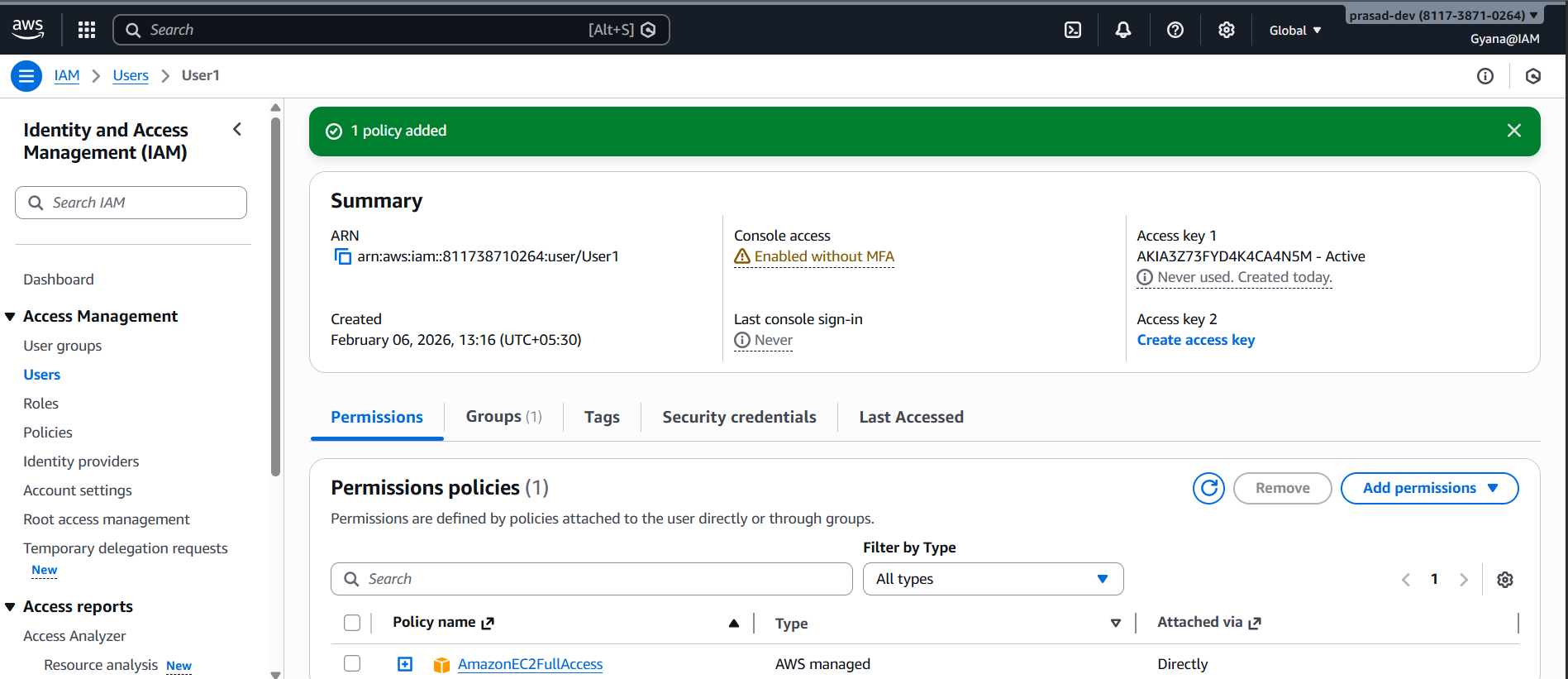
****

****

1. **Attaching one policy (EC2 Full Access) to a User1 IAM user.**

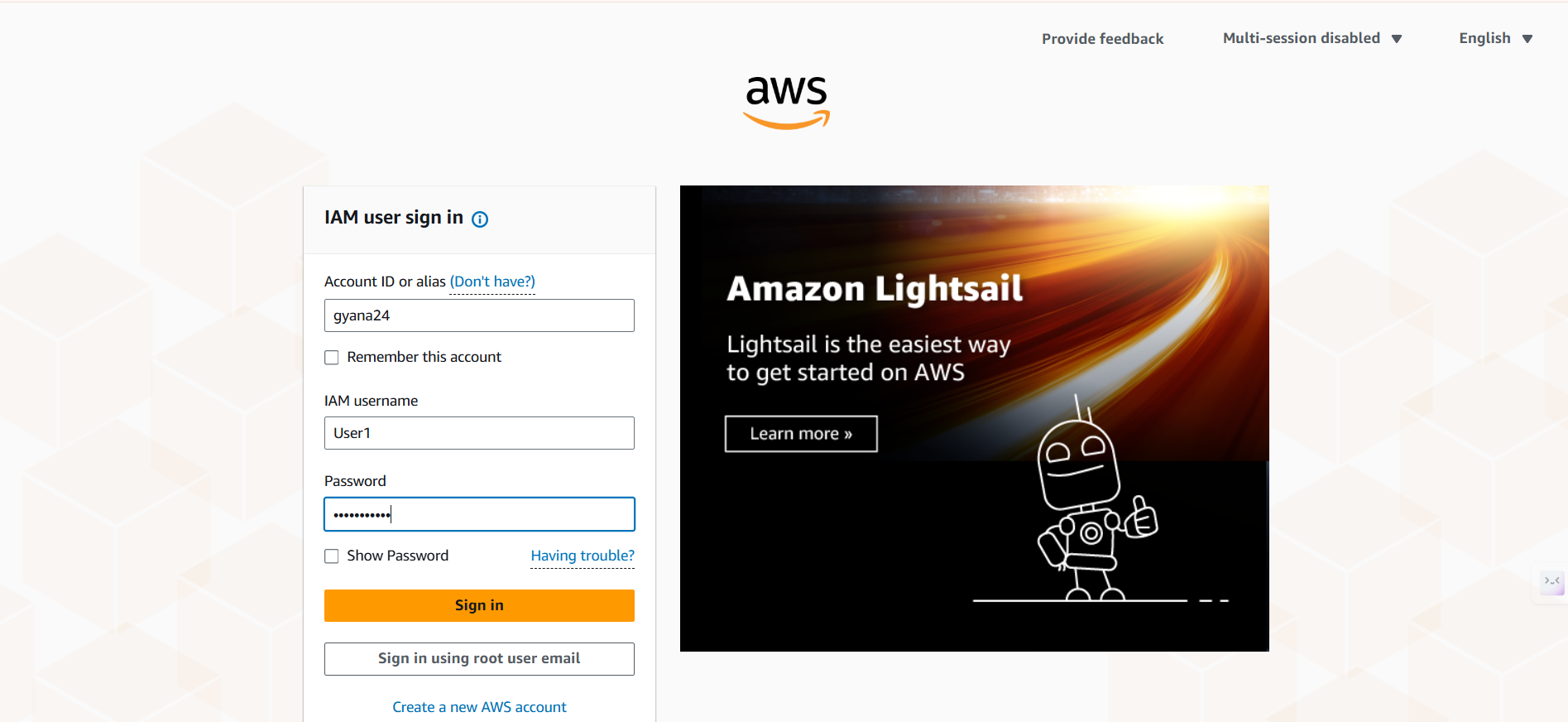
****

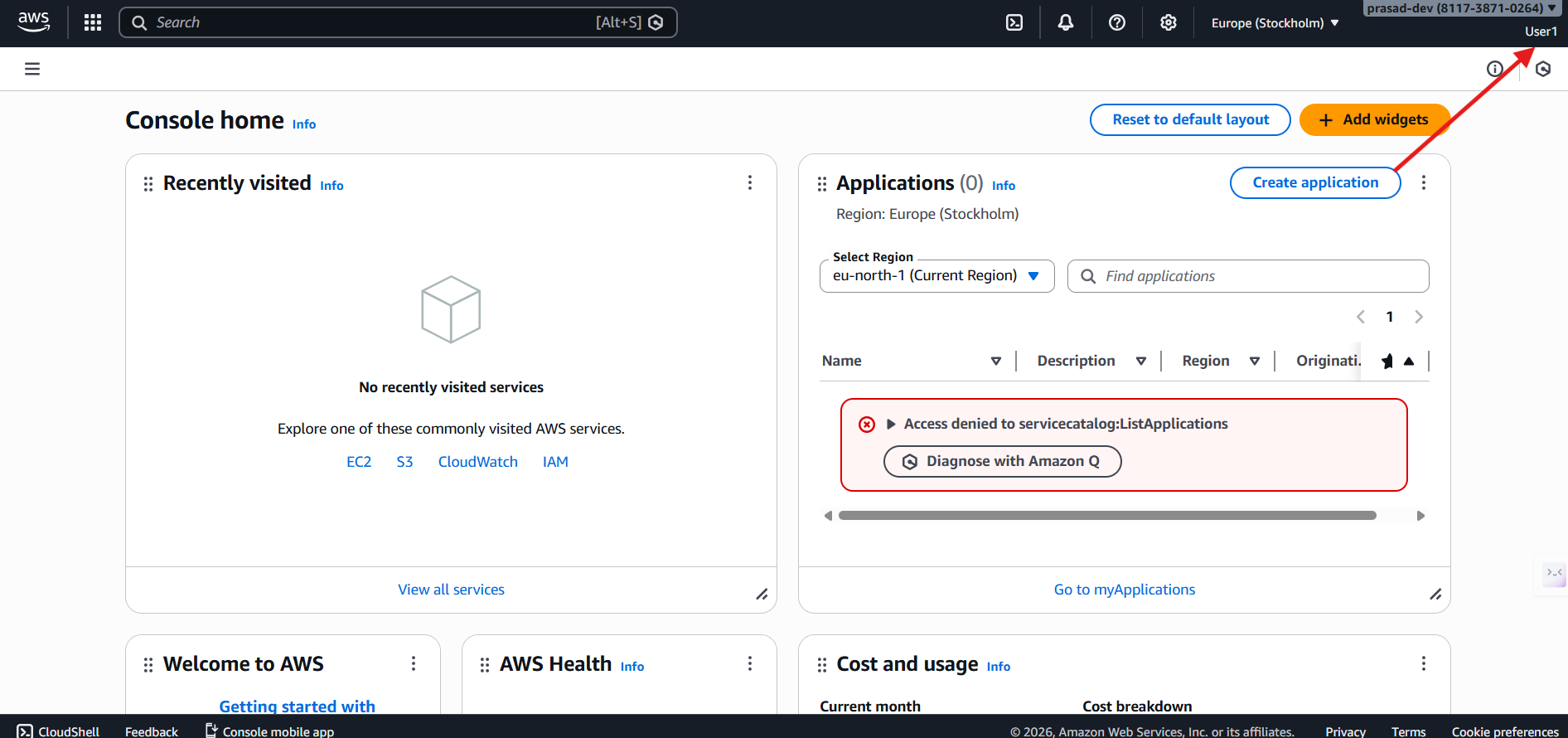
