

Placement Empowerment Program

Cloud Computing and DevOps Centre

Set Up IAM Roles and Permissions

“Create an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.”

Name: DHARSHINI P

DEPARTMENT: IT

Introduction

IAM (Identity and Access Management) roles and permissions are essential for managing access control within a cloud environment. By configuring IAM roles, you can define what actions a Virtual Machine (VM) can perform and which resources it can access. This ensures security, prevents unauthorized access, and follows the principle of least privilege.

Overview

IAM roles are used to grant specific permissions to AWS, GCP, or Azure resources without using long-term credentials. Instead of assigning direct user permissions, IAM roles allow instances, applications, or services to assume predefined access levels dynamically.

Objective

The primary objectives of this POC are:

- Create an IAM role with necessary permissions.
- Attach the role to a VM instance.
- Define policies to allow/restrict access to specific services.
- Improve security by following best IAM practices.

Importance

- **Enhanced Security:** Eliminates the need for storing sensitive credentials within the VM.

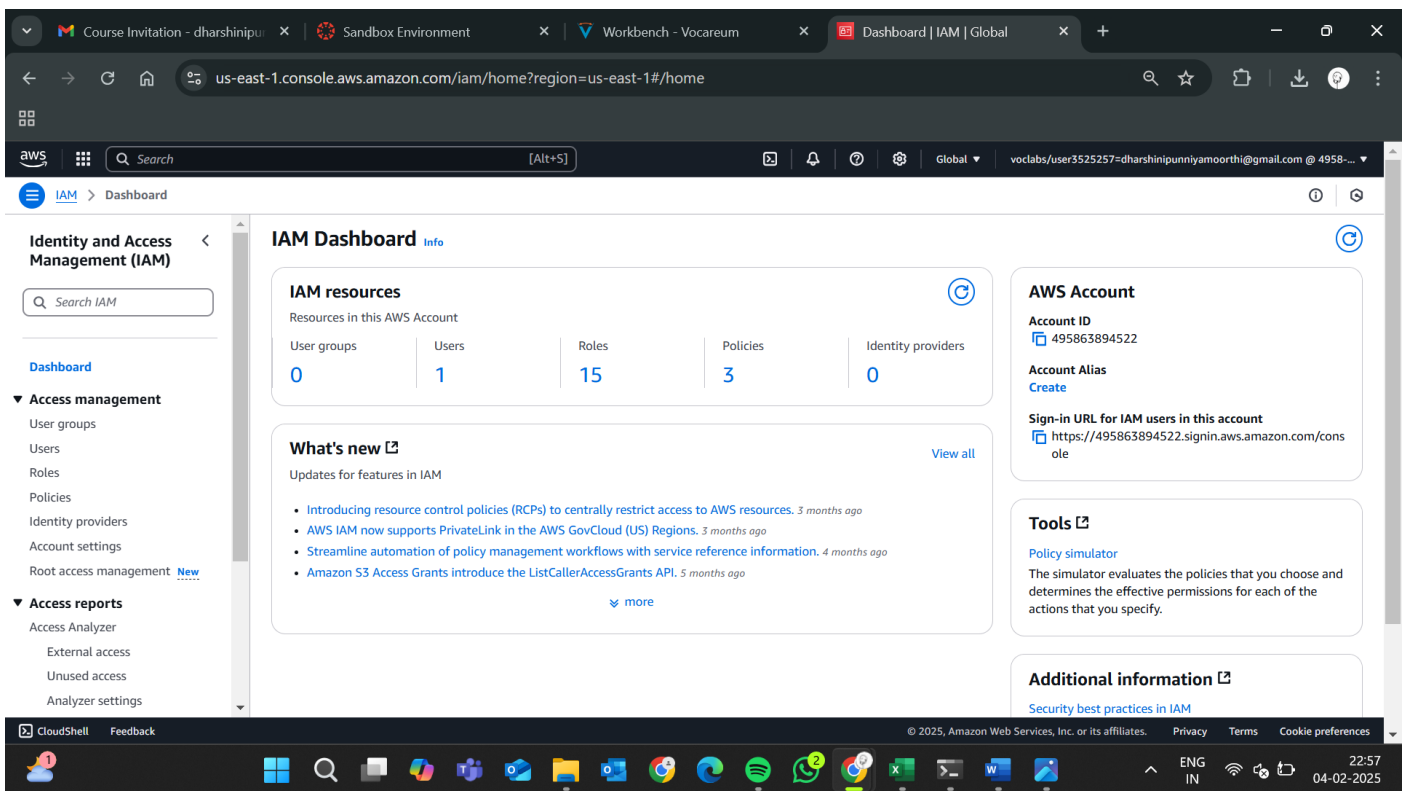
- **Access Control:** Ensures that the VM operates only within the permitted scope.
- **Audit and Monitoring:** Facilitates tracking of access and activities via cloud logs.
- **Scalability:** Allows dynamic role-based access without modifying user-level permissions.

