

Placement Empowerment Program

Cloud Computing and DevOps Centre

Setting Up IAM Roles and Permissions for a Virtual Machine



Name: Vishali V

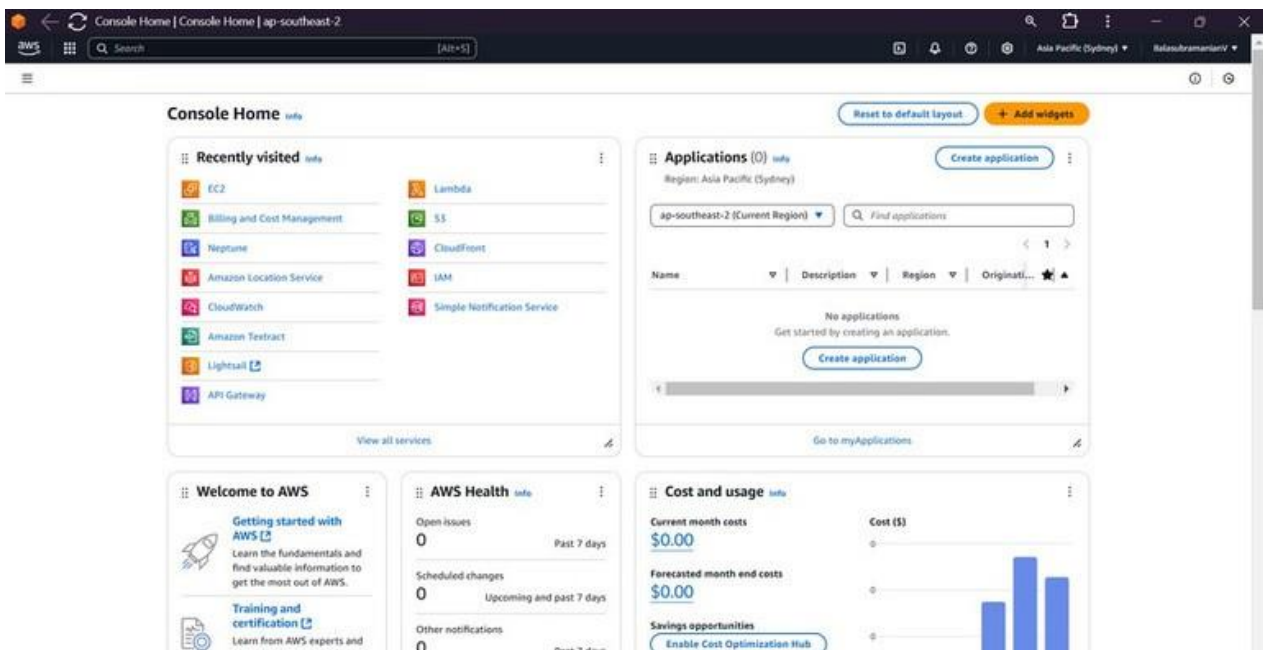
Department : CSE

Introduction

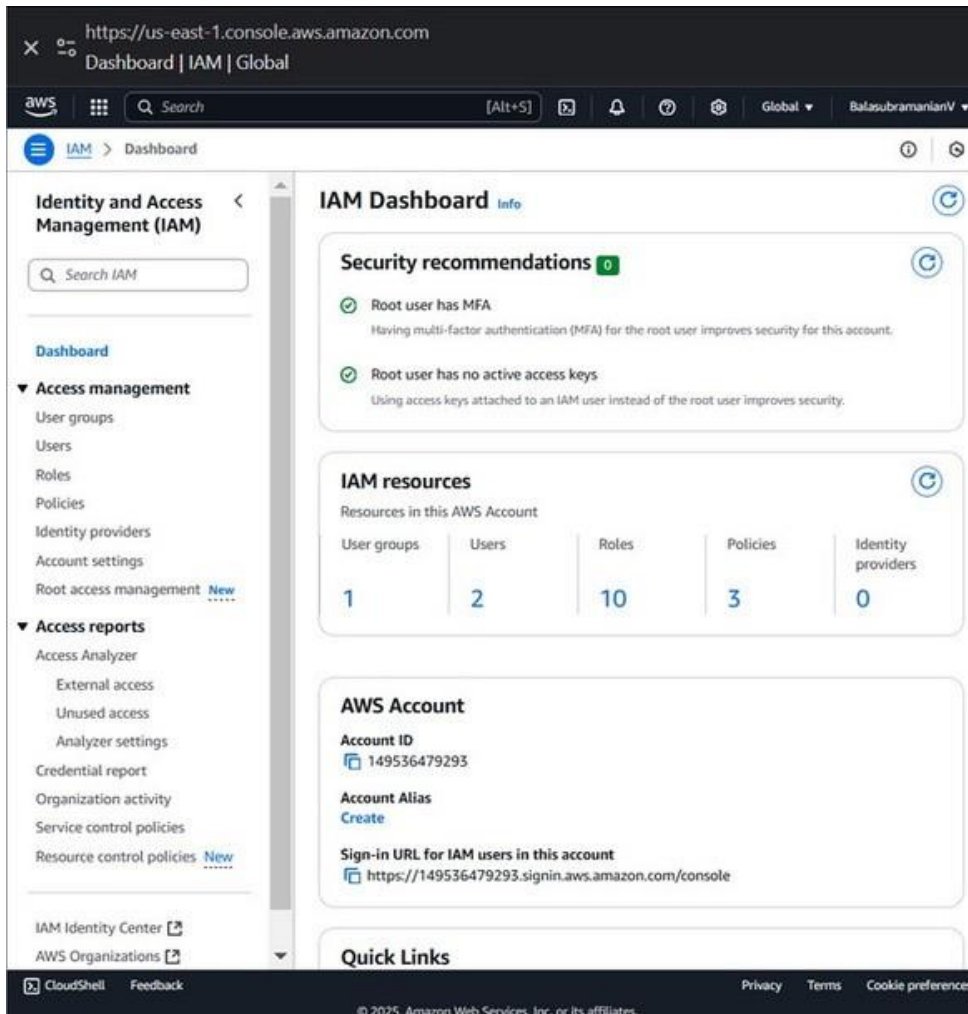
Identity and Access Management (IAM) is a crucial aspect of cloud security that allows administrators to control who can access specific resources and what actions they can perform. By setting up IAM roles and permissions, you ensure that only authorized users or services can interact with your virtual machine (VM). This guide provides step-by-step instructions for creating an IAM role and assigning it to a VM on your cloud platform.

1. Create an IAM Role

- Log in to your cloud provider's console.

