**Cybersecurity 401**

**Module 4 - Cloud Security**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **Lab 16 - Cloud Identity and Access Management (IAM) with AWS**

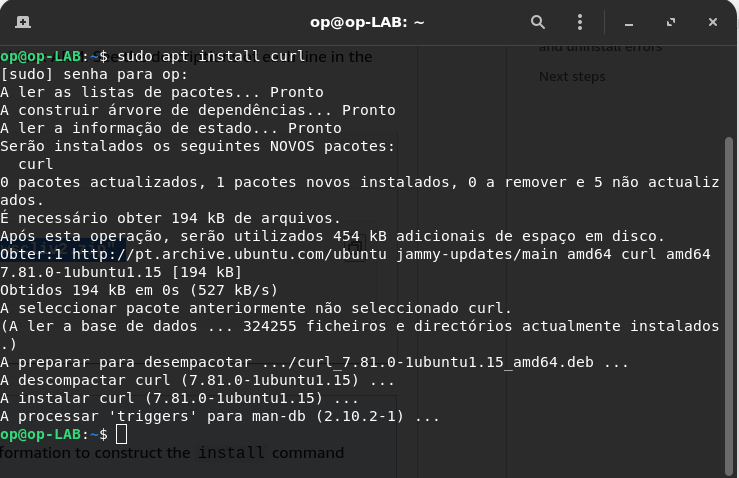
# 

**| Rodrigo Brasil 12/2023 |**

## Part 1: Users and Groups

### AWS CLI installation and configuration

First of all we need to do this exercise we need to install AWS CLI

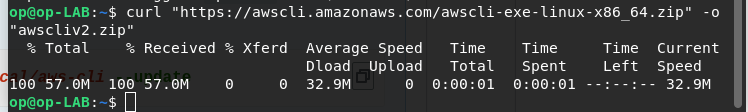


To do so, we need to install curl first.

type the command “**sudo apt install curl**”

Now to install AWS CLI, we are going to follow this guide:

<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>



First use the command:

“**curl https://awscli.amazonaws.com/awscli-exe-linux-x86\_64.zip" -o awscliv2.zip**"

To download AWS CLI installer which is compressed in a zip file



type the command:

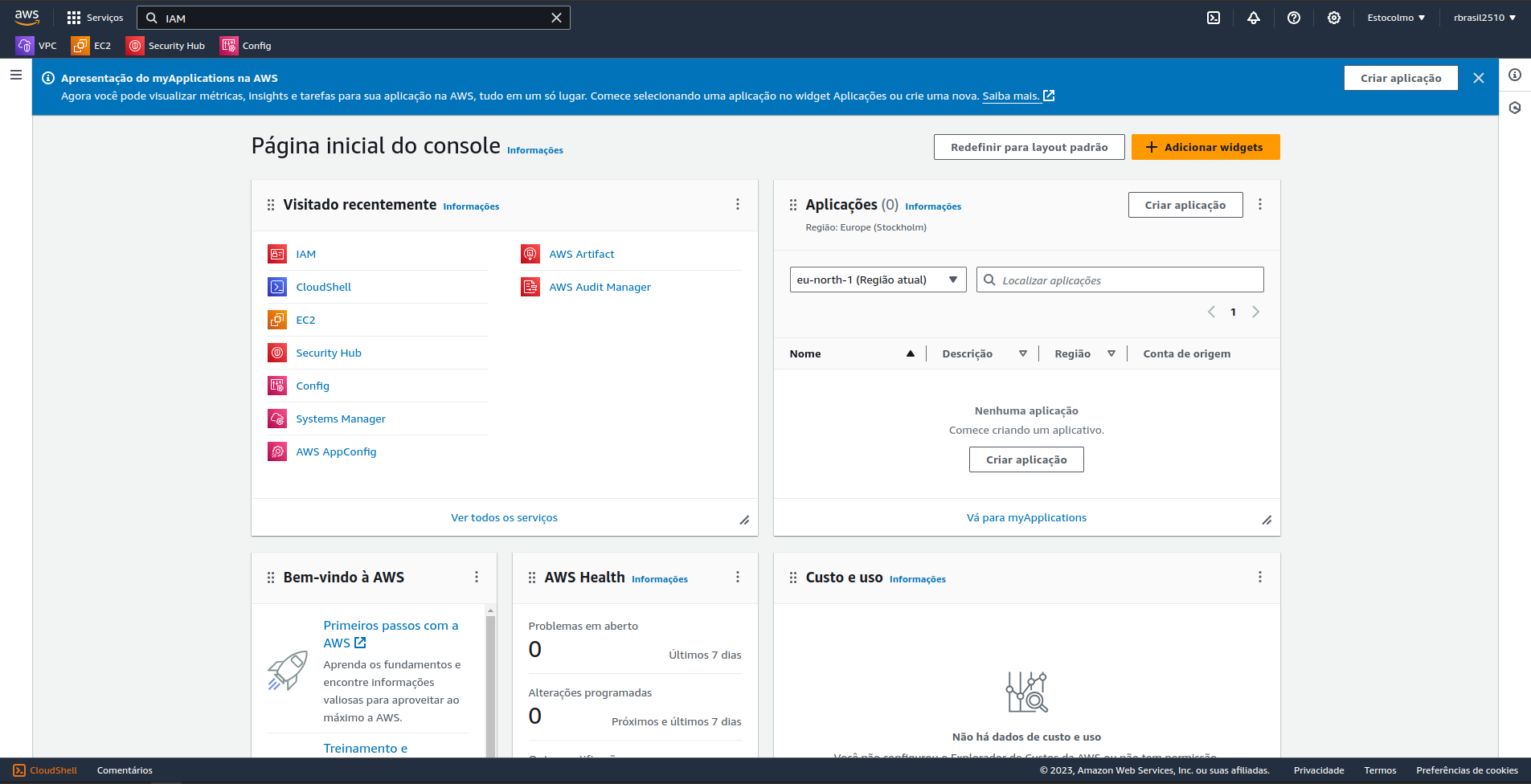
“**unzip awscliv2.zip**”

