Placement Empowerment Program

Cloud Computing and DevOps Centre

Setting Up IAM Roles and Permissions for a Virtual Machine


Name: Stanieio S S

Department : IT

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

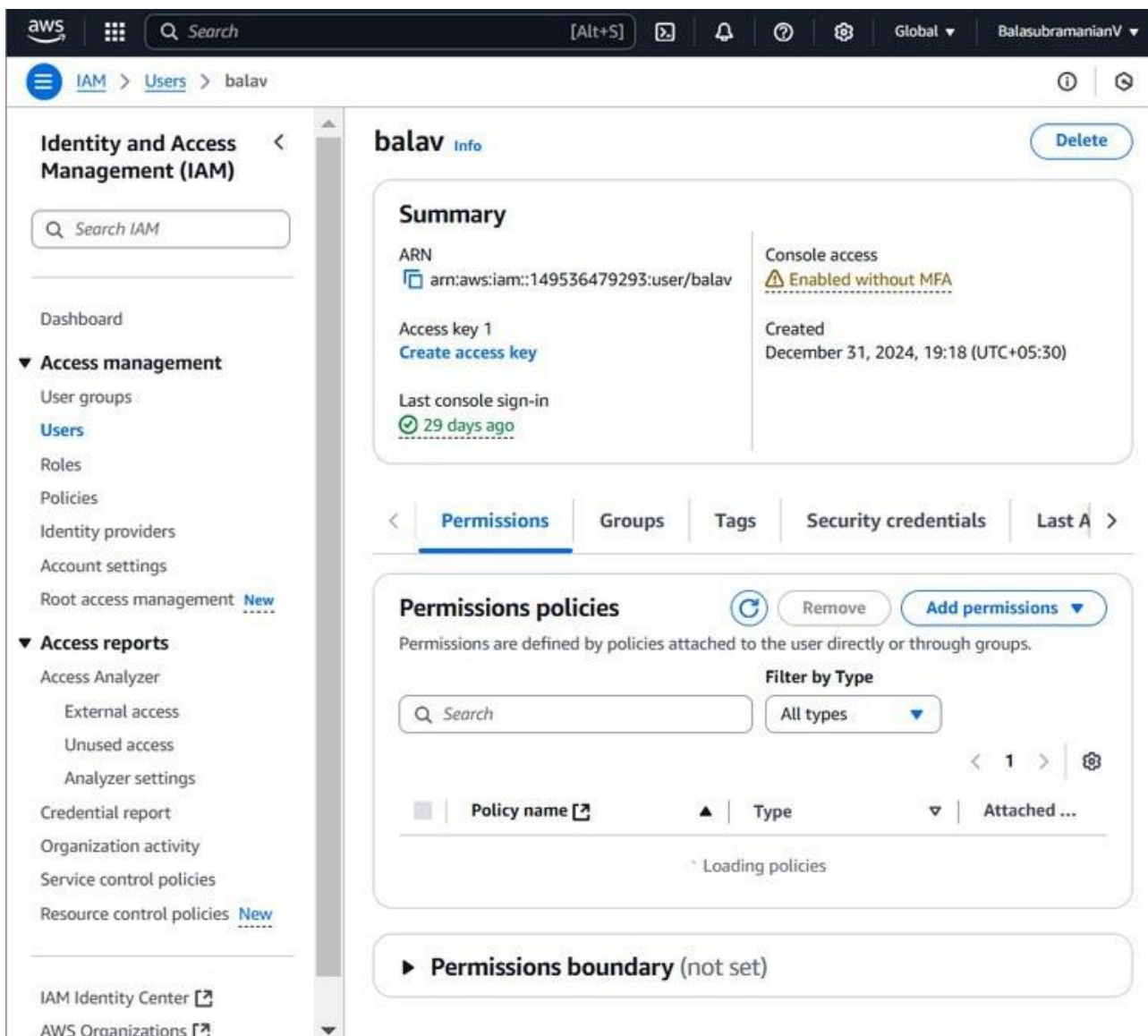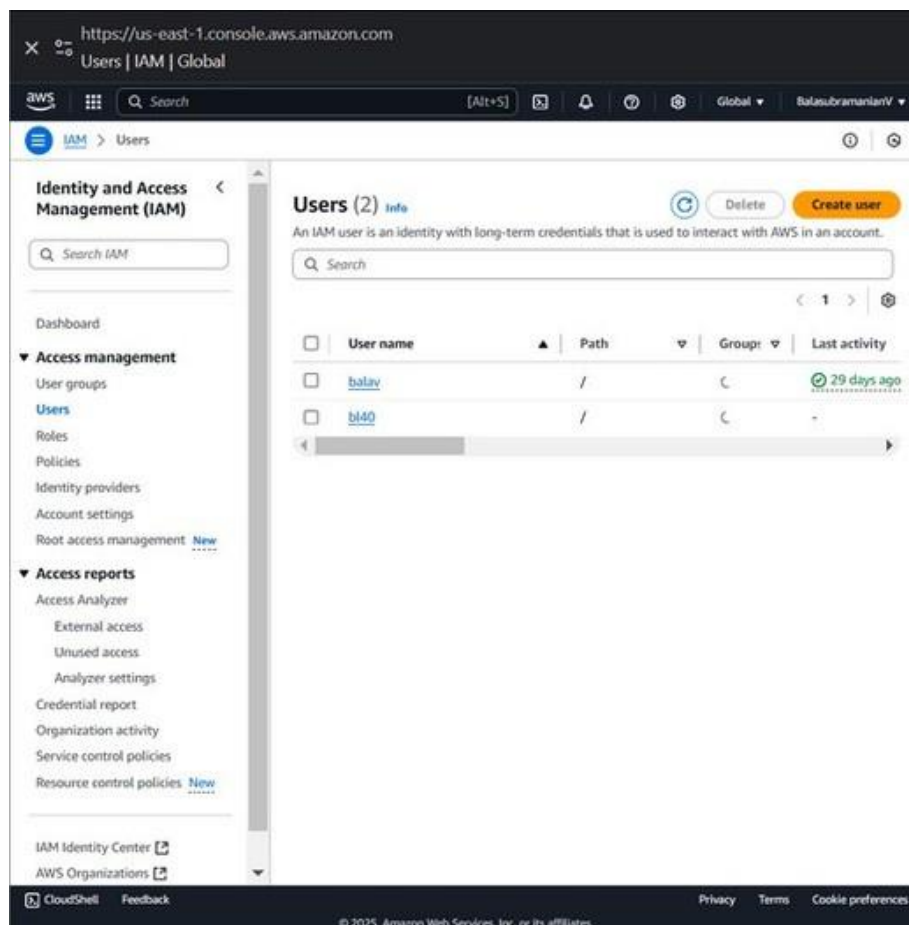- Log in to your cloud provider's console.
