Aim:

To study and implement Identity and Access Management (IAM) practices on AWS.

Theory:

Identity and Access Management (IAM) is a crucial component of any cloud infrastructure, including Amazon Web Services (AWS). IAM plays a critical role in securing your AWS infrastructure by controlling access to resources and actions within your cloud environment. By following these best practices, such as using IAM roles, creating individual IAM users, enforcing strong password policies and enabling Multi-Factor Authentication (MFA), you can help to reduce the risk of unauthorised access to your AWS resources. Additionally, using AWS Security Token Service (STS) and IAM policies can further improve your IAM security posture.

AWS IAM allows you to control who can access your AWS resources and what actions they can perform on those resources. Here are some best practices for implementing IAM on AWS:

* Use the principle of least privilege:

Grant users and applications only the permissions they need to do their jobs. This reduces the risk of accidental or malicious misuse of your AWS resources.

* Use IAM Roles:

IAM Roles provide temporary credentials to AWS services, resources, and applications, making it easier to manage permissions across your infrastructure.

* Create individual IAM users:

Avoid sharing IAM users with other users, applications or services. This allows you to manage permissions and access separately for each user or application, which improves security.

* Enforce strong password policies:

Require users to create strong passwords that are difficult to guess, and enforce password rotation policies to keep your accounts secure.

* Enable Multi-Factor Authentication (MFA):

MFA adds an extra layer of security by requiring a user to enter a password and a unique authentication code generated by a separate device, such as a smartphone or a hardware token.

* Use AWS Security Token Service (STS):

STS enables you to grant temporary access to AWS resources to users, services or applications without requiring long-term credentials. This reduces the risk of unauthorised access to your AWS resources.

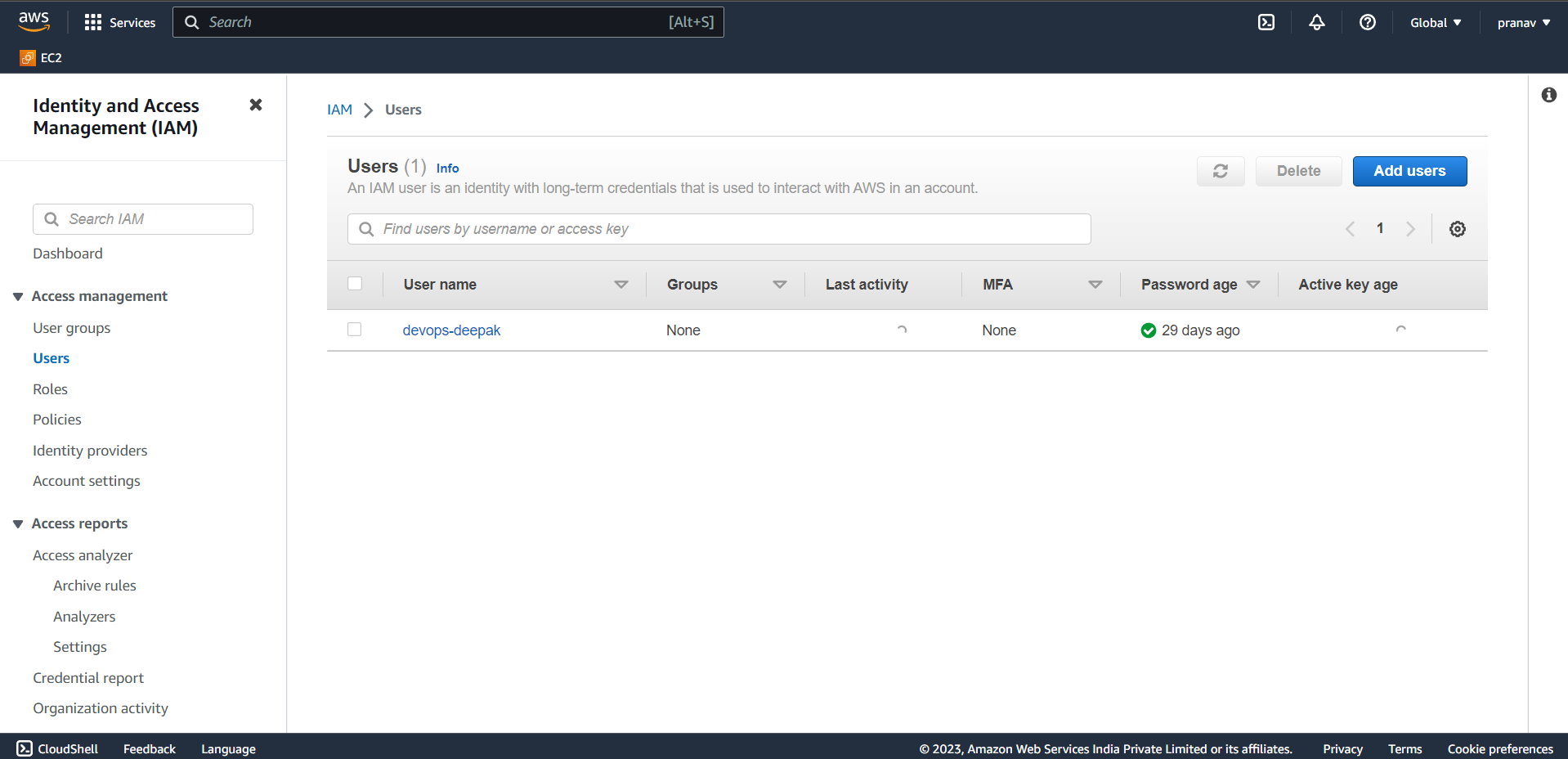
* Use IAM policies:

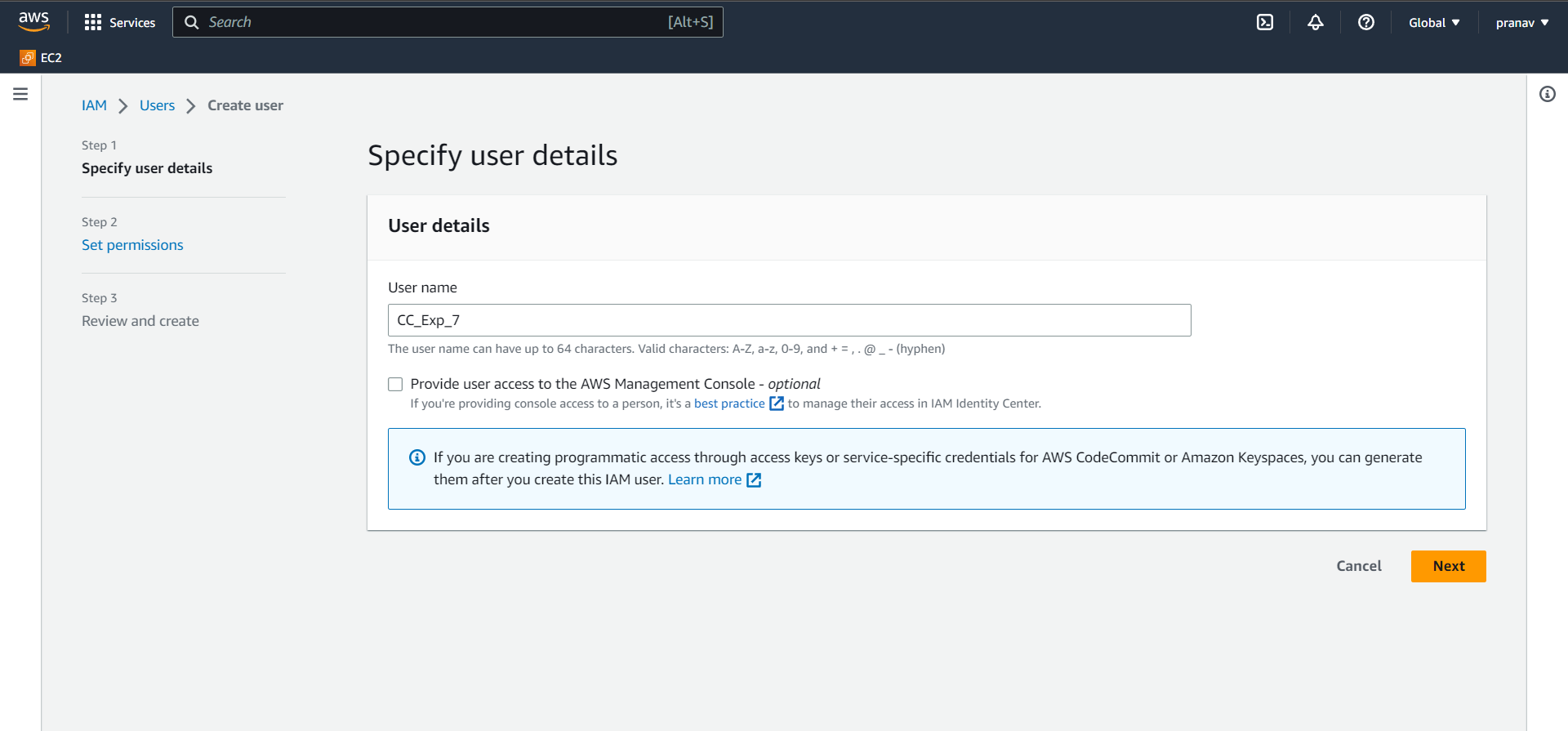
IAM policies are used to define permissions for AWS resources. They can be used to grant or deny access to resources, and can be attached to IAM users, groups, and roles.

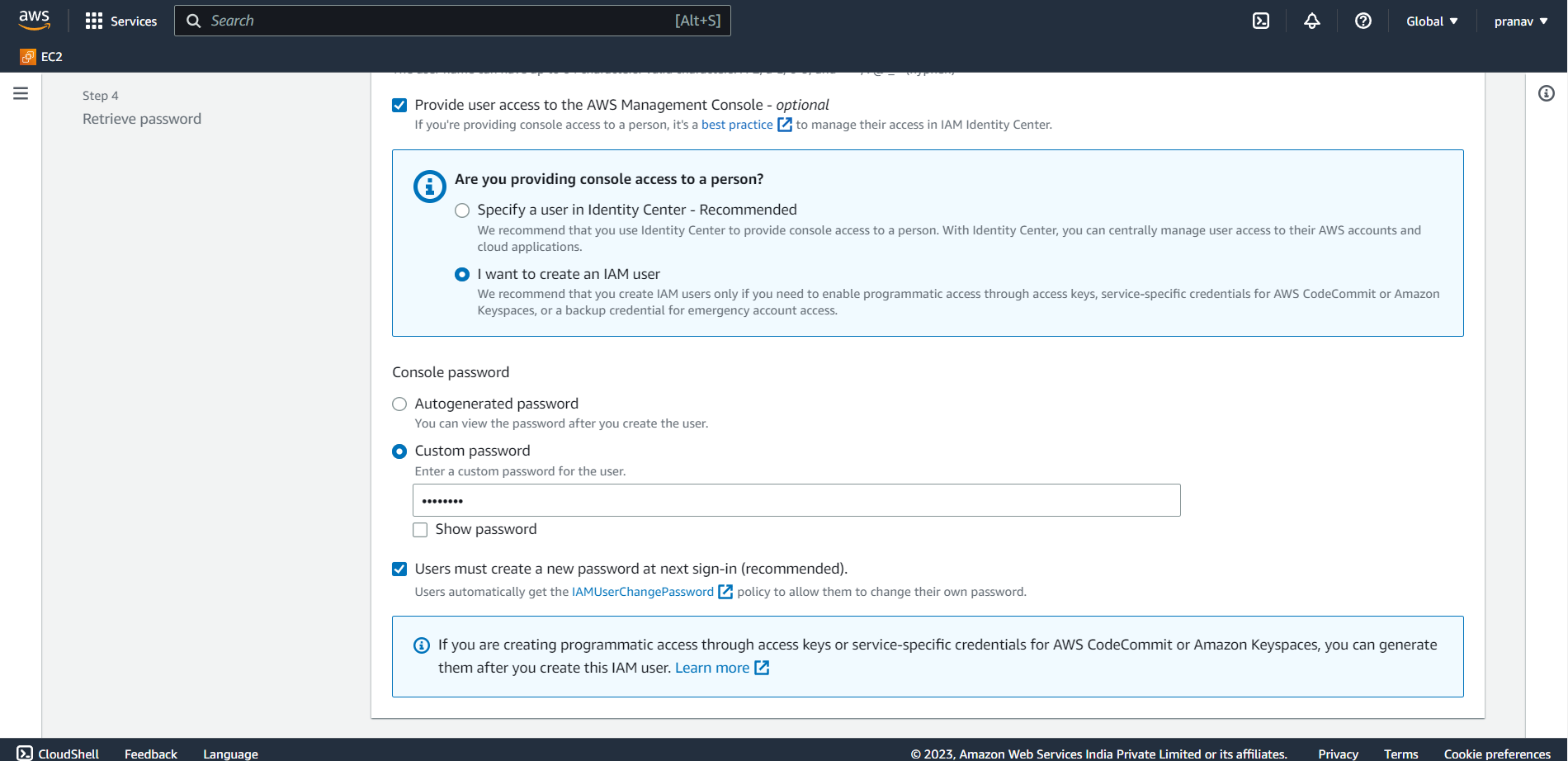
* Monitor your IAM activities:

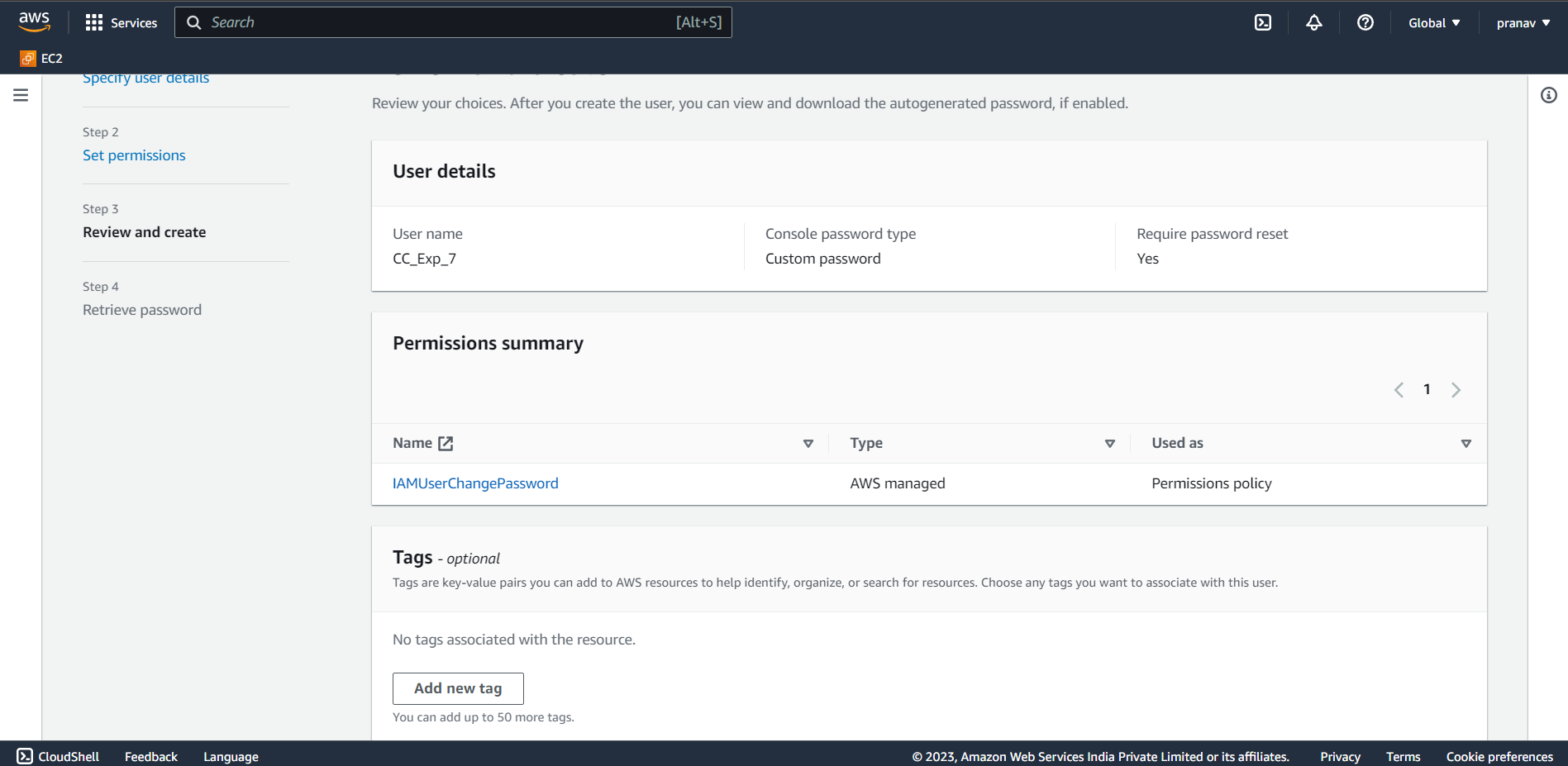
AWS CloudTrail provides an audit trail of all AWS API calls made by your IAM users, so you can identify any unusual or suspicious activity and take appropriate action.