To unzip the file

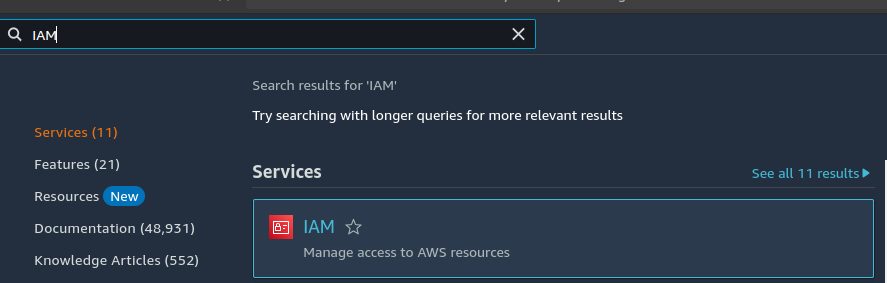


And type the command: “**sudo ./aws/install**”

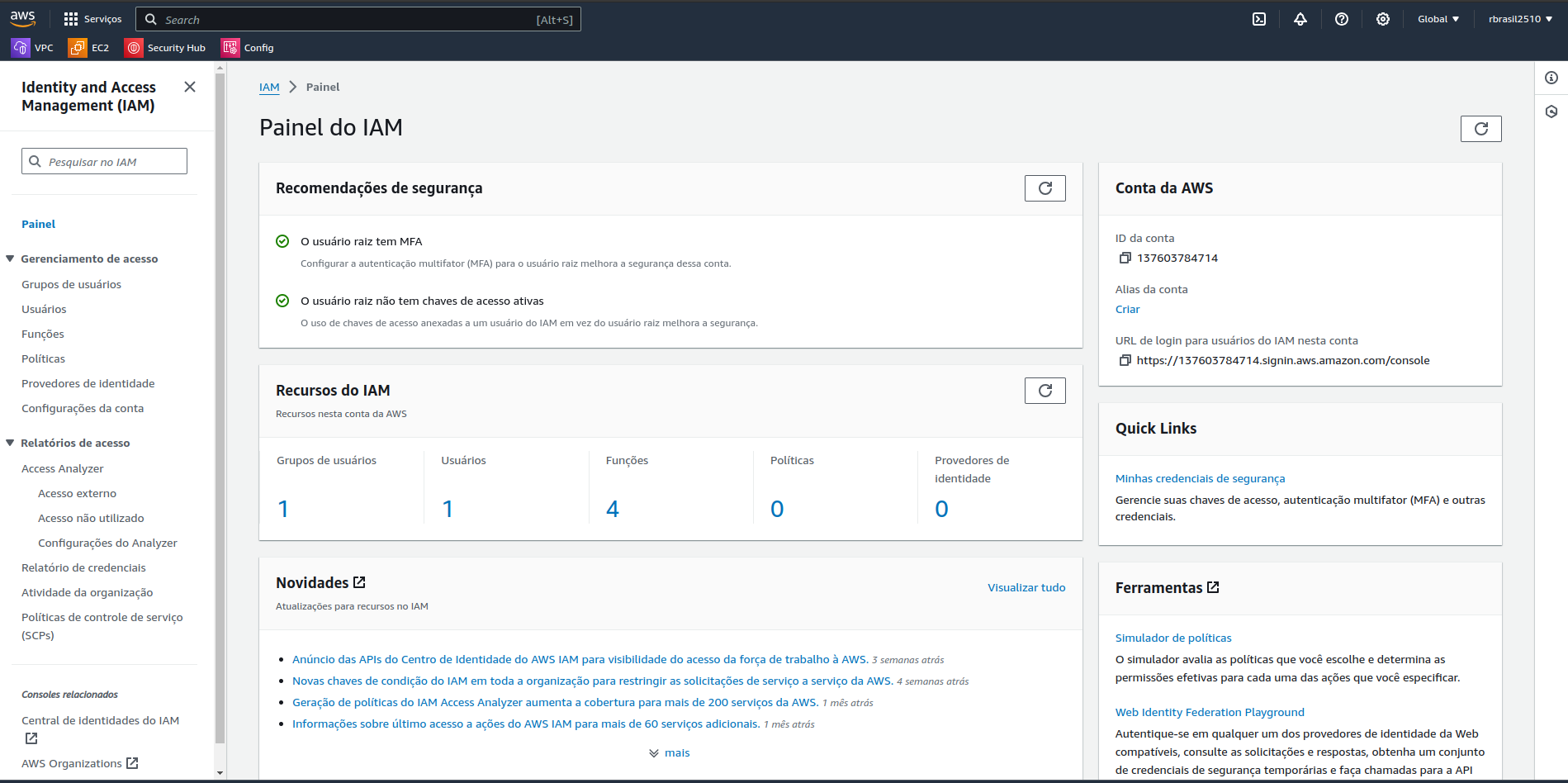
To finally install it



