

Cloud Computing - MEiL WUT

Report

Maciej Morawski

January 2021

1. Course of action

1.1. Educate Starter Account

Until recently, Educate Starter Account (ESA) access was assigned to all students who created an account on AWS Educate (<https://aws.amazon.com/education/awseducate/>) and were successful in the application process. Currently, however, to receive an Educate Starter Account, an account on AWS Educate must be created through an invitation link from an educator who is an AWS Educate member. Once you get an Educate Starter Account, you get a certain amount of dollars to spend on your AWS account. In addition, you don't have to enter your card details when you sign up for the account, so you are protected from losing our money.

1.2. AWS Console

After logging into your AWS Educate account, navigate to AWS Account (Fig. 1.).



Fig. 1.

Next, navigate to your AWS Educate Starter Account (Fig. 2.).

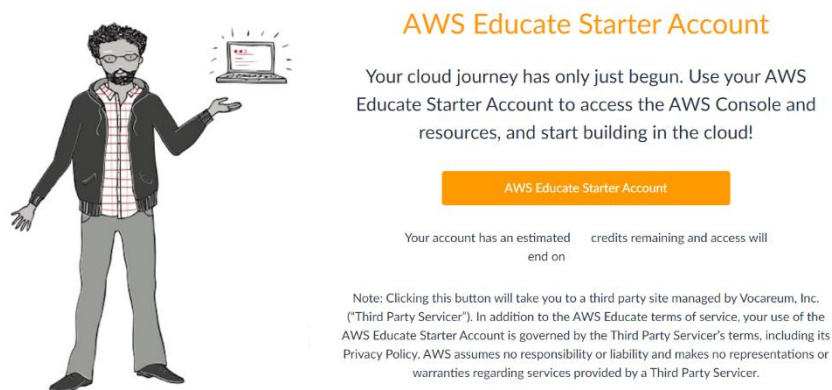


Fig. 2.

After pressing AWS Educate Starter Account, we will be redirected to vocareum.com. This page displays the status of our account. There is also an AWS Console button available, when pressed it is possible to go to our AWS console and use AWS services.

1.3. Security Groups (EC2)

The first service used was the EC2 service (Fig. 3.).



Fig. 3.

After entering this service go to "Security Groups" tab in "Network & Security" section. (Fig. 4.).

▼ Network & Security

Security Groups New

Fig. 4.

A security group is an AWS firewall solution that performs one primary function: to filter incoming and outgoing traffic from an EC2 instance.

Therefore, to ensure the security of our instances' communication, we create a "Security group" by selecting the "Create Security group" button (Fig. 5.).

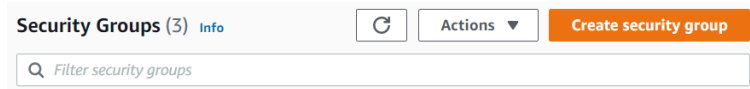


Fig. 5.

First fill in the basic information (Fig. 6.) that is required - the name of the group (which cannot be edited later) and a short description of up to 255 characters.

A screenshot of the 'Basic details' section of the AWS Security Groups 'Create' wizard. It has a title 'Basic details' with an 'Info' link. There are two input fields. The first is labeled 'Security group name' with an 'Info' link; it contains the text 'CloudComputingMM' and has a small note below it stating 'Name cannot be edited after creation.' The second is labeled 'Description' with an 'Info' link; it contains the text 'Allows SSH access to developers'.

Fig. 6.

Then add the "Inbound rule" by clicking the "Add rule" button (Fig. 7.).

A screenshot of the 'Inbound rules' section of the AWS Security Groups 'Create' wizard. It has a title 'Inbound rules' with an 'Info' link. Below the title, it says 'This security group has no inbound rules.' At the bottom left, there is a button labeled 'Add rule'.

Fig. 7.

Change the "Type" field to "All traffic" (Fig. 8.). In the Source field enter 0.0.0.0/0. Leave the rest of the settings as default.

A screenshot of the 'Type' field in the AWS Security Groups 'Create' wizard. It is a dropdown menu with the text 'All traffic' selected. Above the dropdown is the label 'Type' with an 'Info' link.

Fig. 8.

Then we can create the group we configured (Fig. 9.).

A screenshot of the bottom of the AWS Security Groups 'Create' wizard. It shows two buttons: a grey 'Cancel' button and an orange 'Create security group' button.

Fig. 9.

1.4. Amazon Simple Storage Service (S3)

Amazon Simple Storage Service is Amazon's online storage, it has an easy-to-use web interface that allows you to access and manage your stored data. The amount of data stored is virtually unlimited. To create and configure your storage media service, return to the main AWS console. The S3 service is available under "Storage" (Fig. 10.).



Fig. 10.

When you get to this service, select the "Create bucket" button (Fig. 11.).

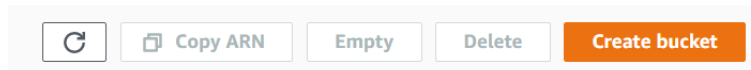


Fig. 11.

Then fill in the basic data such as the name (composed only of lowercase letters, a dot and a dash) and the region (Fig. 12.).

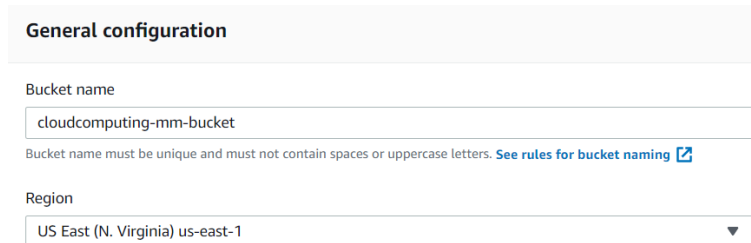
The image shows the 'General configuration' section of the AWS S3 'Create bucket' wizard. It includes a 'Bucket name' text input field containing 'cloudcomputing-mm-bucket', a note that the name must be unique and contain only lowercase letters, dots, and dashes, and a 'Region' dropdown menu currently set to 'US East (N. Virginia) us-east-1'.

