Performing operation on S3 bucket within a EC2 instance using IAM role

An IAM role in AWS (Identity and Access Management) is an AWS identity that you can create and assign to AWS resources. It is a security principle that allows you to grant permissions to entities within AWS, such as EC2 instances, Lambda functions, or other AWS services.

IAM roles provide a centralized and secure way to manage access to AWS resources.

They allow you to grant fine-grained permissions to entities, enforce security best practices, and ensure that resources can be accessed securely without the need for long-term credentials.

Role-Based Access Control: IAM roles provide a way to manage and assign permissions to AWS resources without the need for individual credentials or long-term access keys. Roles follow the principle of least privilege, allowing you to grant only the necessary permissions required for a specific resource or service.

Temporary Security Credentials: IAM roles can be assumed by trusted entities, such as IAM users or AWS services. When a role is assumed, it generates temporary security credentials (access key, secret access key, and session token) that are valid for a limited time. This ensures secure access to resources without the need for long-term credentials.

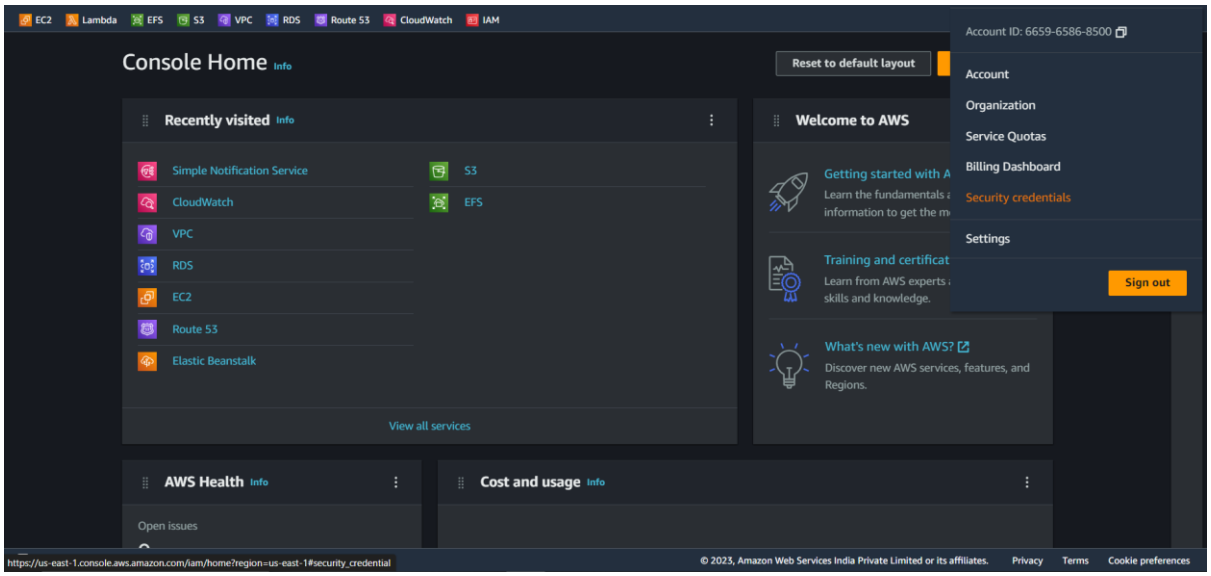
Trust Relationships: IAM roles have trust relationships that define which entities are allowed to assume the role. For example, you can configure a role to be assumed by an EC2 instance, an AWS service, or an IAM user from another AWS account. This establishes a trust relationship between the role and the entity.

Permissions Policies: IAM roles are associated with permissions policies that define the actions and resources that the role can access. These policies can be created using JSON or AWS Policy Language and can be attached to the role directly or inherited from other entities, such as IAM groups or AWS organizations.