After installing we need to configure aws, to do this firstly we will need to go to our aws home page



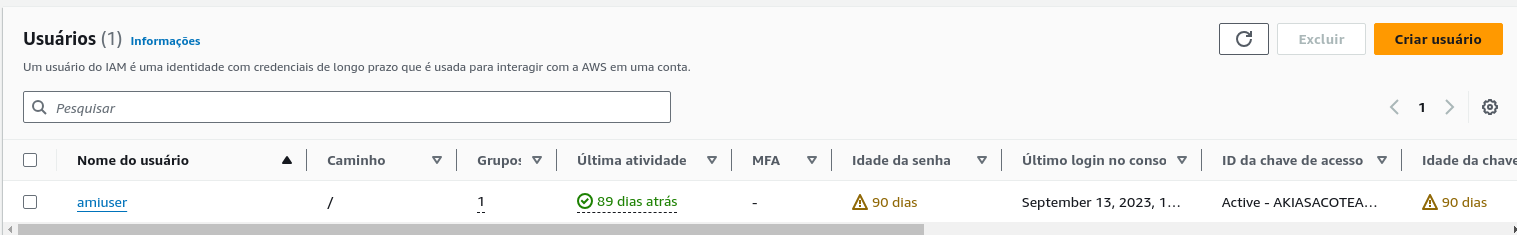
And search on the search bar for **IAM**