Fig. 12.

And then, leaving the other fields as default, we create a "Bucket" (Fig. 13.).

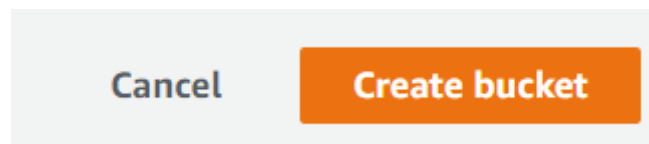


Fig. 13.

Once the "bucket" is created, we go to the Identity and Access Management (IAM) service. In the main AWS console, this is located under "Security, Identity, & Compliance" (Fig. 14.).



Fig. 14.

Once you are in this service, go to the list of users ("Users" in Fig. 15.).

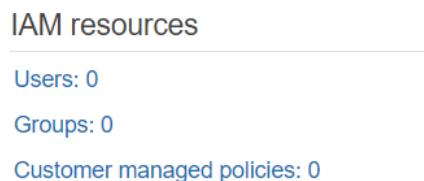


Fig. 15.

And select the "Add user" option (Fig. 16.).

Add user

Delete user

Fig. 16.

In the form provided, add a user. Enter the user's name and mark his access level as "Programmatic access" (Fig. 17.).

User name*

mm-cloudcomputing

+

Add another user

Access type

Users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

☒ Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

Fig. 17.

Then in the "Permissions" section select "Attach existing policies directly" and from the list below select "AmazonS3FullAccess" (Fig. 18.)

▼

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

↺

Filter policies ▼

Showing 1 result

	Policy name ▼	Type	Used as
<input checked="" type="checkbox"/>	<div></div> <div>AmazonS3FullAccess</div>	AWS managed	None

Fig. 18.

We leave the other fields default and finally we get "access ID" and "secret access ID". Keep this data in a safe place.

1.5. Amazon Elastic Compute Cloud (EC2)

Next, we create two EC2 instances. To do so, select the "Launch instance" button (Fig. 19.).

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Note: Your instances will launch in the US East (N. Virginia) Region

Fig. 19.

Next, select the Ubuntu server (for example 18.04 LTS) - Fig. 20.

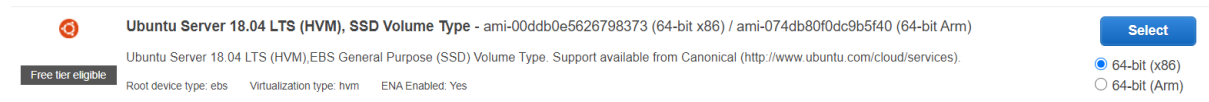


Fig. 20.

And we select t2.micro as the instance type (Fig. 21.).



Fig. 21.

Next, in the "Configure Security Group" section (Fig. 22.) select the previously created group.

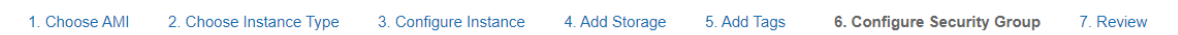


Fig. 22.

Then, after selecting "Launch" at the bottom of the page you will see a window about the access keys. For the first instance, create a new access key (Fig. 23.), and for the second instance, choose the key created when creating the first instance.

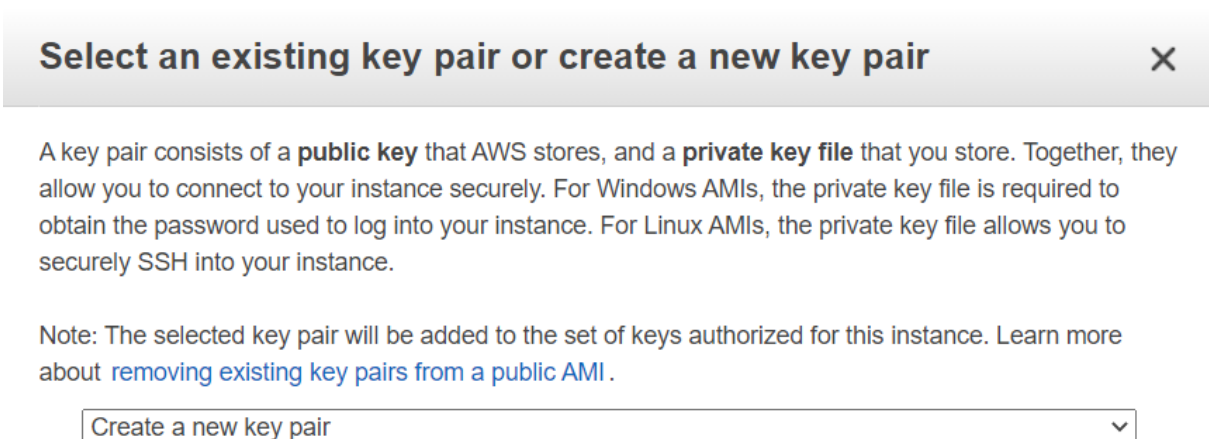


Fig. 23.

Po pobraniu klucza dostępu (przy pierwszej instancji) możemy już ją uruchomić przyciskiem „Launch Instances”.

Po wykonaniu tych czynności możemy przystąpić do konfiguracji środowiska na instancjach.

After downloading the access key (for the first instance), we can already start it with the "Launch Instances" button.

After completing these steps we can proceed to configure the environment on the instances.