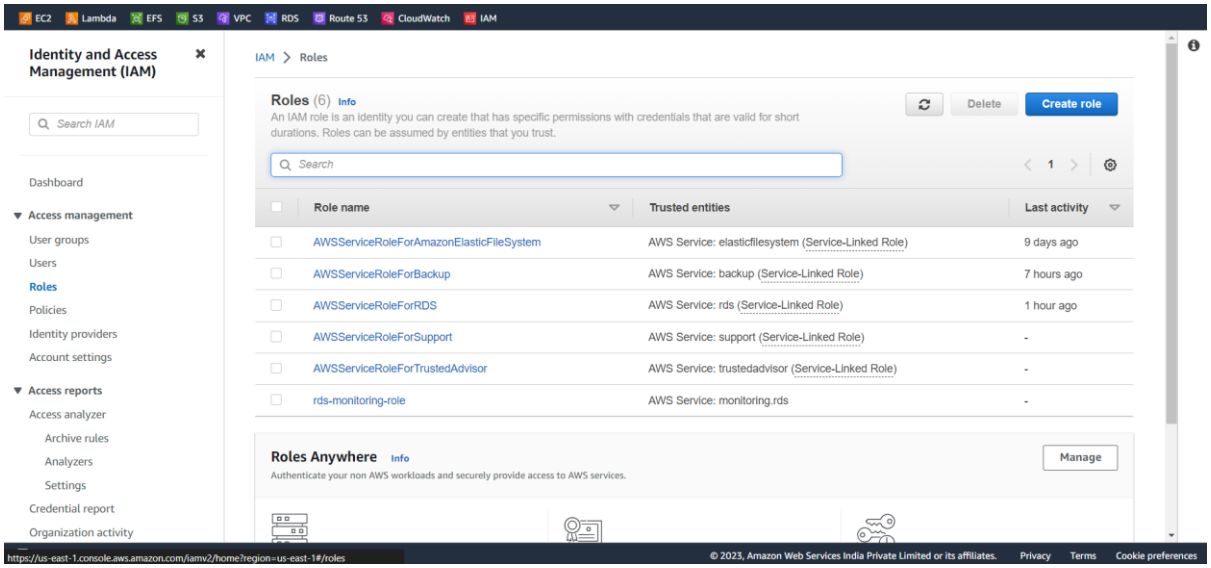
Cross-Account Access: IAM roles can be used to enable cross-account access, allowing entities from one AWS account to access resources in another account. This is useful for scenarios where you want to grant permissions to resources owned by different accounts.

Service Integration: IAM roles are widely used for granting permissions to AWS services. Many AWS services, such as Lambda, EC2, and S3, can assume roles to access resources securely.

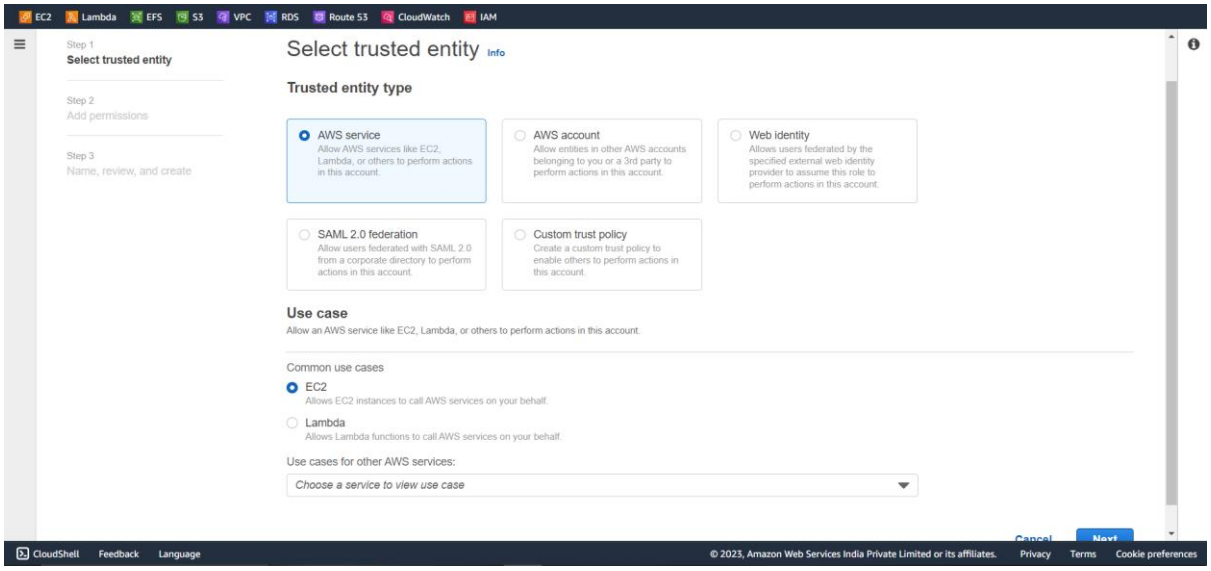
1. Open the IAM console in your AWS Management Console and click on security credentials to open IAM dashboard.



