Lab Guide for Introduction to Cloud Computing

CONTENTS

Day-1 Assignments

Contents

Context

This document contains assignments to be completed as part of the hands on session for the course

Guidelines

- The lab guide has been designed to give hands on experience to map the concepts learnt in the theory session with real life business oriented case studies/assignments.

Assignment 1a: Creating Linux EC2 Instance

Objective: To create and deploy a web application on linux EC2 instance

Problem Description:

An organization wants to host its application on a Linux server.

In order to host we'll see how to create a Linux Instance and how to connect to the Instance.

Estimated time: 15 mins

Solution:

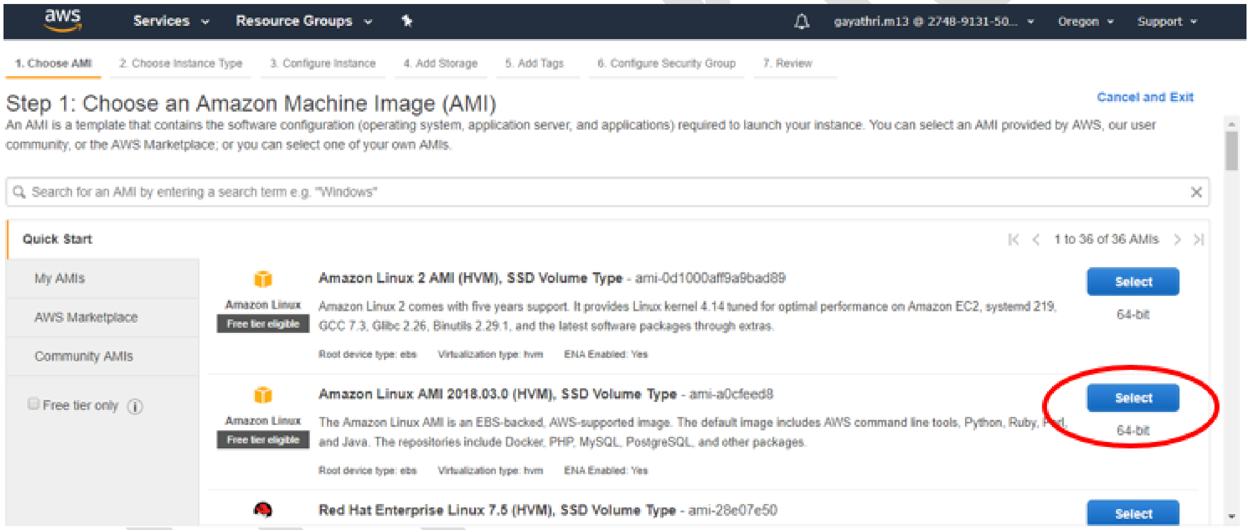
- *We must select the region where the EC2 instance has to be launched, since it is region based.*
- *On the AWS service console, choose EC2 service.*
- *Click on Launch Instance.*

Step 1: *Sign into AWS Management Console 2.   Navigate to EC2 dashboard by Clicking on EC2 under Compute Category*

Step 2: *On EC2 Dashboard, click on Launch Instance Button*

Step 2: Choose AMI

Amazon Machine Images or AMIs are the building blocks of amazon EC2 Instances. An AMI is a base image of a server or EC2 instance, including software configuration of an OS and additional software which runs on AWS.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0d1000aff9a9bad89

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-a0cfeed8

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

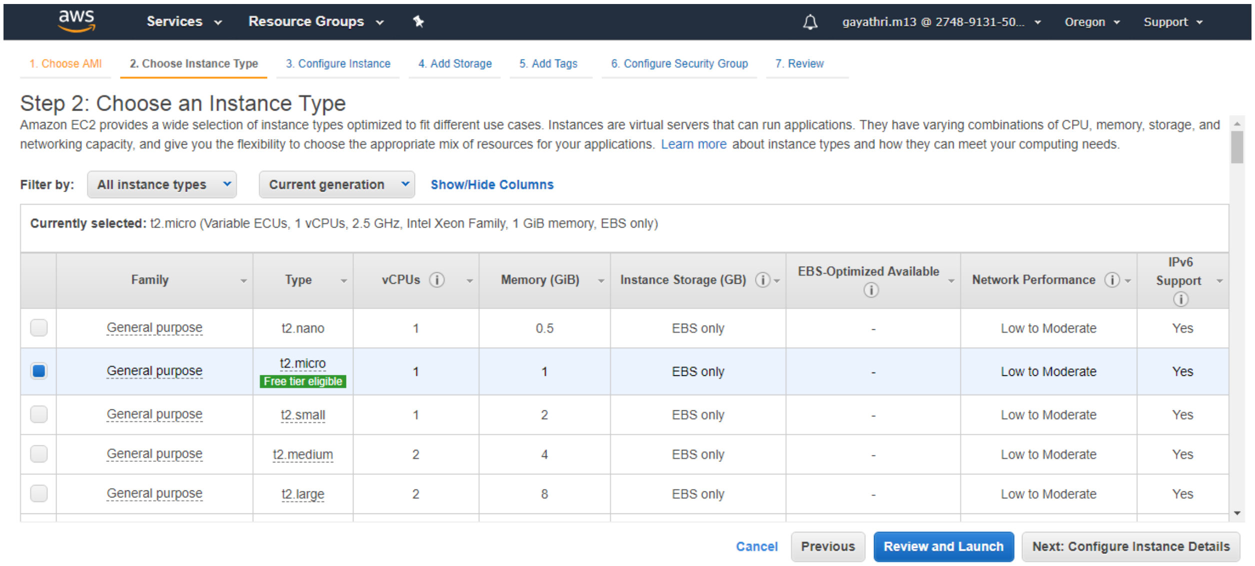
Red Hat Enterprise Linux 7.5 (HVM), SSD Volume Type - ami-28e07e50

AMI page let you choose the Operating Systems image file from the list. Read the available description and choose the appropriate one as per your need. Over here we'll select Amazon Linux AMI 2018.03.0.

