

Placement Empowerment Program

Cloud Computing and DevOps Centre

Setting Up IAM Roles and Permissions for a
Virtual Machine



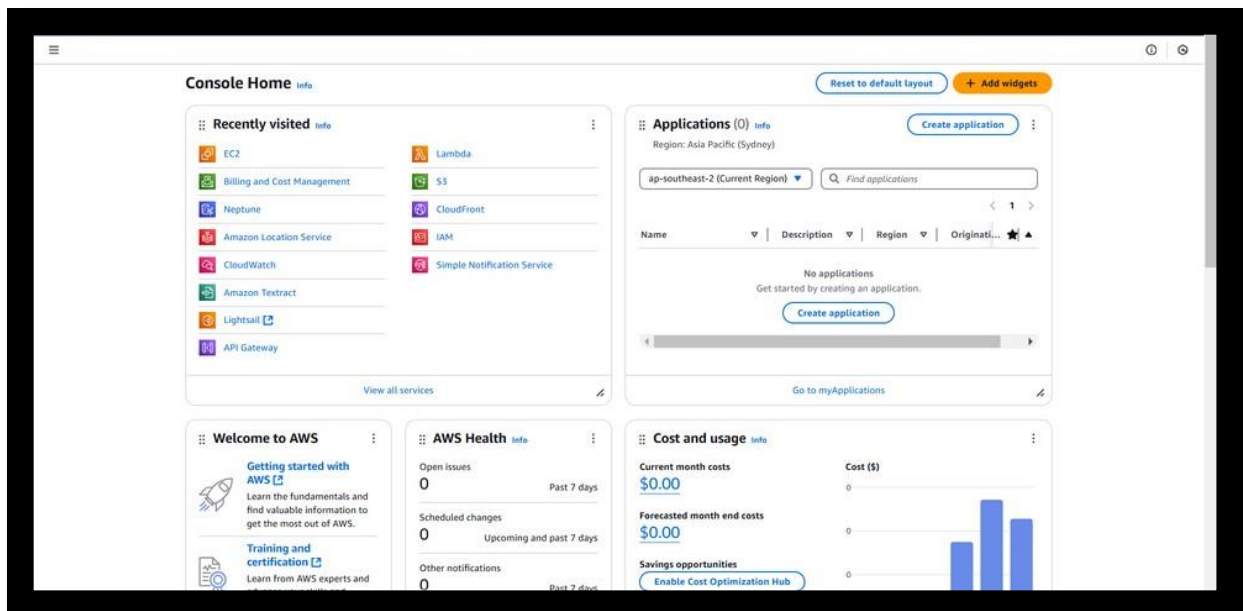
Name: ANANDA KRISHNAN S A
DEPT: INFORMATION TECHNOLOGY