****

****

**Polici added to the User1 IAM.**

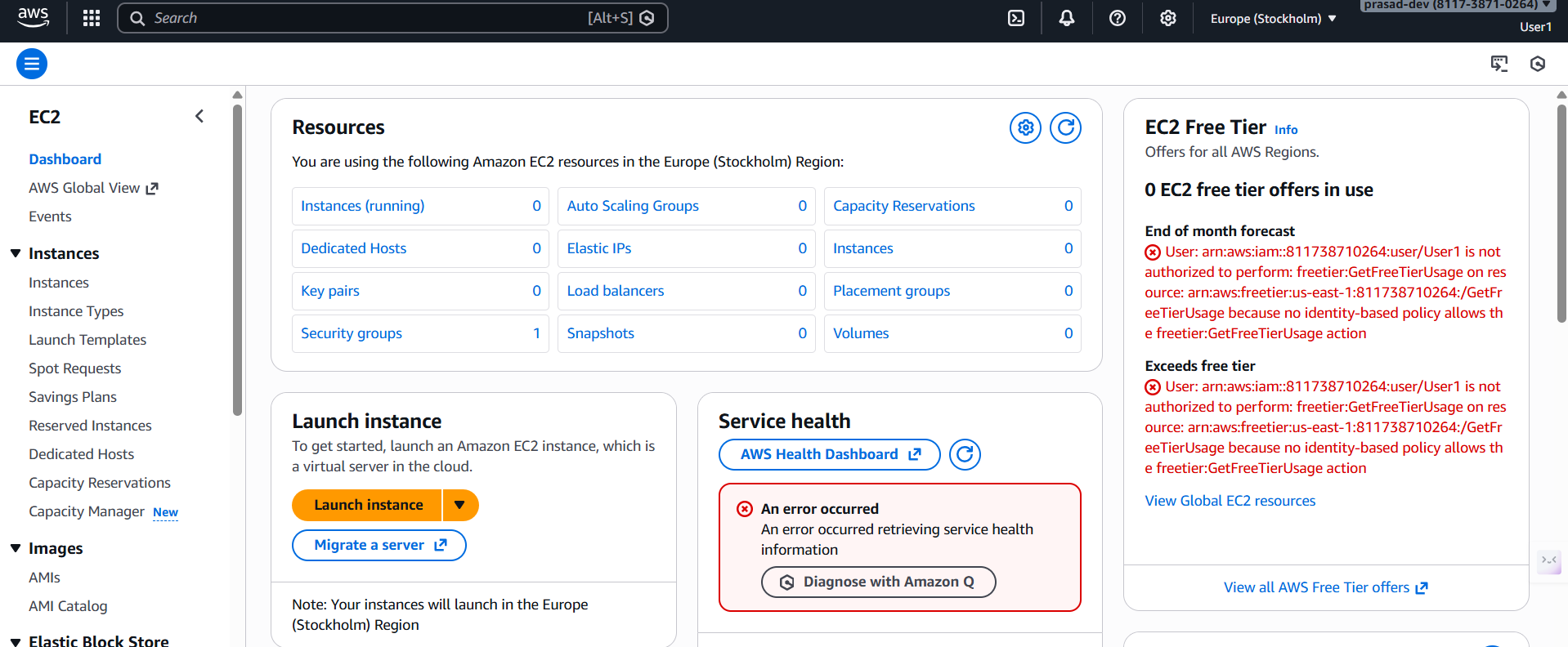
1. **Log in as the user using the AWS Management Console URL, username, and password.**