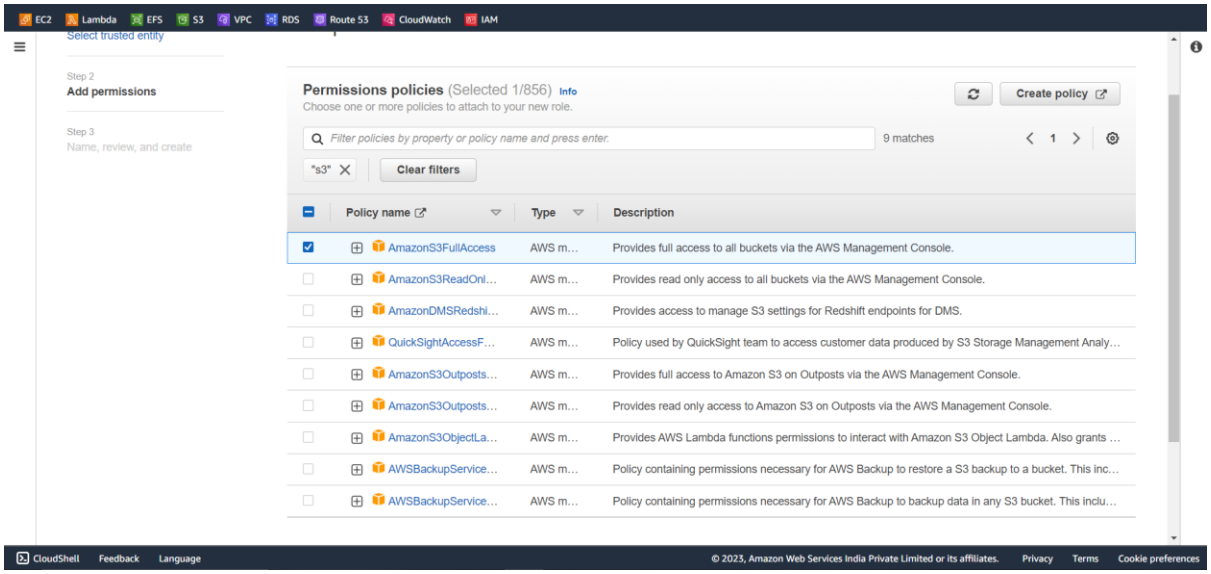
2. Click on "Roles" in the left navigation pane. Click on the "Create role" button.



