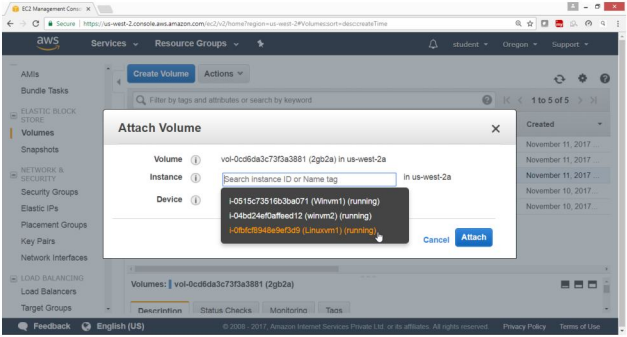
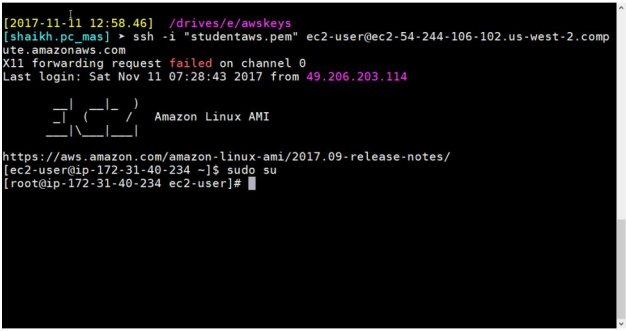
Select Linux instance



Now connect to Linux instance



To verify

Switch to root user and run fdisk -l

$ sudo su

To check list of drives and partitions

fdisk -l

```
[ec2-user@ip-172-31-40-234 ~]$ sudo su
[root@ip-172-31-40-234 ec2-user]#
[root@ip-172-31-40-234 ec2-user]# fdisk -l
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase.
 Use at your own discretion.

Disk /dev/xvda: 8589 MB, 8589934592 bytes, 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt


#         Start          End    Size  Type            Name
 1         4096     16777182      8G  Linux filesyste Linux
128         2048         4095      1M  BIOS boot parti BIOS Boot Partition

Disk /dev/xvdf: 2147 MB, 2147483648 bytes, 4194304 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xb9c39eba
```

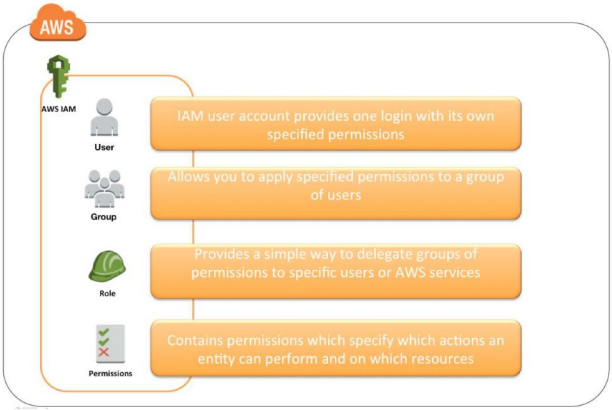
Lab 6: To Manage IAM Users, Groups and Policies

OBJECTIVE

To configure and use AWS IAM Service.

TOPOLOGY

AWS IAM Identities



PRE-REQUISTES

User should have AWS root account

To configure IAM with following task.

Create IAM users, assign password, and change password policy.

Create IAM groups.

Add users to a group.

Add policies to Groups and Users.

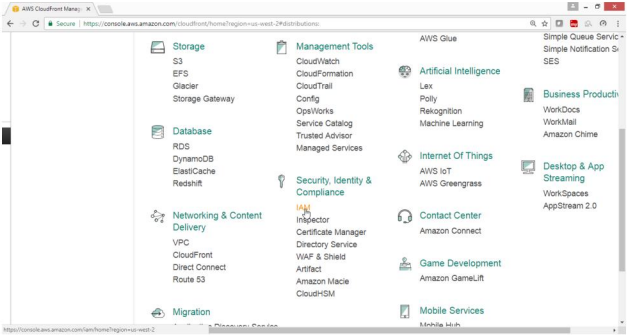
Create your own policies.

Users Login to sign-in page.

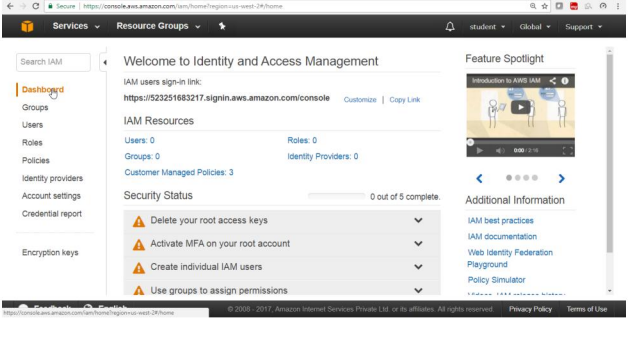
Deleting users and groups.