****

****

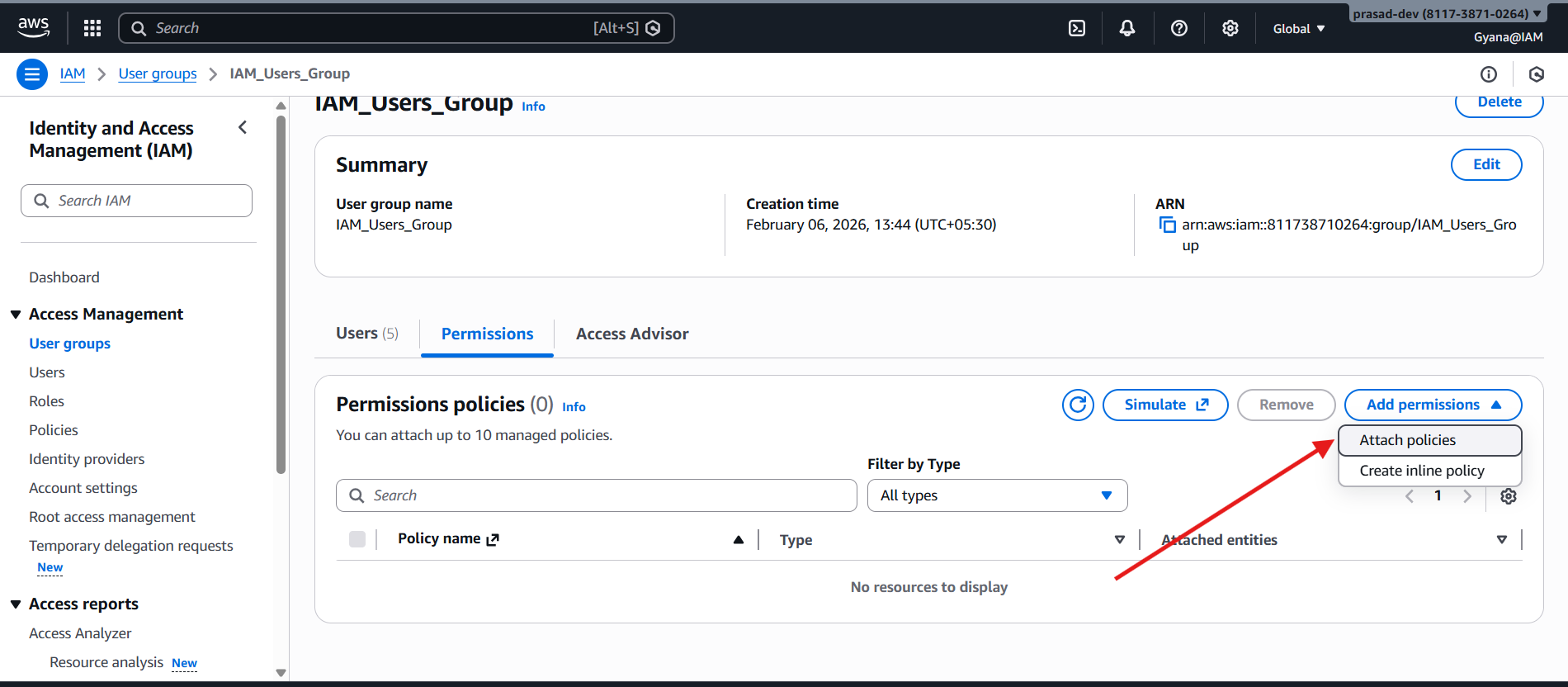
**Logged in to User1 account.**

1. **Verify the EC2 Full Access permissions assigned to the user.**

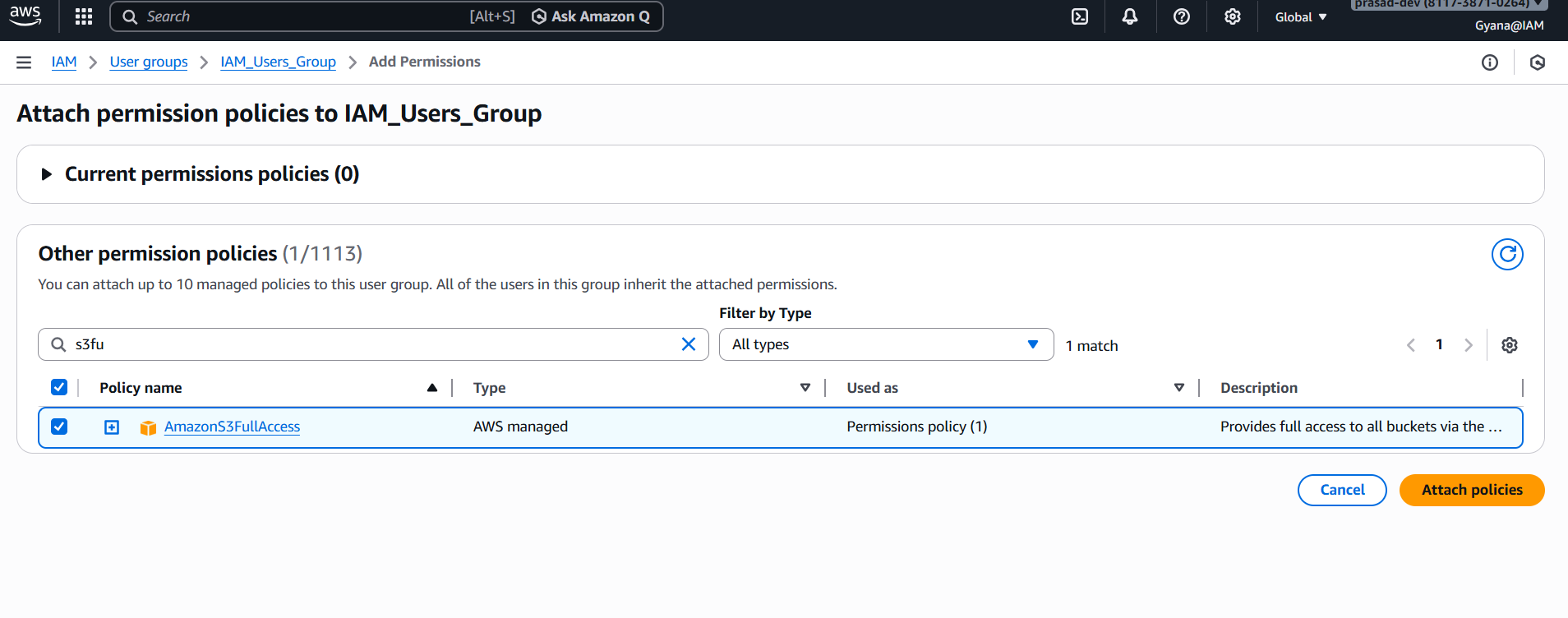
****

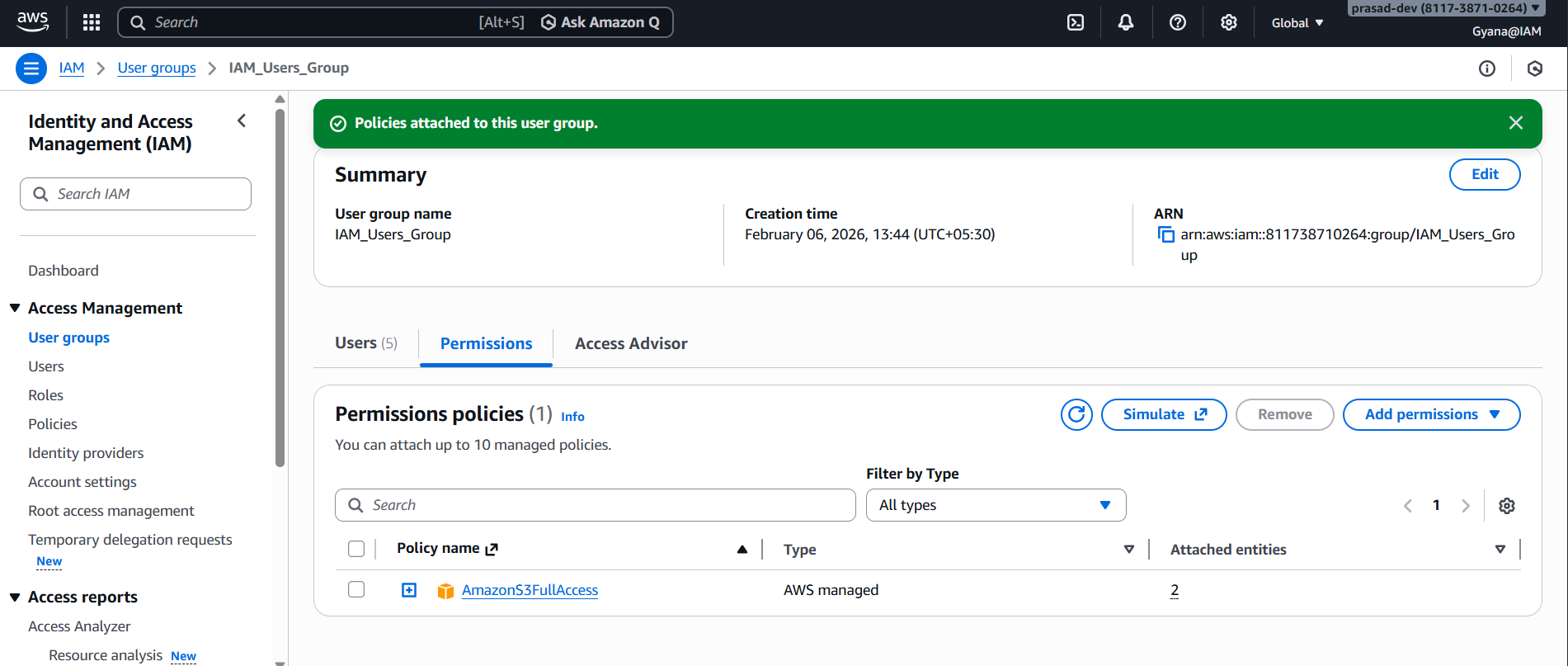