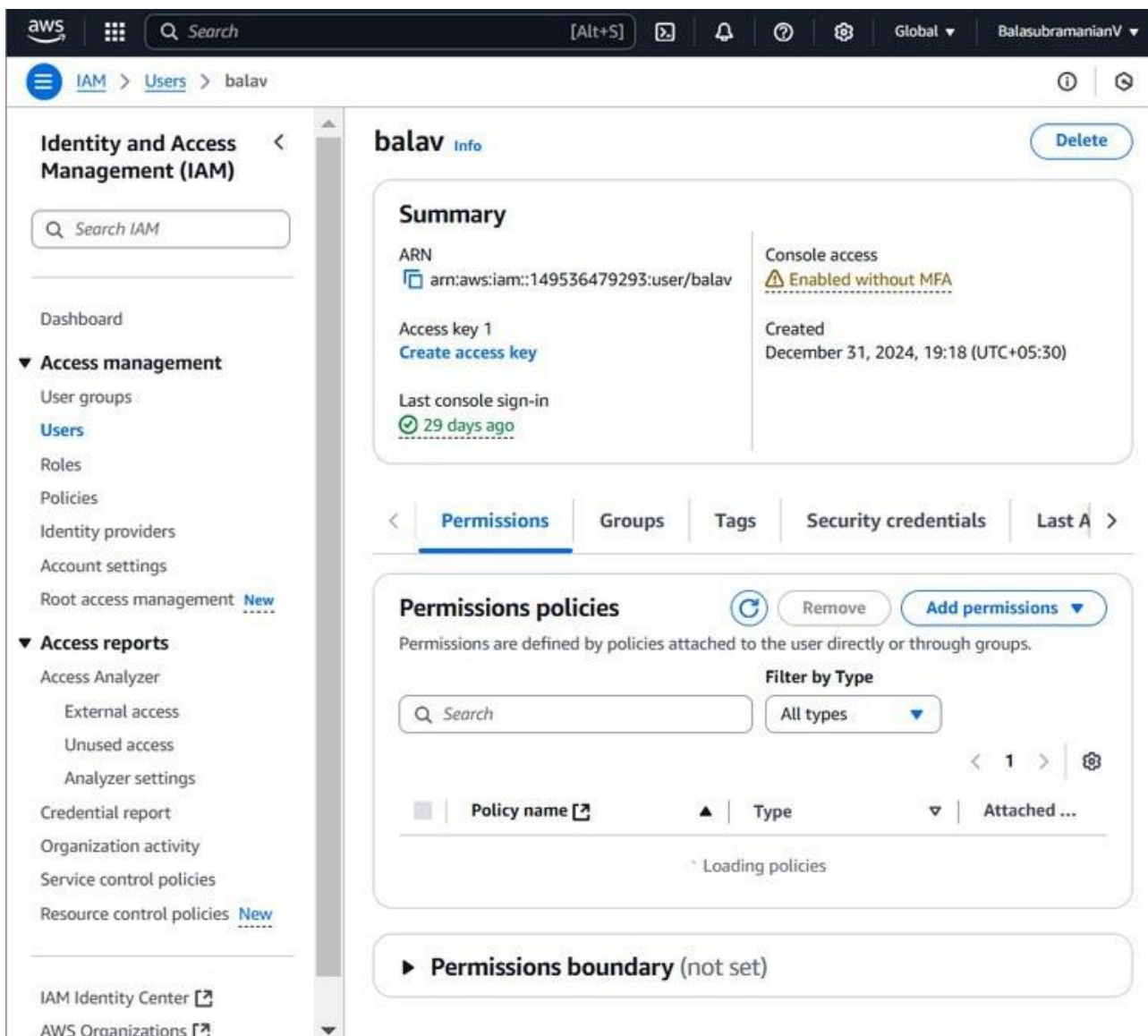