1) To create user, assign password, change password policy.
Open AWS console select **Security, Identity & Compliance**

Click on **IAM** service



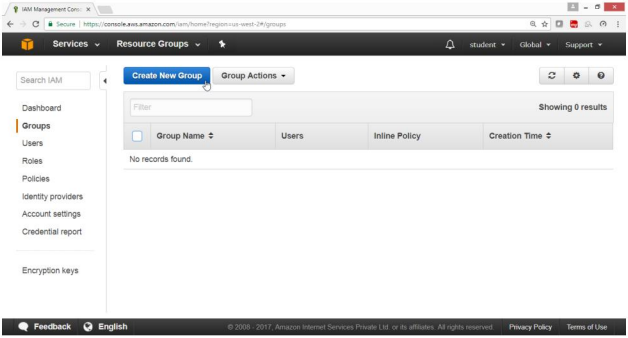
IAM Dashboard panel available



2) To Mange Groups and applying policies

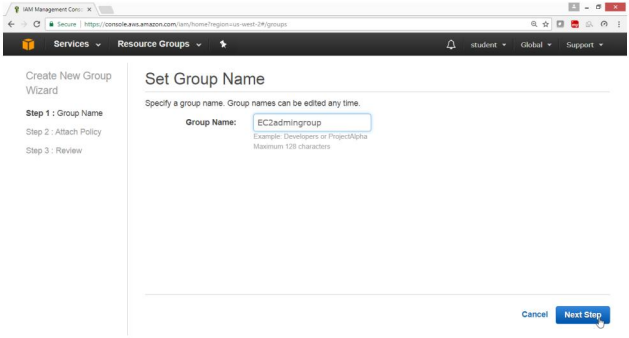
From IAM dashboard, select **Groups**

Click on **Create New Group** button



Give Group Name → EC2admingroup

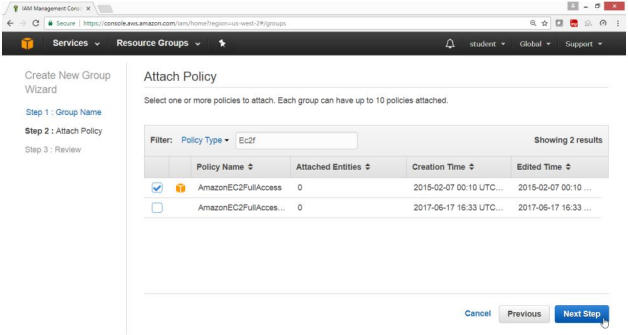
Click on **Next Step** button



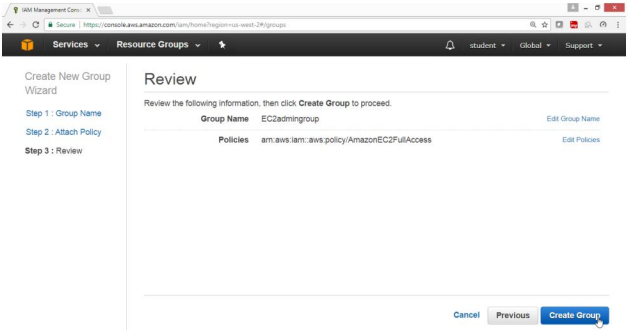
In Filter type → EC2f

Select check box for **AmazonEC2FullAccess**

