# CSE 5234 – Distributed Enterprise Computing

Lab 11 – AWS Compute and Storage

The goal of this lab is to give students a working knowledge of compute and storage in AWS

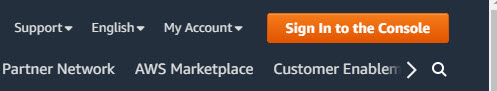
Objectives

1. CREATE A FREE AWS ACCOUNT
2. CREATE AN S3 BUCKET
3. BUILD AN EC2
4. CREATE AN IAM ROLE
5. RUN CLI COMMANDS

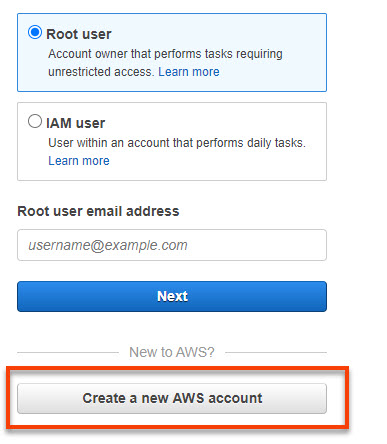
**Objective 1**

**Create a free AWS account**

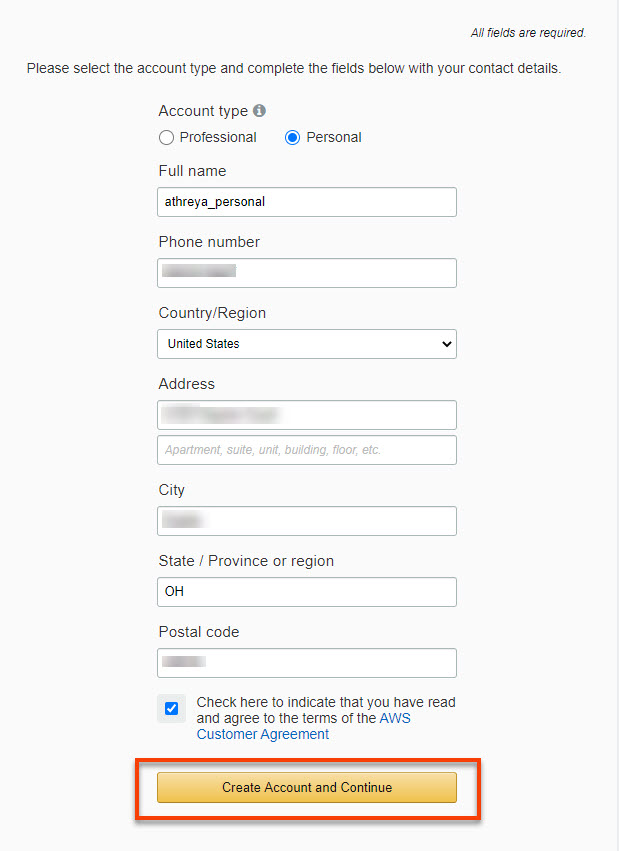
* Go to -> <https://aws.amazon.com/console/>
* Click on **Sign In to the Console** on the top right hand corner

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-signin-button.jpg)

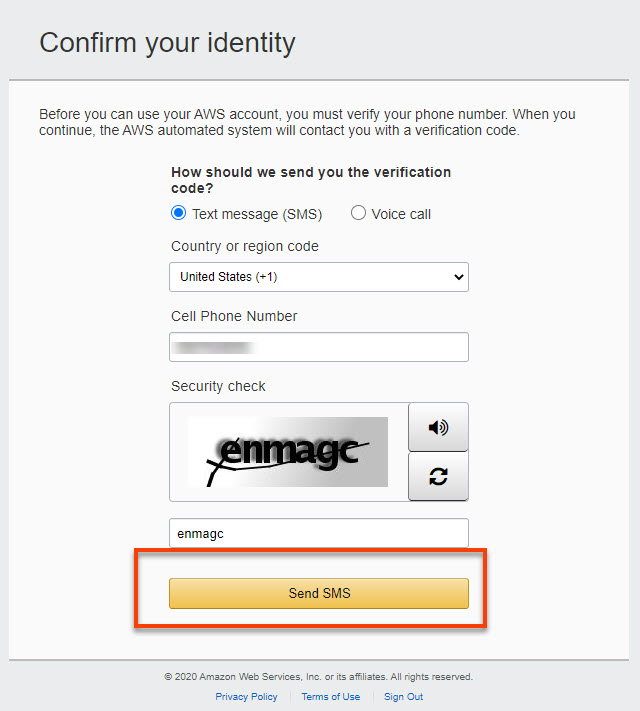
* Click on **Create a new AWS account**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-create-main.jpg)

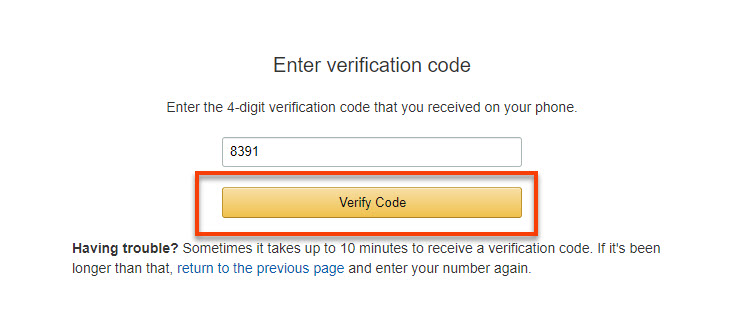
* Enter the details required and click **Create Account and Continue**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-create-details.jpg)

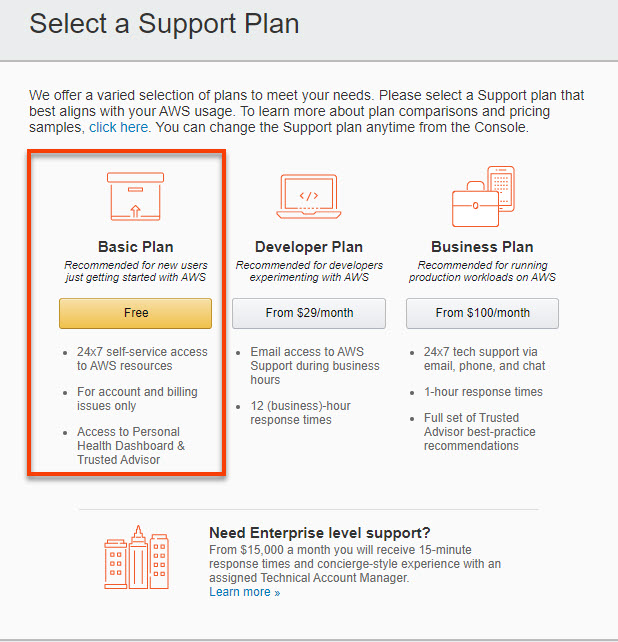
* Enter your **Credit card details**
* Enter a phone number to get verification code

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-create-confirm-identity.jpg)

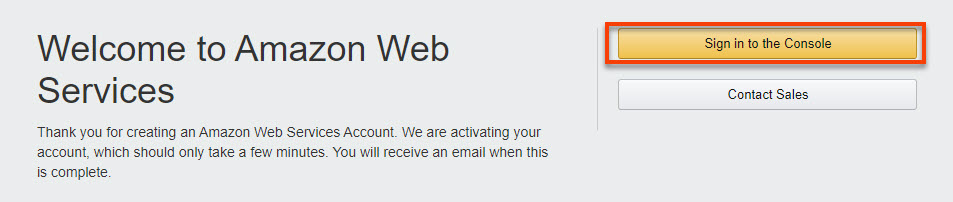
* Enter the code you get on your phone number