Step-by-Step Overview

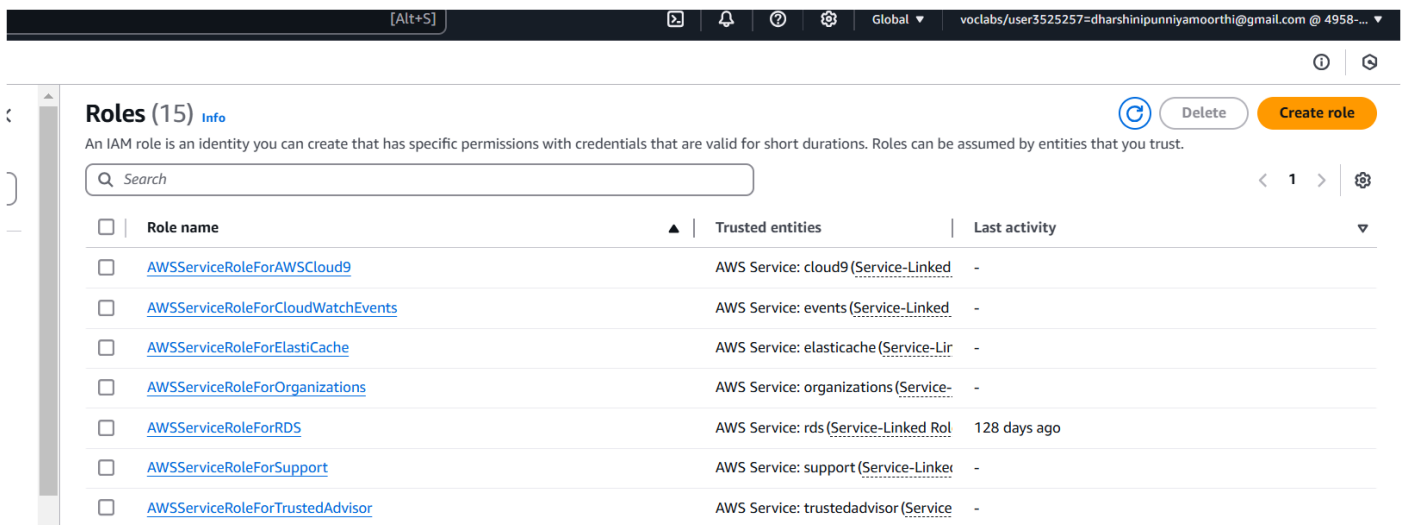
Step 1:

Create an IAM Role:

- Navigate to the **IAM Console** → **Roles**.



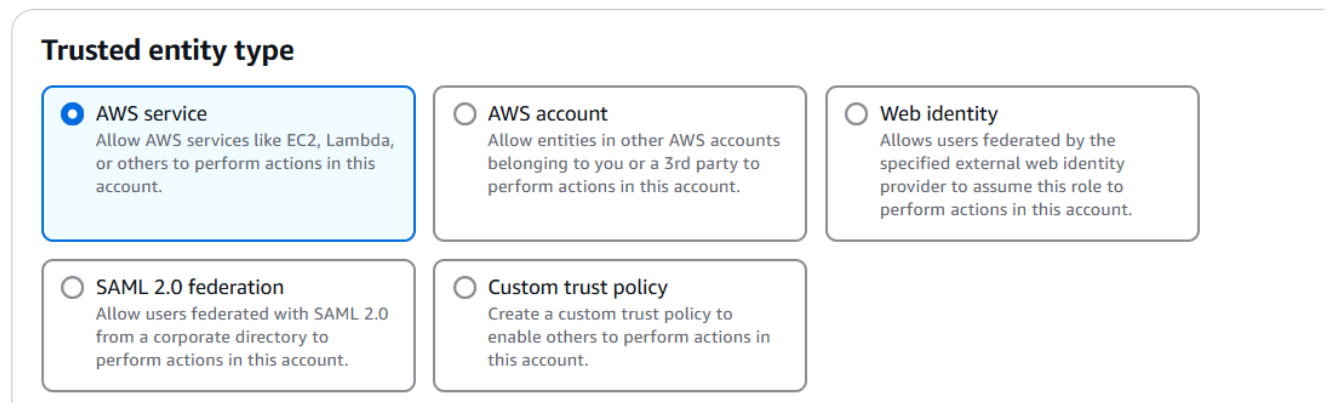
- Click **Create role** and select **AWS service** as a trusted entity.