This is the **IAM** dashboard

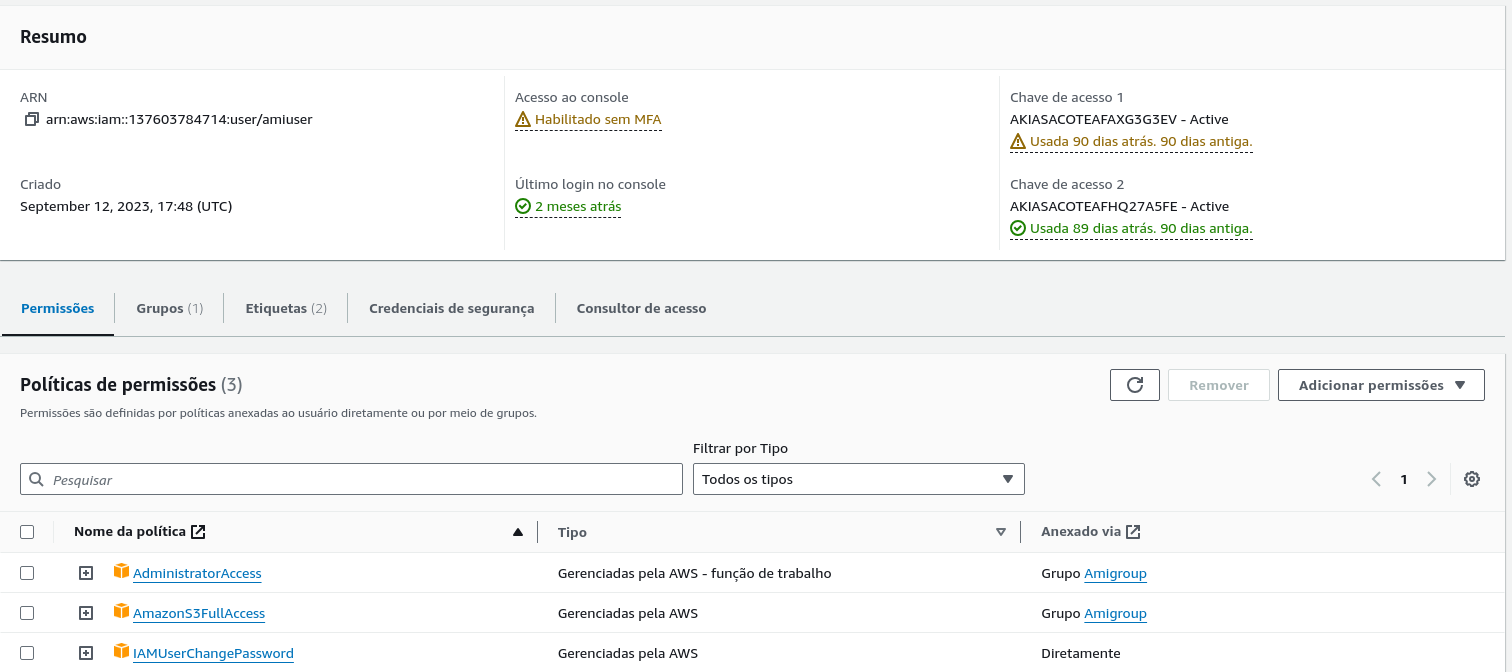
Inside it on the left side there will be this sidebar