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-create-verify-code.jpg)

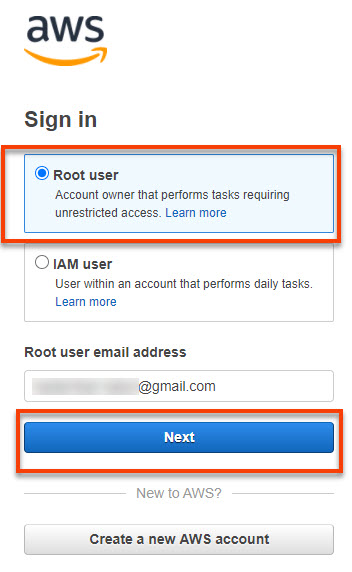
* Next in the **Support Plan** page -> select **Basic Plan**, click on **Free**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-create-support-plan.jpg)

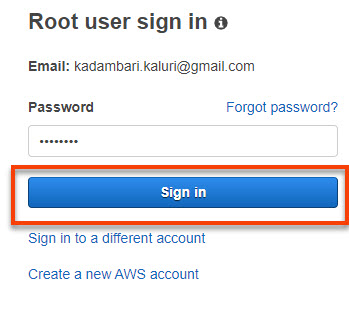
* Click on **Sign into the console**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-login-welcome.jpg)

* This will take you back to the main login page -> Select **Root user** -> use the **email** you created the account with, click **Next**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-login-email.jpg)

* Enter the **password** -> Click on **Sign in**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/aws-login-password.jpg)

**Windows users Only**

* Get the software **Putty** - <https://www.putty.org/> and **PuttGen** - <https://www.puttygen.com/>

**Objective 2**

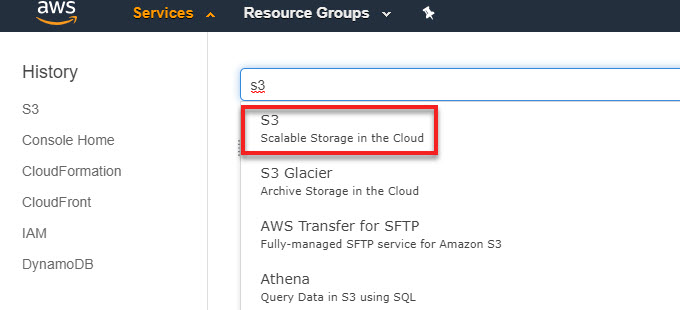
**Introduction**

In this tutorial we will create an s3 bucket in your AWS Account

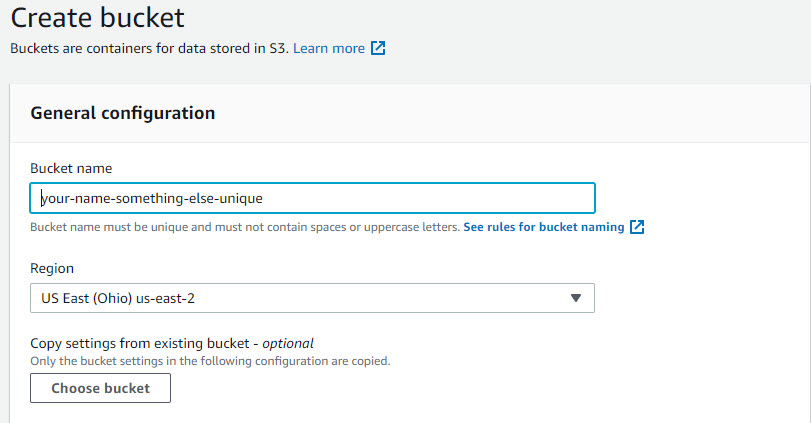
**Lab Guide**

**Create an S3 bucket**

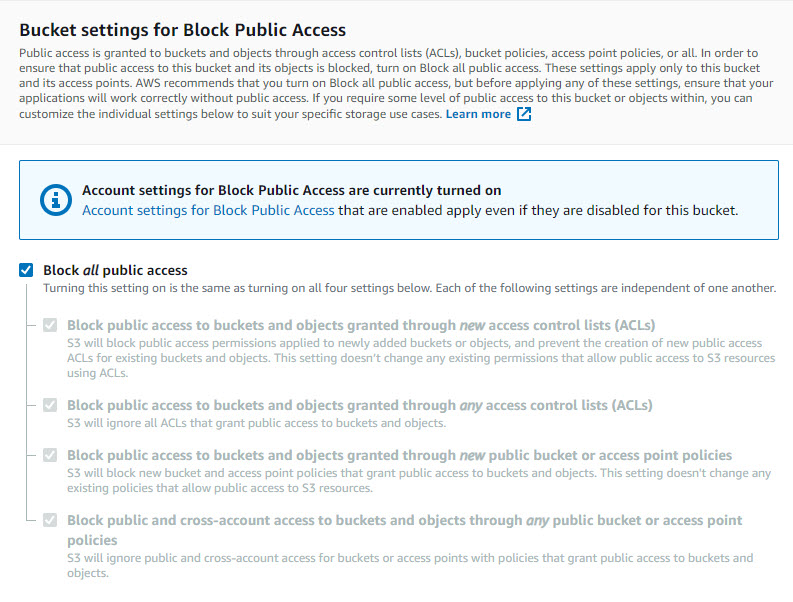
* In the AWS Console select **Services** search for S3 and select S3

[](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/s3-service.jpg)

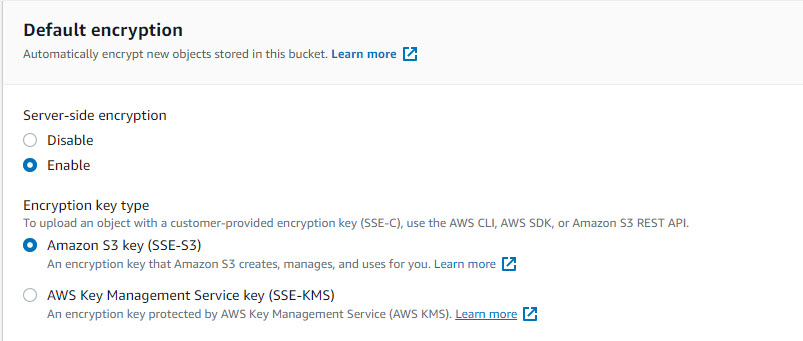
* In the S3 service, select [Create bucket](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/create-s3-bucket.jpg)
* Under **General configuration**, enter the following details
  + Bucket name - e.g. athreya-cohorts-s3lab-bucket. **Remember bucketnames must be globally unique.**
  + Region - US East (Ohio)

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/s3-gen-config.jpg)

* In the **Block public access (bucket settings)** section the box **Block all public access** should be checked. No Public S3 should be created.

[](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/s3-create-bucket-block-public.jpg)

* Disable **Bucket Versioning**
* For **Tags** add
  + ResourceOwner : YourName  
    **Note: Tags are good way to control access and identify what the bucket is for.**
* In **Default encryption** select as listed below
  + Server-side encryption : **Enable**
  + Encryption key type : **AWS S3 key (SSE-S3)**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/s3-encryption-aes256.jpg)

* Select **Create bucket** at the bottom.