You can also browse to various other tabs like My AMIs, Community AMIs and can choose appropriate ones.

Step2: Choose Instance Type:

Instance types comprise of varying combinations of CPU, memory, storage, networking performance, physical processor, clock speed etc. Based on the requirement one among the instance type will be opted.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation | Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes

*Over here, let us opt for type **t2.micro,** as it is eligible for free tier.*

Step3: Configure Instance

The virtual computing environments are called instances.EC2 allows users to rent virtual computers on which they run their own applications. Generally, 1 instance means 1 machine/server (often a virtual machine).

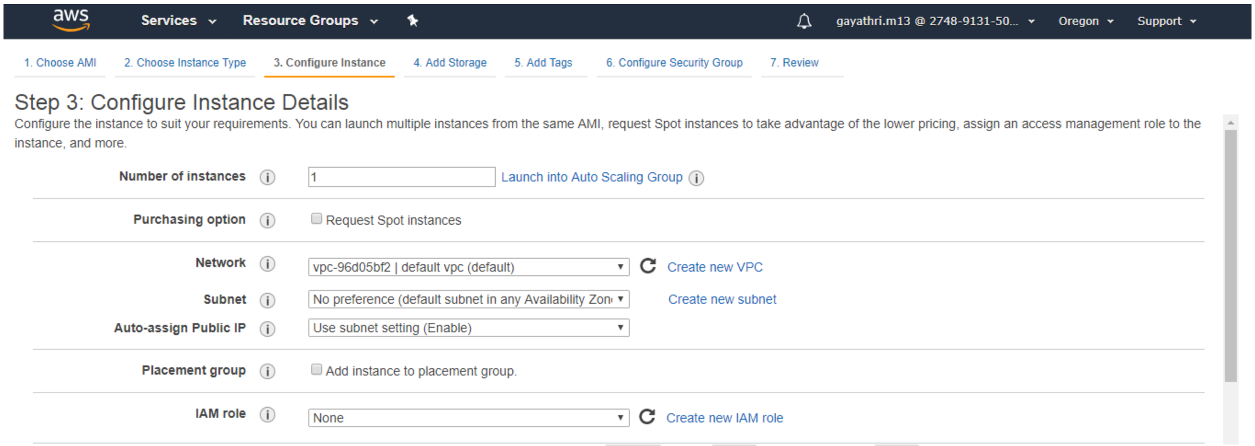
Configuration of instances is the third step in launching an instance. It includes, configuring below details:

1. *Number of instances to launch at a time*
2. ***Selecting purchasing option/ Request instances categories:***
    - *On –Demand Instances: Pay as you use, no long-term contracts.*
    - *Reserved Instances: 1-3 year terms, much hourly discount*
    - *Spot instances are some bid instances, often available at lower prices.*
3. ***Network Addressing or VPC:***

    Specify a network domain, in EC2-classic domain or choose public or private networks/sub-networks from a VPC. Amazon VPC offers greater isolation, and better security.

    This includes, Private IPs, Public IPs, Elastic IPs.
4. ***Subnet**: A range of IP addresses in your VPC.*
5. ***Auto-assign public IP**: to be used to access your instance publically over internet which gets changed each time you stop or the machine.*

    If you require consistent IP addresses, go for Elastic IP's.
6. ***IAM roles** are created to make secure connections to your application via API requests to your instances.*



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-96d05bf2 | default vpc (default) ▾ Create new VPC
Subnet	No preference (default subnet in any Availability Zon ▾ Create new subnet
Auto-assign Public IP	Use subnet setting (Enable) ▾
Placement group	□ Add instance to placement group.
IAM role	None ▾ Create new IAM role

7. ***Shutdown behavior:***

   Specifies whether an instance shutdown should stop or rather terminate.

8. ***Termination Protection:***

   Protects against accidental termination of an instance.

9. ***Monitoring:*** *Use CloudWatch to monitor, collect, analyze, metrics of EC2 instances using alarms, notifications etc. This topic is out of scope in this Course.*

10. ***Shared Tenancy/Dedicated:*** *You can choose to run your instance on a single- tenant dedicated hardware or go for the shared model.*

11. ***Auto-Recovery:***

Automatically recovers the Amazon EC2 instances from any hardware failures. This can be triggered using CloudWatch alarms.

Supported only for C3, C4, M3, R3, T2 instance types also using EBS in a VPC with shared tenancy.

12. ***Source-Destination Check:***

Rejects IP packets not meant for an instance

13. ***User Data:***

   A script written to automatically initialize instances which executes a series of commands and runs once per instance from a new AMI or from while rebooting.