on it we want to click on users

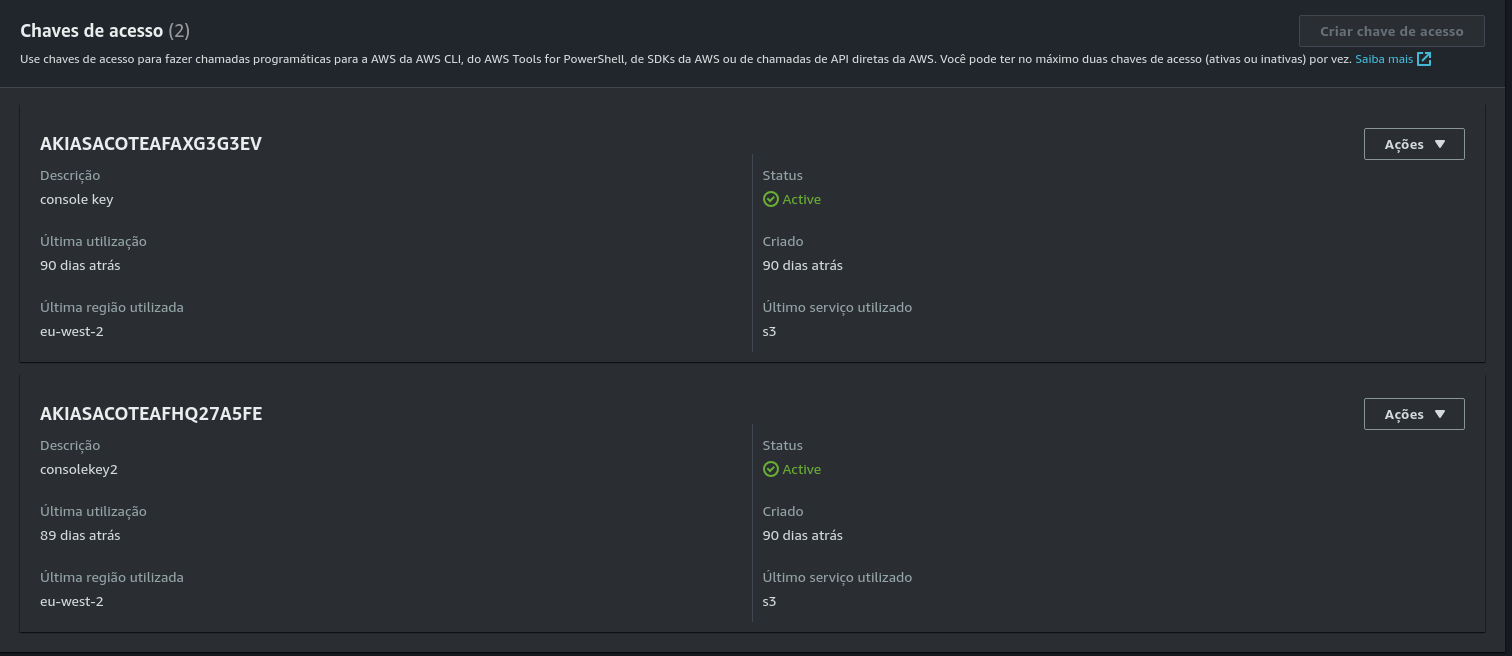


It will look like this.

If you don't have a user, create one by clicking the orange button



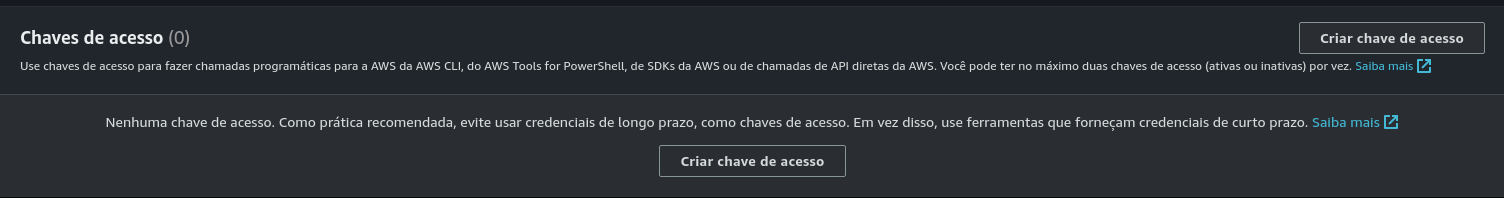
it seems we already have access keys generated



