St. JOSEPH'S GROUP OF INSTITUTIONS
OMR, CHENNAI - 119

Placement Empowerment Program

Cloud Computing and DevOps Centre

Setting Up IAM Roles and Permissions for a Virtual Machine

aws

Name: Veerabuthran J

Department : CSE

St. JOSEPH'S COLLEGE OF ENGINEERING | St. JOSEPH'S INSTITUTE OF TECHNOLOGY

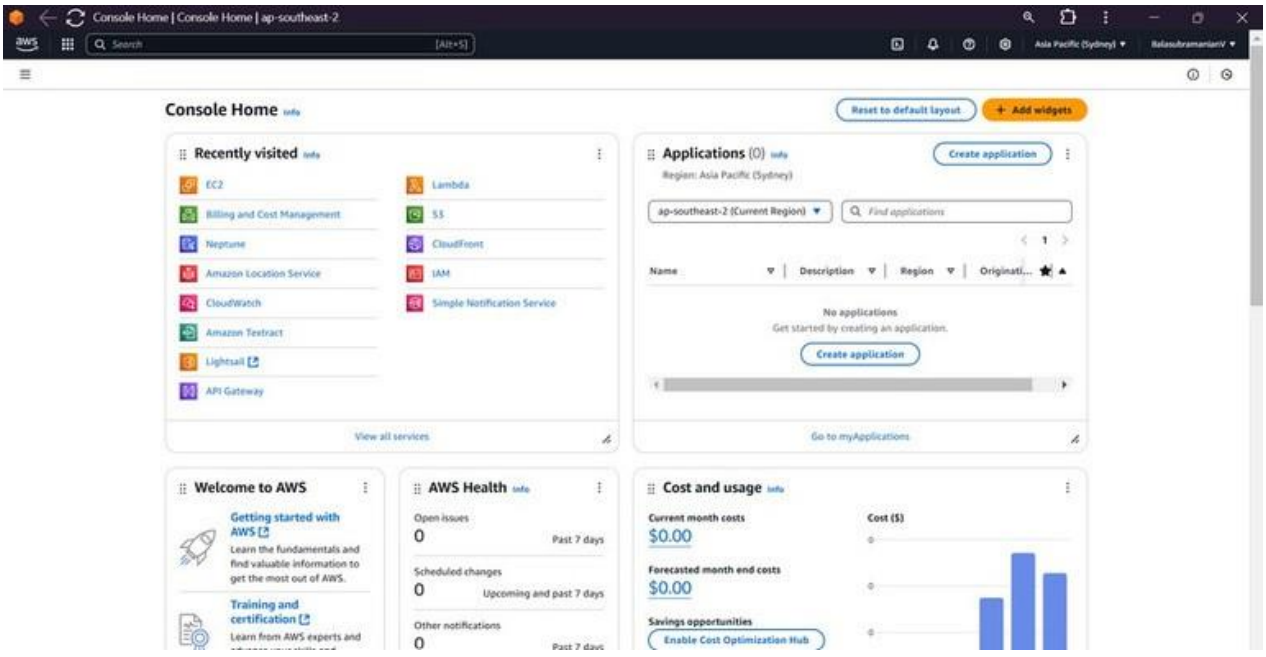
AUTONOMOUS INSTITUTIONS, AFFILIATED TO ANNA UNIVERSITY

Introduction