Click on **Next Step** button

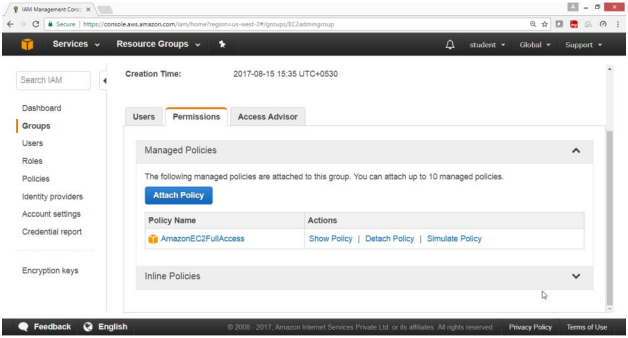


Click on **Create Group**



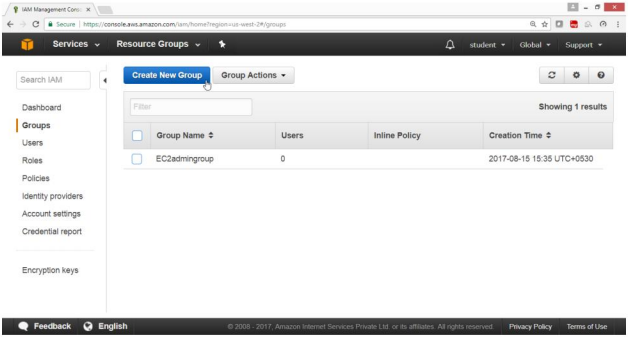
Verify

Group EC2admingrp got created with AmazonEC2FullAccess policy

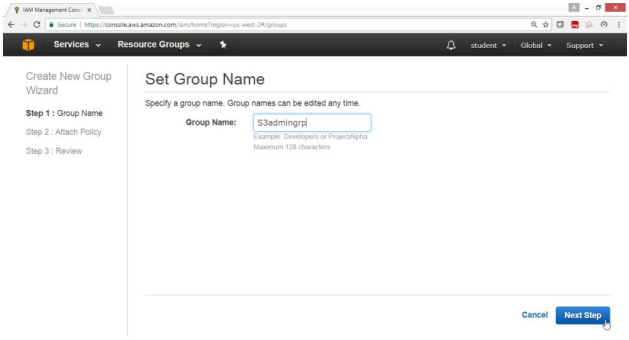


Now again create Another Group

Click on **Create Group** button



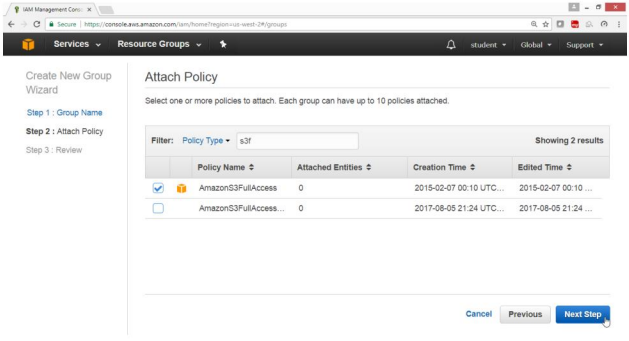
To create a group With S3FullAccess



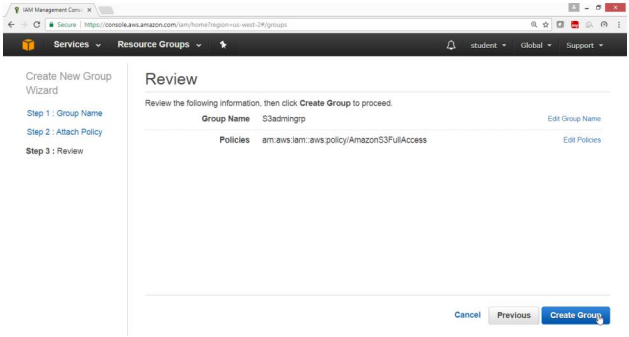
In Filter type → S3f

Select check box for **AmazonS3FullAcess**

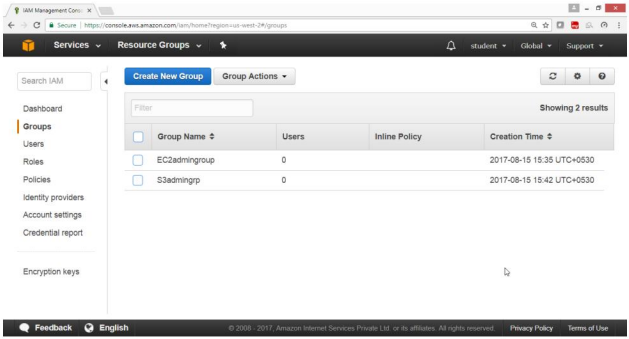
Click on **Next Step** button



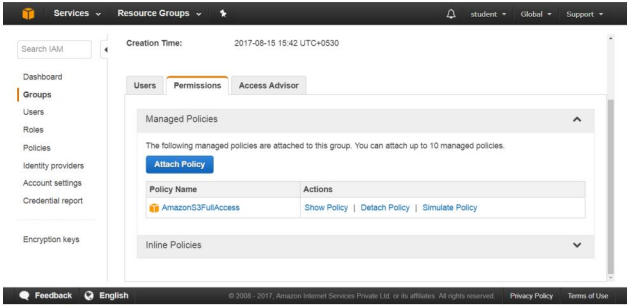