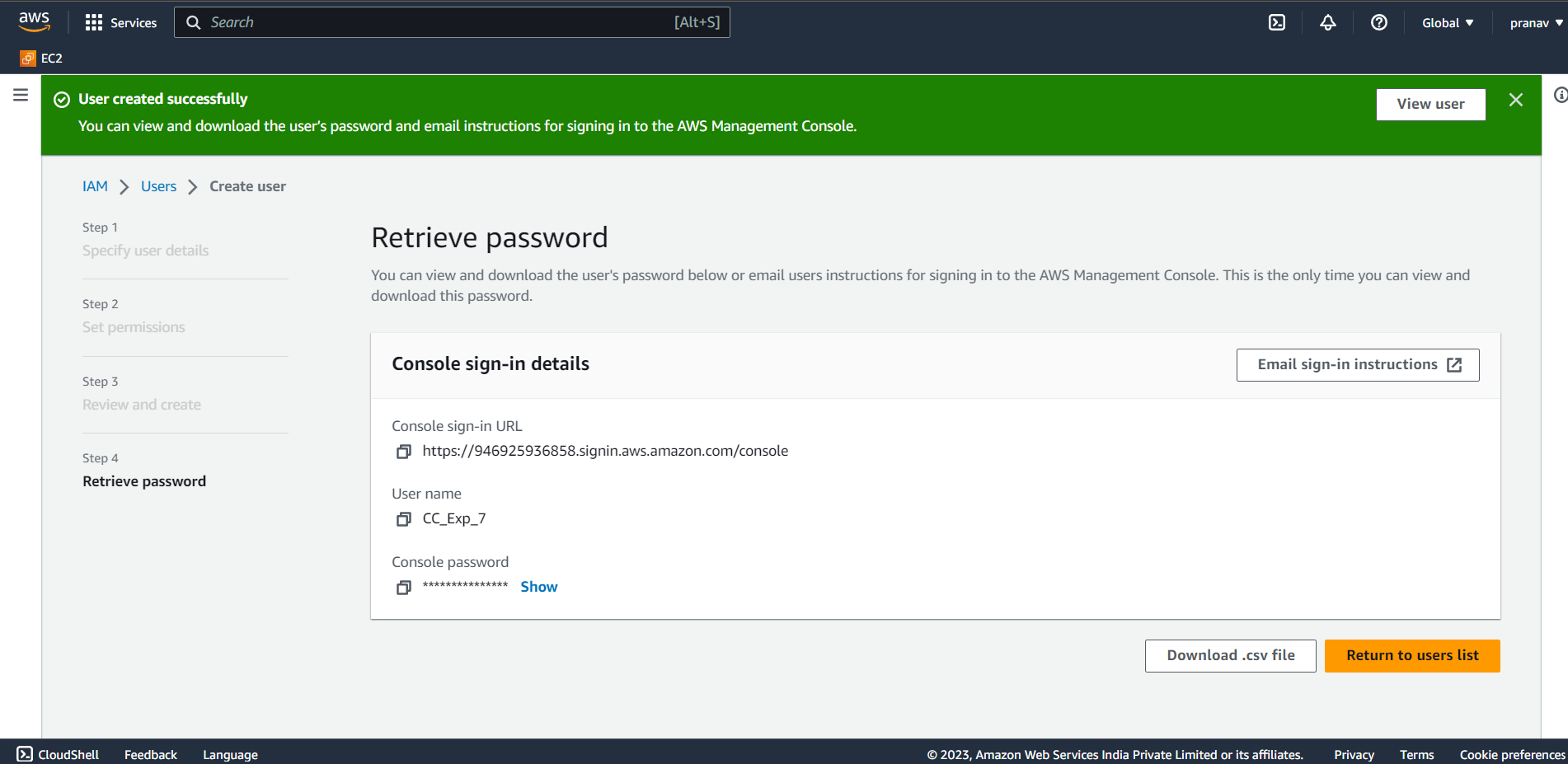
Implementation:

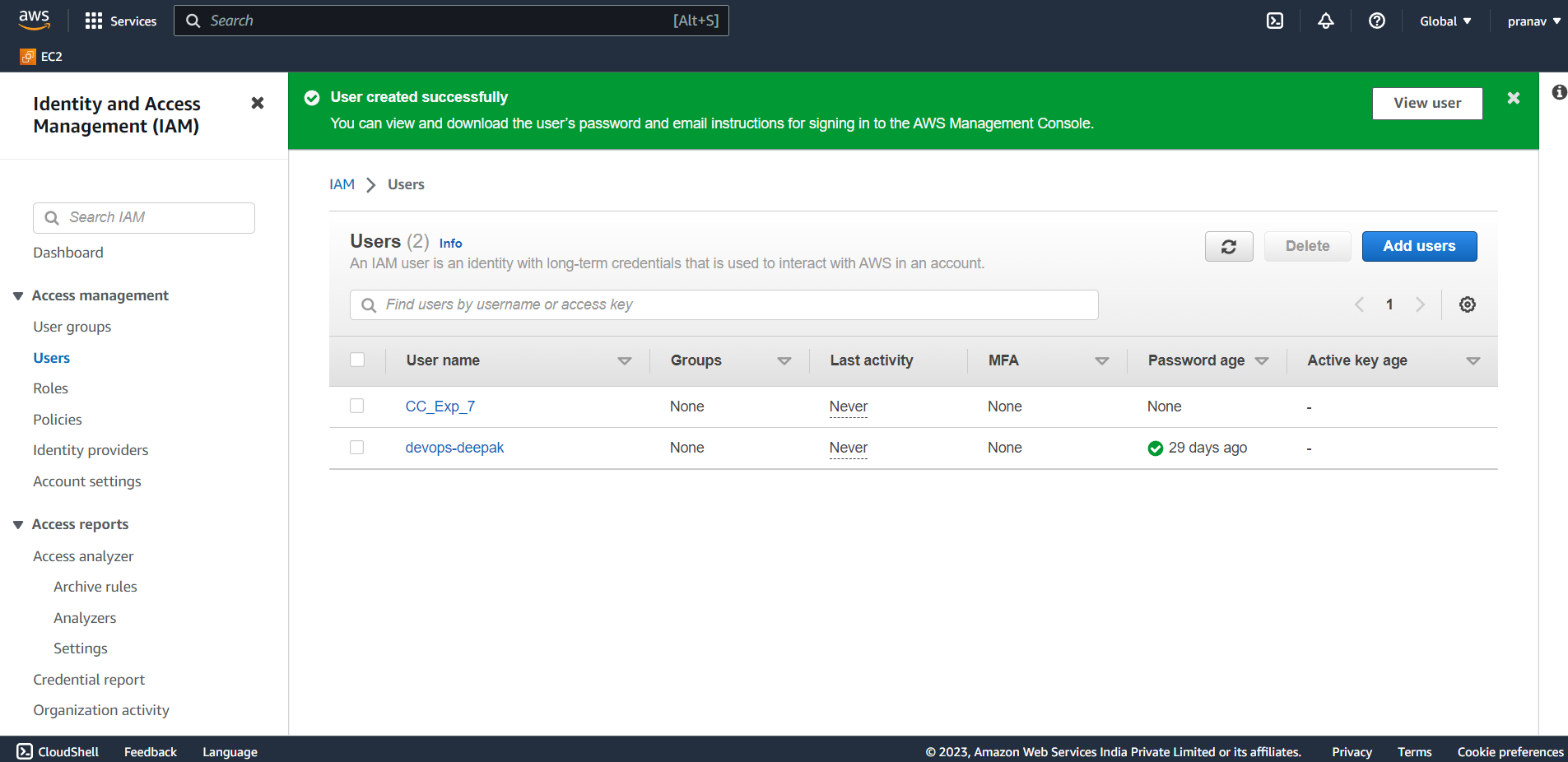




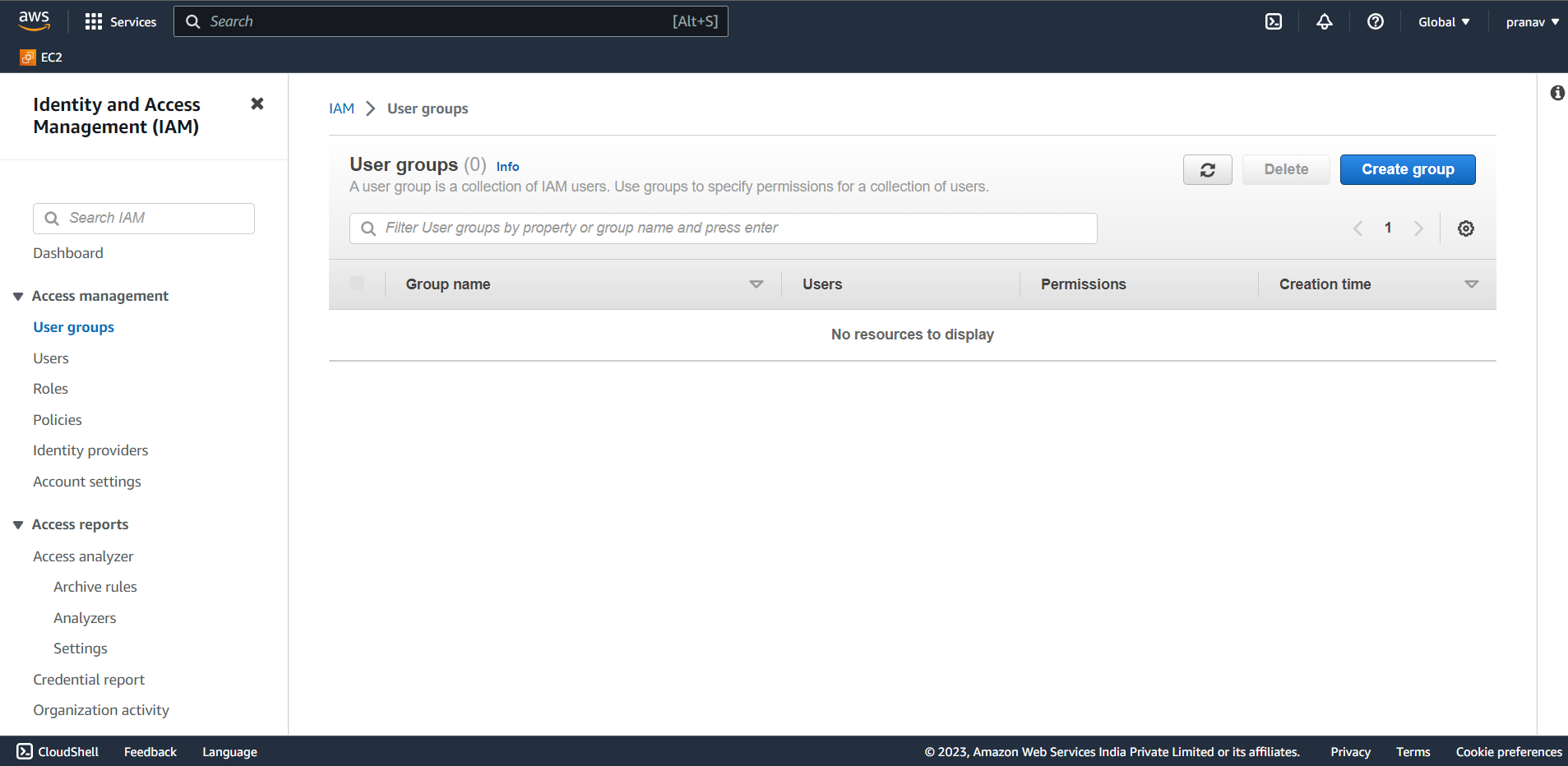