**Upload file to S3 bucket**

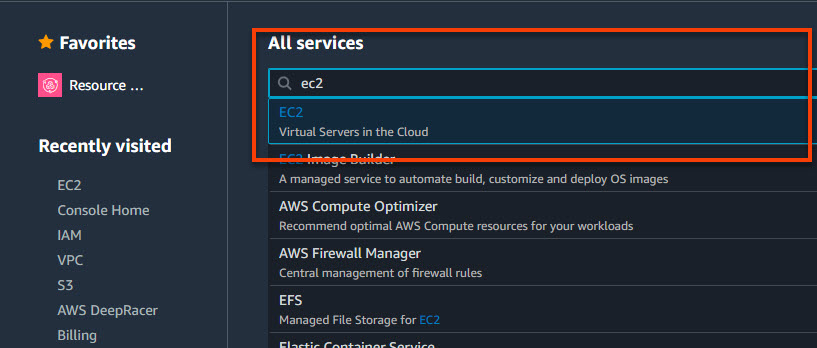
* In the S3 service search and find the bucket you created earlier **e.g. athreya-cohorts-s3lab-bucket**
* Select **Upload** and then select **Add files**. Pick any file from your local machine.
* Expand the **Additional upload options**, **you will not make any changes**, this is more for informational purposes
  + Here you have the option to choose the different **Storage Class**, we will keep the default
  + Change **Encryption** - When upload files to S3 you have an option to change the type of encryption that is being used for the individual files, we will keep the default
  + Update **Access control list**, we will keep the default
  + Add additional tags if needed
* Make no other changes. Click **Upload** at the bottom of the page.
  + Check that the file is available inside your S3 bucket

**Objective 3**

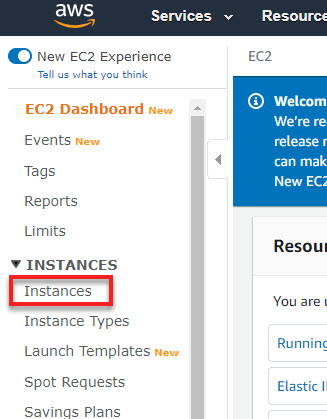
# Lab Guide

## Creating an EC2

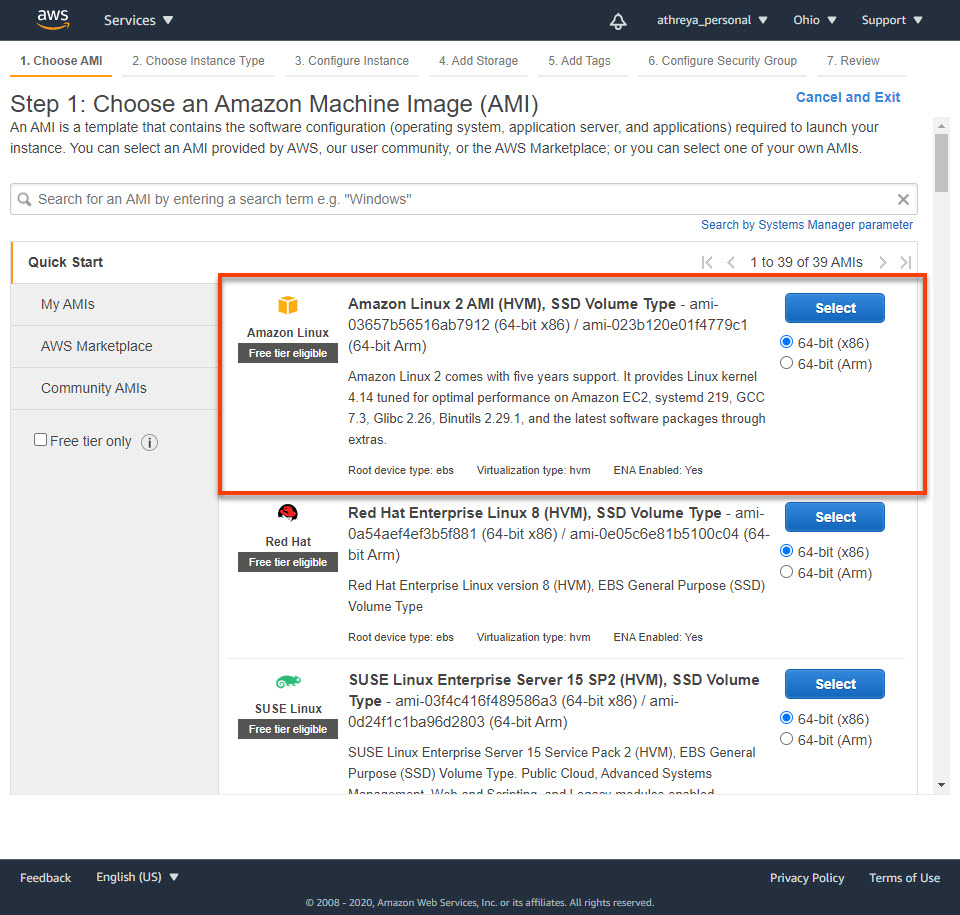
* In the AWS Console select **Services** search for **EC2** and select **EC2**. Check the **Region** to make sure you are in **Ohio**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-search.jpg)

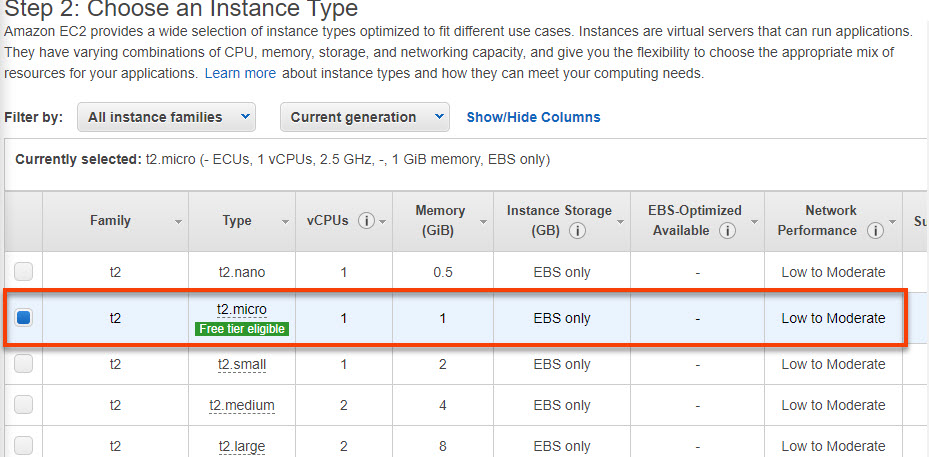
* In the scroll-bar on the left, select **Instances**.

[](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/ec2-console.jpg)