Introduction

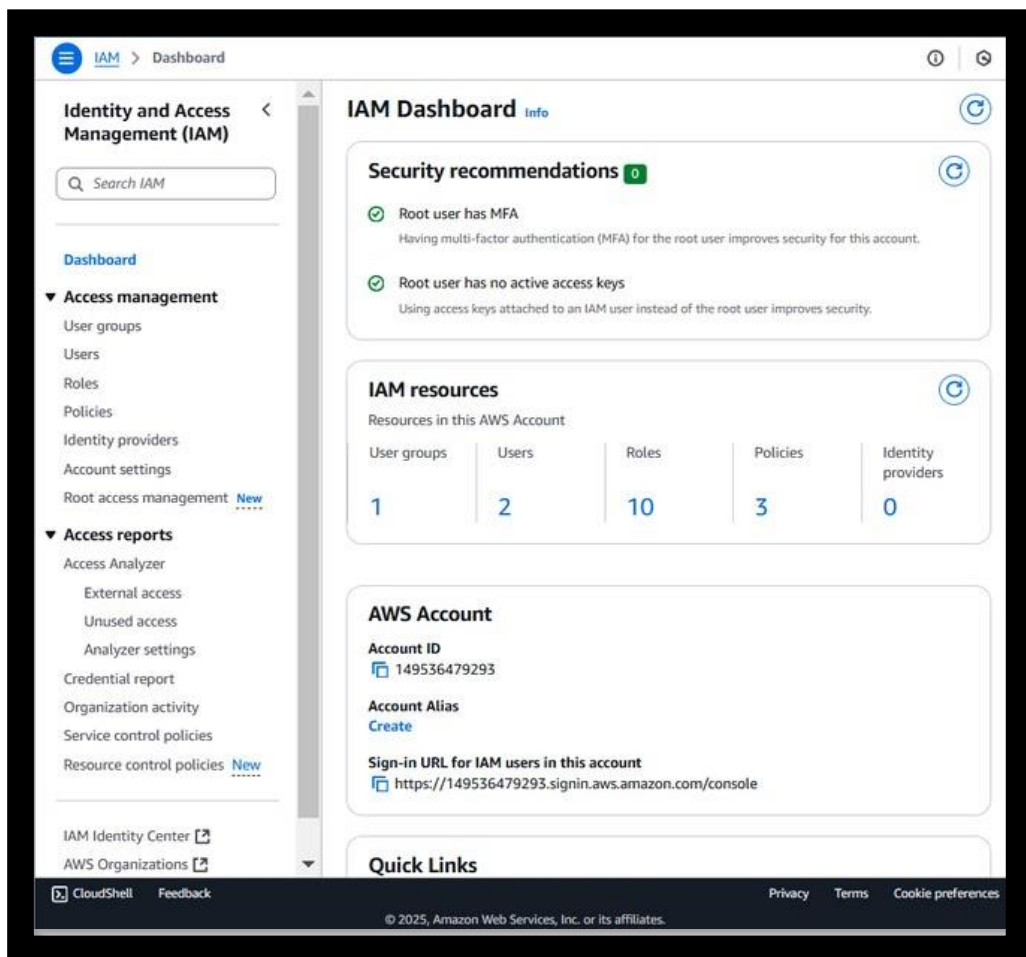
- Identity and Access Management (IAM) is a crucial aspect of cloud security that allows administrators to control who can access specific resources and what actions they can perform. By setting up IAM roles and permissions, you ensure that only authorized users or services can interact with your virtual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

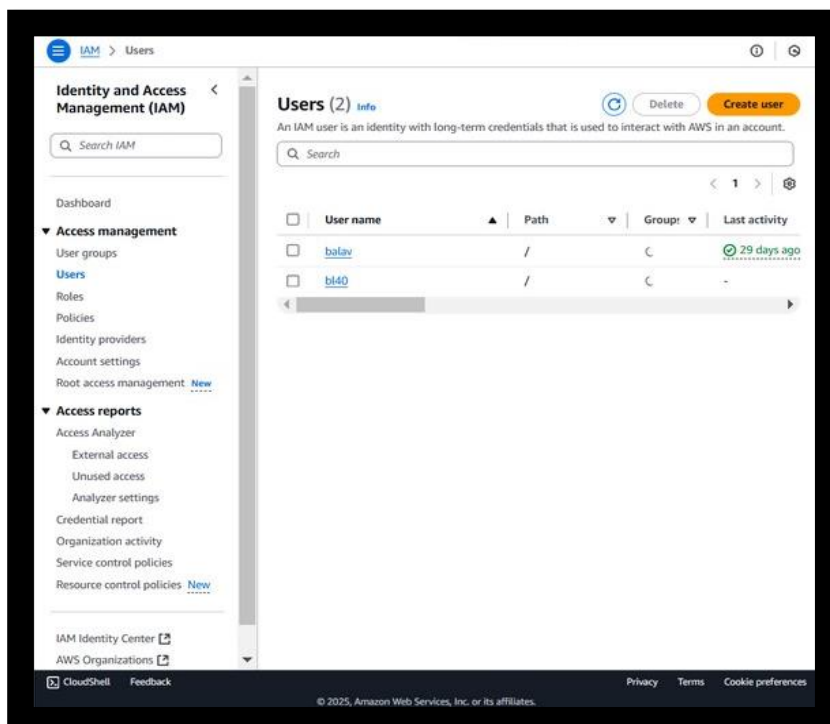
- Log in to your cloud provider's console