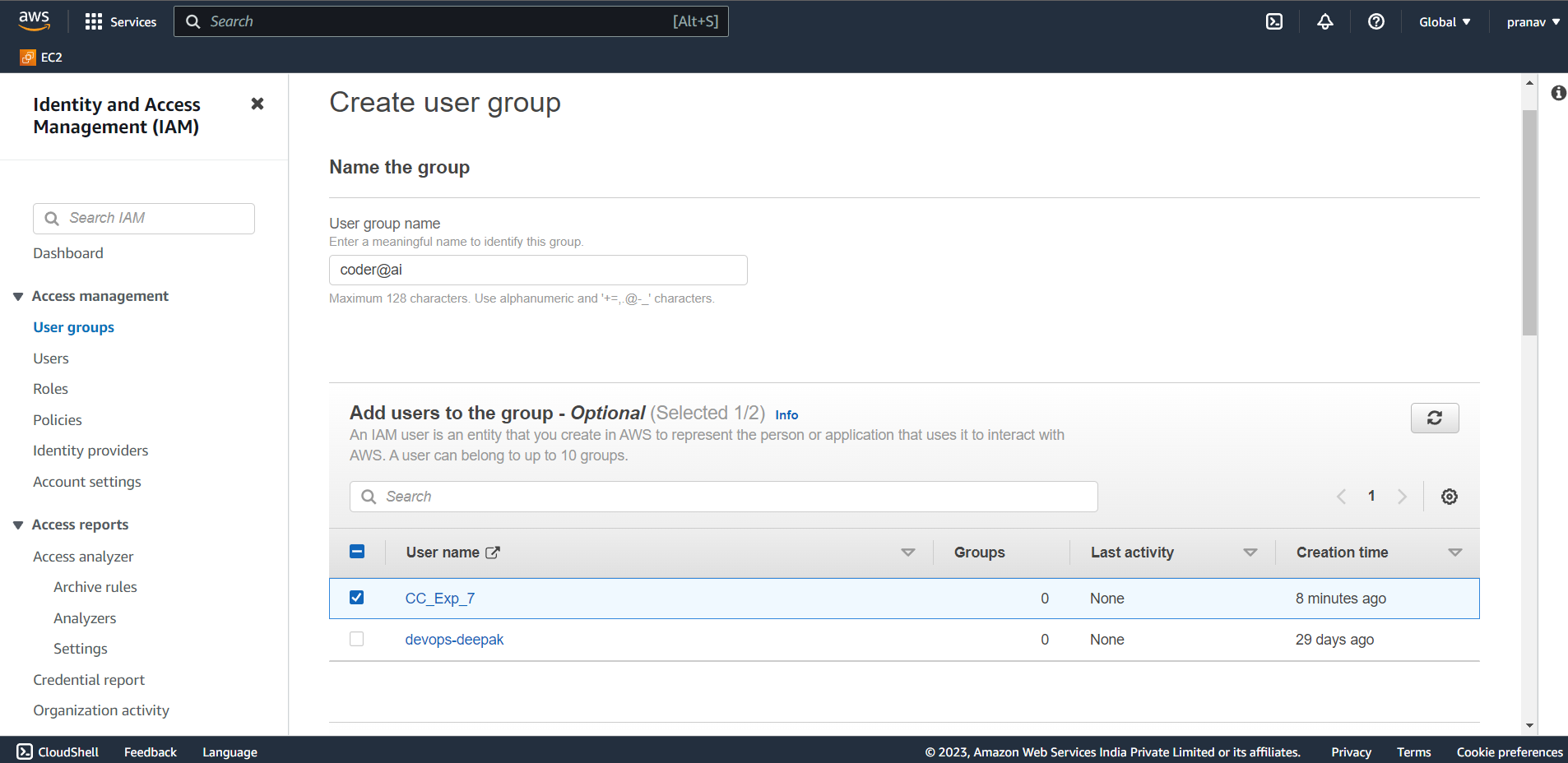


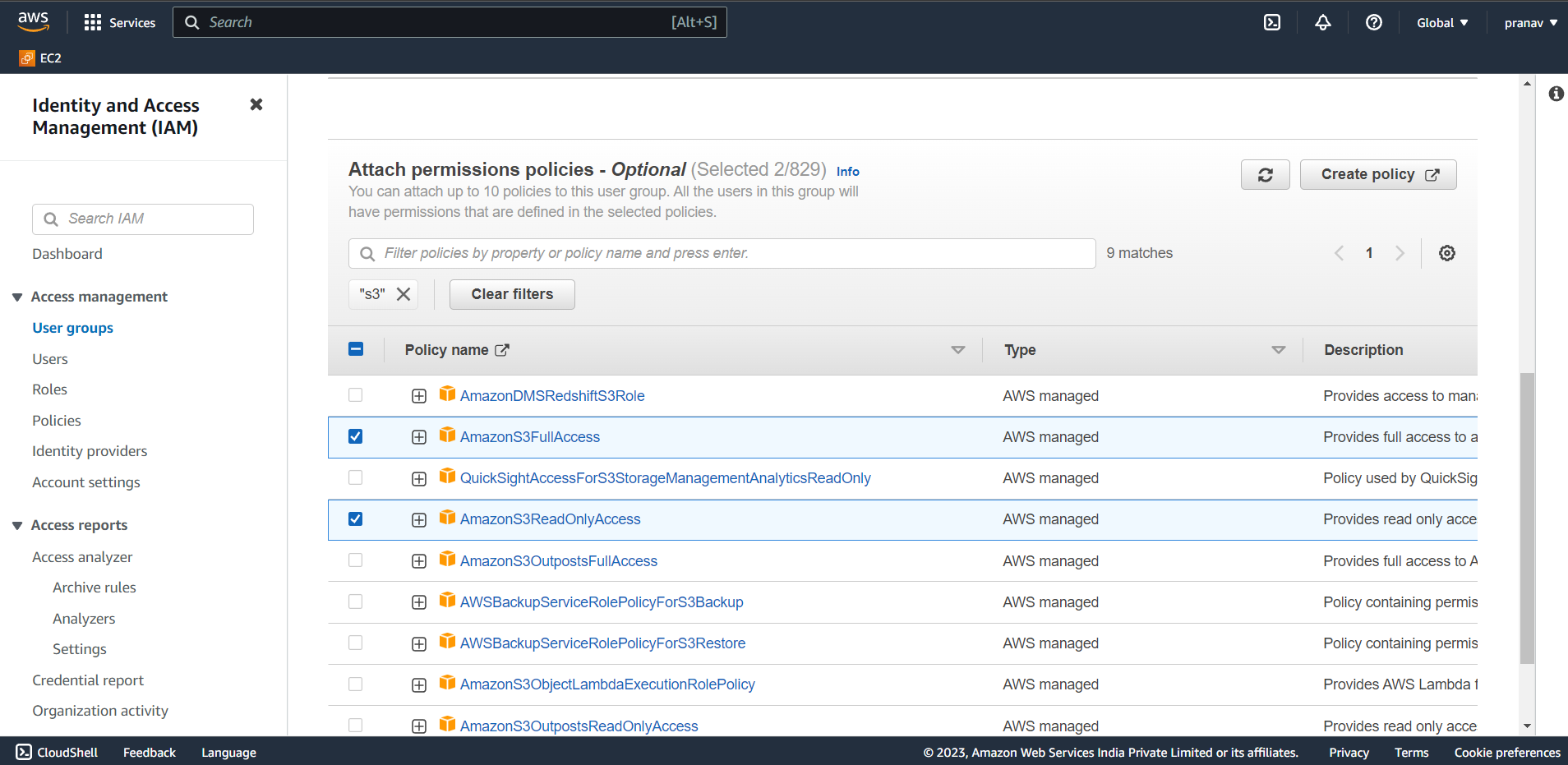


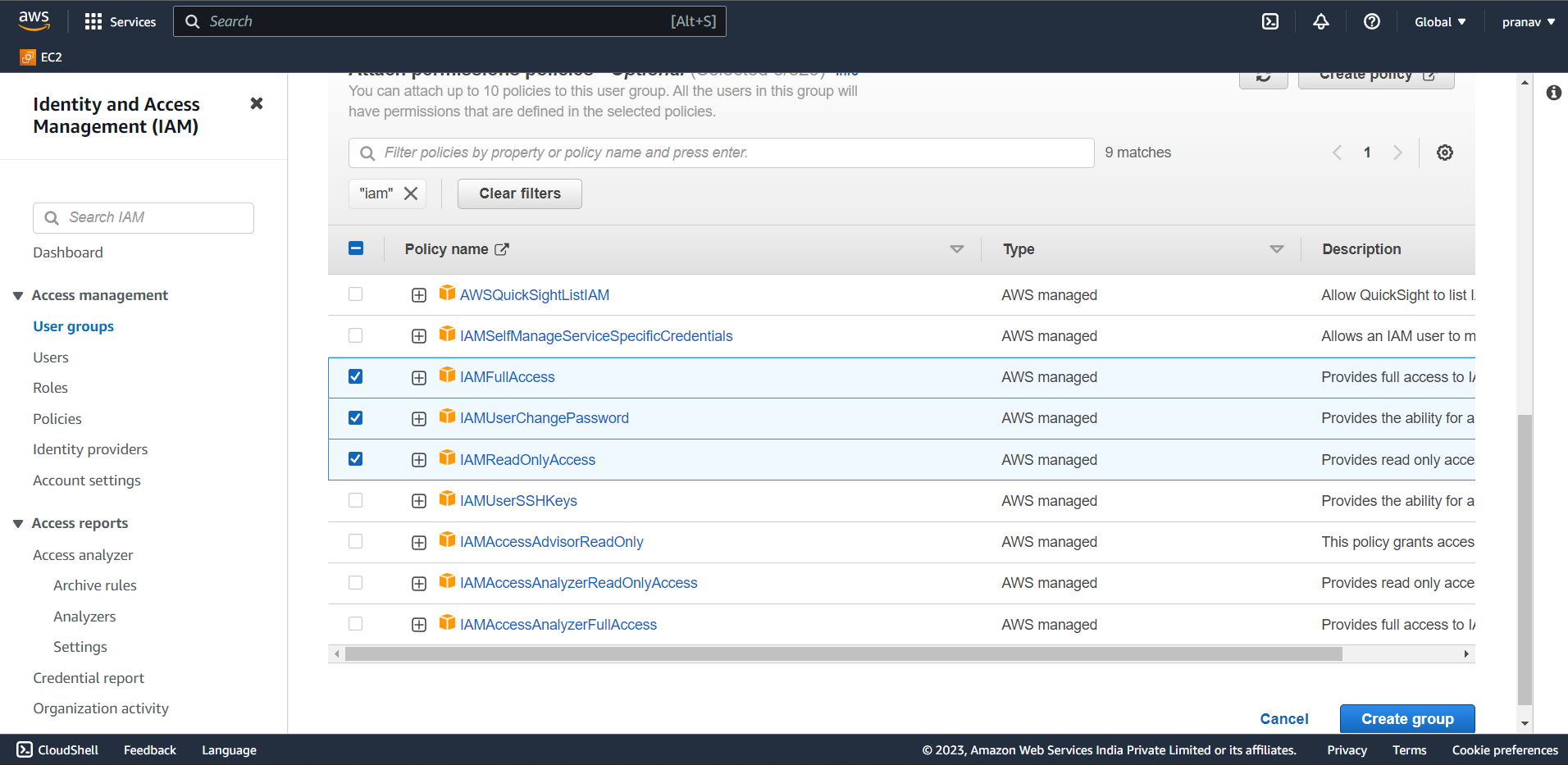