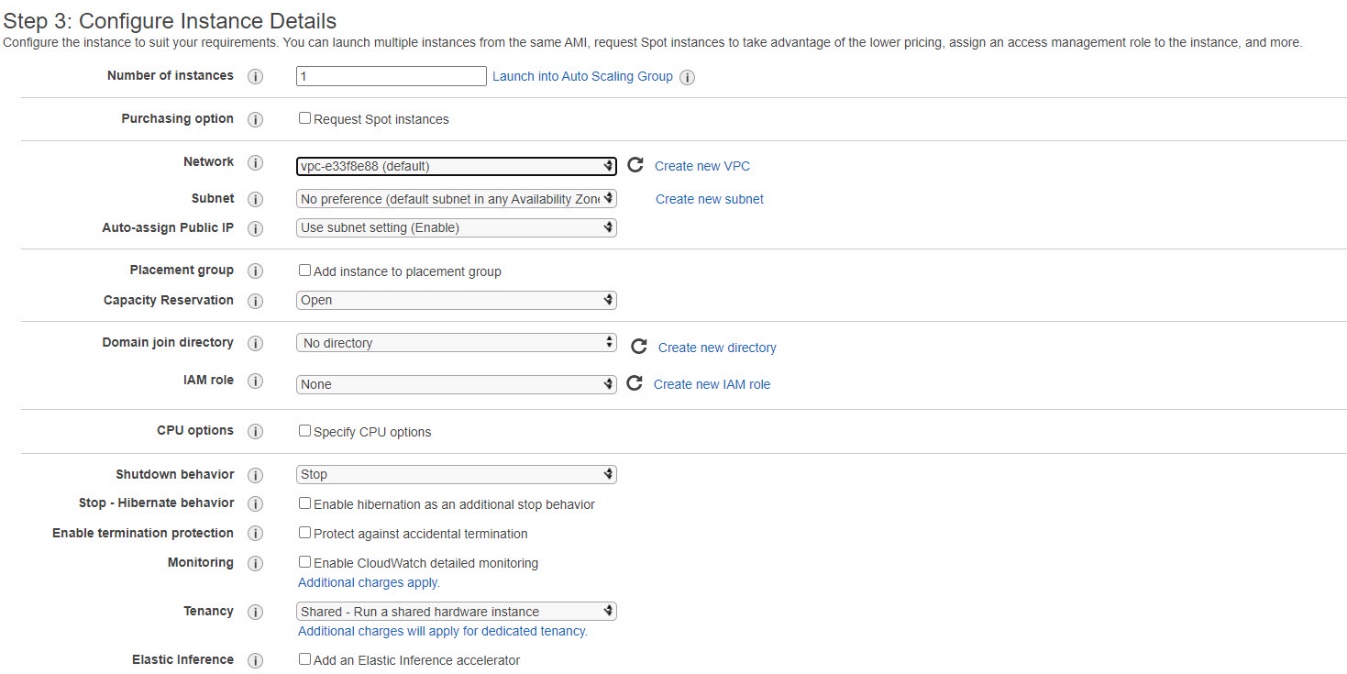
* Select **Launch Instance**.
* Select the **Amazon Linux 2 AMI**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-aws-linux-ami.jpg)

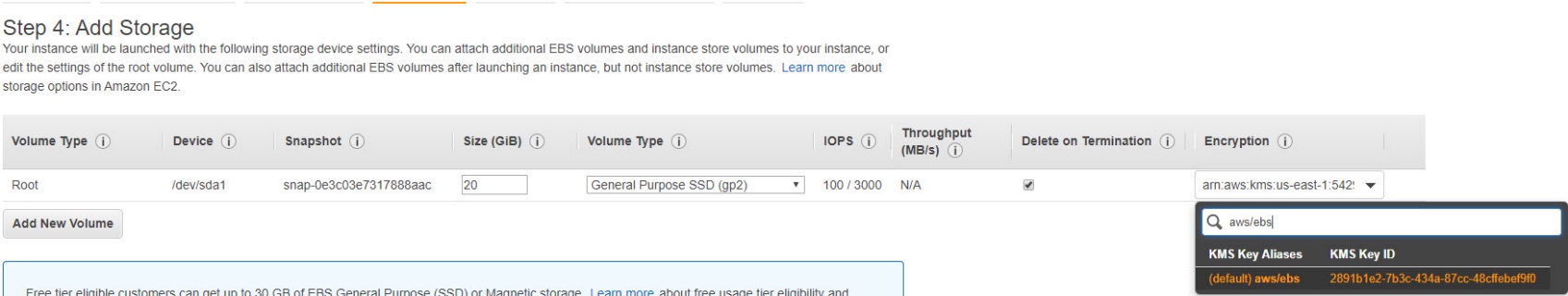
* Select **Next: Configure Instance Details**. You will pick **t2.micro** **Note: There are many options available here based on the use-case of the server**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-instance-t2-micro.jpg)

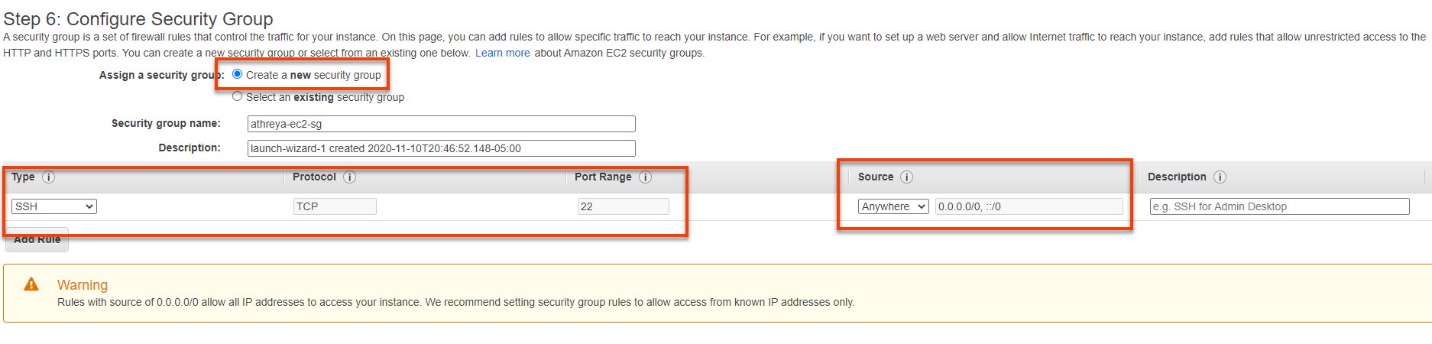
* In the **Configure Instance Details** section we will **leave everything as default** but take a look at the options and click on the **i** to get more details. A few details are listed below on some of the settings
  + **Network** - You will use the default VPC that comes with your AWS account. Advanced setting would be where you chose to create you won VPC and subnets within that.
  + **IAM role** - You will not create an IAM role in this lab. You will need one if you want to access other services within AWS/

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-instance-details.jpg)

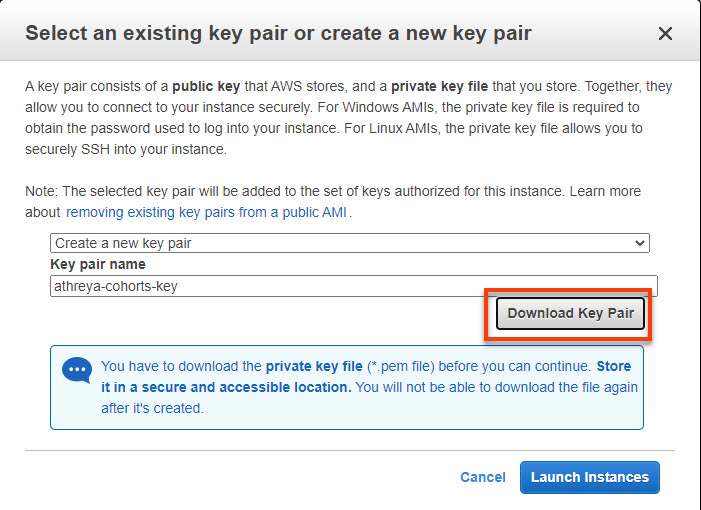
* Select **Next: Add Storage**
* In the **Add Storage** section
  + There will already be a **Root** volume type.
  + Check **Delete on Termination**
  + For **Encrption** is set to the default AWS managed KMS key **aws/ebs**
  + We will not be adding any new volumes at this time

[](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/ec2-storage.jpg)