   It uses Linux shell script, Windows batch or PowerShell Script

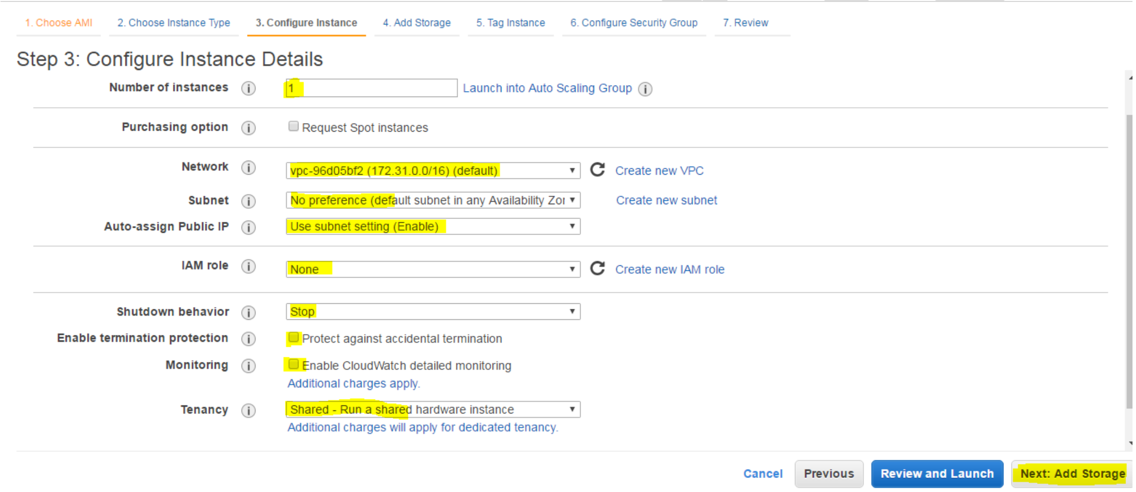
   It could be used for installing any software package, web servers, database servers, configuration management tools.

   Paste the below script in the user data section

```
#!/bin/bash

yum -y install httpd

systemctl enable httpd

systemctl start httpd

echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html
```

Select configurations as per your requirement and complete this step in launching an EC2 instance.

- *Network, Subnet and Auto-assign Public IP (enable) as default.*
- *You can create an IAM role if you want your instance to be accessed by a group of users, otherwise leave in as None.*
- *Select shutdown behavior as Stop or Terminate, both options will take away the virtual machine allocated to you when you shut down the instance but Terminate will clear the memory storage also.*
- *You can restart your instance in case of Stop but it is not possible if you are selecting Terminate.*



Step 3: Configure Instance Details

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-96d05bf2 (172.31.0.0/16) (default) — Create new VPC

Subnet: No preference (default subnet in any Availability Zo — Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

IAM role: None — Create new IAM role

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

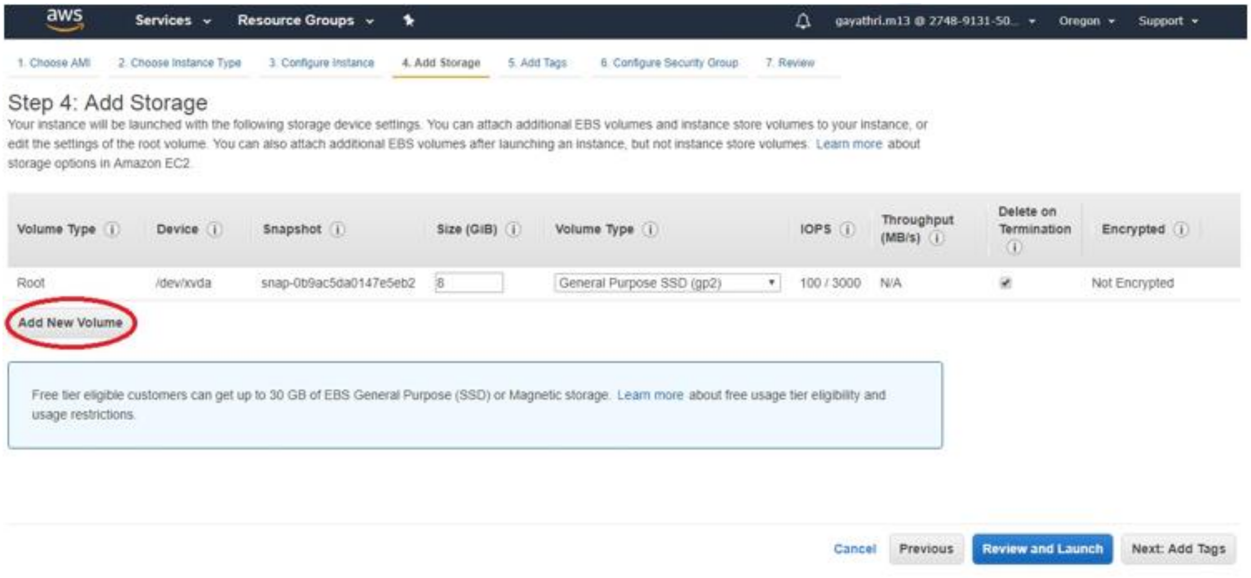
Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Step4: Add Storage

By default, all Amazon EC2 AMIs are backed up by Amazon EC2 Instance Store.

AMIs can also be chosen to be backed up by Amazon EBS volume (faster and persistent).