**We can access EC2 in the User1 account as the permission given.**

1. **Attach one policy (S3 Full Access) to the user group.**

****

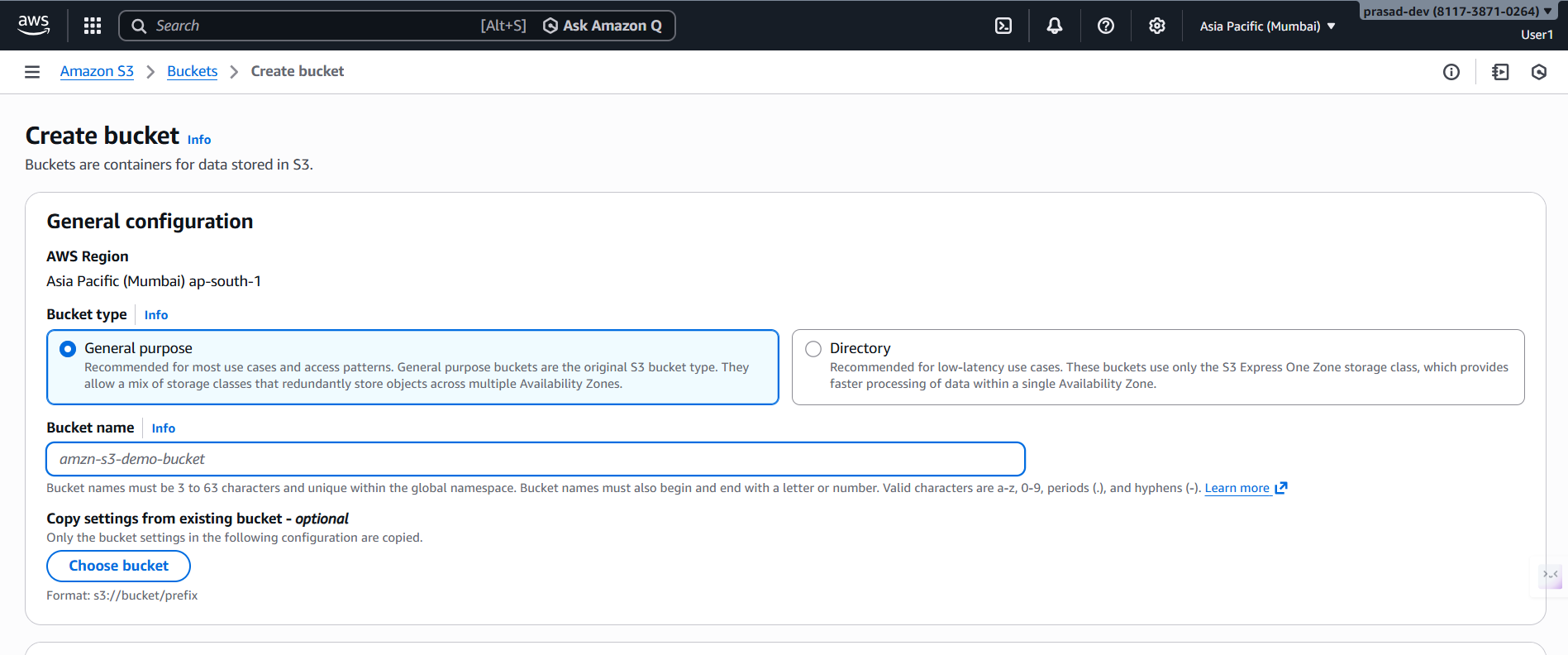
**Click on Attach Policies(AWS Managed policy) under the Add Permissions button in the permission section of IAM\_Users\_Group.**