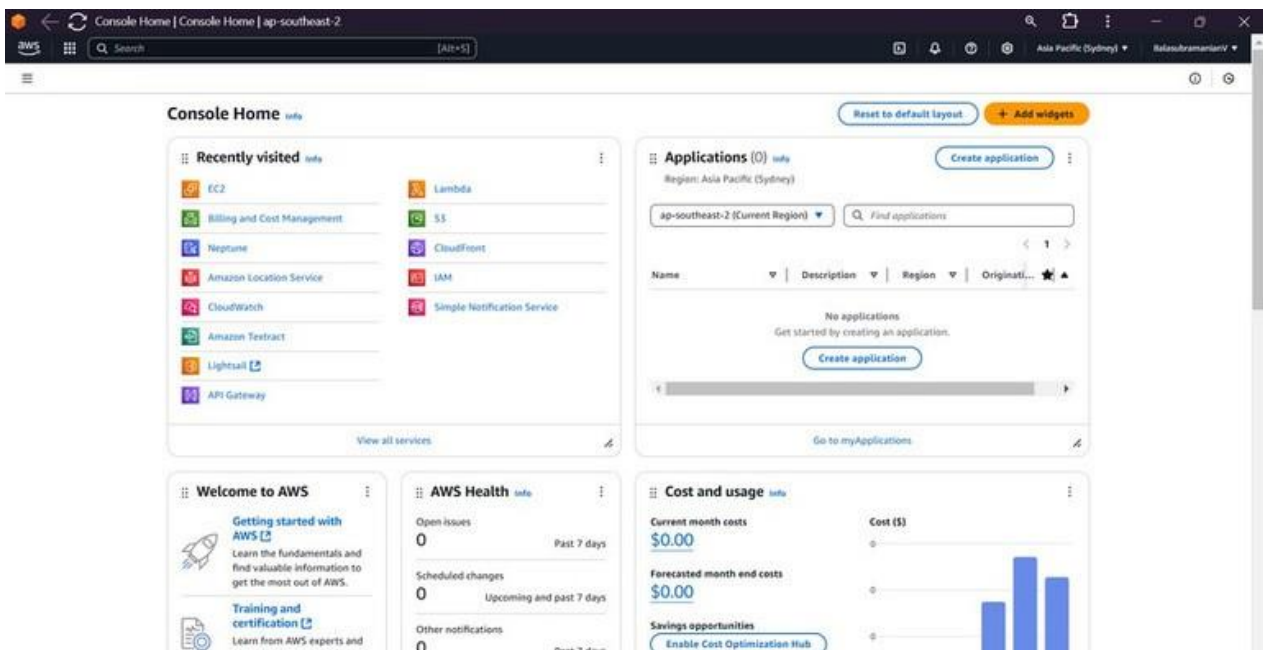
- **Navigate to the IAM service.**
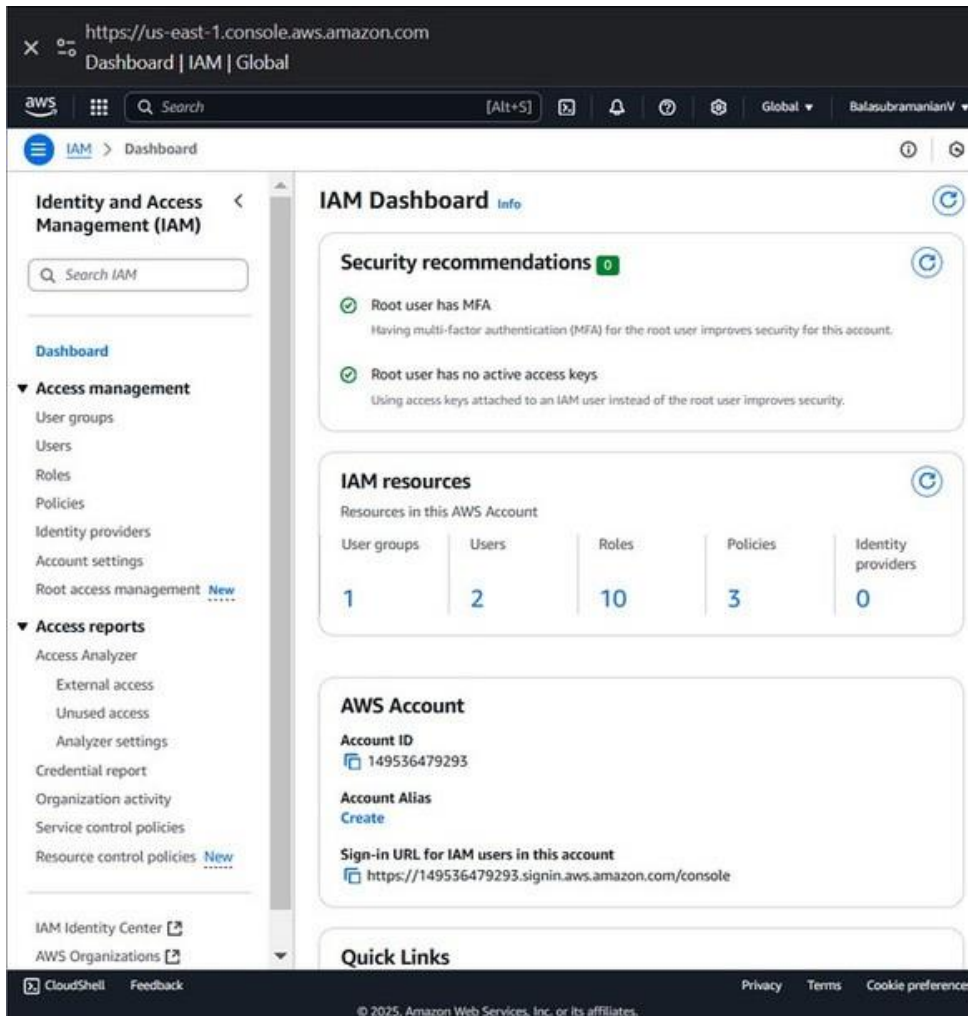
- Create a new role: Choose the service that
- will use this role (e.g., Compute Engine for
  Google Cloud or EC2 for AWS). Select the
  type of trusted entity (such as a service
- account or a specific user group). Steps
  are mentioned below