Click on **Create Group** button



Verify EC2admingroup & S3admingr groups got created



Verify S3 policy is attached



Create user tom and join to EC2admingroup

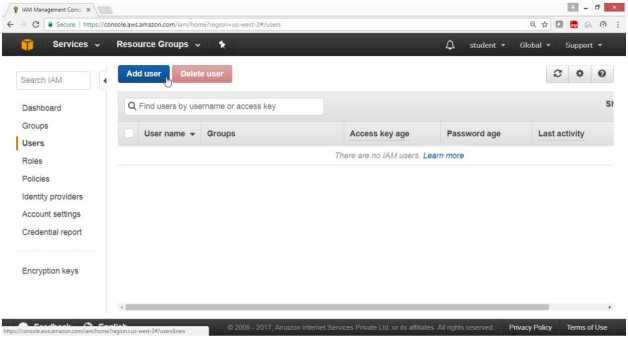
Create user john and join to S3admingroup

Create a user sai add Ec2fullaccess and S3fullacces Policy

From IAM dashboard

Select **Users**

Click on **ADD Users** button



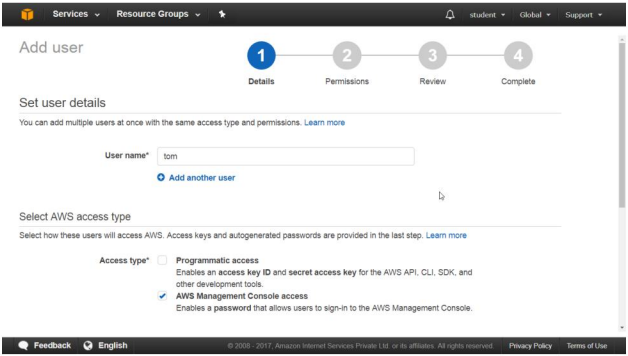
Scenario 1)

Create user tom and join to EC2admingroup

For User name → tom

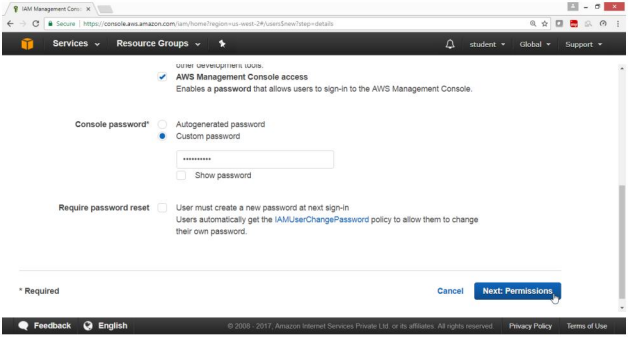
For Access type → AWS Management Console access

