Launching an EC2 instance from the command line using an IAM user.

My login credentials from my Group Team Lead

```
HP@DESKTOP-VPGBO3R MINGW64 ~
$ aws iam create-user --user-name Kelly
{
    "User": {
        "Path": "/",
        "UserName": "Kelly",
        "UserId": "AIDAS5OILEFGXJLOZFCHC",
        "Arn": "arn:aws:iam::200673009997:user/Kelly",
        "CreateDate": "2023-09-23T22:46:08+00:00"
    }
}

HP@DESKTOP-VPGBO3R MINGW64 ~
$ aws iam create-access-key --user-name Kelly
{
    "AccessKey": {
        "UserName": "Kelly",
        "AccessKeyId": "AKIAS5OI
        "Status": "Active",
        "SecretAccessKey": "ZFbIbCILqxTg43WzX63g7XG
        "CreateDate": "2023-09-23T22:46:38+00:00"
    }
}

HP@DESKTOP-VPGBO3R MINGW64 ~
$ aws iam create-login-profile --user-name Kelly --password
{
    "LoginProfile": {
        "UserName": "Kelly",
        "CreateDate": "2023-09-23T22:46:55+00:00",
        "PasswordResetRequired": false
    }
}
```

Requirements
AWS account
AWS CLI installed and configured with IAM user credentials
IAM user group with necessary permissions
Step 1
*Install AWS CLI
*Run aws configure and input IAM user credentials (access key and secret key) along with default region settings.

```
MINGW/.../Users/RUKKYVIBES
RUKKYVIBES@CYBERSPACE MINGW64 ~
$ aws configure
AWS Access Key ID [****************M2WM]: AKIA
AWS Secret Access Key [****************D: ZFbIbCILqxTg43
Default region name [us east 2]: us east 1
Default output format [json]: json

RUKKYVIBES@CYBERSPACE MINGW64 ~
$
```

Step 2

Creating a Key Pair with the command line below:

) *aws ec2 create-key-pair --key-name (keypair-Name) --query 'KeyMaterial' –output text > (keypair-Name.pem)*

) aws ec2 create-key-pair --key-name eby --query 'KeyMaterial' --output text > rukky.pem

"rukky" is the unique key pair name.

Key pair created successfully.

STEP3

Creating Security Group with the command line Below:

) *input aws ec2 create-security-group --group-name (security group Name) --description (Description)*

) aws ec2 create-security-group --group-name DeltaSecurityGroup --description "Delta security group"

Security group created successfully

STEP4

Allow SSH Port with command line below:

) *aws ec2 authorize-security-group-ingress --group-id (security group Id) --protocol tcp --port (port Number) --cidr (ip address)*

) aws ec2 authorize-security-group-ingress --group-name DeltaSecurityGroup --protocol tcp --port 22 --cidr 0.0.0.0/0

Successfully done.

STEP5

Launching the instance with command line below:

∫ *aws ec2 run-instances --image-id (ami-Id) --count 1 --instance-type (type) --keyname (keypair-Name) --security-groups (security grp Name)*

∫ aws ec2 run-instances --image-id ami-03a6eaae9938c858c --count 1 --instance-type t2.micro --key-name eby --security-groups DeltaSecurityGroup


Ec2 Instance Launched Successfully.

STEP7

View instance on your AWS management console

∫ Log in to your AWS account using your IAM user credentials.

∫ In the AWS Management Console, search for "EC2" to access the EC2 Dashboard.

∫ In the EC2 Dashboard, you'll find the "Instances" option, click on it to view your EC2 instances.

∫ You'll find a list of launched instances, click on the one you just created and view the details by clicking on the description tab.
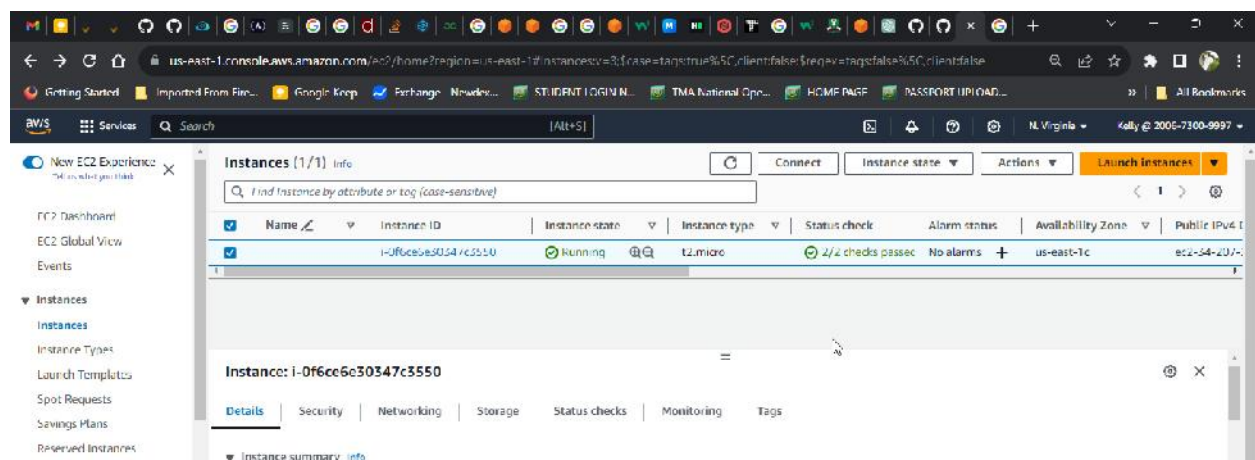
Confirming the Launched instance from my console page.
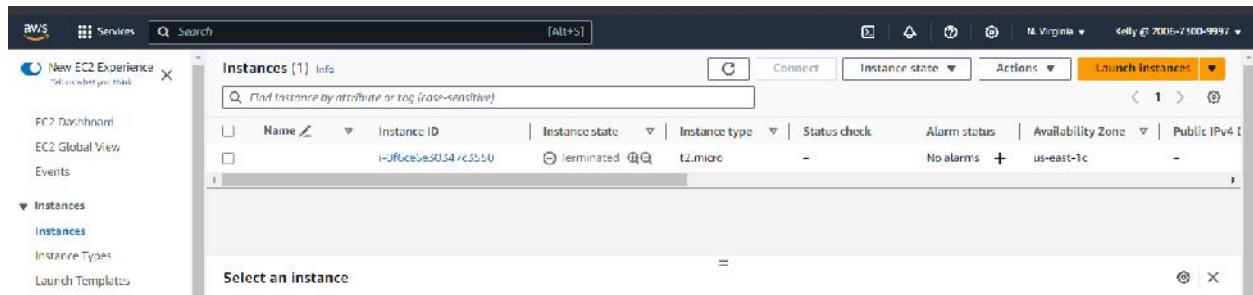
STEP8

Terminate running instance with command line below:

aws ec2 terminate-instances --instance-ids (Instance-Id)

aws ec2 terminate-instances --instance-ids i-0f6ce6e30347c3550

Instance terminated successfully

Confirmation from your console page.

The End!!!