if we scroll a bit down we will see our access keys

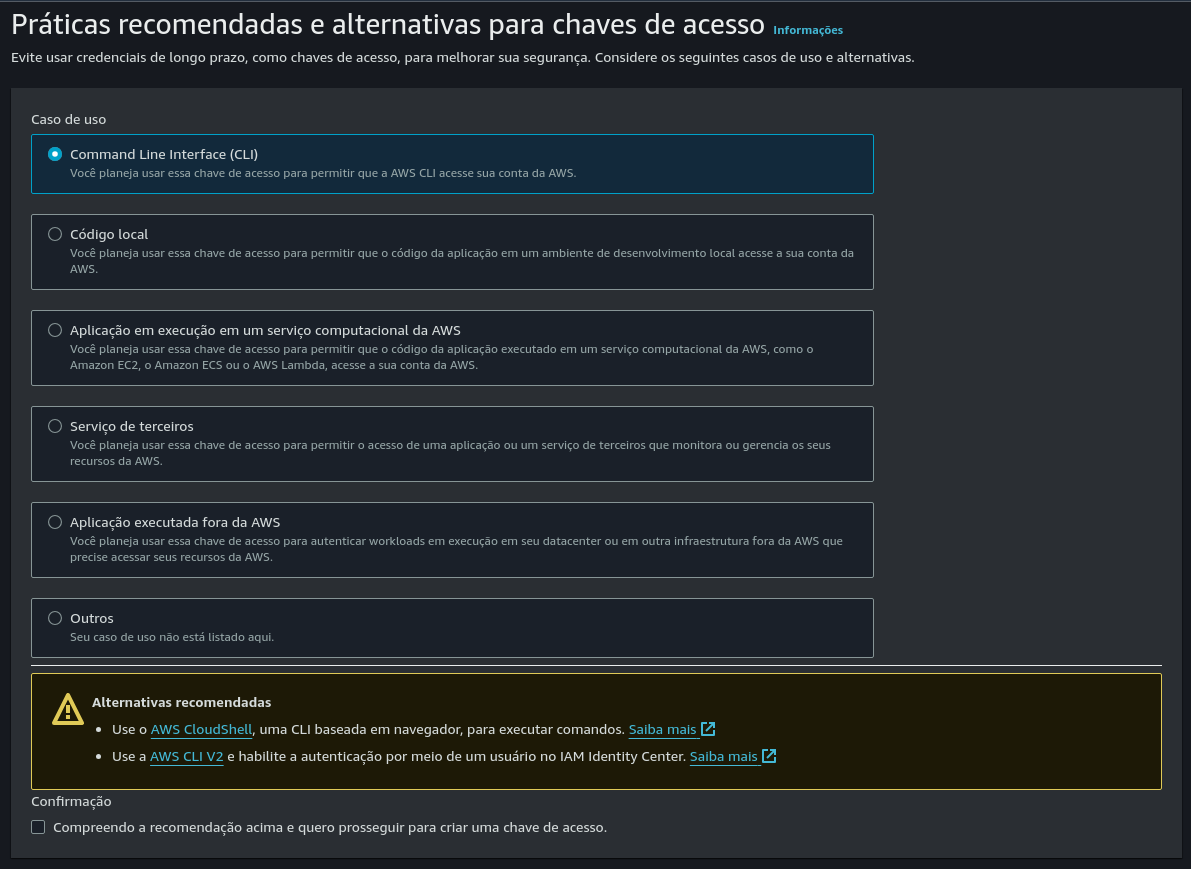
and it seems they are 2 months old

for security purposes i will delete them and create new ones



Now after deleting it will look like this

to create new ones just click the create access keys button

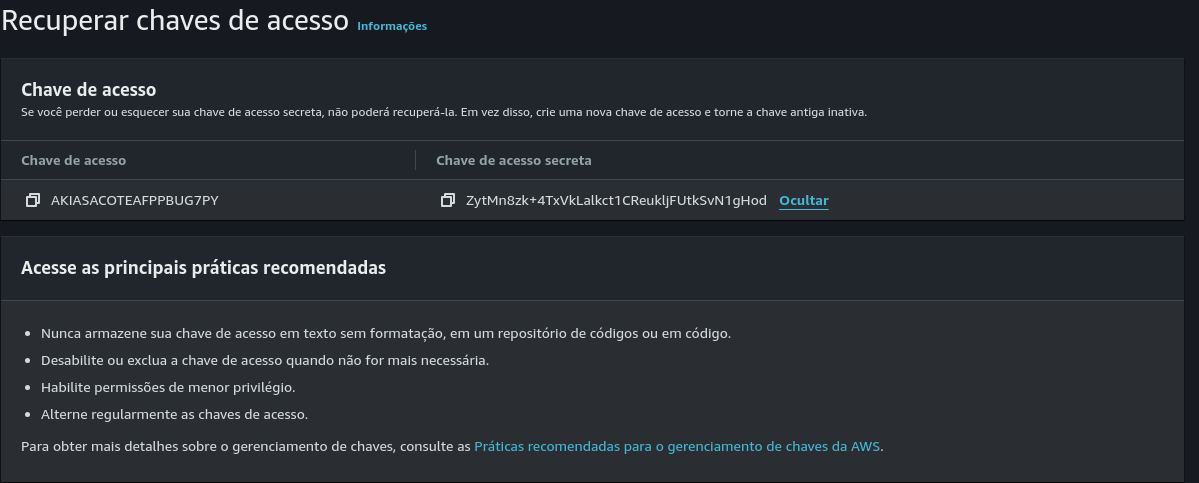


There will be 3 steps to create an access key, first what is the key for? for us we want a key to be able to access AWS CLI on our linux terminal

so we will click the first option (CLI)

There is a step that will ask to give a description to the key.