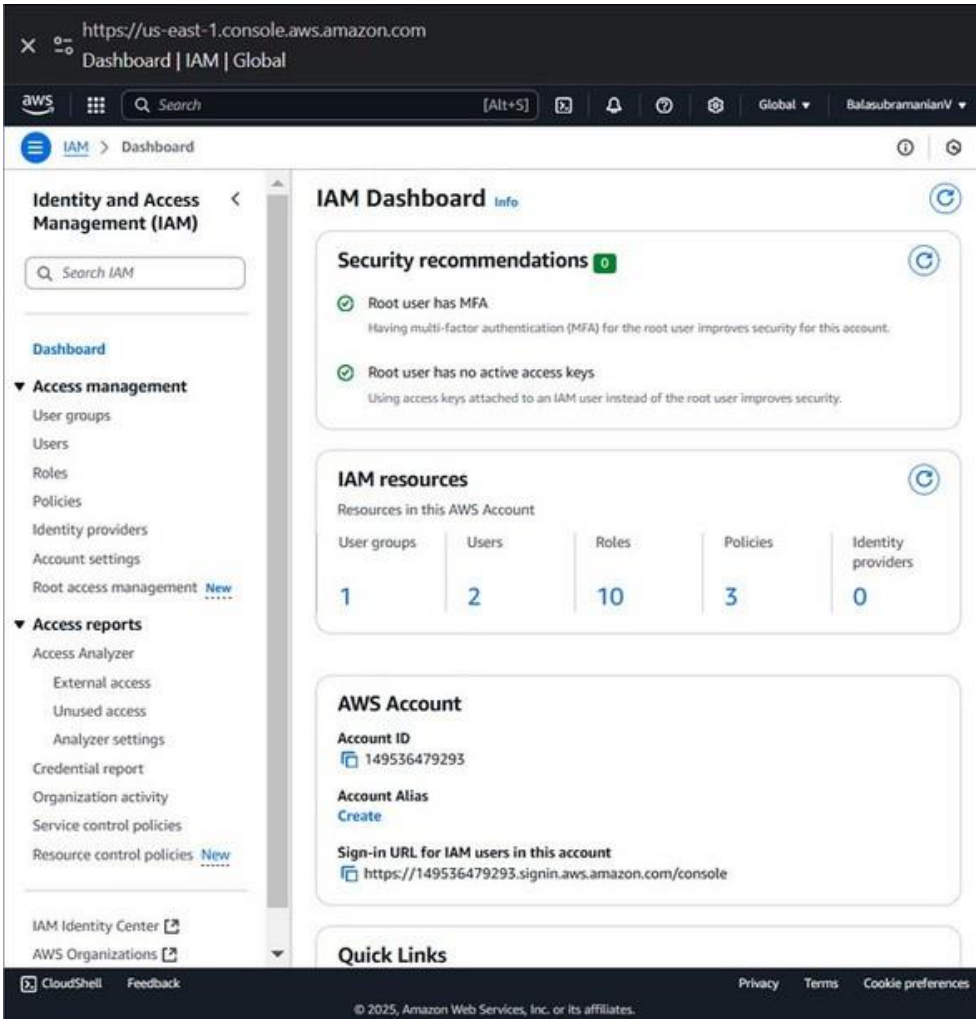
Identity and Access Management (IAM) is a crucial aspect of cloud security that allows administrators to control who can access specific resources and what actions they can perform. By setting up IAM roles and permissions, you ensure that only authorized users or services can interact with your virtual 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.