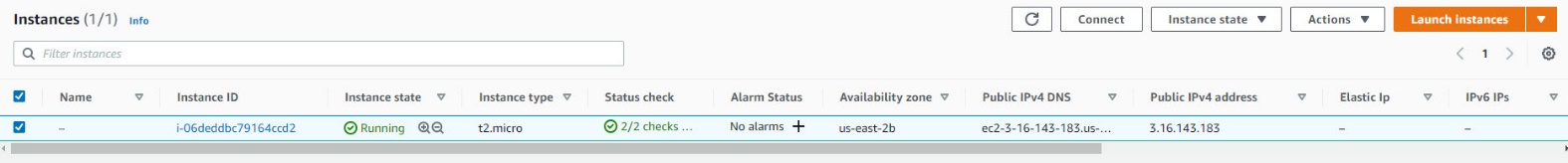
* Select **Next: Add Tags**, add one tag
* |ResourceOwner|your-name|
* Select **Next: Configure Security Group**
  + Security Groups are firewall rules that control the traffic to your instance.
  + You will set is so that you can SSH to this box from your laptop.
  + Select **Create a new security group** and give it a proper name **e.g. your-name-ec2-sg**
  + Change the **Source** to **0.0.0.0/0**. **You are making your ec2 open to the world**
  + You need to have port 22 open so you can SSH into the ec2 instance

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-public-sg.jpg)

* Select **Review and Launch**
* Review and select **Launch**
* In the pop-up window
  + Select **Create a new key pair**
  + Enter a name e.g. **athreya-cohorts-key**
  + Select **Download Key Pair**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-key-pair.jpg)

* Select **Launch Instances**
* Select **View Instance** which will redirect you to the EC2 instances window
* Search for your EC2 instance by the name you added to the tag. It will take a few minutes to sometimes showup in the list

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-instance-running.jpg)

## Login into EC2 using SSH Private Key

* We will login into the EC2 instance using the private key you associated with your instance when you created the ec2

## MAC Users

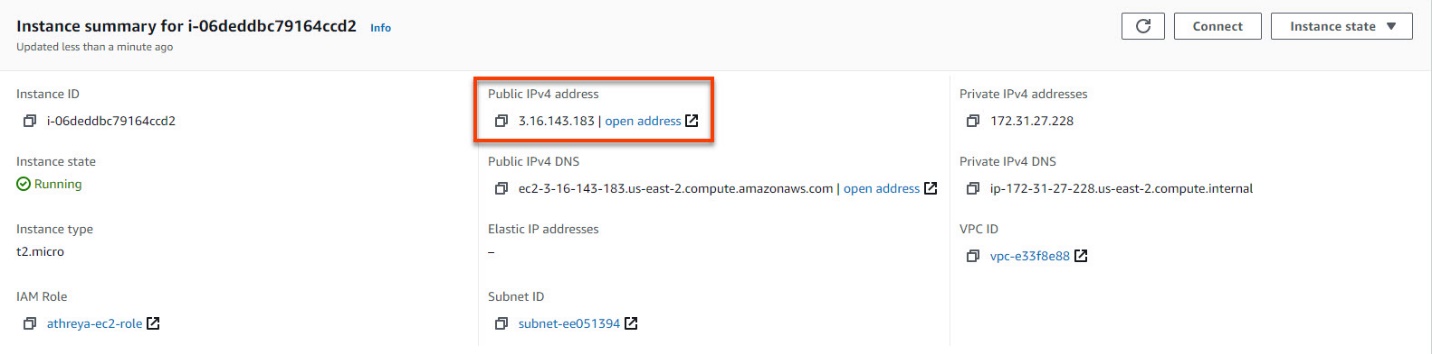
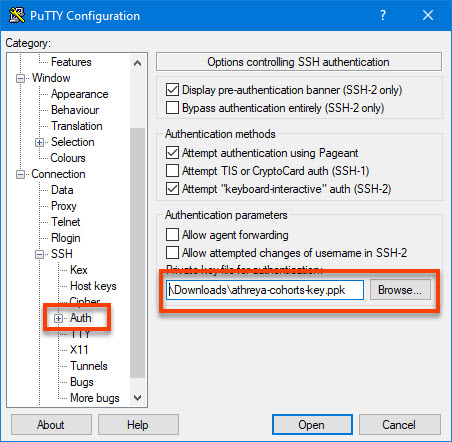
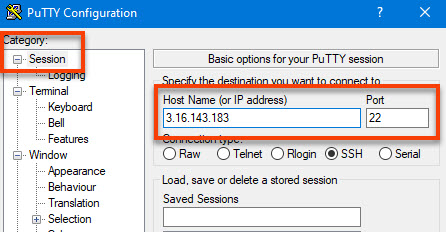
* Open your command line shell and change the directory to the location of the private key file that you created when you launched the instance.
* Use the chmod command to make sure your private key file isn't publicly viewable. a
  + For example, if the name of your private key file is my-key-pair.pem, use the following command:
  + chmod 400 my-key-pair.pem
* Use the following SSH command to connect to the instance:
* ssh -i /path/my-key-pair.pem ec2-user@public-ip

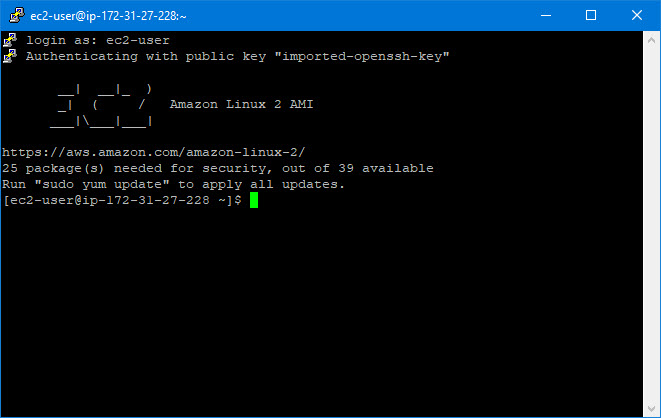
## Windows Users

### Convert PEM to PPK

* The key you download from AWS is a .PEM key, we will need to convert this to using [PuttyGen](https://www.puttygen.com/) to ppk to use it with [Putty](https://www.puttygen.com/download-putty)
* Follow the [instructions on AWS page to convert your key](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html#putty-private-key)

### Login with PPK using putty

* Get the **PublicIP** of your EC2 from the AWS Console [](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-public-ip.jpg)
* In **Putty**
  + Goto **Category -> Connection -> Auth** . Click on **Browse** and select you ppk you converted using PuttyGen e.g. **athreya-cohorts-key**  
    [](https://github.nwie.net/Nationwide/osu-training/blob/master/images/putty-auth-ppk.jpg)
  + Goto **Category -> Session**. Enter the Private IP of the EC2 and select **Open**  
    [](https://github.nwie.net/Nationwide/osu-training/blob/master/images/putty-session.jpg)
* Select **Yes** for the popup
* In the command prompt - Enter **ec2-user** as the user

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/putty-login.jpg)

**Objective 4**

# What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

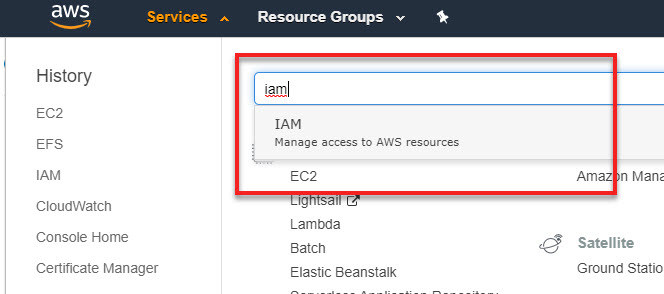
* IAM user in another account
* Application code running on an EC2 instance that needs to perform actions on AWS resources
* An AWS service that needs to act on resources in your account to provide its features
* Users from a corporate directory who use identity federation with SAML
* IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