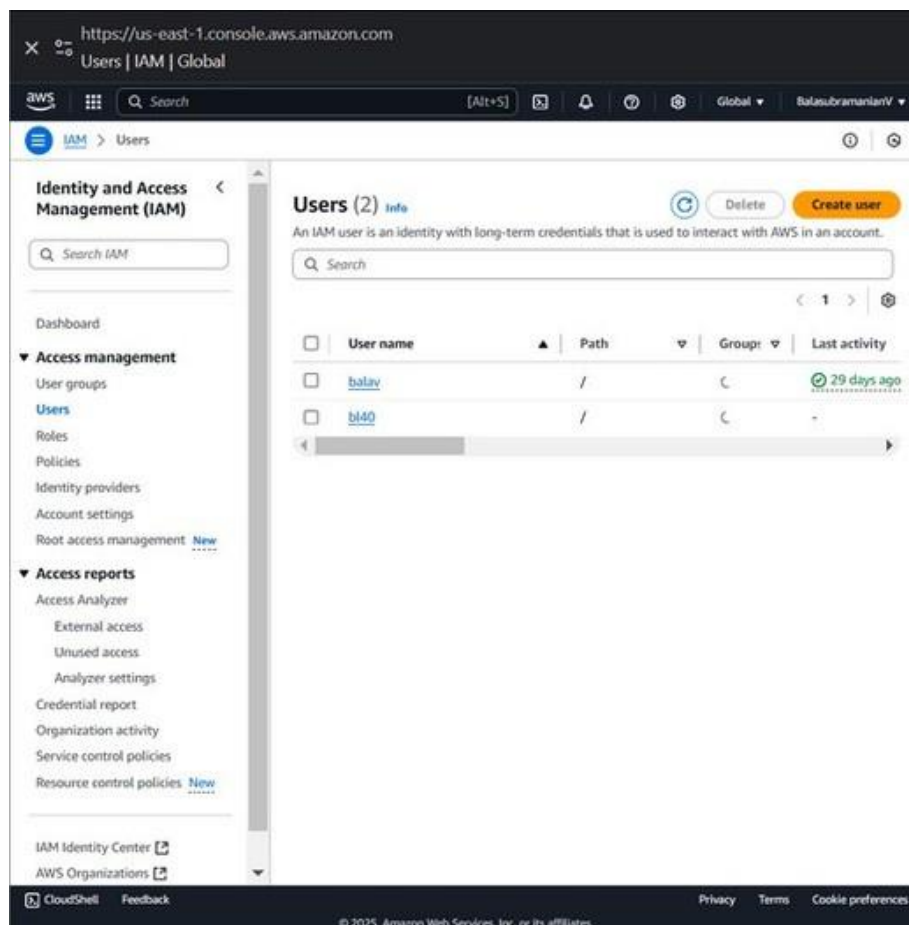