Drag down



For Console password → ******

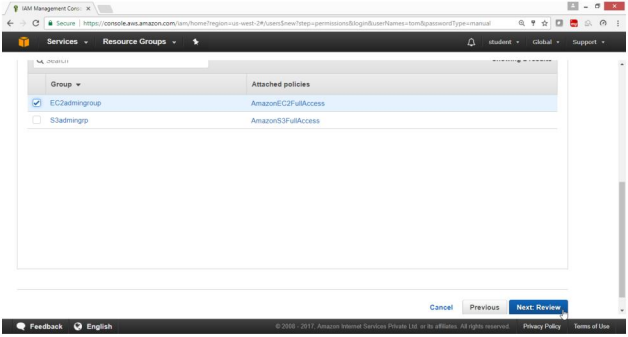
Click on Next **Permissions** button



Under Group column

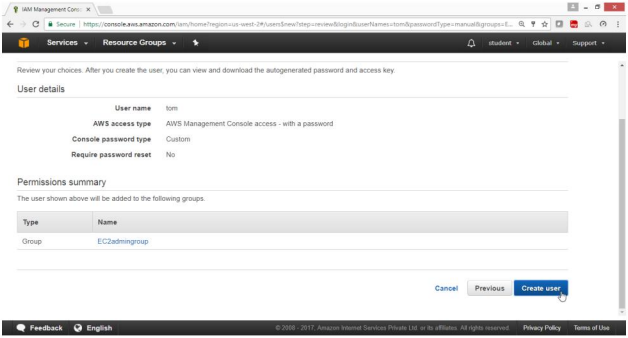
Select EC2admingroup

Click on **Next Review**

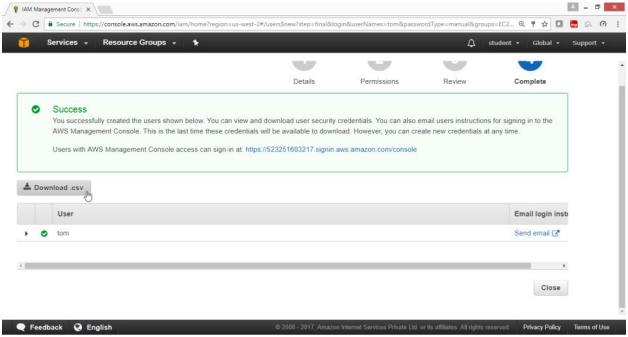


Verify users detail

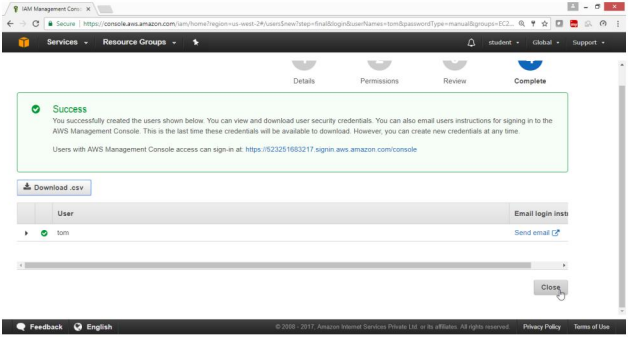
Click on **Create user** button



Down the .csv file



Click on **close** button

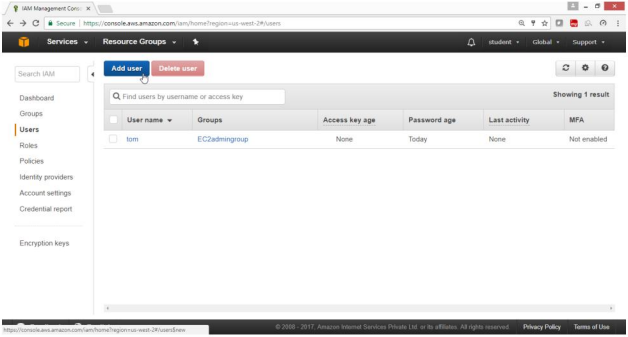


Scenario 2)

Create user john and join to S3admingroup

Select user

Click on **Add user** button

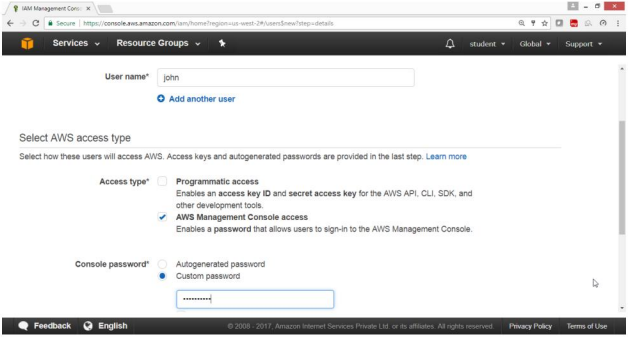


For user name → john

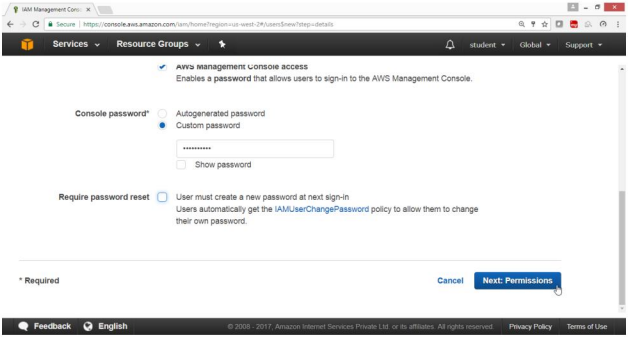
For Access type → AWS Management Console access