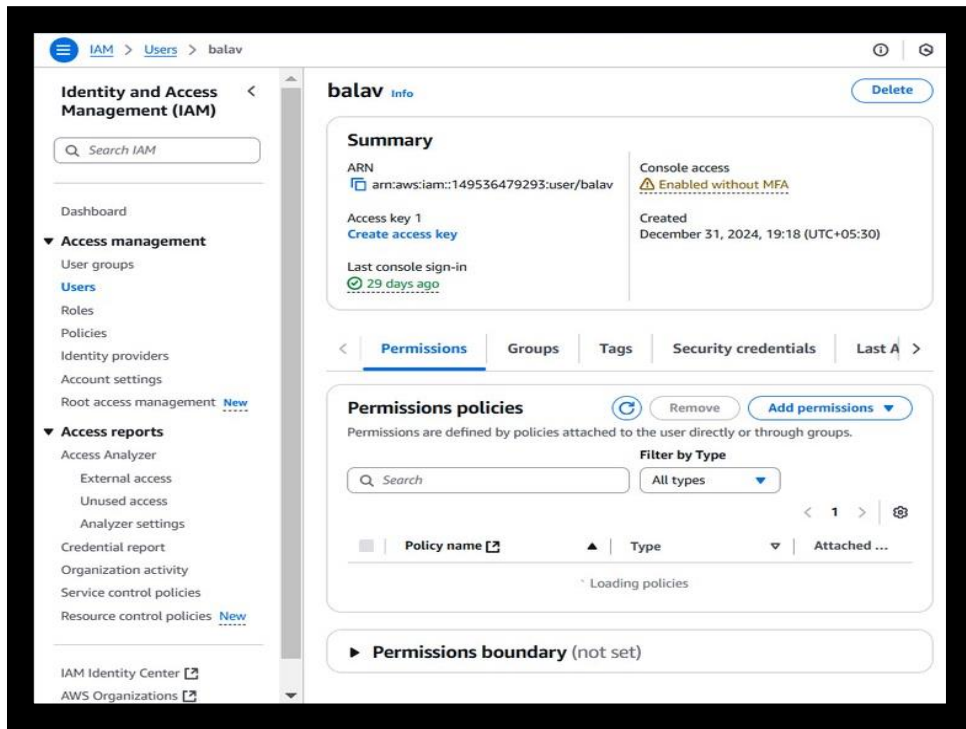


- Navigate to the IAM service.