**Additional resources:**

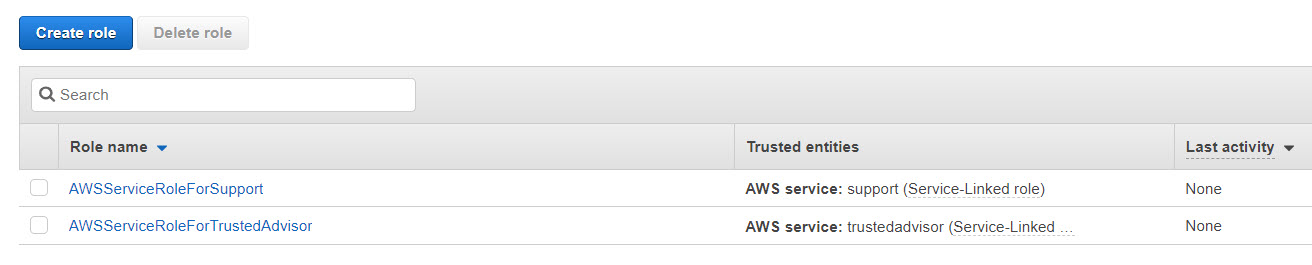
* [IAM Roles FAQ](https://aws.amazon.com/iam/faqs/)
* [IAM Roles Documentation](http://docs.aws.amazon.com/console/iam/roles)
* [Tutorial: Setting Up Cross Account Access](http://docs.aws.amazon.com/console/iam/tutorial-cross-account)
* [Common Scenarios for Roles](http://docs.aws.amazon.com/console/iam/roles-scenarios)

## Creating a Role

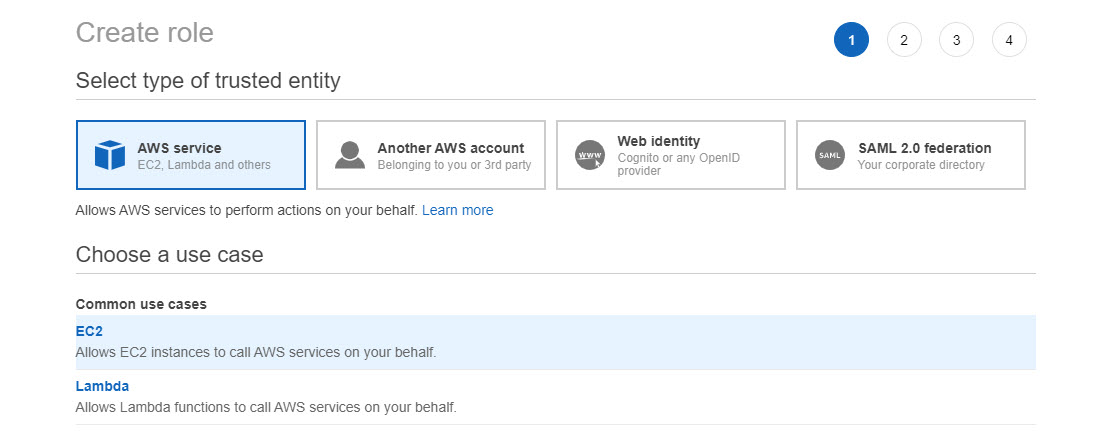
* In the AWS Console select Services search for IAM and select IAM. Check to make sure the **Region** is **Ohio**

[](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/iam-search.jpg)

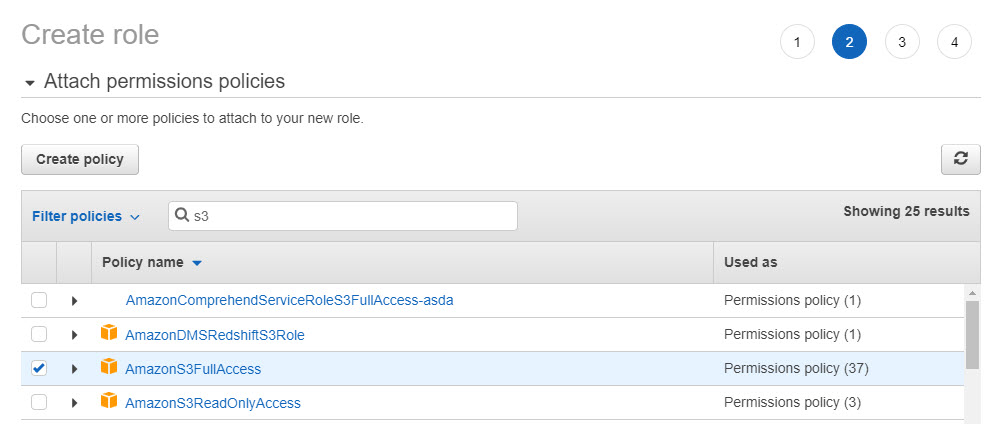
* In the scroll-bar on the left, select **Roles** -> select **Create role**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/iam-roles.jpg)

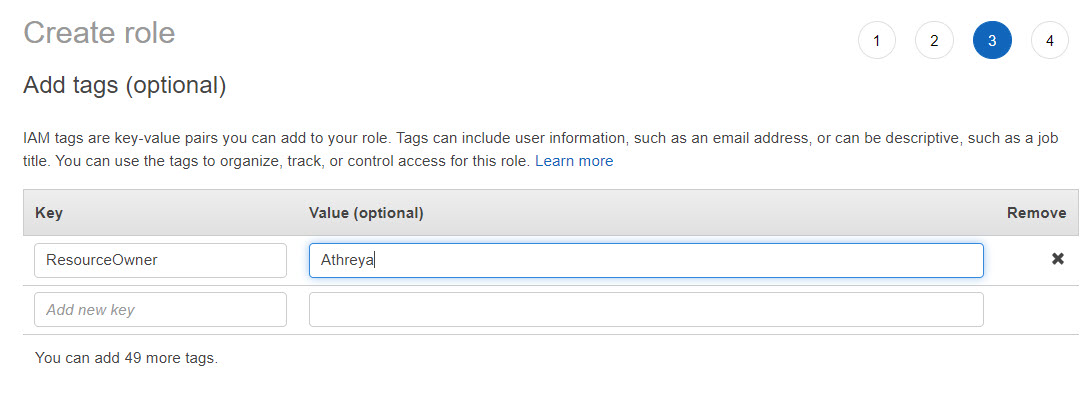
* Next you will need to choose who will **USE** this role
  + Select **AWS service**
  + Under "Choose a use case", select **EC2**

[](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/iam-service-ec2.jpg)

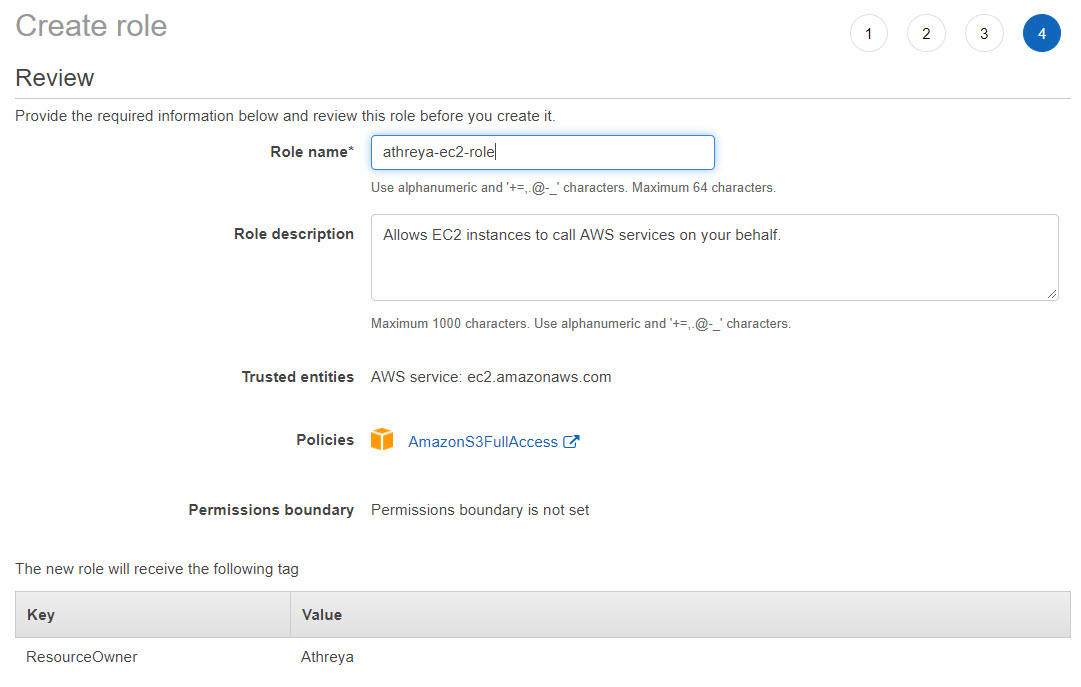
* Select **Next: Permissions**
* In the **Attach permissions policies** page you will select what kind of access to give to the role you are creating.
  + A policy is a json file that has the permissions that has all the permissions
  + AWS provides some policies out of box that we can use and associate with the role.
  + You can also create your own custom policy
  + We will use one of the existing policies
  + Search for S3 and select **AmazonS3FullAccess**
  + In a real use-case, you will not give a role full access but limit it only to what is needed.