You can increase (or decrease) the memory size for the instance and change the Volume Type also. You can select it from Instance or Ephemeral Stores for your EC2 instance.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

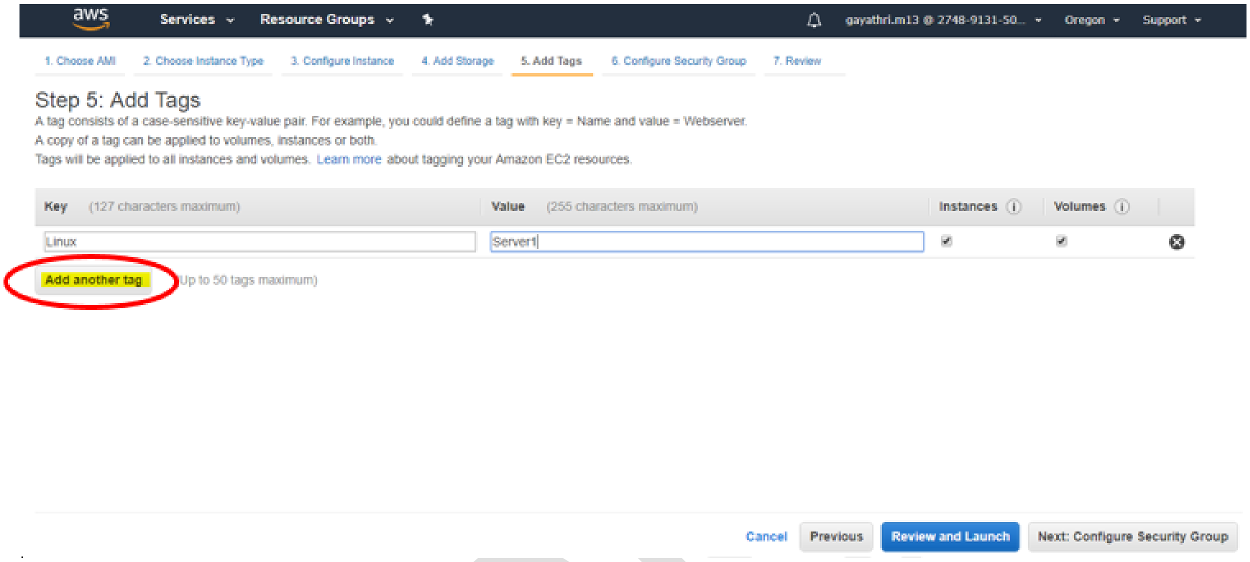
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0b9ac5da0147e5eb2	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Let us opt for the default storage, click on Next.

Step5: Add Tags:

*Tag is a simple **label** consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources.*



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes
Linux	Server1	✓	✓

(Up to 50 tags maximum)

Provide Key and Value and click on Next.

Step6: Configure Security Group:

Security Group consists of rules to govern inbound and outbound traffic. Security groups are bound to a specific region.

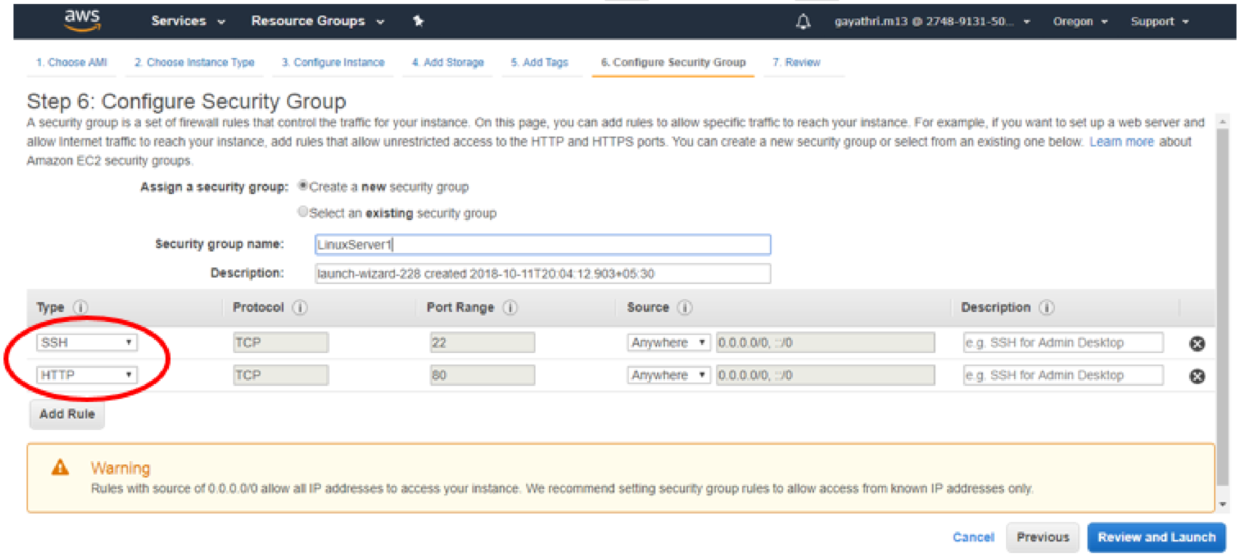
Click on ***Create a new security group.***

Define rules/protocols for inbound and outbound traffic. Specify port range, IP range, etc.

*In the source, if you are selecting **anywhere,** then your resources will be accessible from anywhere. **My IP** means only your machine can access the resources. Similarly, can define **a Custom IP** for your resources for each rule. Add some more rules according to your requirements by clicking on '**Add Rule**'.*

Based on the type of Operating System the remote protocol has to be added. We have selected Linux machine; hence we have chosen SSH protocol.