****

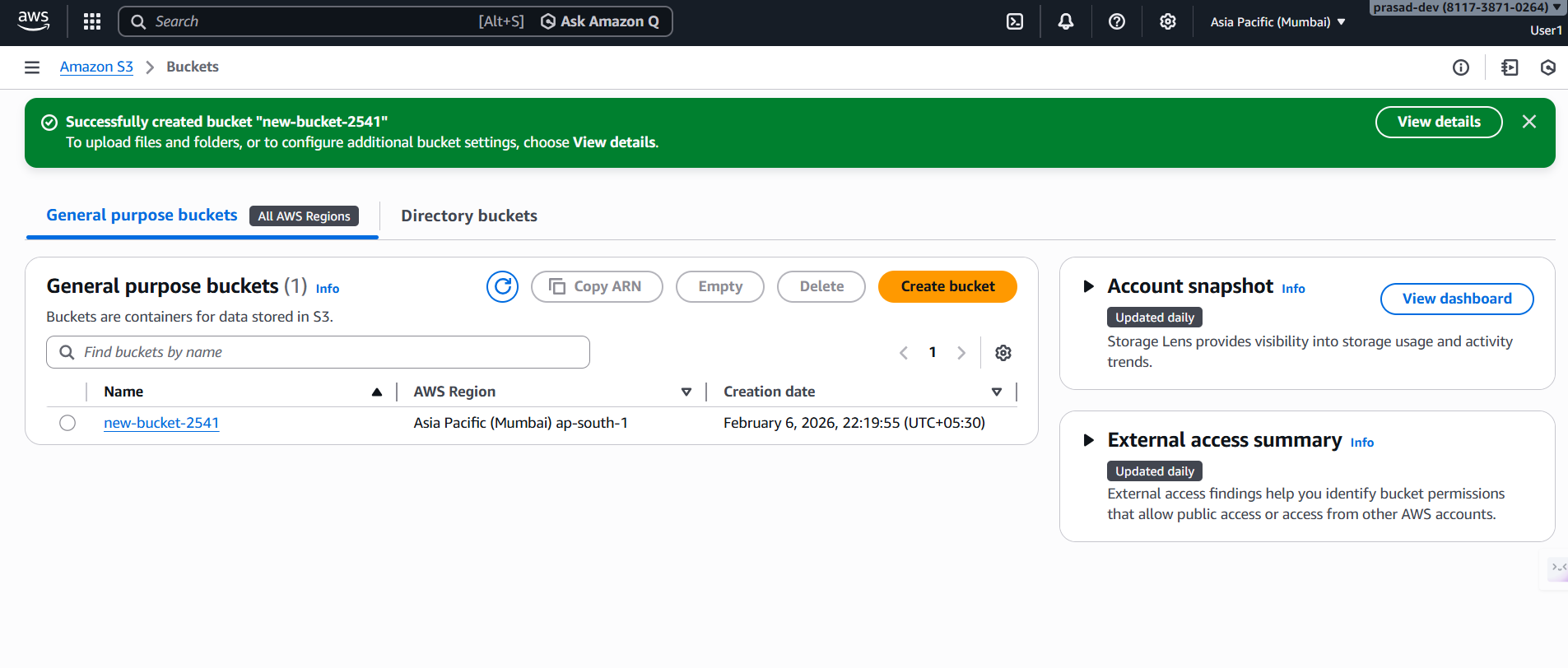
****

1. **Verifying that all users in the group can access the S3 service based on the assigned policy.**