[](https://github.nwie.net/Nationwide/cloud-tutorials/blob/master/images/iam-attach-policy.jpg)

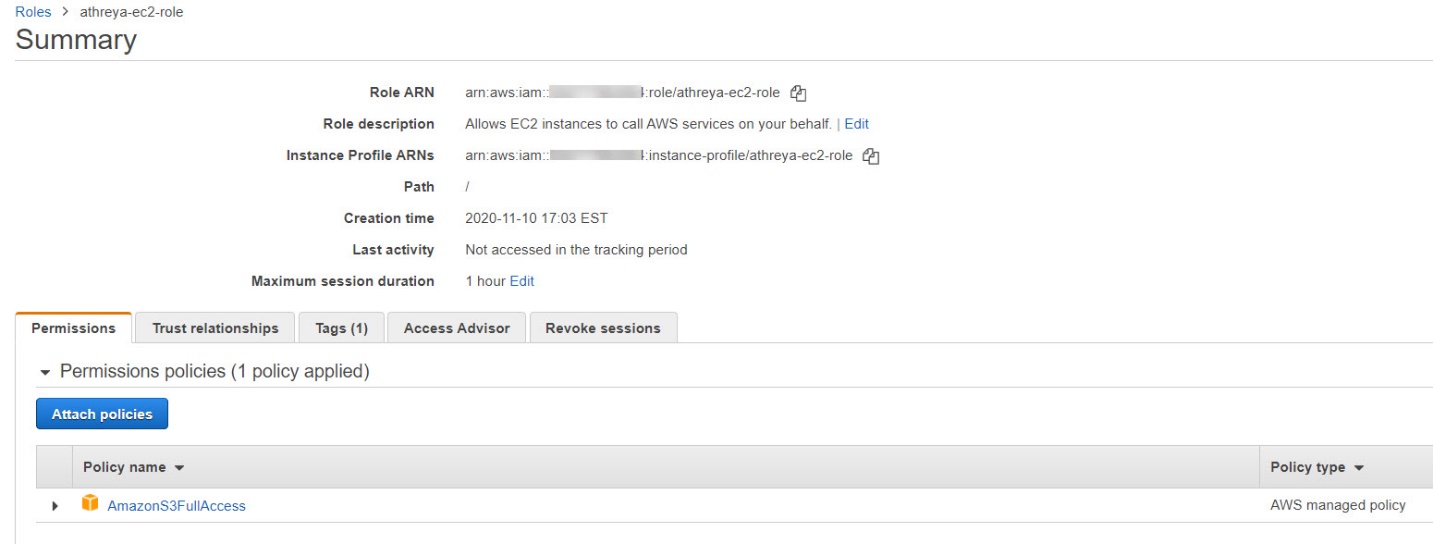
* Tags - **Add the ResourceOwner tag like the previous lab**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/iam-tags.jpg)

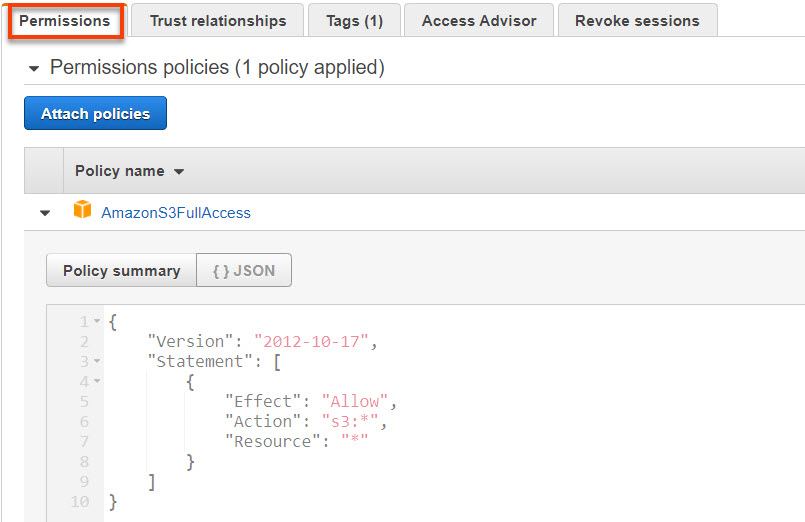
* In the **Review** page fill in the details as below and select **Create role**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/iam-review.jpg)

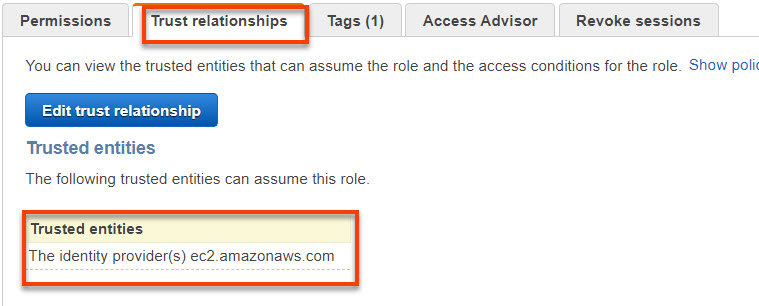
* Goto **Services -> Roles** and search for the role you just created **athreya-ec2-role**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/iam-summary.jpg)

* Expand and see the S3 policy and see the **Permissions** section. This defines the rules of **WHAT can be accessed by this role**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/iam-policy-json.jpg)

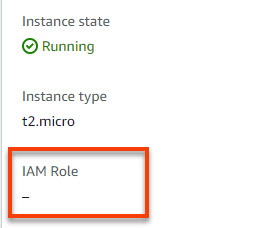
* Check the **Trust relationships**. This defines the rules of **WHO can be use this role**. Only an EC2 can use this role.