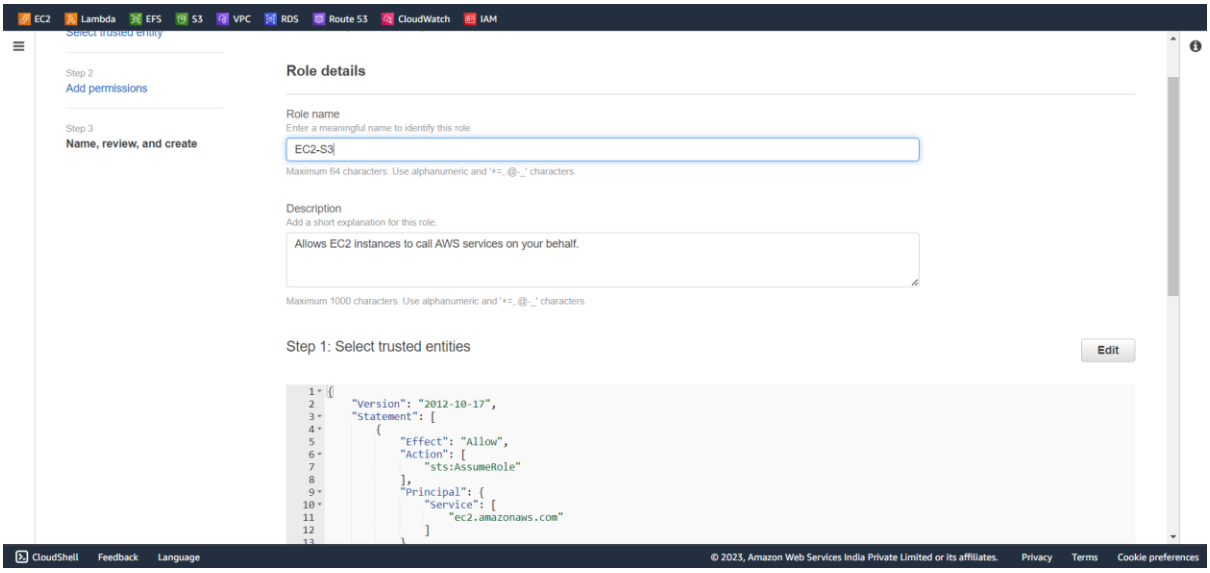
3. Select the service that will use this role (in this case, select EC2) and click on "Next: Permissions".



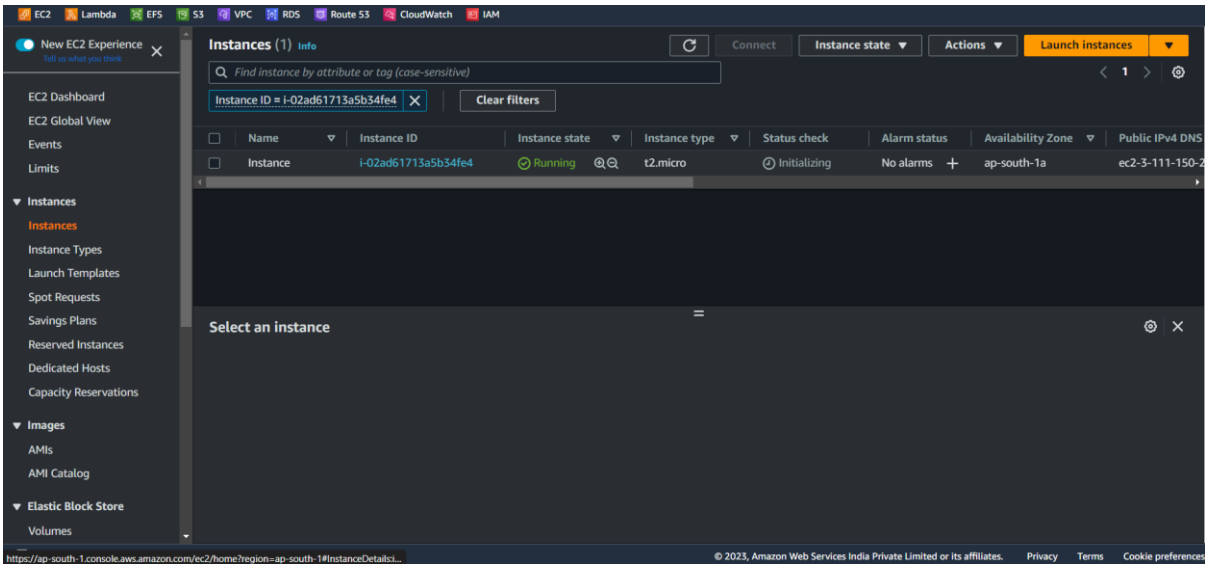
4. Choose the necessary permissions for the role. To access S3, you can attach the managed policy called "AmazonS3FullAccess" or create a custom policy with specific S3 permissions.