**Creating S3 Bucket.**

****

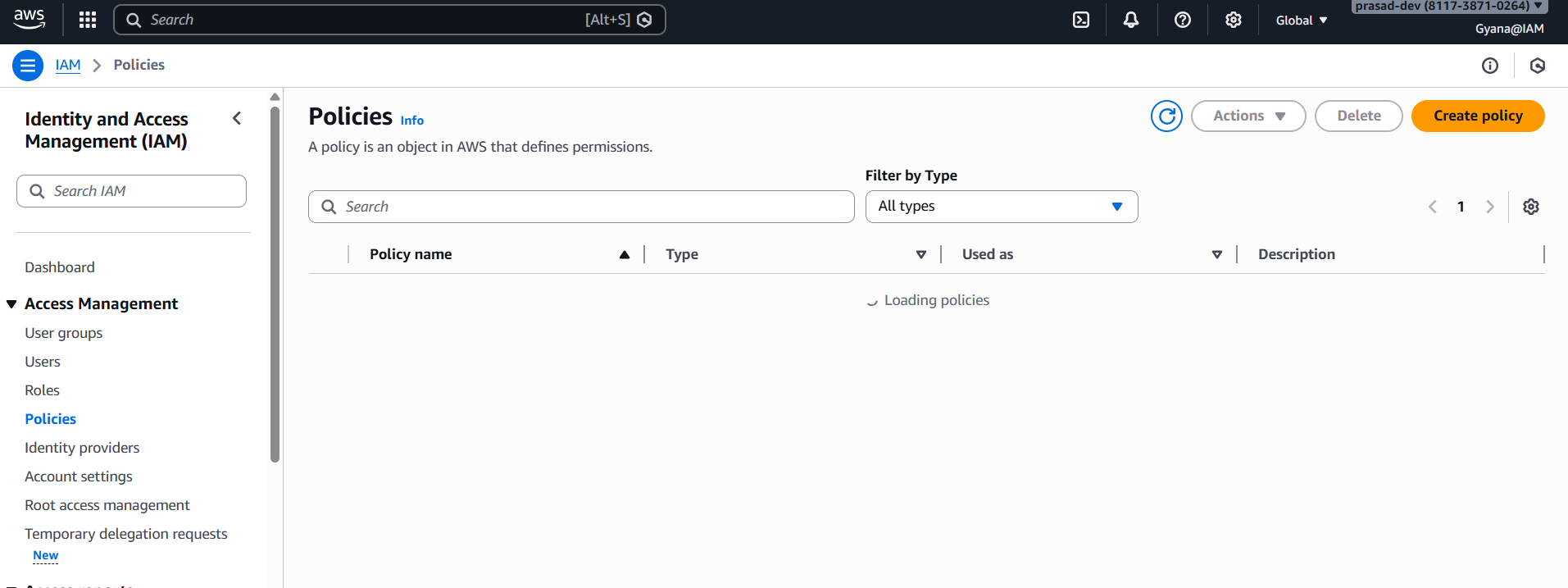
**User created successfully in User1.**

****

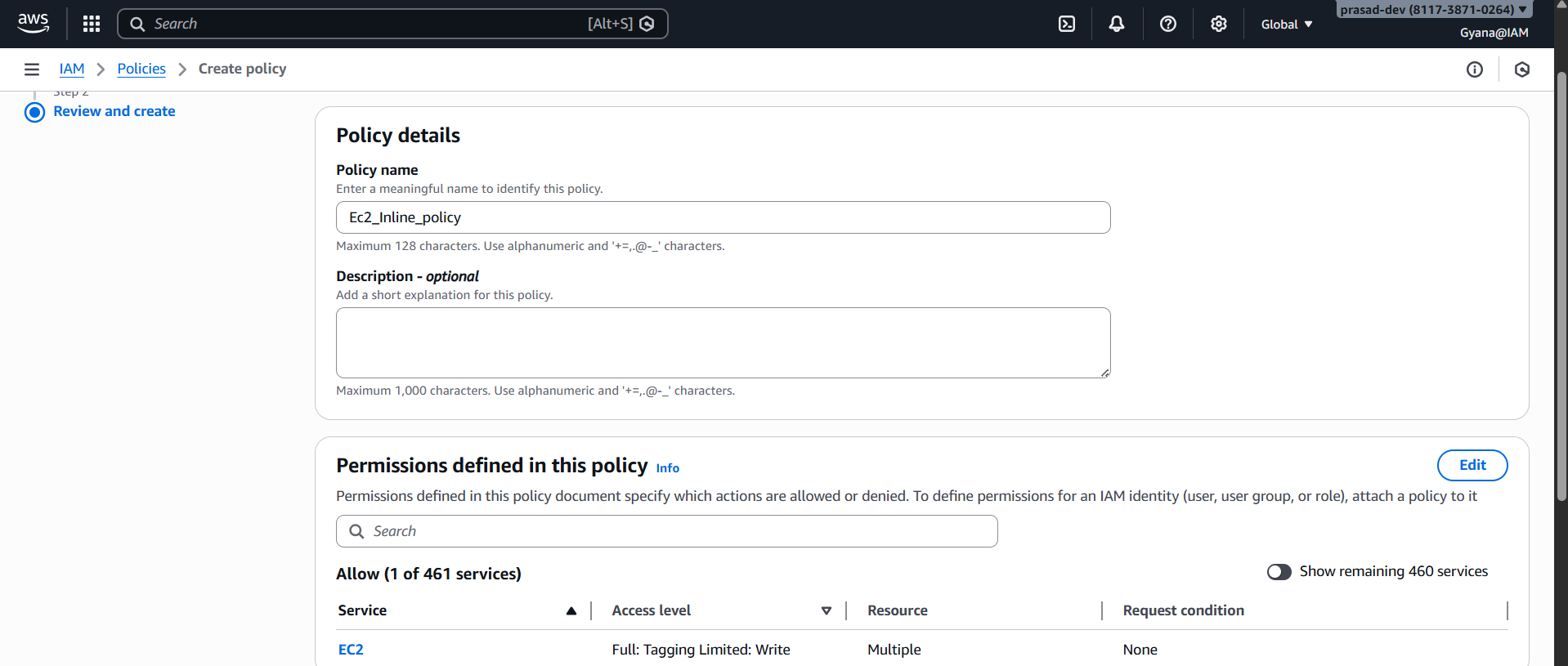
**Same like in other user its creating the buckets.**

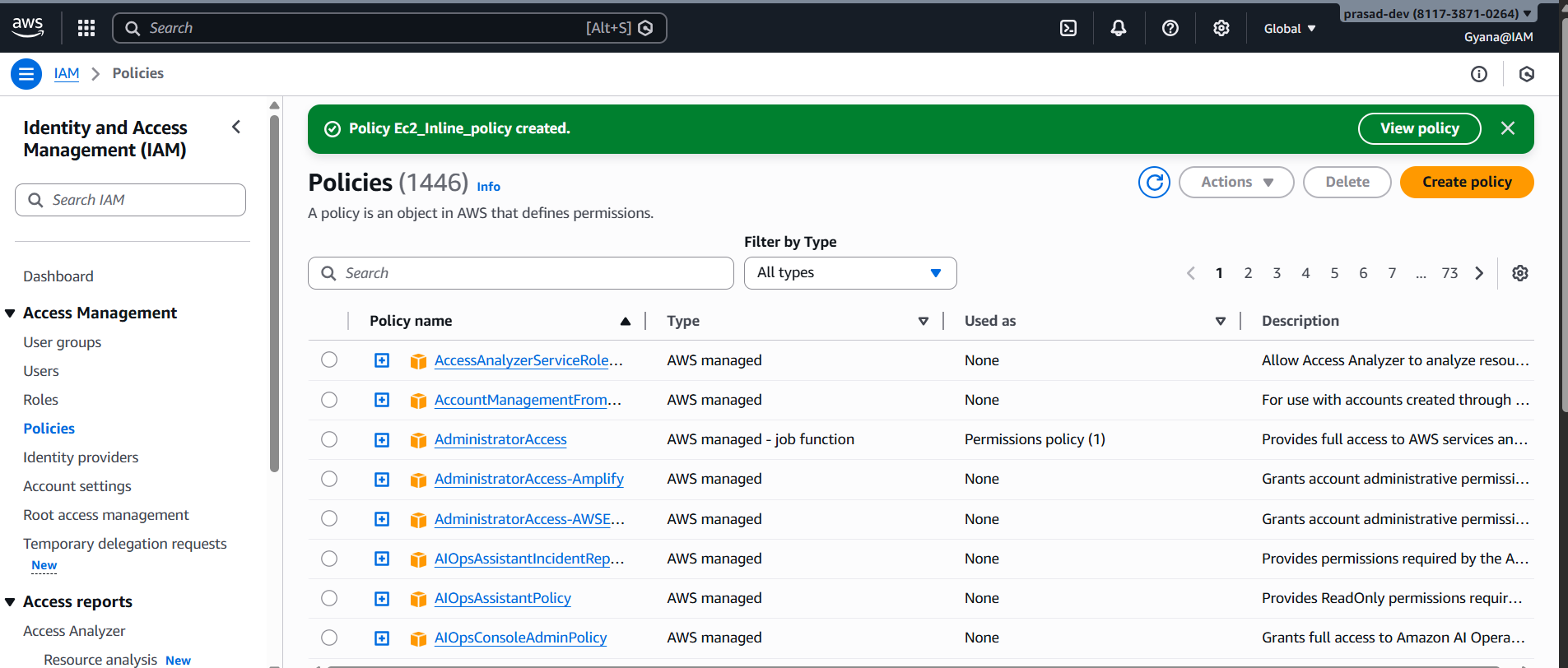
1. **Create a customer-managed inline policy.**