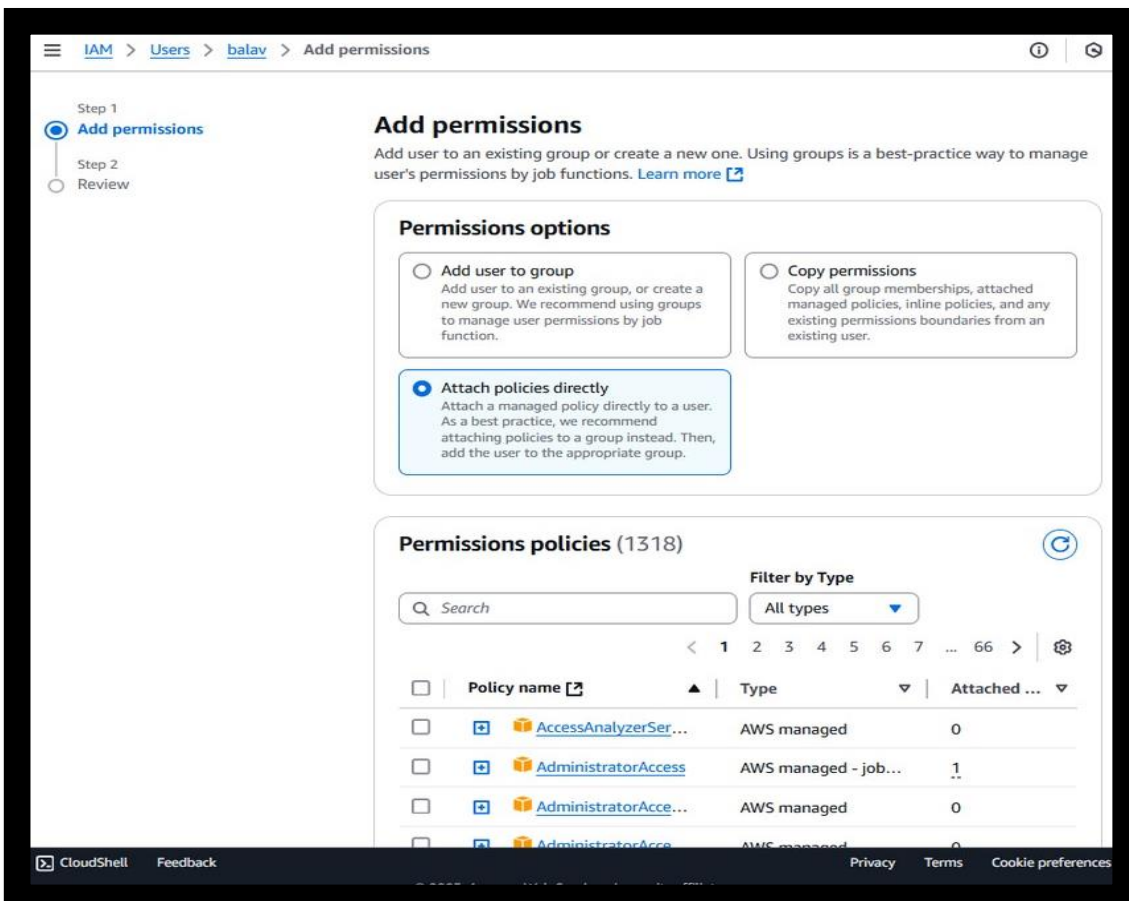


- Create a new role.
- Choose the service that will use this role (e.g., Compute Engine for Google Cloud or EC2 for AWS).
- Select the type of trusted entity (such as a service account or a specific user group).
- Steps are mentioned below.





- Attach necessary permissions.
- Assign policies that define allowed actions (e.g., read-only access, full control, or specific API permissions).



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

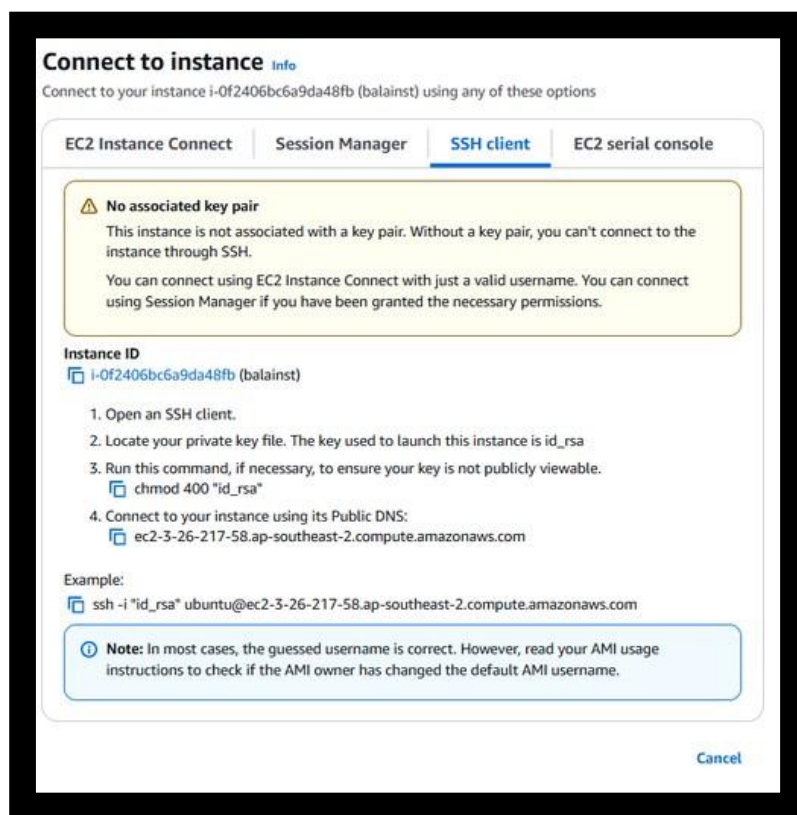
Assign the Role to a Virtual Machine

The screenshot shows the AWS Management Console interface for modifying an IAM role on an EC2 instance. The breadcrumb navigation at the top reads: **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 interface displays the **Instance ID** as **i-Of2406bc6a9da48fb (balainst)**. Under the **IAM role** section, it says: "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" with a downward arrow. Below the dropdown is a link that says "Create new IAM role" with a circular arrow icon and an external link icon. A yellow warning box contains the text: "⚠ 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 two buttons: a blue "Cancel" button and an orange "Update IAM role" button.

- 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.

THANK YOU!