The screenshot shows the AWS IAM console 'Roles' page. At the top, there's a header with navigation icons and a user profile. Below the header, the 'Roles (15)' section includes a search bar and a 'Create role' button. A table lists various roles with columns for 'Role name', 'Trusted entities', and 'Last activity'. The roles listed are AWSServiceRoleForAWSCloud9, AWSServiceRoleForCloudWatchEvents, AWSServiceRoleForElasticache, AWSServiceRoleForOrganizations, AWSServiceRoleForRDS, AWSServiceRoleForSupport, and AWSServiceRoleForTrustedAdvisor.

Role name	Trusted entities	Last activity
AWSServiceRoleForAWSCloud9	AWS Service: cloud9 (Service-Linked)	-
AWSServiceRoleForCloudWatchEvents	AWS Service: events (Service-Linked)	-
AWSServiceRoleForElasticache	AWS Service: elasticache (Service-Linked)	-
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked)	-
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	128 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked)	-

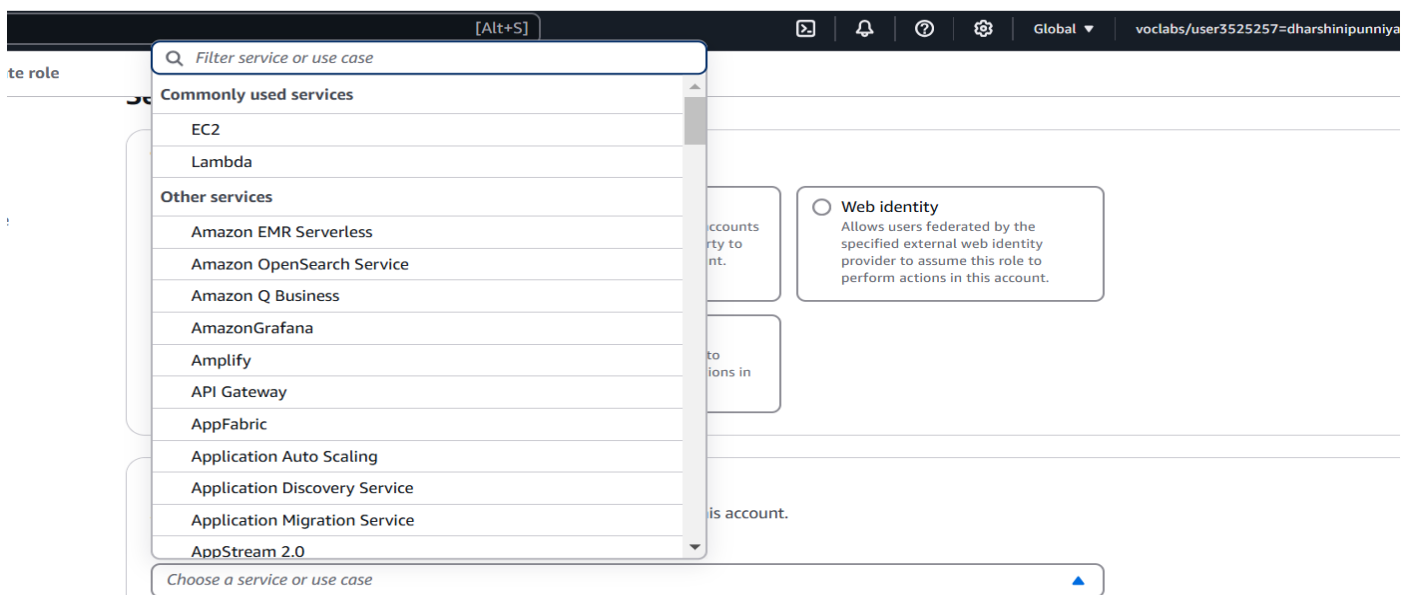
Select trusted entity Info



The screenshot shows the 'Select trusted entity' page. Under the 'Trusted entity type' section, there are five radio button options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Each option has a brief description of what it allows.