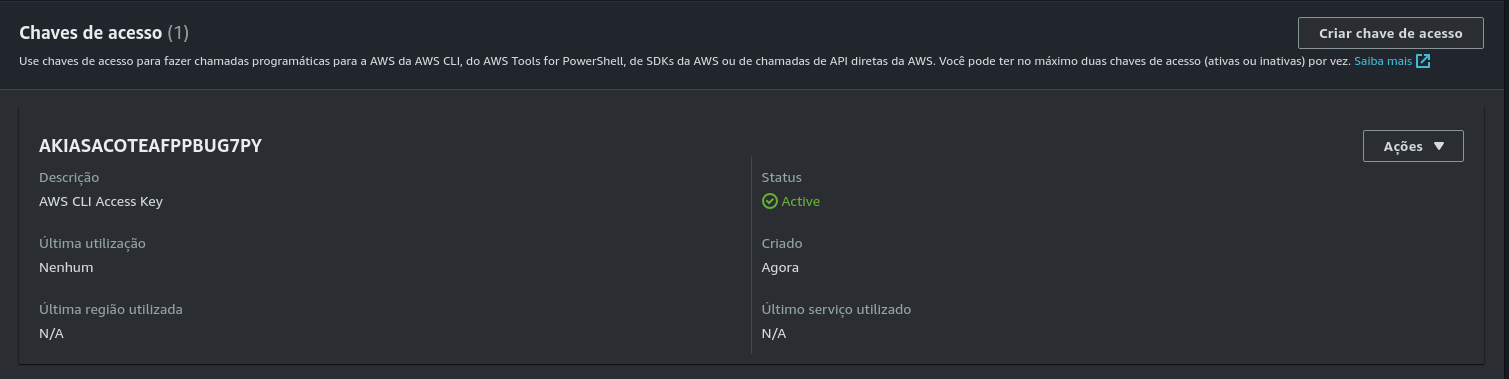
I gave mine “**AWS CLI ACCESS KEY”**



This is the access key and the secret access key, it is necessary to take note of both these keys because we will used to configure the AWS CLI on our terminal

There will be 2 buttons on the bottom one to download and csv file, this file contains the access keys

and another one to conclude



We have successfully created the key



Now on our terminal type the following command: “**aws configure**” to start configuring our aws cli

It will ask is for four parameters

our access key

our secret access key

our default region name

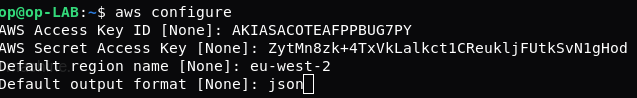
and output format

we already have our keys because we saved them

all we have to do is copy and paste them

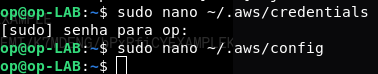
for the region name it is personal choice because i'm on the EU i chose eu-west-2 which is London, UK

and for the output format we want json



your configuration should look like this.

and its configured!



if it is still not working, use the config and credentials files to check if there are any typing mistakes.

### 

### S3 bucket, Groups and users creation

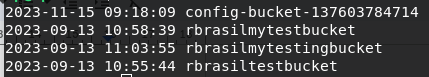
#### S3 bucket creation

Now we will create a s3 bucket

but before we do that let's verify if we already have a s3 bucket



Type the command: “**aws s3 ls**”



it seems we already have 4 s3 buckets

but for the purpose of this exercise we will create a new one



To create a new bucket type the command: “**aws s3api create-bucket --bucket lab16s3bucket --region eu-west-2**”

This command will create a bucket with a name of our choice and its region

My bucket name is **lab16s3bucket** and it's on the region eu-west-2 like on configuration



if it is giving this error

This might be because the user does not have permissions to create a bucket.

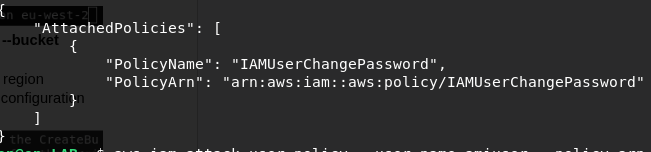
so we will give him.

First let's verify what permissions it has



Type the following command: “**aws iam list-attached-user-policies --user-name amiuser**”

where it says amiuser type your username



here we an see we only have permission to change the password

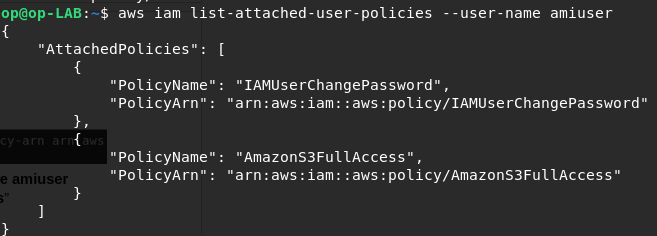
So let's give him the permission



To do so type the command: “**aws iam attach-user-policy --user-name amiuser --policy-arn arn:awsiam::aws:policy/AmazonS3FullAccess**”

again where it says --user-name type your username

Now lets verify if we have the permission now



Now we can see we have the permissions to create a bucket!

If you still can't create a bucket using the AWS CLI feel free to use the dashboard GUI

After creating the bucket we will upload a test txt file.