Click on Add rule and add Http protocol, then click on next.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: LinuxServer1

Description: launch-wizard-228 created 2018-10-11T20:04:12.903+05:30

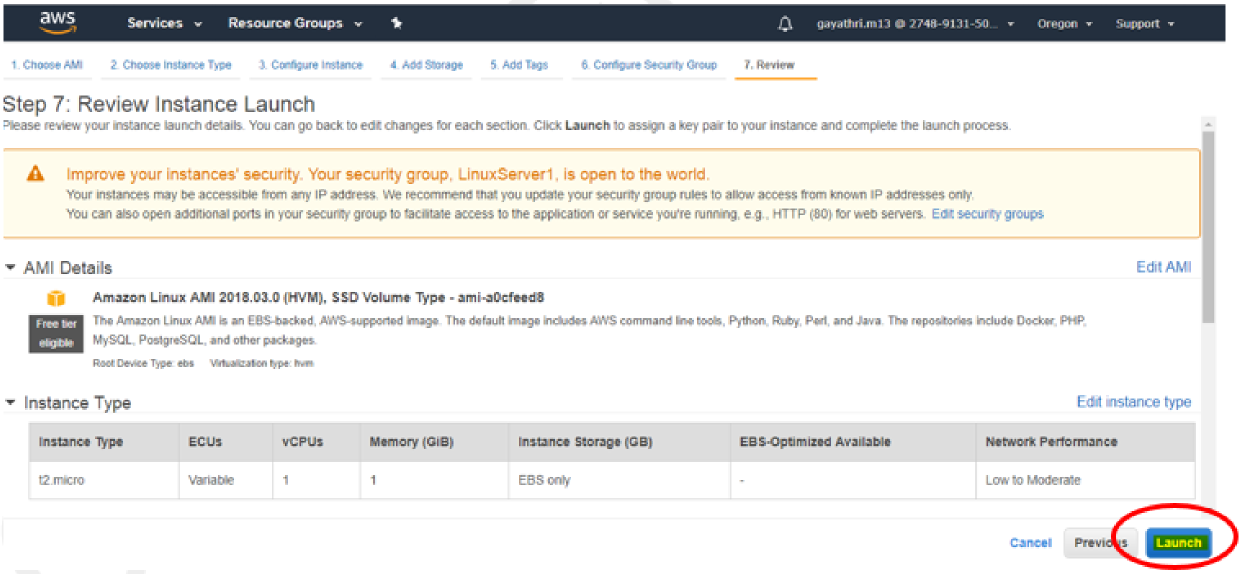
Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Step7: Review

Review the configurations and click on Launch.



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, LinuxServer1, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details — Edit AMI

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-a0cfeed8

Free tier eligible

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root Device Type: ebs   Virtualization type: hvm

Instance Type — Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

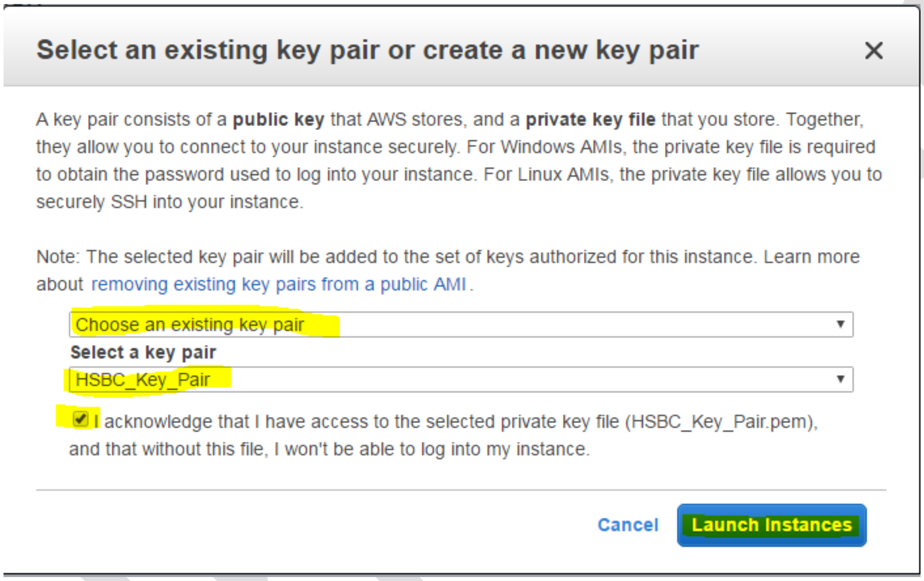
Step8: Configure Key Pair:

AWS provides encryption to login using Public Key cryptographic keys where Public key is placed on the Amazon server and Private key (.pem extension) is ought to be downloaded to the user's local machine.

Click on create new key-pair, provide name and download the key-pair.

You can also click on existing key-pair, if you have any.

Then Launch the instance.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

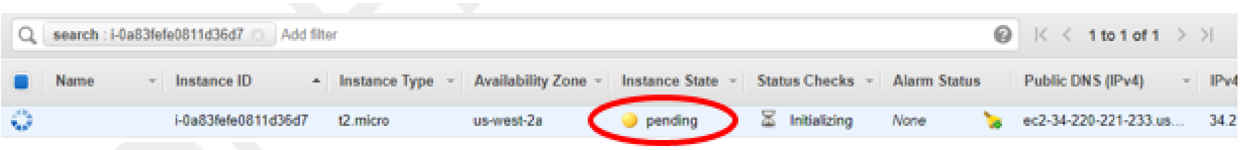
Choose an existing key pair

Select a key pair

HSBC_Key_Pair

☑ I acknowledge that I have access to the selected private key file (HSBC_Key_Pair.pem), and that without this file, I won't be able to log into my instance.