- AWS service** (selected): Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account**: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity**: Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation**: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy**: Create a custom trust policy to enable others to perform actions in this account.

- Choose **EC2** as the use case.



The screenshot shows the 'Choose a service or use case' dropdown menu. The menu is open, displaying a list of services under 'Commonly used services' and 'Other services'. 'EC2' is selected under 'Commonly used services'. The 'Web identity' option is visible in the background.

- Commonly used services**
 - EC2 (selected)
 - Lambda
- Other services**
 - Amazon EMR Serverless
 - Amazon OpenSearch Service
 - Amazon Q Business
 - Amazon Grafana
 - Amplify
 - API Gateway
 - AppFabric
 - Application Auto Scaling
 - Application Discovery Service
 - Application Migration Service
 - AppStream 2.0

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

EC2

Use case

- ☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.
- ☐ **EC2 Role for AWS Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- ☐ **EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- ☐ **EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- ☐ **EC2 - Spot Fleet Tagging**

- ## Add permissions [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type	
<input type="text" value="Search"/>	All types
Policy name	Type
<input type="checkbox"/> AdministratorAccess	AWS managed - job function
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed
<input type="checkbox"/> AIOpsAssistantPolicy	AWS managed
<input type="checkbox"/> AIOpsConsoleAdminPolicy	AWS managed

- ### Name, review, and create

Role name

Enter a meaningful name to identify this role.

myrole-dha

Maximum 64 characters. Use alphanumeric and '+,=,@-_' characters.

Description

Description
Add a short explanation for this role.

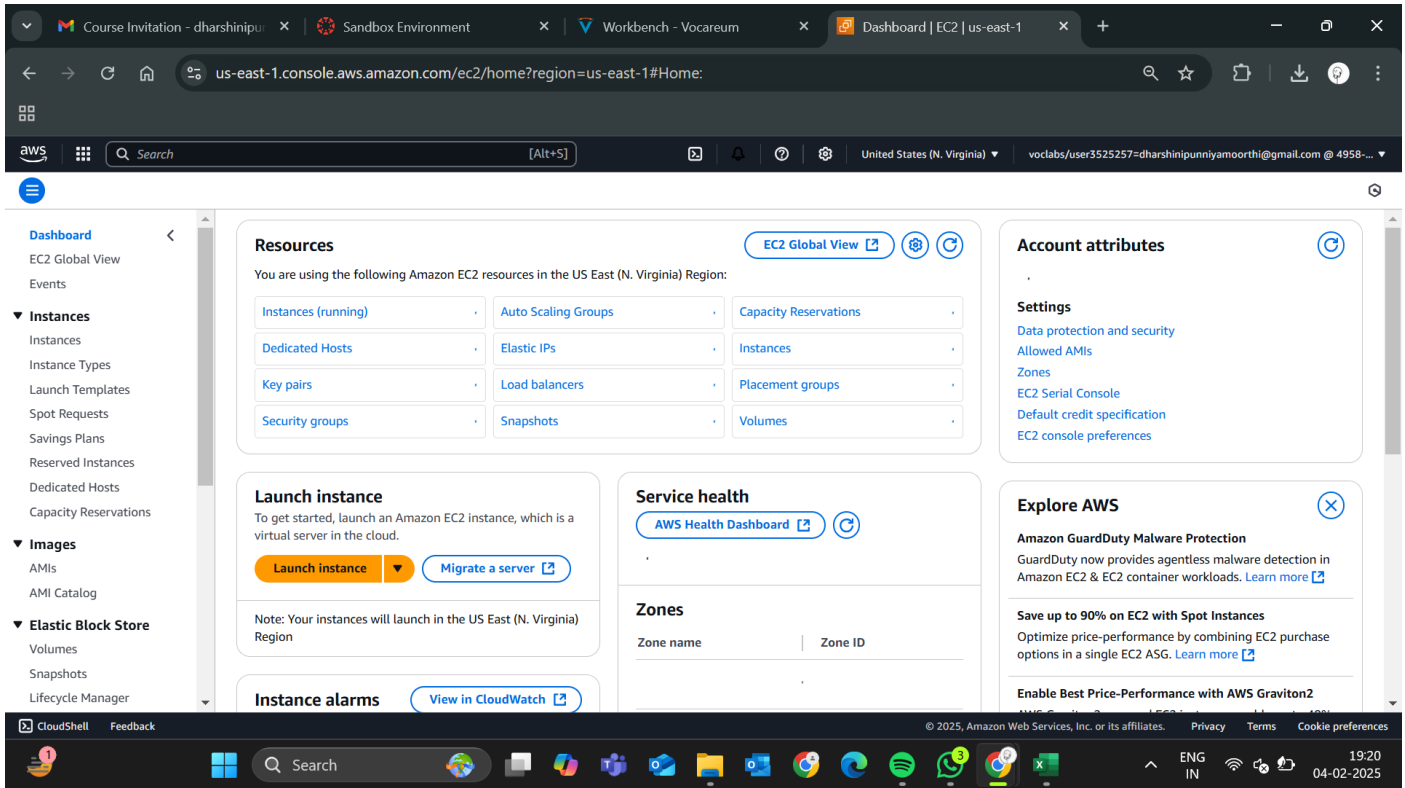
Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: + = . , @ - / [() ! # \$ % ^ & * () ; ' " `