To do so lets create it first



To simply create a test txt file, type the command: “**echo “hello world!” > test-file.txt** ”

This command will create a txt file named test-file.txt with the text “hello world!” inside it



now to upload it to the bucket simply type the command: “**aws s3 cp test-file.txt s3://lab16s3bucket/**”



if successful this message will appear

#### Groups Creation

Now let’s create the groups

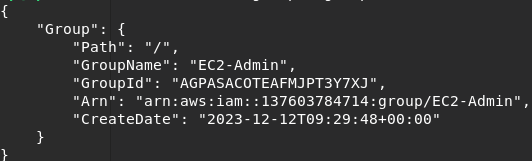
We are going to create 3 groups:

1. **EC2-Admin**
2. **EC2-Support**
3. **S3-Support**

Let’s start by creating the EC2-Admin group



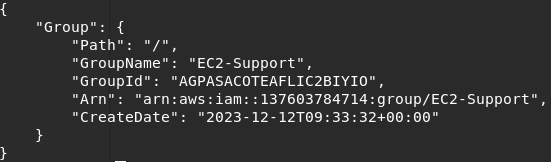
To do so type the following command: “**aws iam create-group --group-name EC2-Admin**”



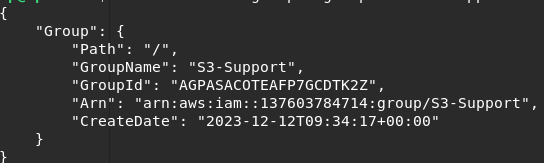
It will output this message

Do the same to the other 2 groups



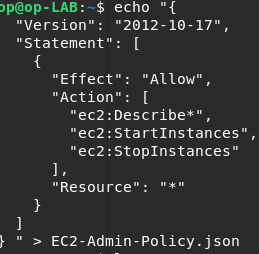






After creating the 3 groups we need to set appropriate permissions for them

We will start with EC2-Admin



Let’s create a json file with certain policies inside

To do so type the following commad:

“**echo "{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Action": [**

**"ec2:Describe\*",**

**"ec2:StartInstances",**

**"ec2:StopInstances"**

**],**

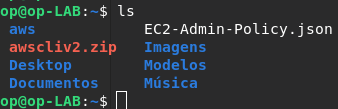
**"Resource": "\*"**

**}**

**]**

**} " > EC2-Admin-Policy.json**

”



This will create a .json file with the permissions inside

If we type the command “**ls**” to list the contents in the directory we are in we can see the .json file

Now we need to give it to the group



To do so type the command: “**aws iam put-group-policy --group-name EC2-Admin --policy-name EC2-Admin-Policy --policy-document file://EC2-Admin-Policy.json**”



If it gives the following error:

“**An error occurred (MalformedPolicyDocument) when calling the PutGroupPolicy operation: Syntax errors in policy.**”

Its because there is syntax errors in the .json file

We can fix them by editing the .json file

To edit type the following command:” nano EC2-Admin-Policy.json”



Make sure it looks like this.

Now to save the file on nano press ctrl + o and click ENTER

To exit nano press ctrl + x



If successful it will not give an error anymore.

Now let's give permissions to the other 2 groups

Because they are not admins they will have different permissions

for this we will not need to pass them a .json file

we will attach an already existing policy called “**AmazonEC2ReadOnlyAccess”**

For EC2-Support

****

To do this type the command: ”**aws iam attach-group-policy --group-name EC2-Support --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess**”

For S3-Support



To do this type the command: ”**aws iam attach-group-policy --group-name S3-Support --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess**”

#### Users Creation

Now we will create the users for each group

We will only create 1 user per group, so 3 users

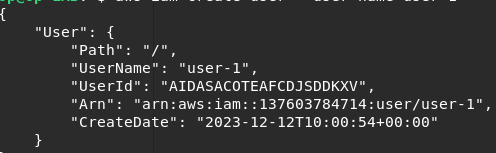
Give each of them a password

And associate them with their respective group

First let’s create the users



To do so type the command: ”**aws iam create-user --user-name user-1**” to create the first user

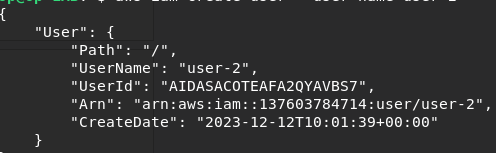


it will give us this output

Do the same for the other 2 users

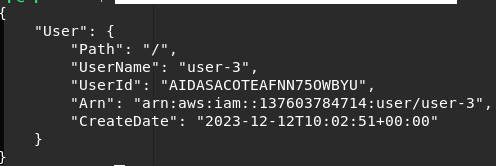


User 2: ”**aws iam create-user --user-name user-1**”

  
user 2 output



User 3: “**aws iam create-user --user-name user-3**”



User 3 output

Now let’s associate them to their respective groups

## 

## Part 2: Testing and Validation

## 

## Part 3: Reporting