- **Navigate to the IAM service.**



- **Create a new role: Choose the service that**
- **will use this role (e.g., Compute Engine for Google Cloud or EC2 for AWS). Select the**
- **type of trusted entity (such as a service**
- **account or a specific user group). Steps**
- **are mentioned below**

-



- **Attach necessary permissions:**
- **Assign all policies to the user (e.g., read-only access, full control, or specific API permissions).**

The screenshot shows the AWS IAM console interface. The browser address bar displays `https://us-east-1.console.aws.amazon.com` and the page title is 'Add permissions | IAM | Global'. The navigation bar includes the AWS logo, a search bar, and the user's name 'BalasubramanianV'. The breadcrumb trail is 'IAM > Users > balav > Add permissions'.

On the left, a step indicator shows 'Step 1 Add permissions' (selected), 'Step 2 Review', and 'Review'.

The main heading is 'Add permissions', followed by the instruction: 'Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)'.

The 'Permissions options' section contains three radio buttons:

- ☐ Add user to group: Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- ☒ Attach policies directly: Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
- ☐ Copy permissions: Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

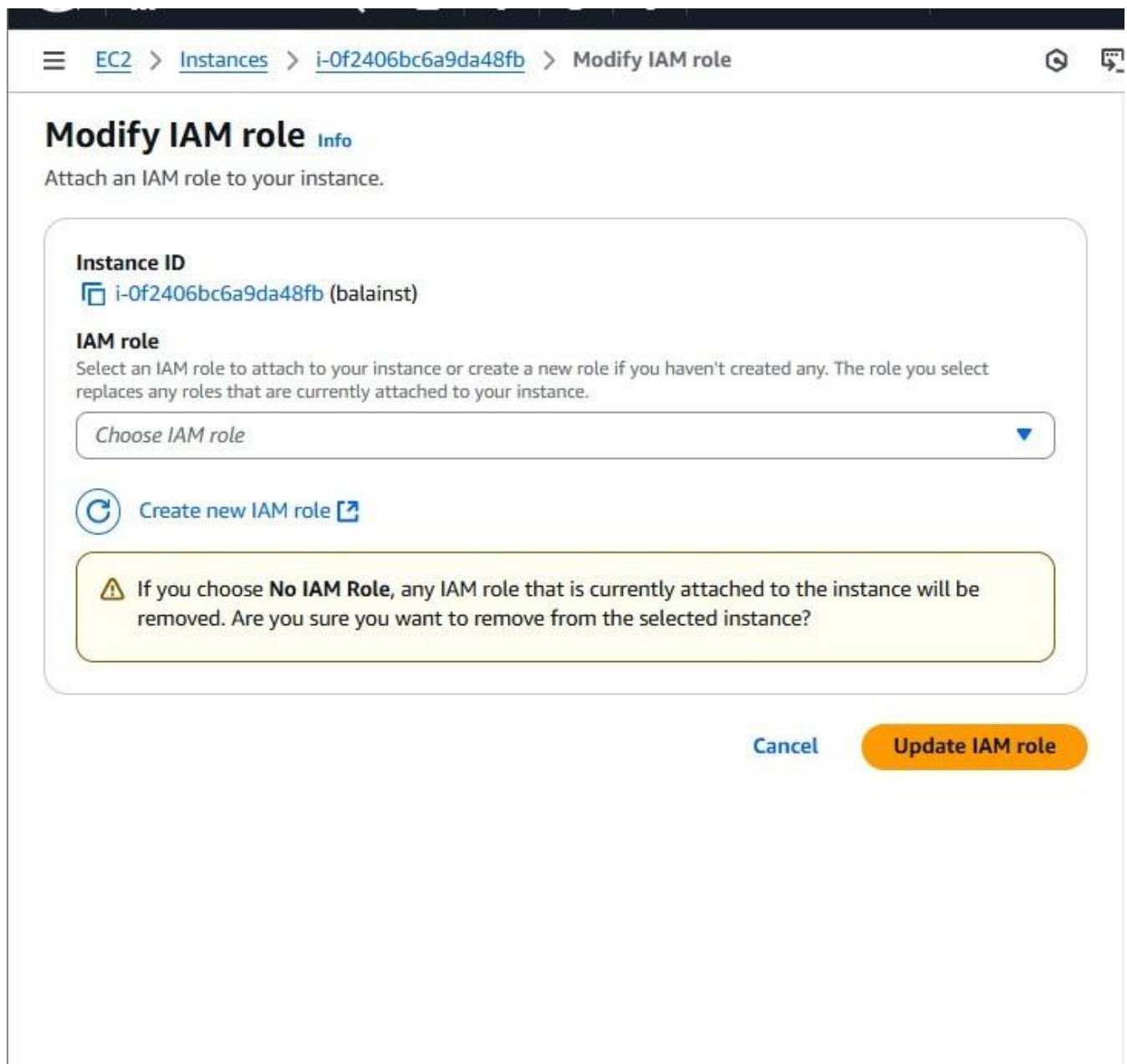
The 'Permissions policies (1318)' section features a search bar, a 'Filter by Type' dropdown set to 'All types', and a table of policies. The table has columns for 'Policy name', 'Type', and 'Attached ...'.