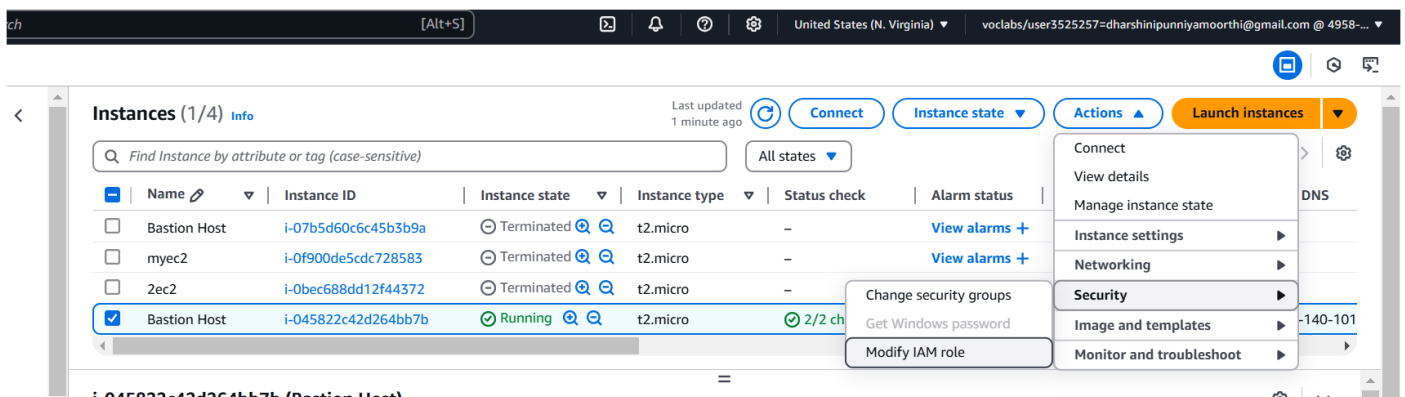
Step 2:

Attach the Role to an EC2 Instance:

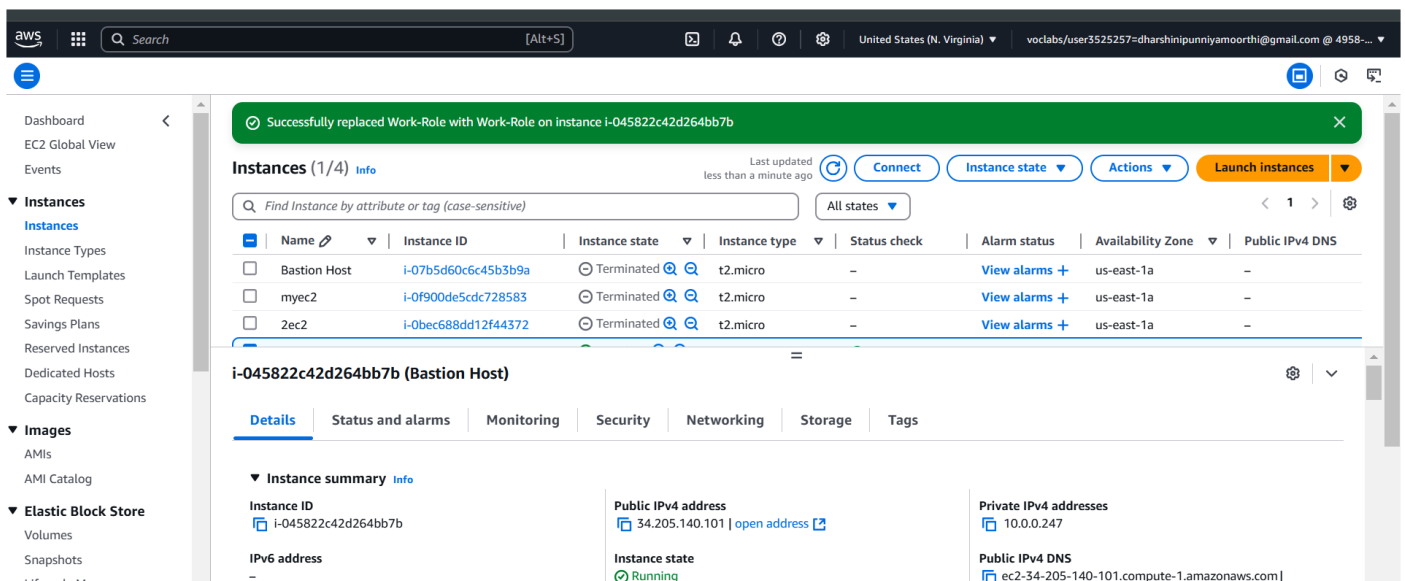
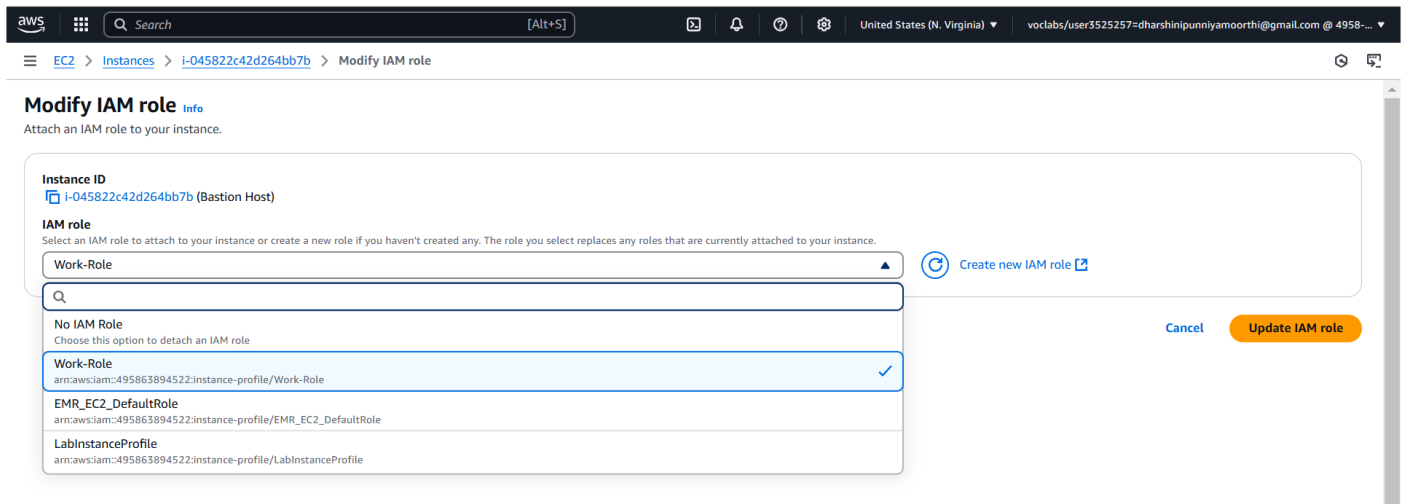
- Go to **EC2 Console** → Select your instance.



- Click **Actions** → **Security** → **Modify IAM Role**.



- Select the newly created IAM role and attach it.



Expected Outcome:

By the end of this process, you will have:

- The IAM role is successfully created and assigned to the VM.
- The VM is granted only the specified permissions without using credentials.
- The configured access restrictions work as expected, improving security.
- The role-based access can be monitored and modified as needed.

By following these steps, you ensure secure and efficient access control for your cloud-based virtual machines.