For console password → ******

Drag down

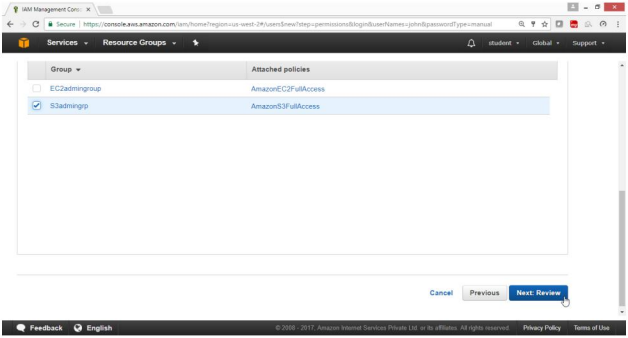


Click on **Next Permission** button



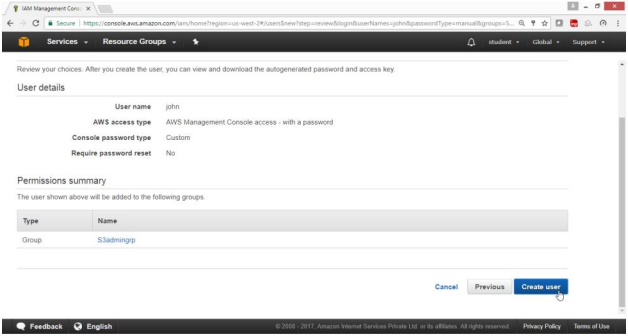
Select S3admingrp

Click on **Next Review** button



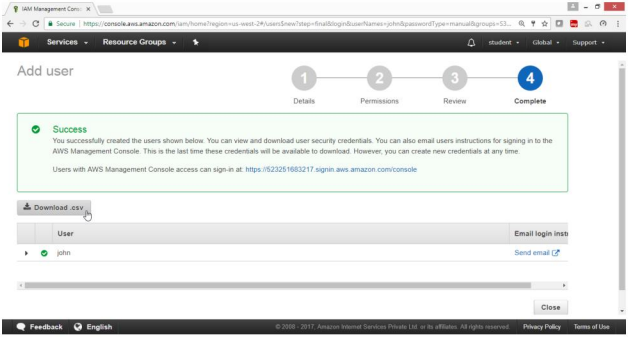
Verify user details

Click on **Create user** button



Download .csv file

Click on **Close** button



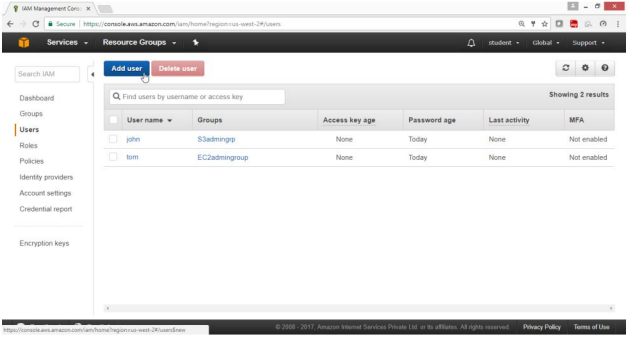
Scenario 3)

Add a user individual user sai without joining to any group

Attach EC2FullAccess and S3FullAccess policy

Select User

Click on **Add user** button

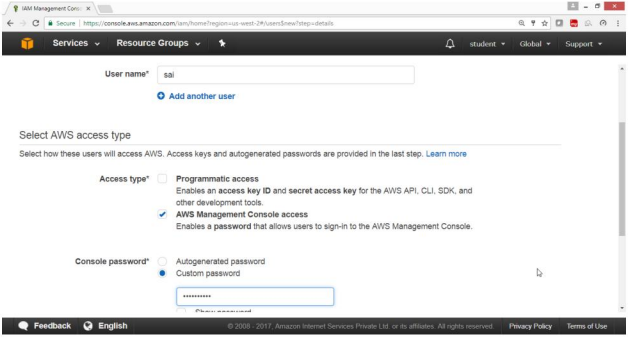


For User name → sai

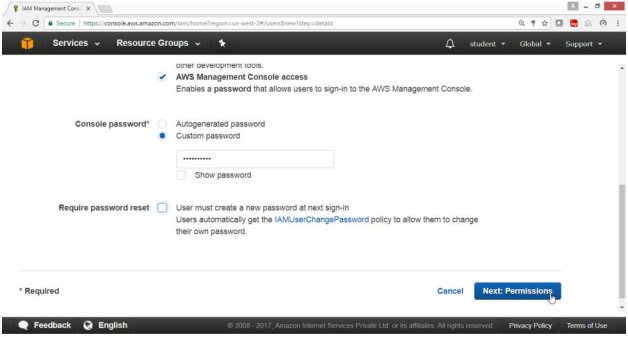
For Access type → AWS Management Console access