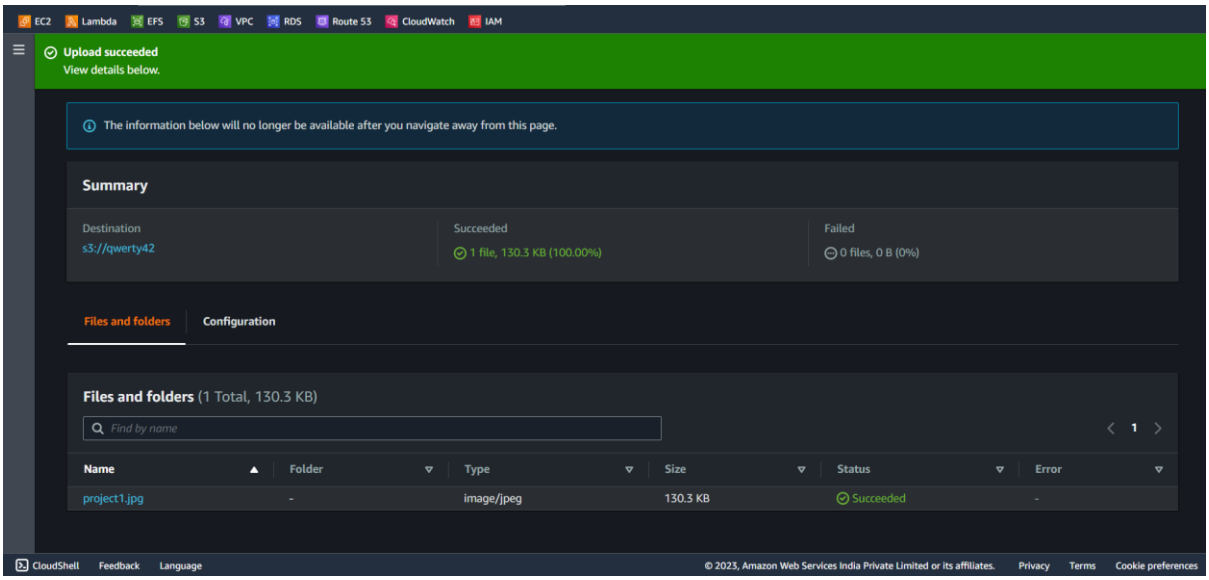
5. Continue through the remaining steps, providing a name and optional description for the role, and click on "Create role".



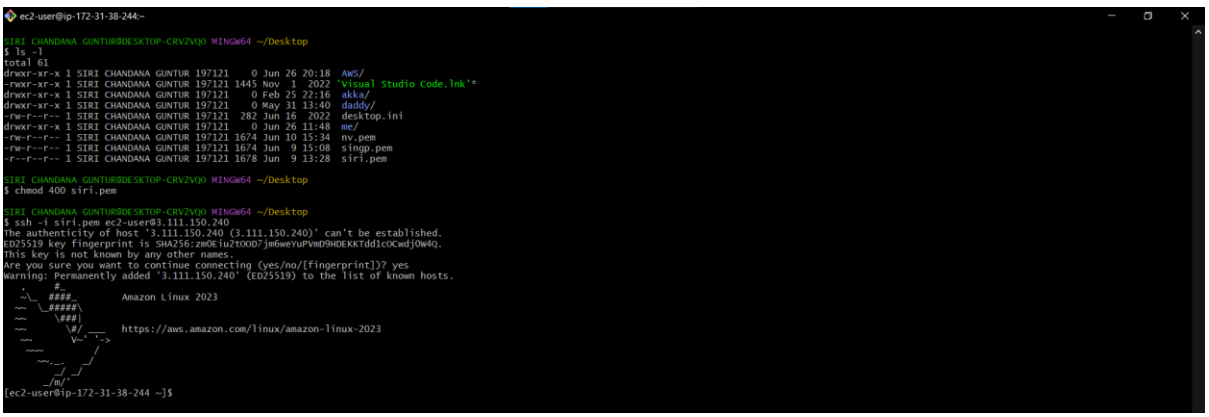
6. Launch an Amazon Linux instance using the EC2 service in your AWS Management Console. In the "Configure Instance Details" section, expand the "IAM role" dropdown menu. Select the IAM role you created in the previous step and complete the instance configuration as needed. Launch the EC2 instance.



