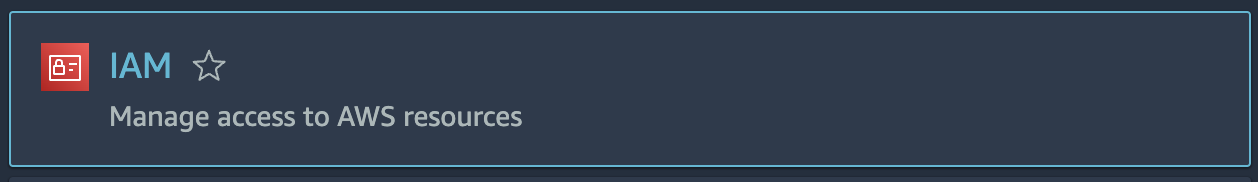
**Introduction**

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.

*Warning*: Because of our strict policy, you have to use the same names provided in the lab for each resource that needs to be created (group, users, etc.).

**Instructions**

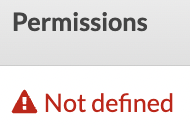
1. In the AWS Management Console search bar, enter *IAM*, and click the **IAM** result under **Services**:



2. From the IAM dashboard, click on **User groups** link in the sidebar menu:



*Note:* You will see errors indicating your student user does not have permissions to perform specific actions:

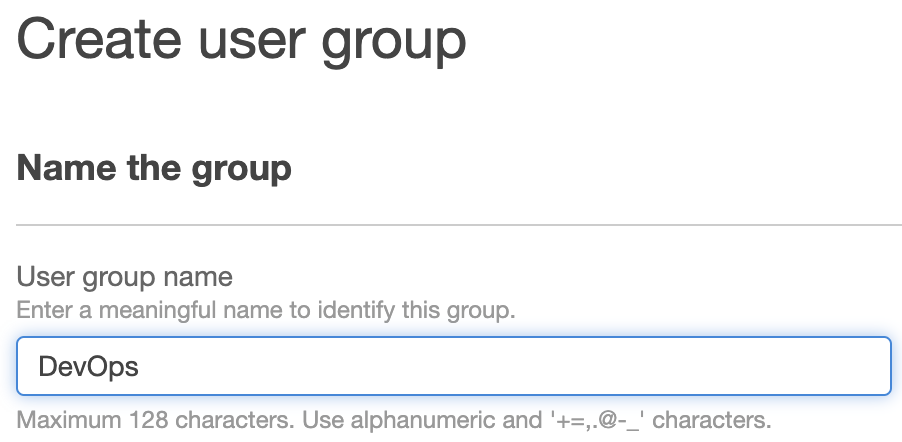


This is expected and just means that your permissions are limited to the scope of this lab.

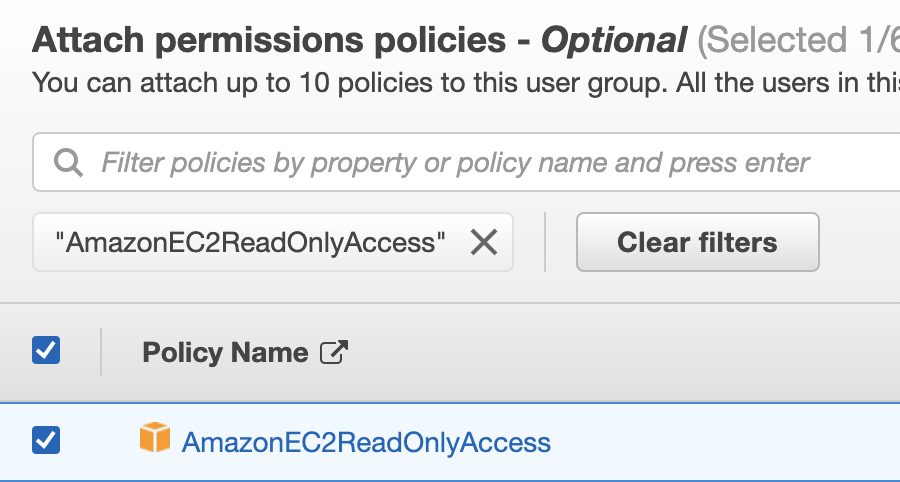
3. Click on the **Create Group**blue button for creating a new IAM group:



4. In the **User group name** field, enter *DevOps* as the name of the group:



5. Skip down to the **Attach permissions policies** section, enter *AmazonEC2ReadOnlyAccess* into the search bar and select the resulting policy: **AmazonEC2ReadOnlyAccess**:



6. Click **Create Group.**

The **Groups** page now lists the new group and you are able to assign the DevOps group to any available user:



**Summary**

In this Lab Step, you used the IAM Management console to create an IAM group.

VALIDATION CHECKS

**2Checks**

Check again

**Created IAM Group**

Check that an IAM Group with the specified name exists

AWS Identity and Access Management (IAM)

**Attached Policy to IAM Group**

Check that only the specified policy was attached to the IAM Group

AWS Identity and Access Management (IAM)