For Console password → ******

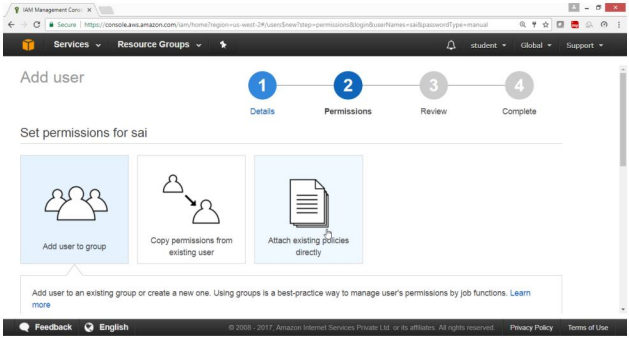
Drag Down



Click on **Next permission** button

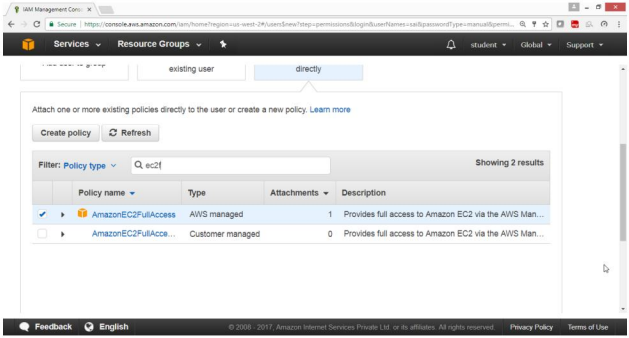


Click on **Attach existing policies directly** box



In Filter type search for ec2f

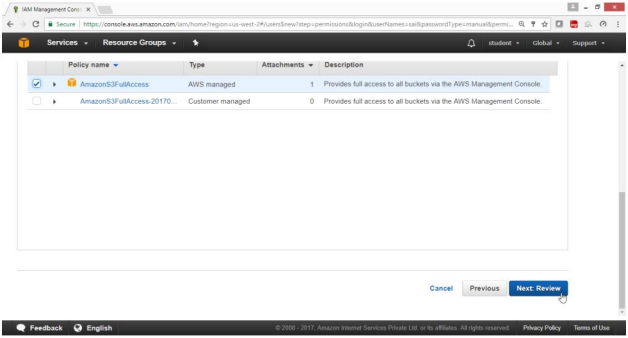
Select AmazonEC2FullAccess check box



In Filter type search for s3f

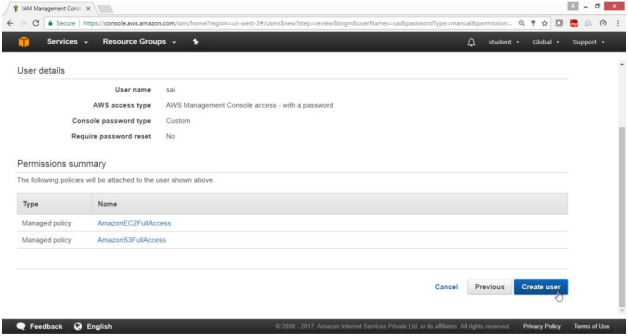
Select AmazomS3FullAccess check box

Click on **Next Review** button



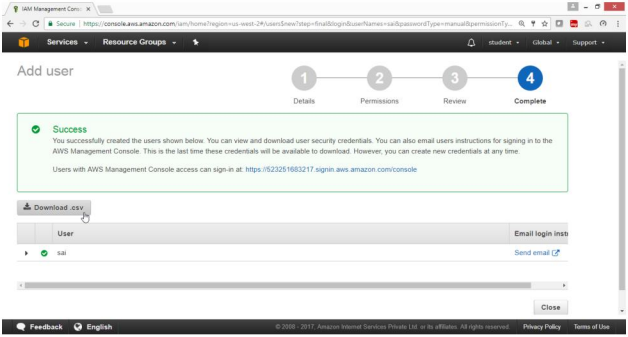
Verify users detail

Click on Create user button



Download .csv file

Click on **Close** button



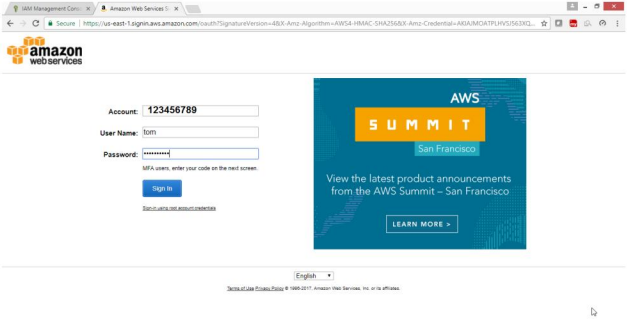
To verify wheather users can access particular Service