7. Create a S3 bucket and add any file to it acknowledge that a file exists in the bucket in ec2 console.

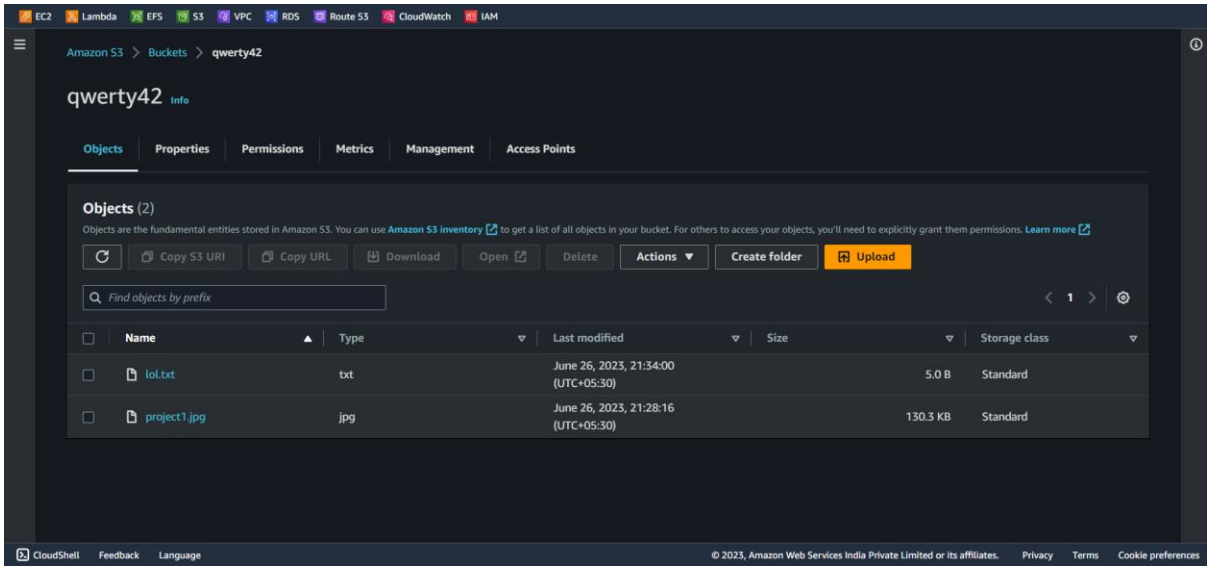


8. Obtain the public IP or DNS of the EC2 instance from the EC2 console. Open your SSH client and connect to the instance If prompted, confirm the SSH connection by typing "yes". You should now be connected to the EC2 instance using SSH.