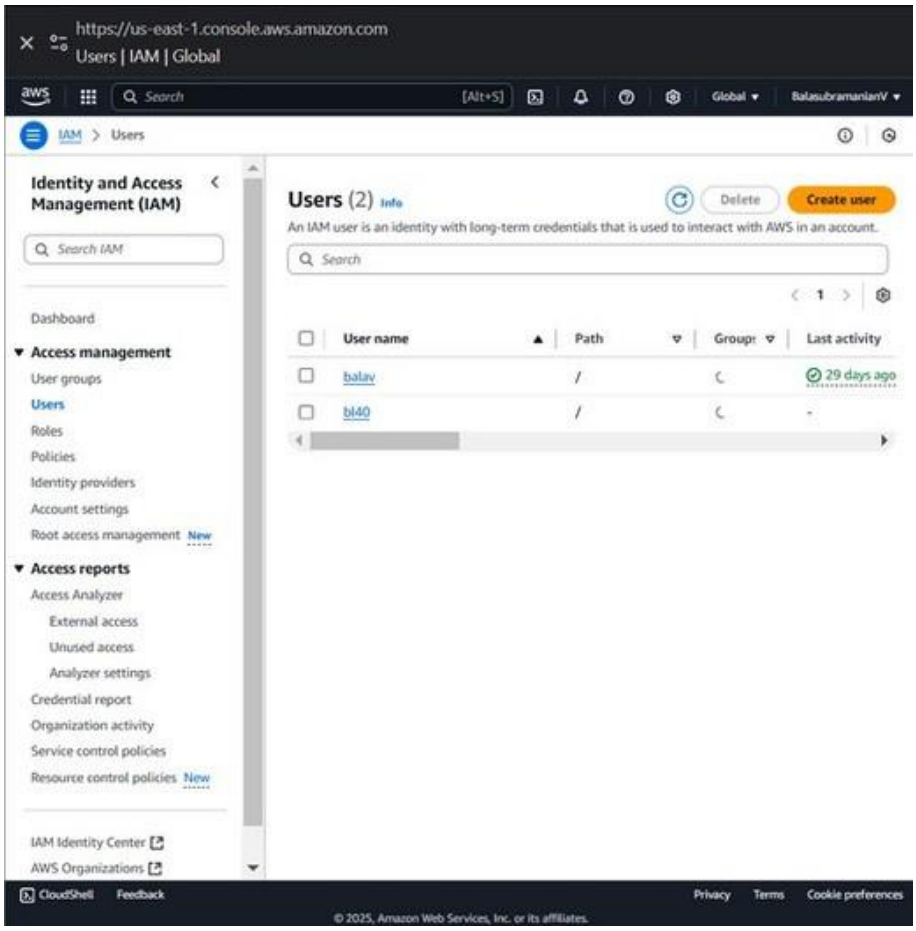


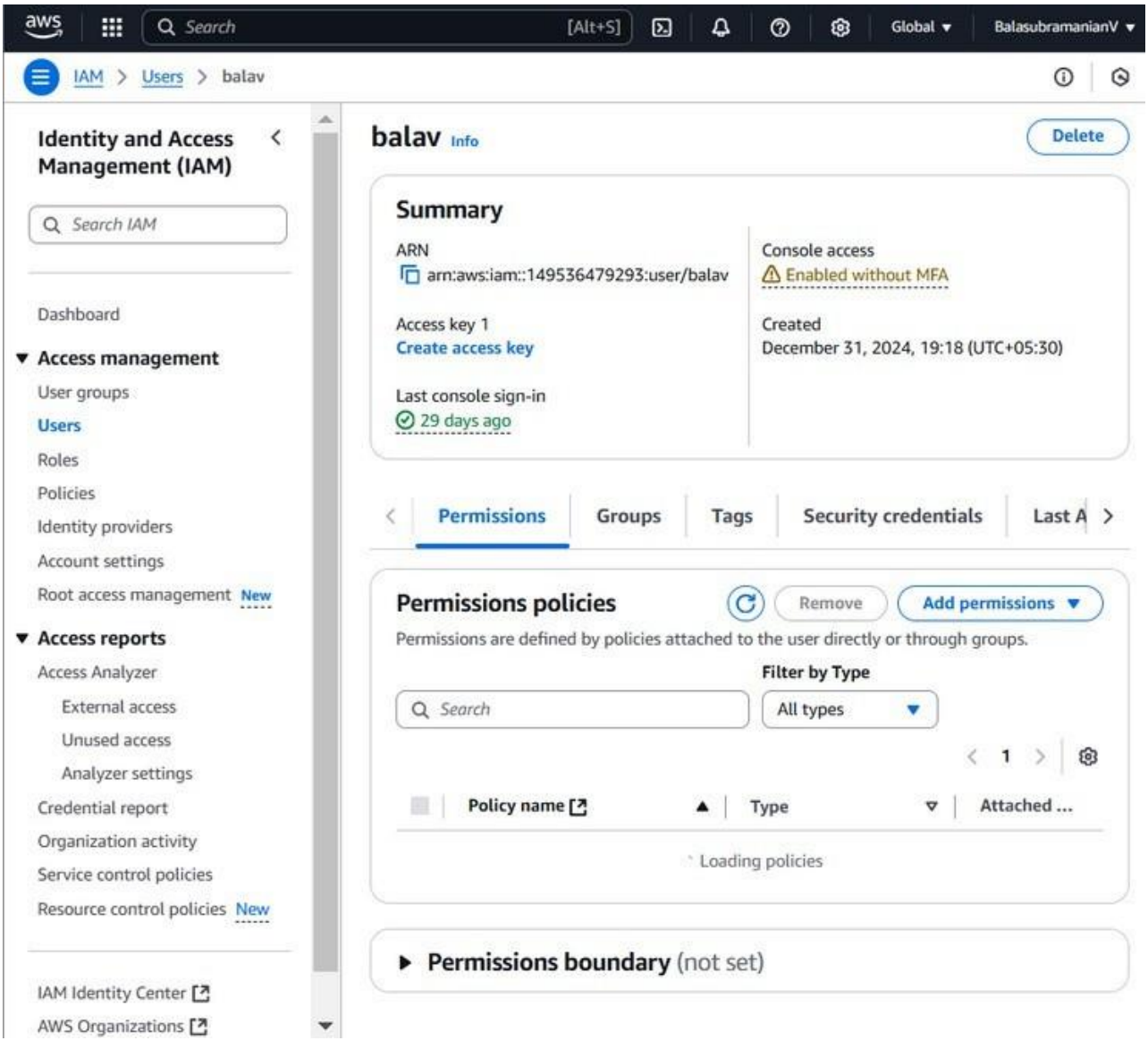
- **Navigate to the IAM service.**



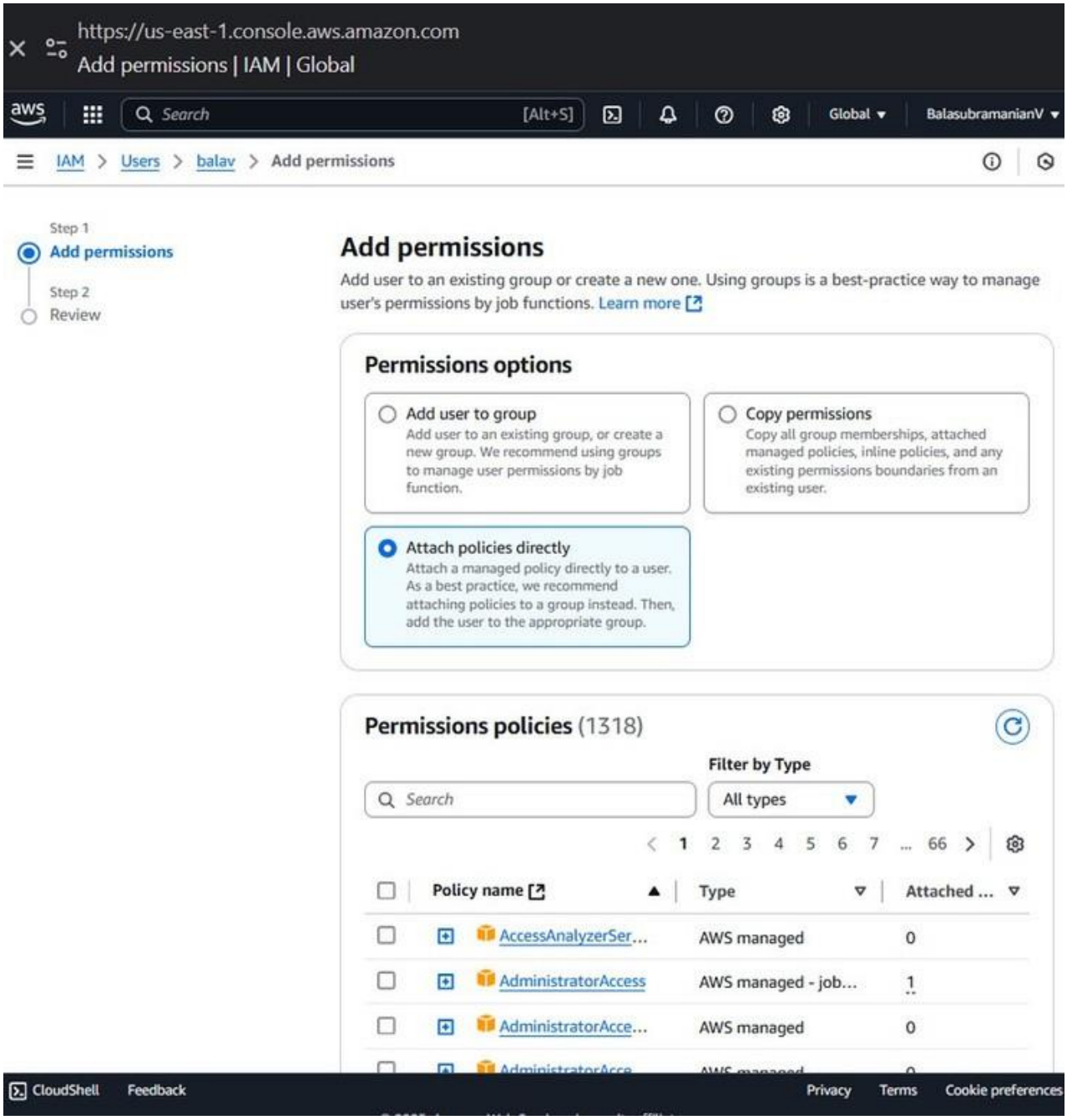
- **Create a new role: Choose the service that**
- **will use this role (e.g., Compute Engine for Google Cloud or EC2 for AWS). Select the type of trusted entity (such as a service**
- **account or a specific user group). Steps are mentioned below**