The instance takes few minutes to Initialize.

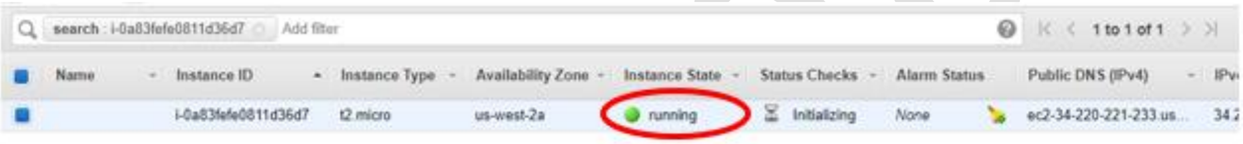


search : i-0a83fefe0811d36d7 Add filter

1 to 1 of 1

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4
		i-0a83fefe0811d36d7	t2.micro	us-west-2a	pending	Initializing	None	ec2-34-220-221-233.us...	34.2

Once the instance is launched, the instance state changes to Running from Pending.



search : i-0a83fefe0811d36d7 Add filter

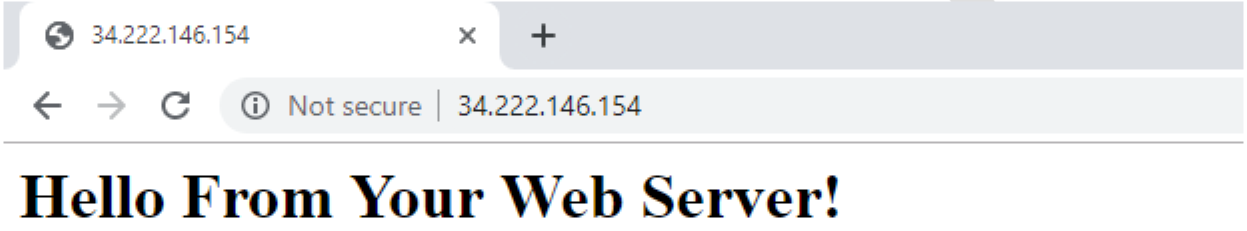
1 to 1 of 1

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv
		i-0a83fefe0811d36d7	t2.micro	us-west-2a	running	Initializing	None	ec2-34-220-221-233.us...	34.2

You can see the current status of this instance and note down the Public IP and Public DNS to connect to this instance.

***Note:** Do not forget to stop your instance when it is not in use. EC2 services are chargeable on time duration basis. Generally, they will charge you on the basis of total running hours of all the instances and memory storage used.*
*Go to '**Actions**' and Stop your instance when not in use or terminate it if you don't want to use it anymore.*
Termination will delete the memory space associated with the instance and you will not be able to restart it again.
Similarly, you can create a Linux instance also based on your need.

Step 9: *Refer to the Public IP address of your instance and open the host address/ IP address for this instance on a browser as shown:*



Hello From Your Web Server!

Summary of this assignment: *In this assignment, you have learnt how to deploy a static page in Linux EC2 instance.*

Assignment 1b: Creating Windows Ec2 instance

Objective: To create a Windows EC2 instance

Solution:

Refer : https://aws.amazon.com/getting-started/tutorials/launch-windows-vm/?trk=gs_card

Summary of this assignment: *In this assignment, you have learnt how to connect to Linux EC2 instance in AWS.*

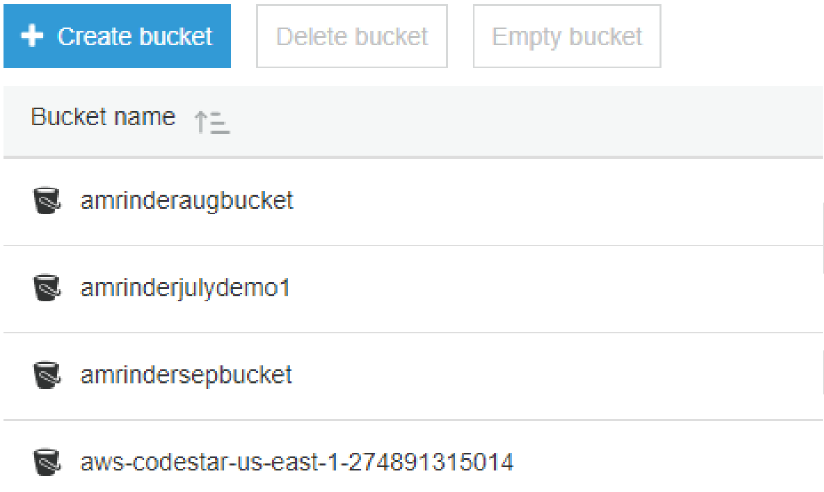
Assignment 2a: Create an Amazon S3 bucket

Objective: To learn how to create an S3 bucket.