-

aws | ::: | Q Search | [Alt+S] | ⌘ | ⌂ | ? | ⚙ | Global ▾ | BalasubramanianV ▾

☰ **IAM** > Users

ⓘ ⊘

Identity and Access Management (IAM) ‹

Q Search IAM

Dashboard

▼ **Access management**
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New

▼ **Access reports**
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New

IAM Identity Center 🗗
AWS Organizations 🗗

▷ CloudShell   Feedback

Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

⟳ | Delete | **Create user**

Q Search

‹ 1 › ⚙

☐	User name	▲	Path	▽	Group; ▽	Last activity
☐	balav		/		⟲	✓ 29 days ago
☐	bl40		/		⟲	-

Privacy   Terms   Cookie preferences

---

aws | ::: | Q Search | [Alt+S] | ⌘ | ⌂ | ? | ⚙ | Global ▾ | BalasubramanianV ▾

☰ **IAM** > **Users** > balav

ⓘ ⊘

Identity and Access Management (IAM) ‹

Q Search IAM

Dashboard

▼ **Access management**
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New

▼ **Access reports**
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New

IAM Identity Center 🗗
AWS Organizations 🗗

balav Info

Delete

Summary

ARN
🗐 arn:aws:iam::149536479293:user/balav

Console access
⚠ Enabled without MFA

Access key 1
Create access key

Created
December 31, 2024, 19:18 (UTC+05:30)

Last console sign-in
✓ 29 days ago

‹ | **Permissions** | Groups | Tags | Security credentials | Last A | ›

Permissions policies

⟳ | Remove | **Add permissions ▾**

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

Q Search

All types ▾

‹ 1 › ⚙

☐	Policy name 🗗	▲	Type	▽	Attached ...

⟲ Loading policies

▶ **Permissions boundary** (not set)

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

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

Assign the Role to a Virtual Machine

- **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.