-


https://us-east-1.console.aws.amazon.com
Users | IAM | Global
Search
[Alt+S]
Global
BalasubramanianV
IAM > Users
Identity and Access Management (IAM)
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
Users (2) Info
Delete
Create user
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
User name
Path
Groups
Last activity
balav
/
29 days ago
bl40
/
-
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

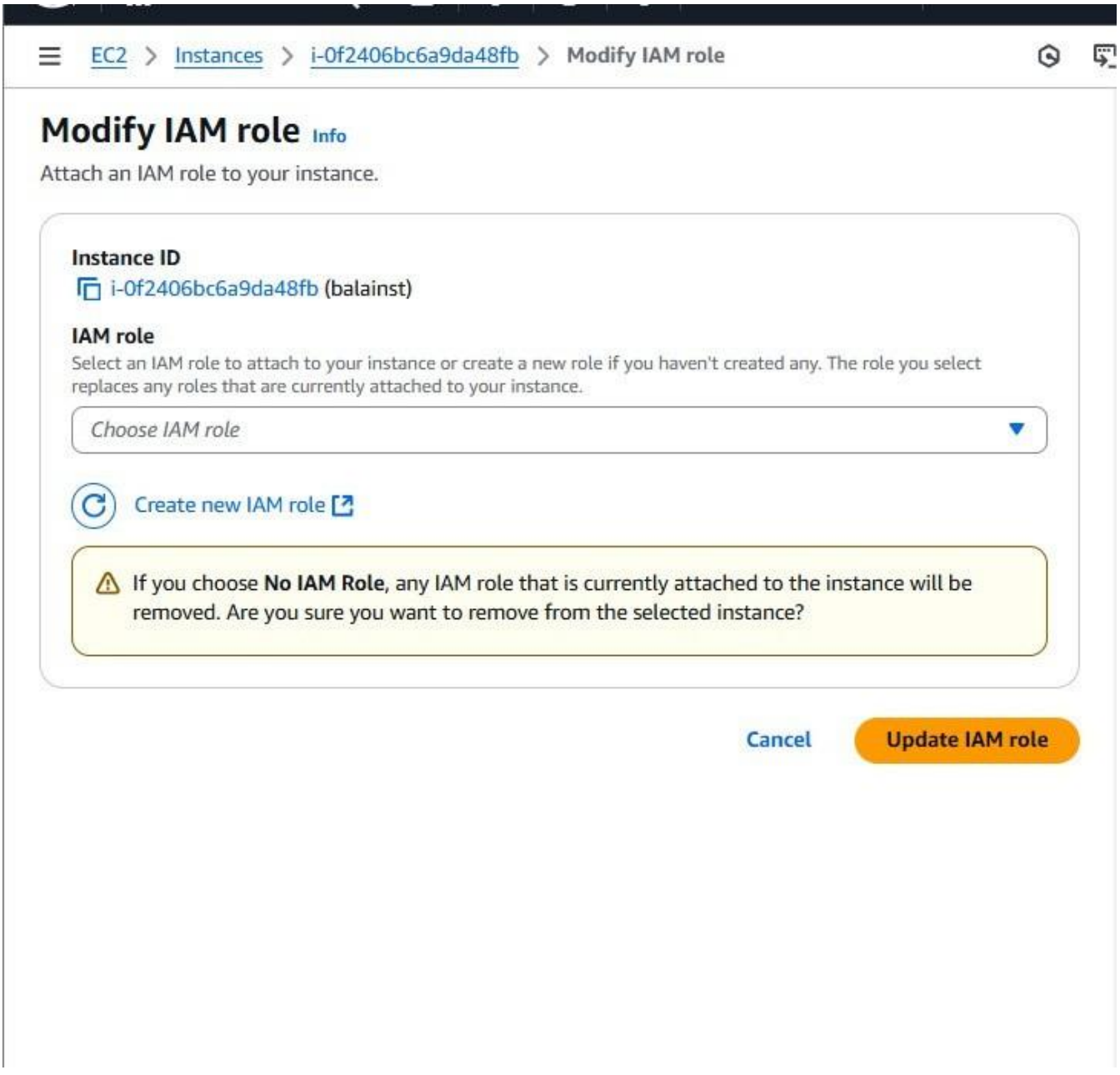

Search
[Alt+S]
Global
BalasubramanianV
IAM > Users > balav
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer 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
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:**

- **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.