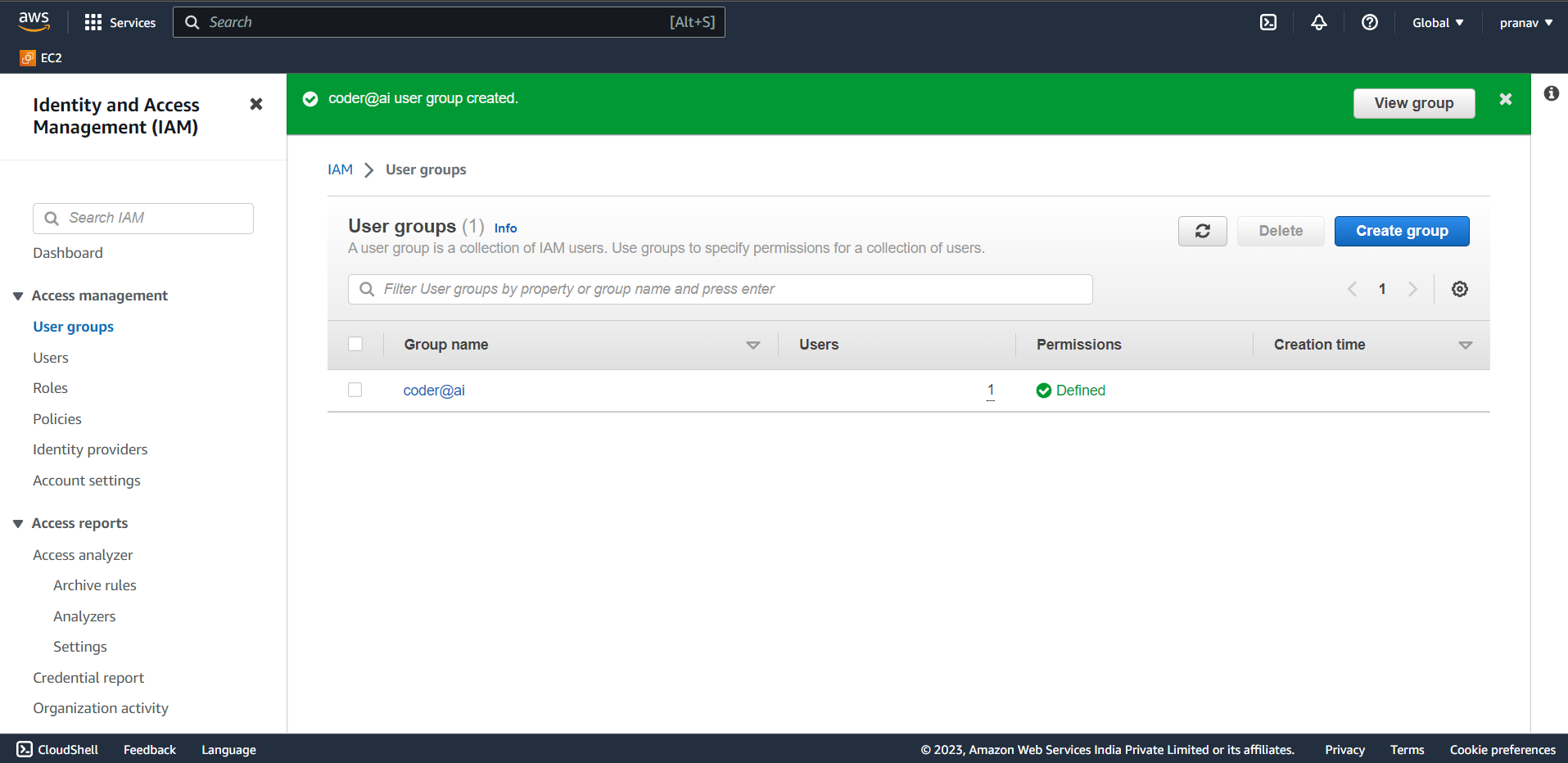
Create Iam groups

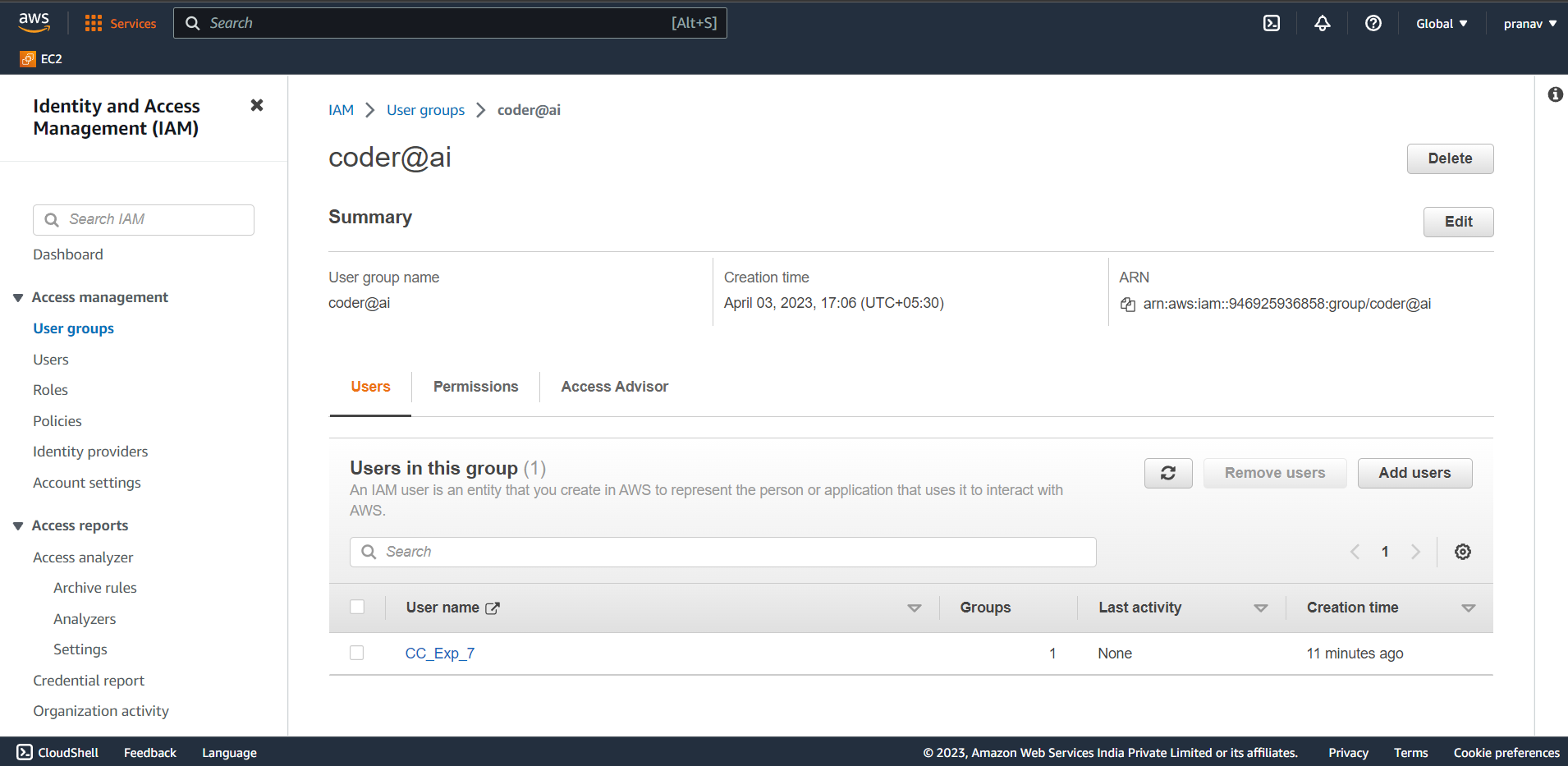












Conclusion:

In this experiment we successfully implemented AWS IAM and learned about it.