**Introduction**

You have the ability to create IAM Roles using the AWS Management Console. An IAM role is an IAM entity that has specific permissions. An IAM role is similar to an IAM user in that you can manage its access to AWS resources using policies. IAM roles are attachable to other IAM services like AWS EC2 and AWS Lambda, to manage resource access for those services. In this Lab Step, you will practice creating an IAM role.

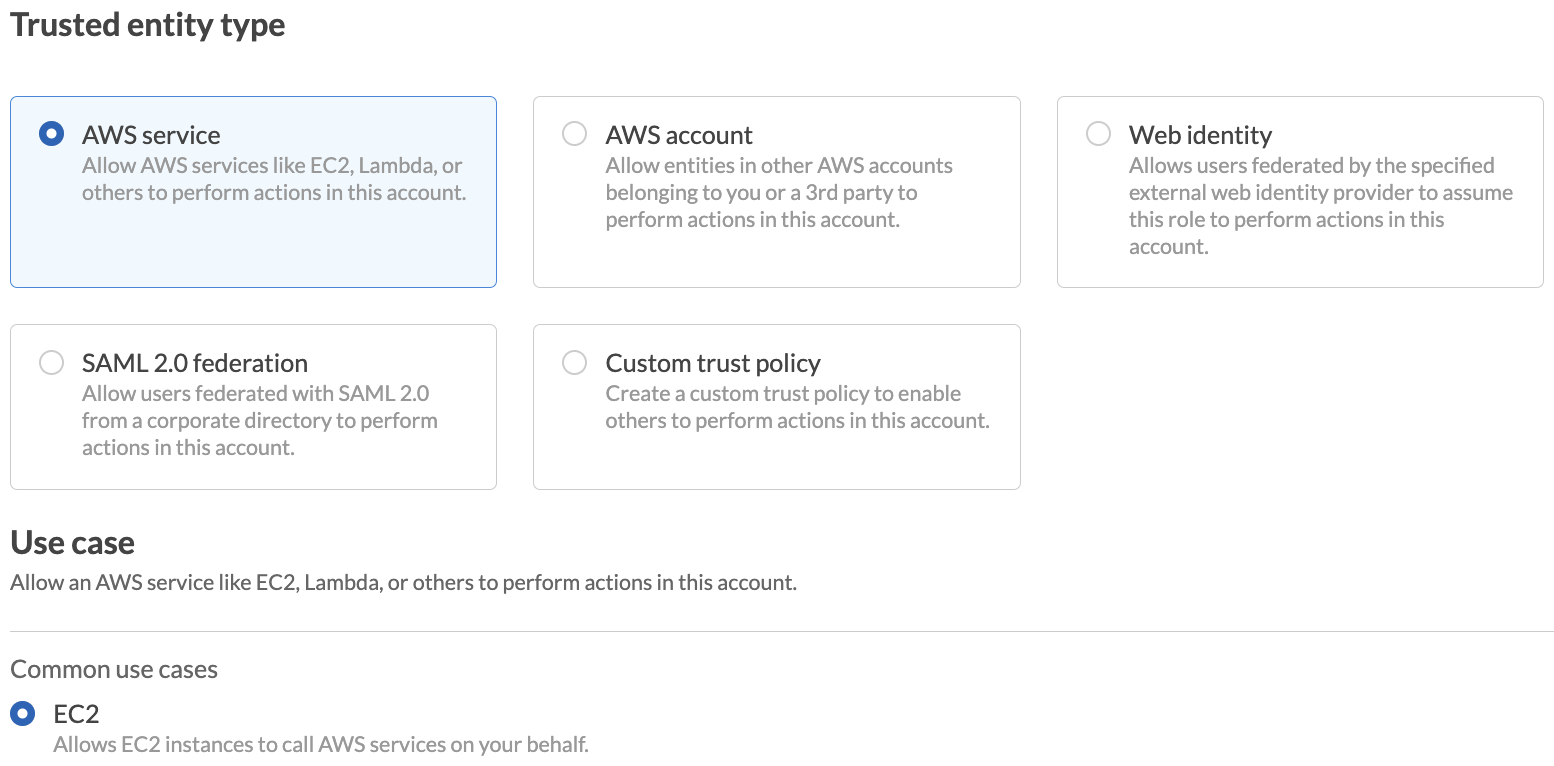
1. From the **Identity & Access Management** dashboard, click **Roles**:



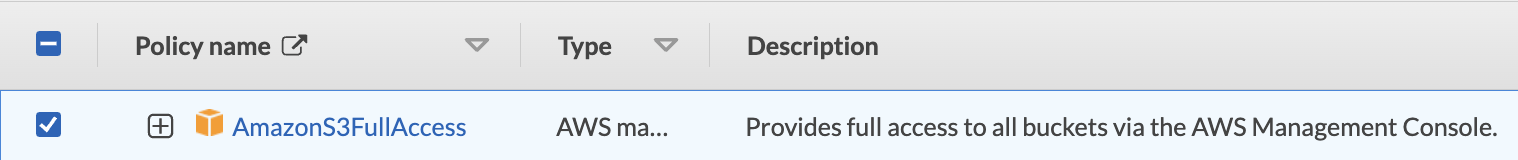
2. Click**Create role**:



3. On the **Create Role** page, select **AWS service**under **Trusted entity type** and **EC2**under **Use case**, then click **Next**:

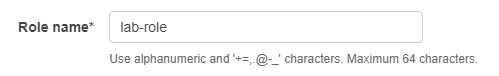


4. On the **Attach permissions** page, filter for the name *S3Full* and select the policy **AmazonS3FullAccess**:



5. Click **Next**.

6. Set the **Role name** to *lab-role*:



7. Click **Create Role**:

alt

8. Click on the role you created to inspect its details:

alt

**Summary**

In this Lab Step, you used the **IAM Management**Dashboard to create an IAM role.

VALIDATION CHECKS

**1Checks**

Check again

**Created IAM Role**

Check that an IAM role with the given name and attached policy exists

AWS Identity and Access Management (IAM)