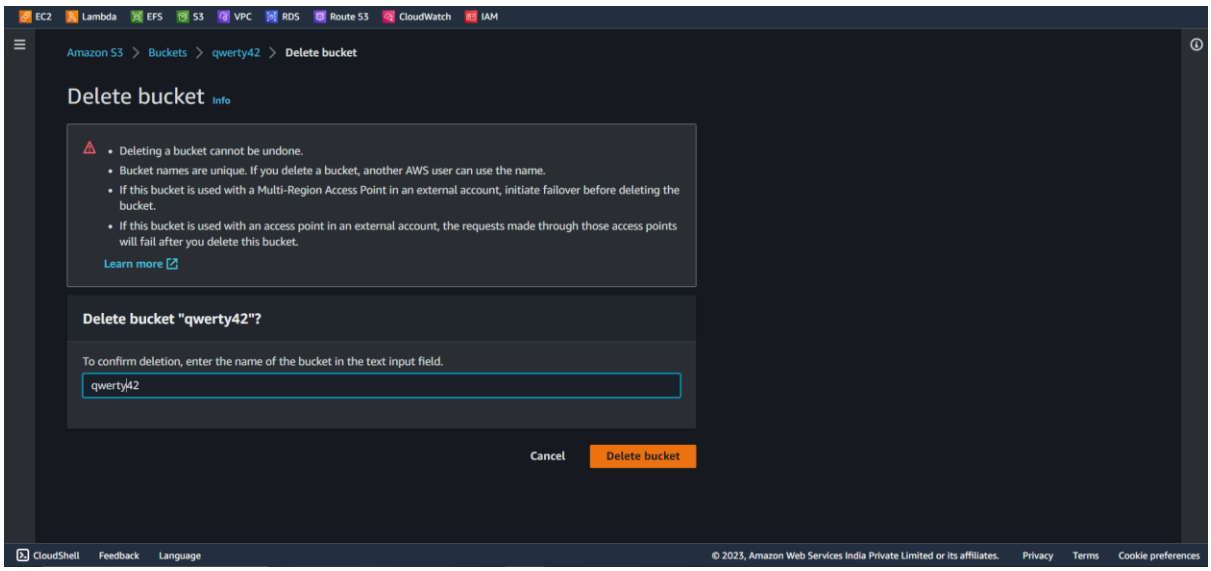
9. Now create a new file and copy the file to S3 bucket by connecting to S3 bucket using EC2

10. Verify whether the file has been added into bucket or not.

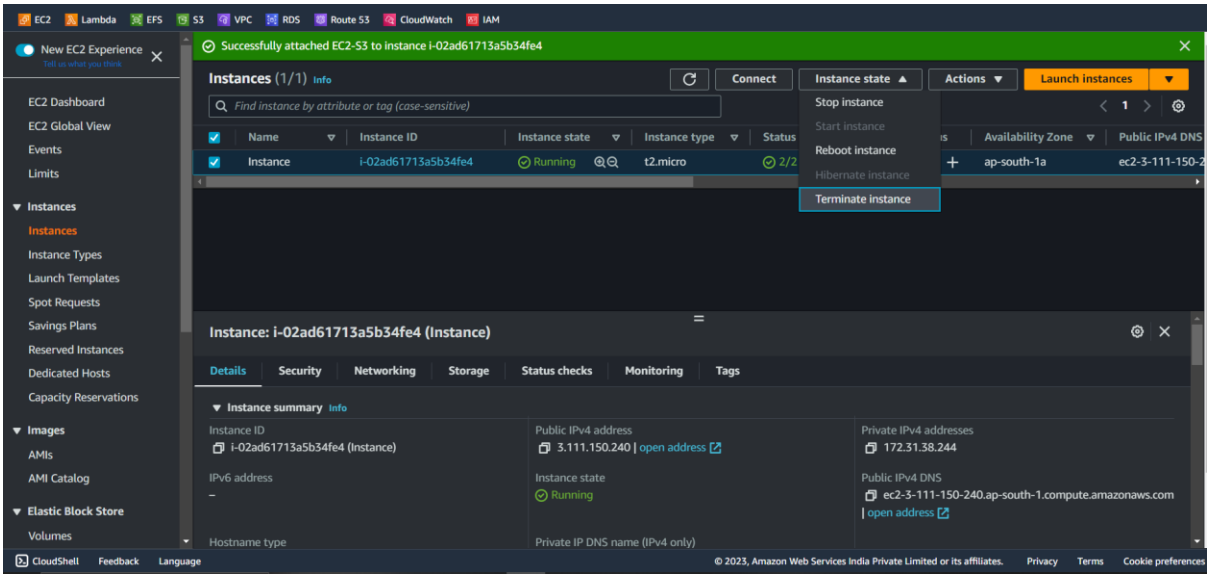


Cleaning Up

1. Empty the bucket first and delete the bucket



2. Terminate the instance.



3. Delete the IAM role by selecting the role and click on delete and confirm the delete.