Solution:

Step** 1: Click Services and select **S3

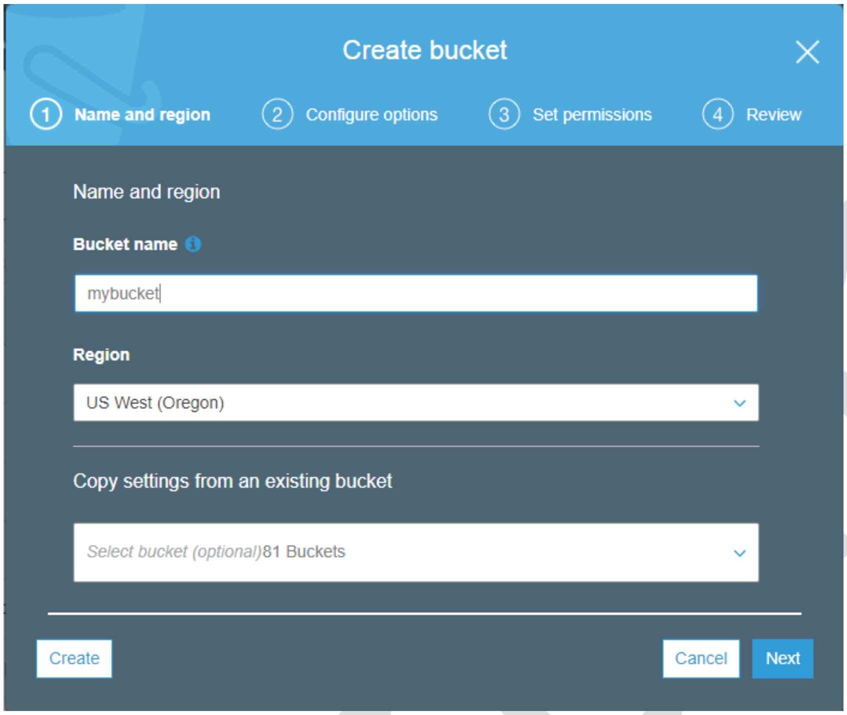
Step** 2: Click **Create Bucket



Bucket name ↑☰
amrinderaugbucket
amrinderjulydemo1
amrindersepbucket
aws-codestar-us-east-1-274891315014

__Step__ 3: In the create a bucket, select a unique name for your bucket and select the region.

Click on Next to configure bucket permission and settings, else click create.



Name and region

Bucket name: mybucket

Region: US West (Oregon)

Copy settings from an existing bucket: Select bucket (optional)81 Buckets

Summary of this assignment: *In this assignment, you have learnt how to create an Amazon S3 bucket.*

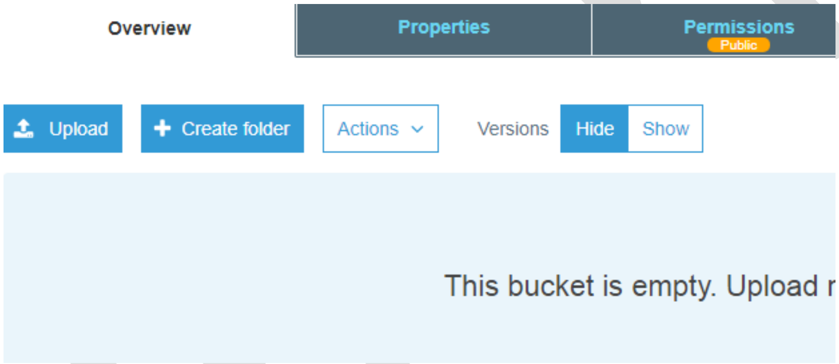
Assignment 2b: Upload objects in to S3 bucket

Objective: To upload a file in Amazon S3 bucket.

Solution:

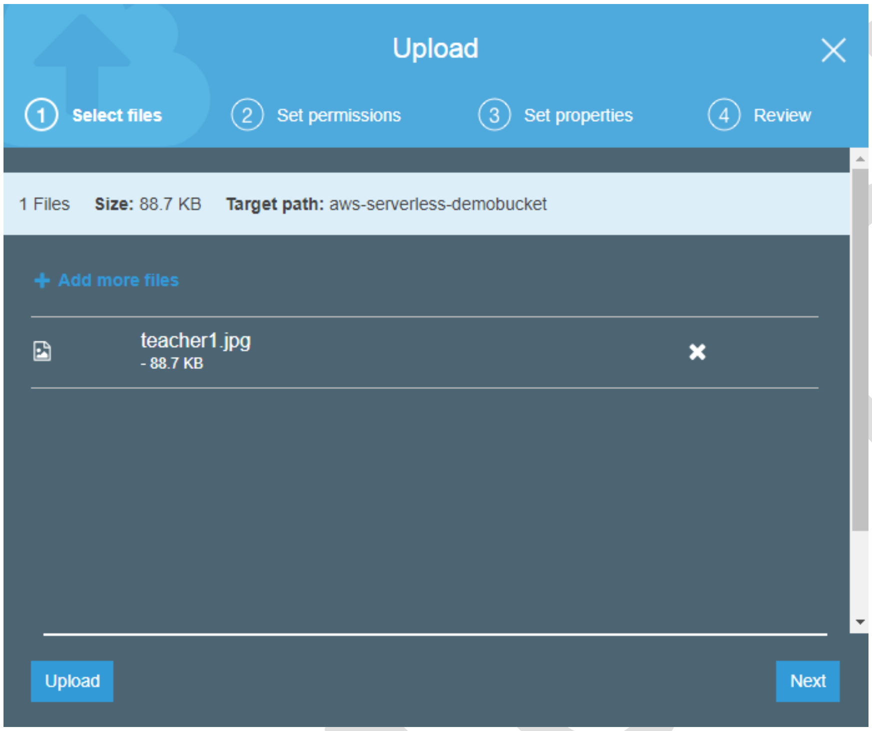
Step1: *Click on the bucket name that you created.*