* **By using the Create policy we can create customer edit policy.**

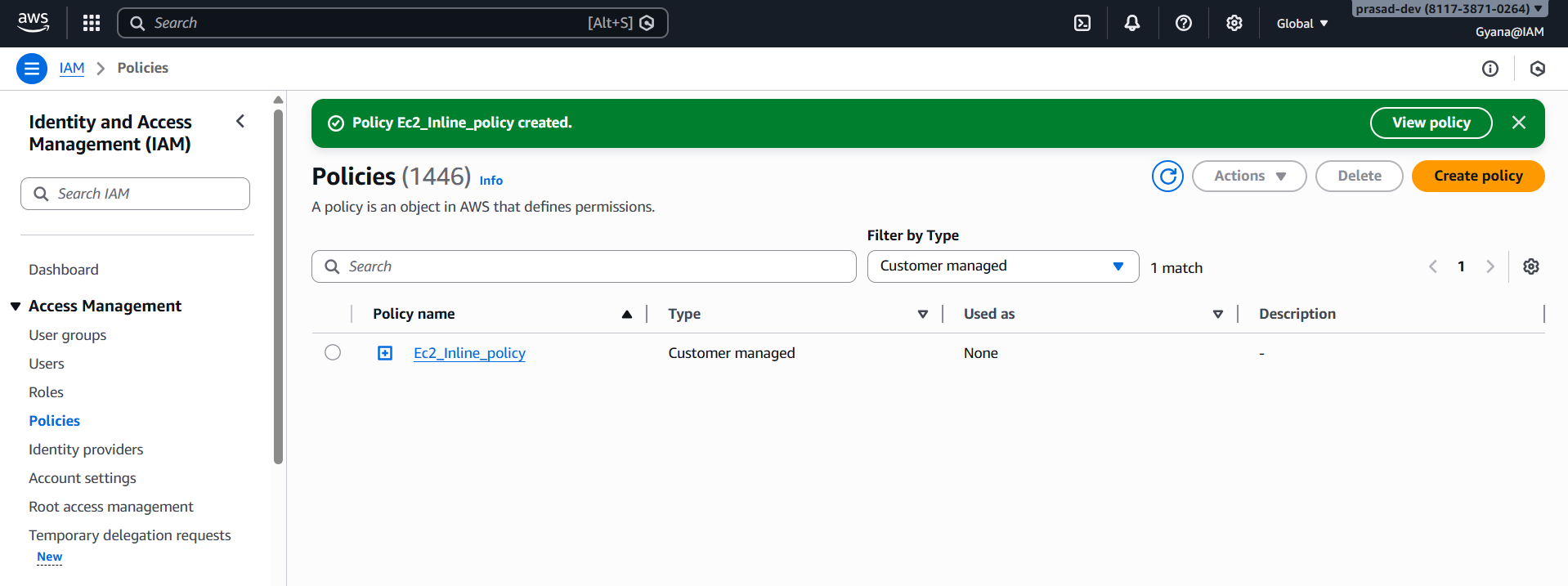
****

**Creating Policy**

****

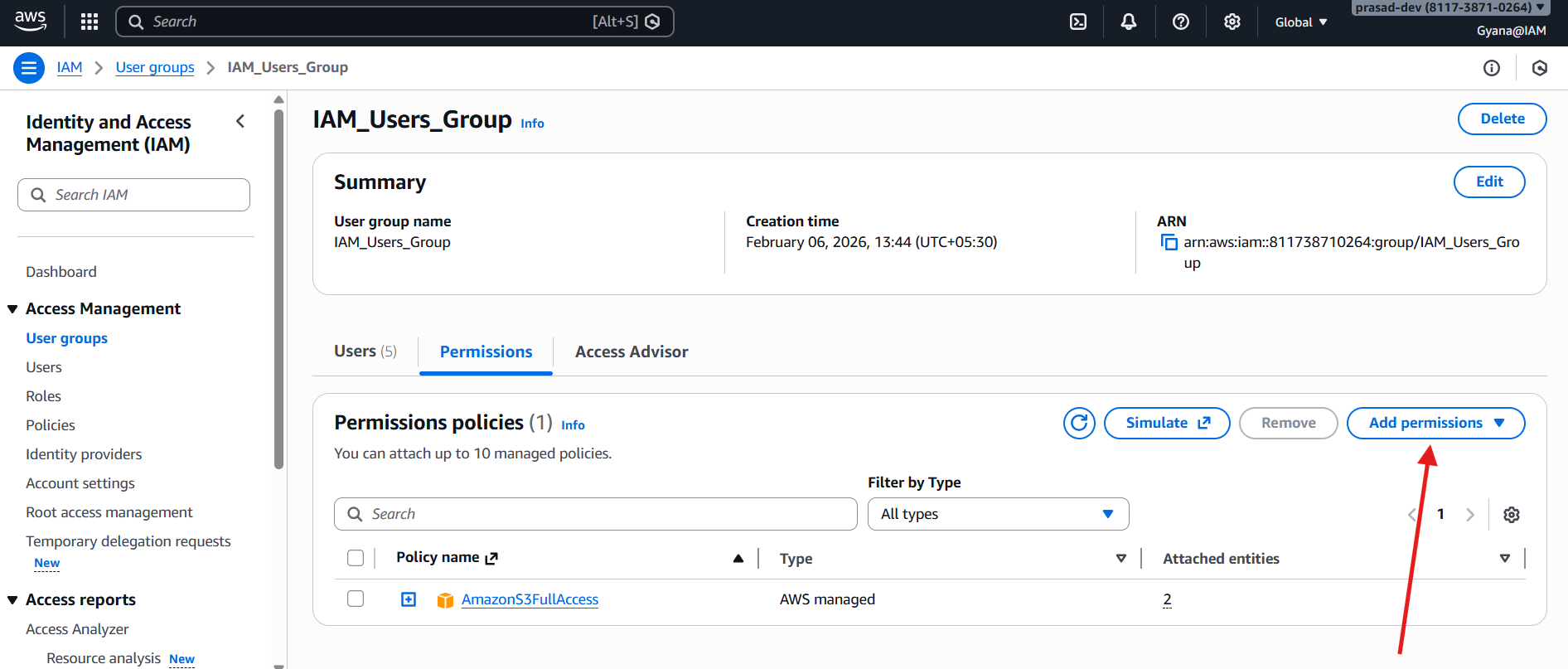
****

**Inline policy named EC2\_Inline\_Policy got created.**

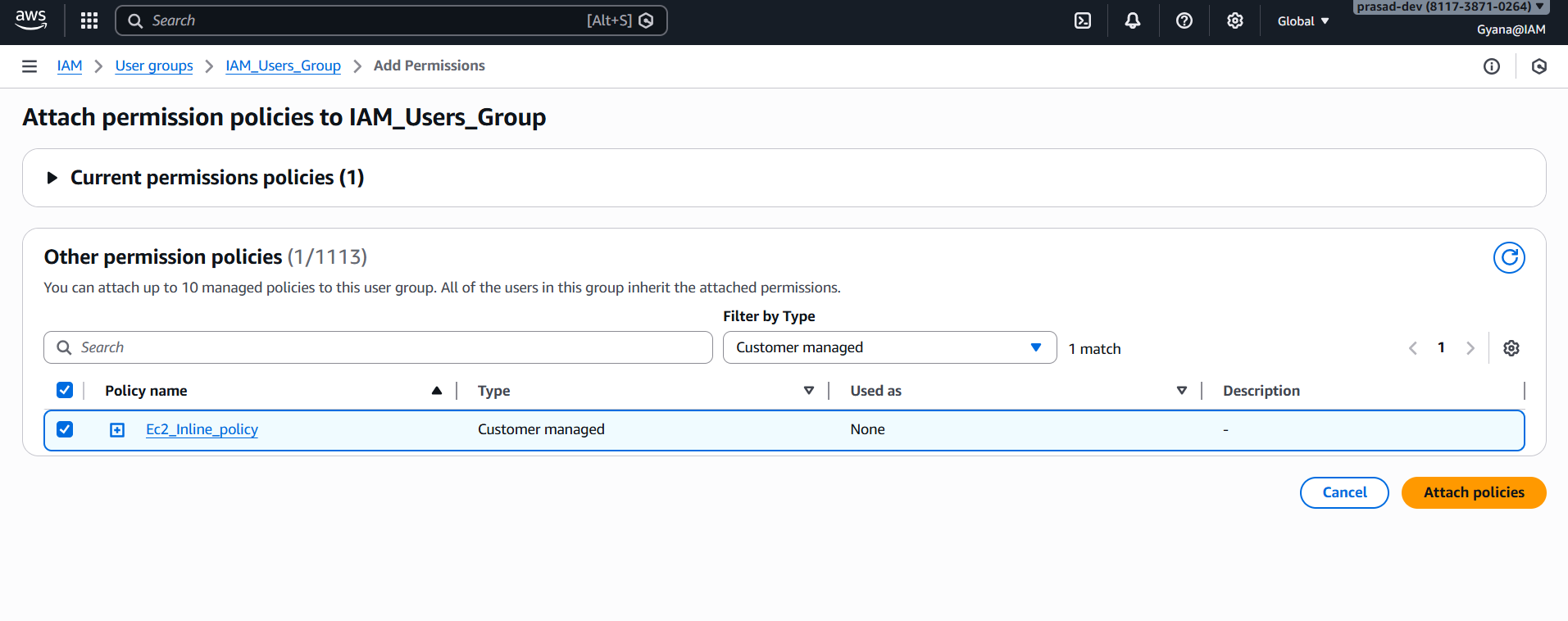