Policy name	Type	Attached ...
AccessAnalyzerSer...	AWS managed	0
AdministratorAccess	AWS managed - job...	1
AdministratorAcce...	AWS managed	0
AdministratorAcce...	AWS managed	0

The footer includes 'CloudShell', 'Feedback', 'Privacy', 'Terms', and 'Cookie preferences'.

- **Provide a meaningful name and description for the role.**
- **Save the role.**

Assign the Role to a Virtual Machine



The screenshot shows the AWS Management Console interface for the 'Modify IAM role' page. The breadcrumb navigation at the top indicates the path: EC2 > Instances > i-Of2406bc6a9da48fb > Modify IAM role. The main heading is 'Modify IAM role' with an 'Info' link. Below the heading is the instruction 'Attach an IAM role to your instance.' The 'Instance ID' section shows the instance 'i-Of2406bc6a9da48fb (balainst)'. The 'IAM role' section includes a description: 'Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.' There is a dropdown menu labeled 'Choose IAM role' and a link 'Create new IAM role'. A yellow warning box states: 'If you choose No IAM Role, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance?'. At the bottom right, there are 'Cancel' and 'Update IAM role' buttons.

EC2 > Instances > i-Of2406bc6a9da48fb > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID
i-Of2406bc6a9da48fb (balainst)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Choose IAM role ▼

[Create new IAM role](#)

⚠ If you choose **No IAM Role**, any IAM role that is currently attached to the instance will be removed. Are you sure you want to remove from the selected instance?

[Cancel](#) [Update IAM role](#)

- **Modify Instance IAM Role:**
- **Select the EC2 instance you want to assign the IAM role to.**
- **Click Actions > Security > Modify IAM Role.**
- **Choose the IAM role created earlier from the dropdown.**
- **Click Update IAM Role.**

3. Verify IAM Role Permissions

- **Connect to the EC2 instance:**
- **Use SSH or AWS Systems Manager Session Manager to access the instance.**
- **Test Role Permissions:**
- **Run AWS CLI commands to verify permissions.**
- **Example: To check S3 access, run:**

Connect to instance Info

Connect to your instance i-0f2406bc6a9da48fb (balainst) using any of these options

EC2 Instance Connect
Session Manager
SSH client
EC2 serial console

No associated key pair

This instance is not associated with a key pair. Without a key pair, you can't connect to the instance through SSH.

You can connect using EC2 Instance Connect with just a valid username. You can connect using Session Manager if you have been granted the necessary permissions.

Instance ID

i-0f2406bc6a9da48fb (balainst)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is id_rsa
3. Run this command, if necessary, to ensure your key is not publicly viewable.

```
chmod 400 "id_rsa"
```
4. Connect to your instance using its Public DNS:

```
ec2-3-26-217-58.ap-southeast-2.compute.amazonaws.com
```

Example:

```
ssh -i "id_rsa" ubuntu@ec2-3-26-217-58.ap-southeast-2.compute.amazonaws.com
```

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

- **Ensure that restricted actions are blocked and allowed actions work as expected.**
- **Check IAM Logs:**
- **Navigate to AWS CloudTrail to monitor access logs and verify any unauthorized attempts.**

Conclusion:

Setting up IAM roles and permissions for your EC2 instance ensures secure and controlled access to AWS resources. Regularly review and update permissions to align with security best practices. By implementing IAM roles correctly, you reduce security risks and maintain a secure AWS environment.