Step2: *Click on upload button to upload file or Create folder to create a subfolder inside the bucket.*



This bucket is empty. Upload r

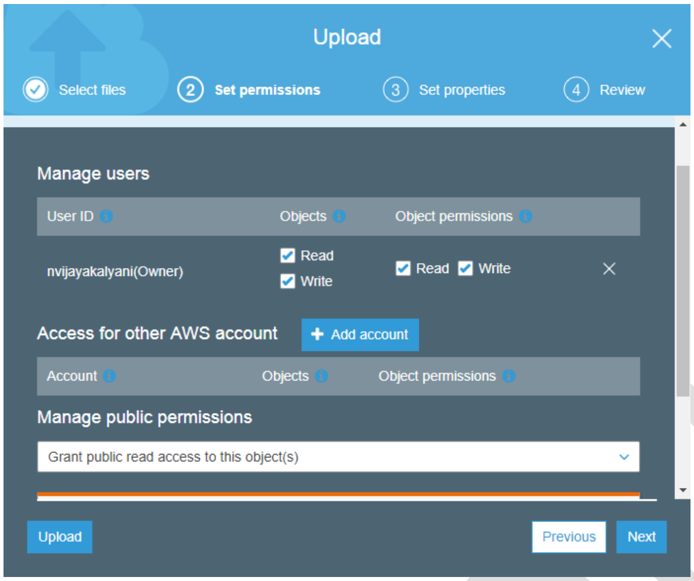
Step3: *Once you click on Upload, click on add files and select the appropriate file that has to be uploaded. Then you can click on Next to configure permissions for the file.*



1 Files **Size:** 88.7 KB **Target path:** aws-serverless-demobucket

teacher1.jpg
- 88.7 KB

In Set permission tab, review the permission setting and then click on Upload.



Manage users

User ID	Objects	Object permissions
nvijayakalyani(Owner)	☑ Read ☑ Write	☑ Read ☑ Write

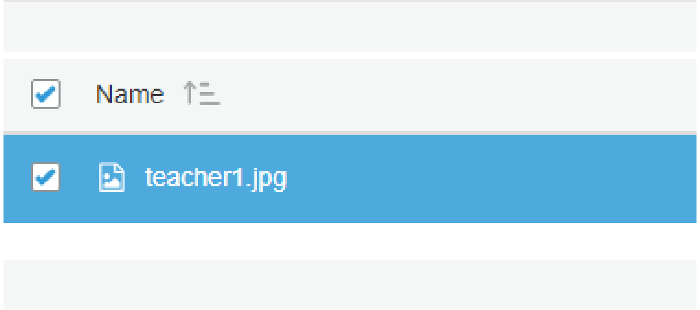
Access for other AWS account

Account	Objects	Object permissions

Manage public permissions

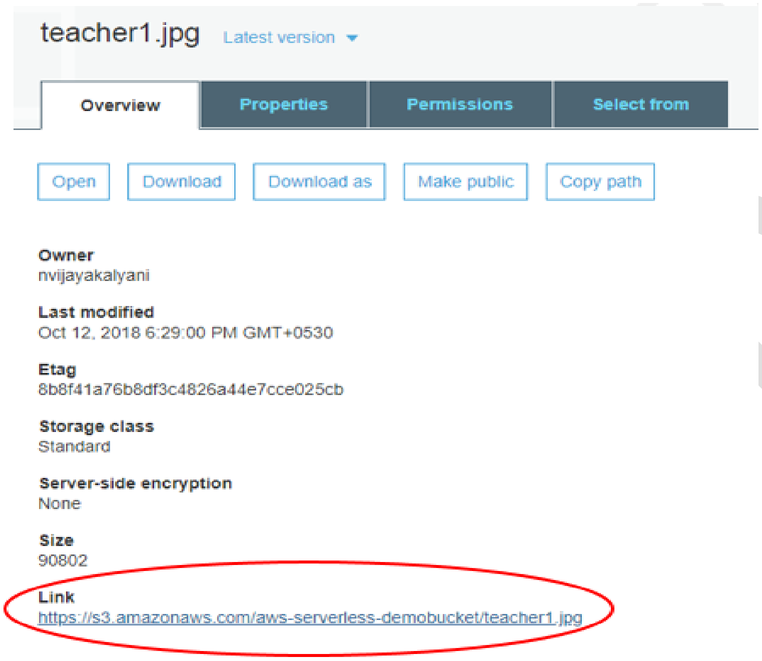
Grant public read access to this object(s)

Once the document is uploaded it will be shown in the bucket.



☑	Name
☑	teacher1.jpg

Click on the file, use the link provided to access the file.



Owner
nvijayakalyani

Last modified
Oct 12, 2018 6:29:00 PM GMT+0530

Etag
8b8f41a76b8df3c4826a44e7cce025cb

Storage class
Standard

Server-side encryption
None

Size
90802

Link
https://s3.amazonaws.com/aws-serverless-demobucket/teacher1.jpg

Summary of this assignment: *In this assignment, you have learnt how to upload file into Amazon S3 bucket.*