**Introduction**

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

You can create customer-managed policies to define sets of permissions to attach to principal entities (users, groups, and roles) in your AWS account

**Instructions**

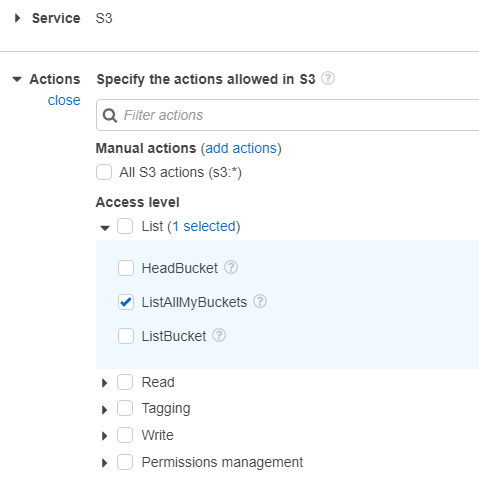
1. On the **Identity & Access Management** dashboard, click **Policies** on the left:



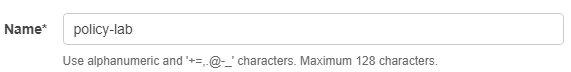
2. Click **Create Policy**:



3. Select **S3**for the **Service** and **ListAllMyBuckets** for the **Action**:



4.  Click **Next: Tags**, and click**Next: Review** and in Policy Name field insert *policy-lab*:



5. Choose **Create Policy**to save your new policy.

**Summary**

In this Lab Step, you used the **Identity & Access Management** dashboard to create a customer-managed IAM policy.

VALIDATION CHECKS

**1Checks**

Check again

**Created Customer Managed IAM Policy**

Check that a customer managed IAM policy with the given name exists

AWS Identity and Access Management (IAM)