COURSEWARE

AWS IAM Users

Contents

Overview

Identity Access Management (IAM) is a service which can allow the root user to create account, roles and groups.
The root user also can grant permissions and has no restriction, this is mainly because the root user is paying for all the services being used.
So, if a developer needs access to EC2 instance, rather than providing the credentials for the root user, the root user will create an account which has only access to EC2 instance.
This is known as **Principle of least privilege**.

This tutorial will guide you on how to create a user which should be your main account as best practice.

When creating a user there are 2 options for the access type:

- Programmatic Access
- AWS Management Console access

These types of access types are discussed further.

Programmatic Access

This type of access would usually be only needed for specific job roles, meaning for accounts that only need access through the AWS CLI.
When creating a user with this type of access, the user would only be provided with *Access* and *Secret* key.
This would only allow the user to access AWS resources depending on the policies attached to the user created.

AWS Management Console access

This type of access allows users to have access to the console, again should be only specific to the business need.
This would allow you to create a user, set up using their email and a password will be auto-generated.
You will be given the option to email the user the credentials through AWS or download the *.csv* file and send out the email seperately.

You will also have 3 options to setting a user its permissions:

- Add user to group
- Copy permissions from existing user
- Attach existing policies directly

Add user to group

This option is useful when creating multiple user accounts.
So if a group already exists with certain policies attached, you can add a user to this group.
All users in this group will have the same permissions, and you will be able to update all users policies by modifying the policies for the group.
Great way of managing an entire team of developers whom might only need access to EC2 Instances.
You can also remove users from this group.

Copy permissions from existing user

This setting is useful for reusing policies.
If you need a quick solution to providing the exact same policy, then this setting would resolve the issue.
If a user already has administrative access, you can select that user and provide the same administrative access to the new user.

Attach existing policies directly

When creating a new user whom would require completely new policies to be attached, this is the option you would require.
You have the options to attached *Managed Policies*, these are policies which have been created by AWS.
You can also create your own custom policies.
These policies would be written in JSON format.

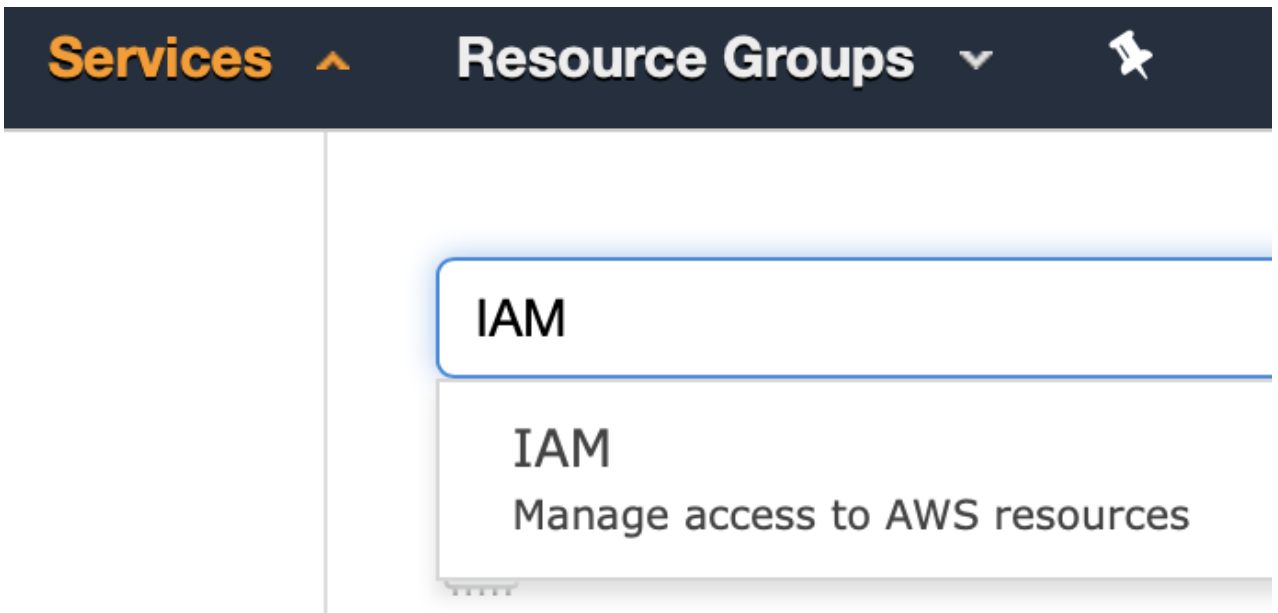
Pre-requisite

Topics:

- AWS SignUp

Tutorial

1. Navigate to the AWS Console and sign in here
2. Search for IAM under the services drop-down menu.



3. You will then be redirected to the IAM Dashboard.
   On the left navigation panel, click on the *Users* section.
4. This will show an overview of all the users that have been created.
   Click on the **Add user** button.
5. Provide this user a name, this name will be used to keep a track on who has AWS access to your account.
   Provide a meaningful names, creating a user called *steve* for *bob* will get confusing when steve joins the company.
6. We will give this user **AWS Management Console Access**, as this should be the main account you login as to ensure we follow AWS recommended security checks.

7. You will given more options when check **AWS Management Console Access**.
   Leave it as default.

8. Click on **Next: Permission** button.

9. You have options for selecting the type of permissions to attach to this user.
   Click on the *Attach existing policies directly* tab.
   From this, search for **Admin**, and check **AdministratorAccess**.

10. Continue to **Next** until you create the account.
    There is no need to create a tag.

11. The final step will prompt you to either download the *.csv* file or to send this out as an email through AWS.
    Ensure you download this file, as you will be login in as this user.

Exercises

Create a user which has only access to EC2 Instances. This can be used later on when going over EC2 Instances.