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/iam-trust-policy.jpg)

**Objective 5**

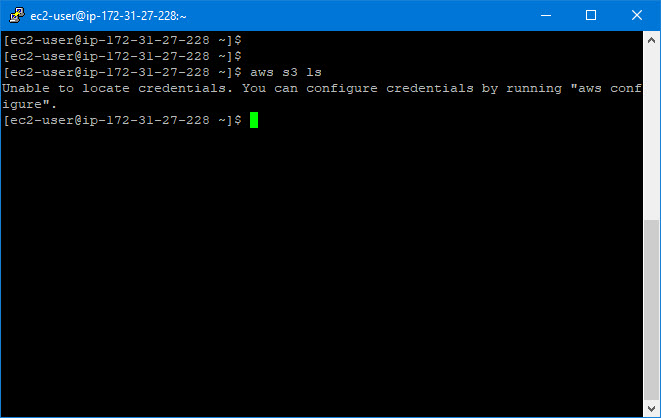
## EC2 Instance Role

* In the previous lab you created an ec2 instance, the instance does not have an IAM role associated with it

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-iam-empty.jpg)

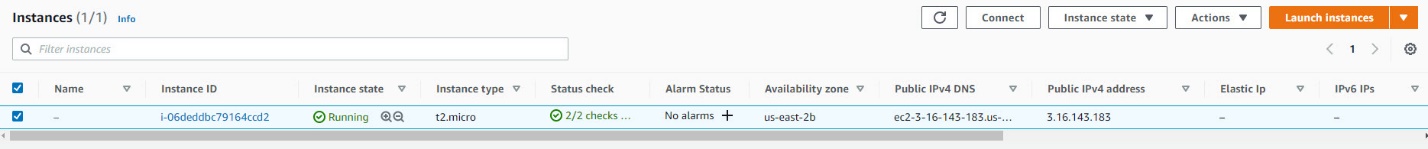
## AWS CLI

* AWS CLI is a command line interface you can use to manage your services in AWS. More details can be found here - <https://aws.amazon.com/cli/>
* The EC2 instance already comes with this command line tool installed. You will run a few basic commands in this lab
* Try running an AWS CLI command after logging into the EC2 as in the previous lab. The command below lists all the s3 buckets in your AWS account.
* aws s3 ls
* **You will get an error**. This is because the EC2 instance does not know what credential to use when trying to connect to the AWS S3 service

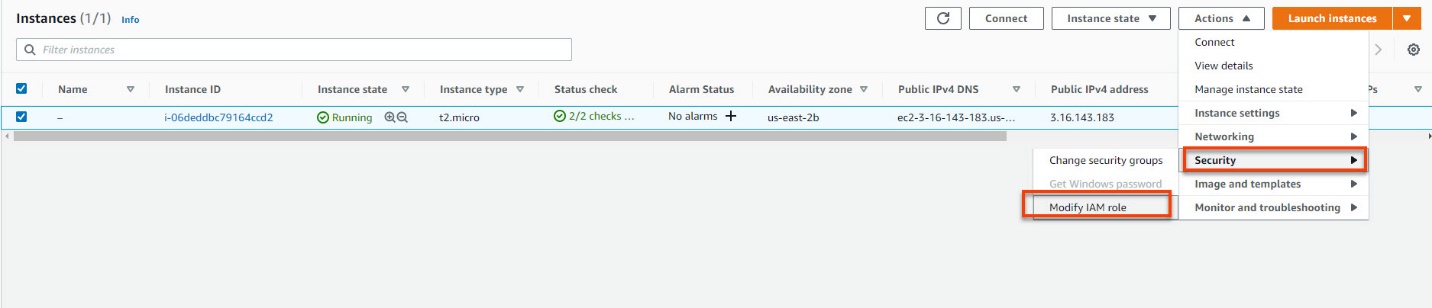
[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-cli-fail.jpg)

## Attaching an IAM role to an EC2

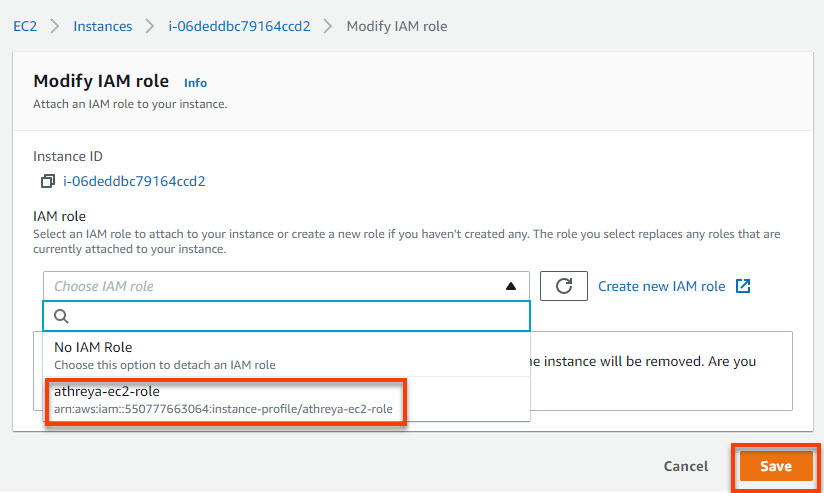
* We will now assign the IAM role we created in the previous lab to the EC2 instance
* When you access an AWS service, the EC2 assumes the IAM role associated with the instance
* In the AWS console and goto EC2 service and search for the instance you created earlier.

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-instance-running.jpg)

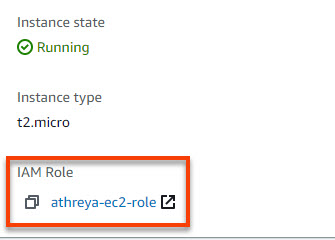
* Select **Actions -> Security -> Modify IAM**

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-action-iam.jpg)

* Search and select the role you created and **Save**

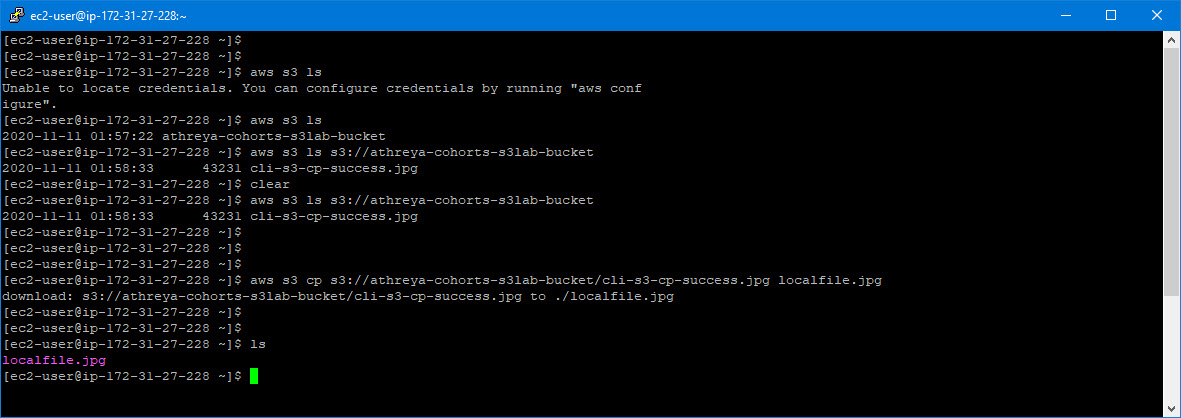
[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-iam-search.jpg)

* Your EC2 instance now has a role associated with it.

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-iam-assigned.jpg)

## Running an AWS CLI Commands

* Let's try to a few CLI commands.
  + Run the same command as before, to get a list of buckets in your account. **They will all be successful now**
  + aws s3 ls
  + List the contents of your s3 bucket
  + aws s3 ls s3://<your-bucket-name>
  + e.g. aws s3 ls s3://athreya-cohorts-s3lab-bucket
  + Download the file from your S3 bucket.
  + aws s3 cp s3://<your-bucketname>/<your-filename> <localfilename>
  + e.g. aws s3 cp s3://athreya-cohorts-s3lab-bucket/cli-s3-cp-success.jpg localfile.jpg

[](https://github.nwie.net/Nationwide/osu-training/blob/master/images/ec2-cli-success.jpg)