****

1. **Attaching the inline policy to the user group and verify access to the service.**

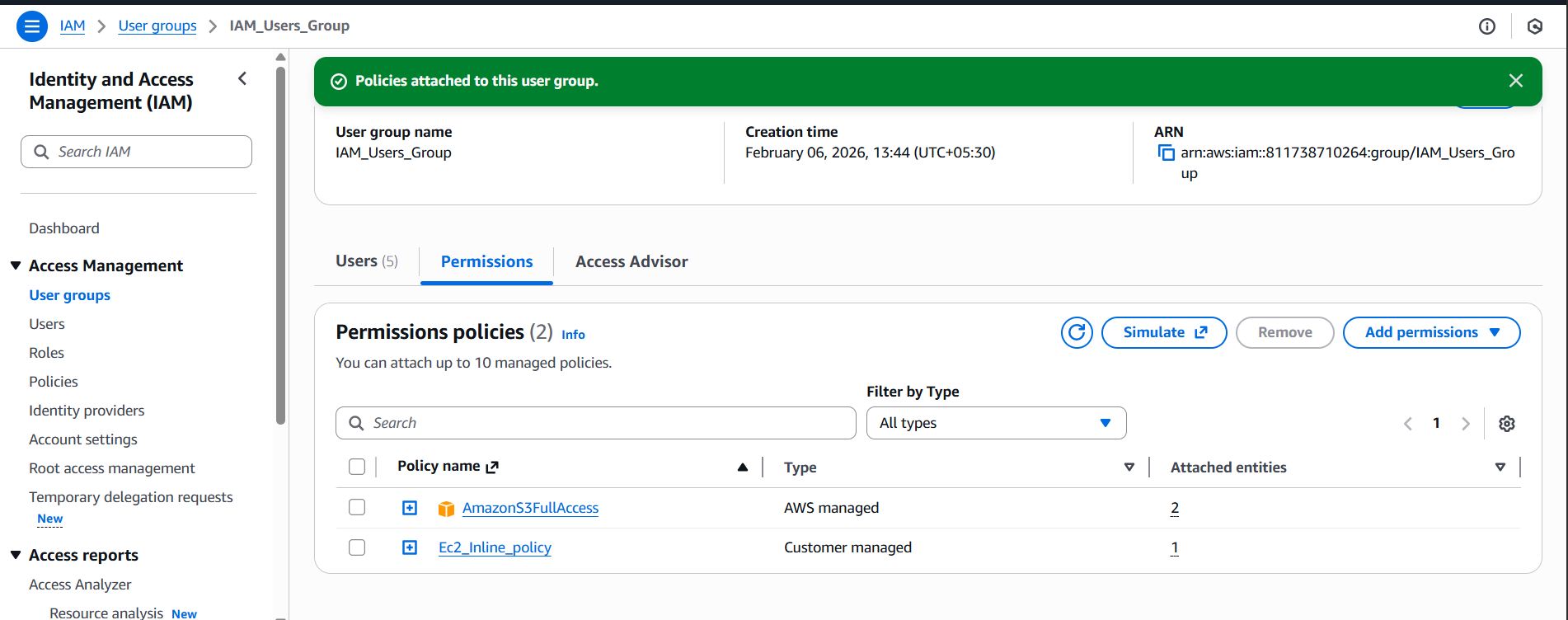
* **Attaching the policy to group in the Add permissions section.**

****

* **Attaching the Customer managed inline policy.**

****

* **Policy is Attached to the group.**

****