Login as tom user

Provide the following url in Browser

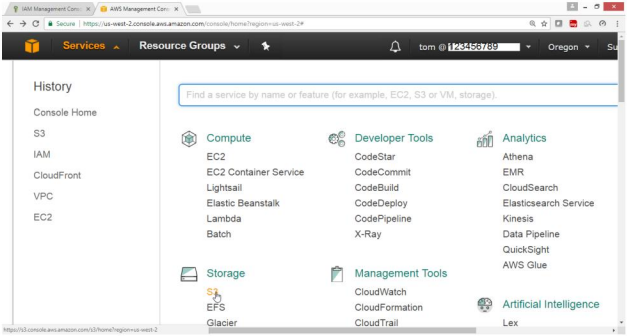
https://123456789.signin.aws.amazon.com/console

Click on Sign in button



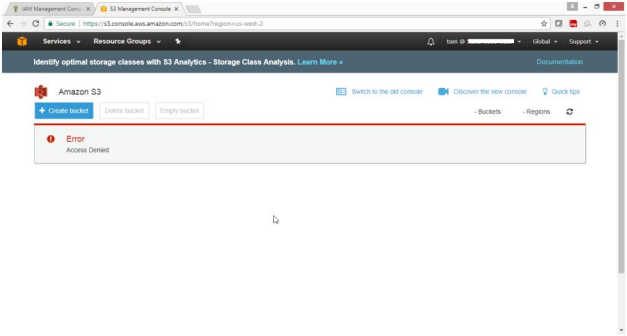
User tom is not having S3 access

Click on S3 verify the access

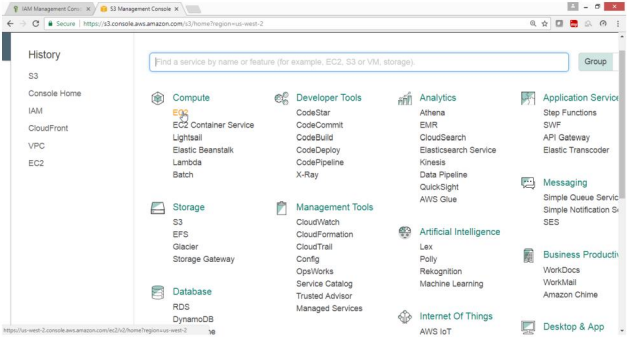


Verification

Error Access Denied

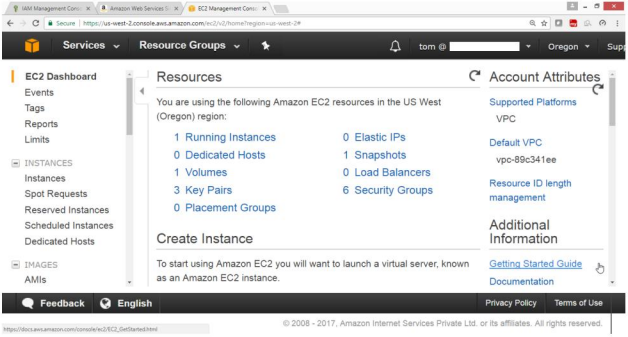


Now select EC2 service



Verification

User tom can access EC2 service.



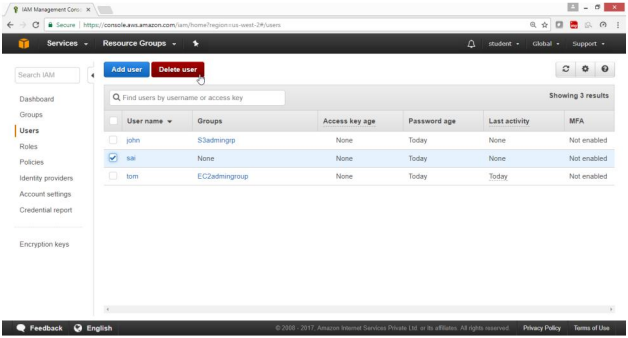
Similarly check for user john

To Delete users and groups

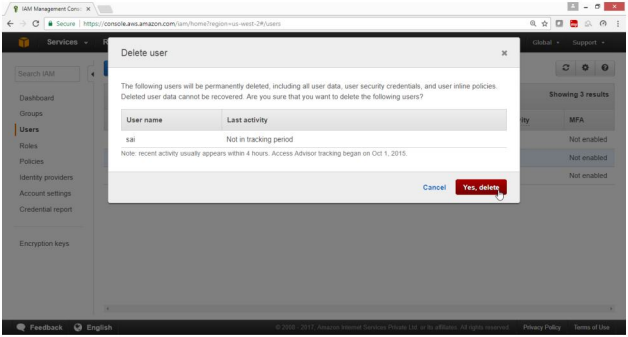
From IAM dashboard, select **Users**

Select the users, drop down **Action** button

Click on **Delete Users** button

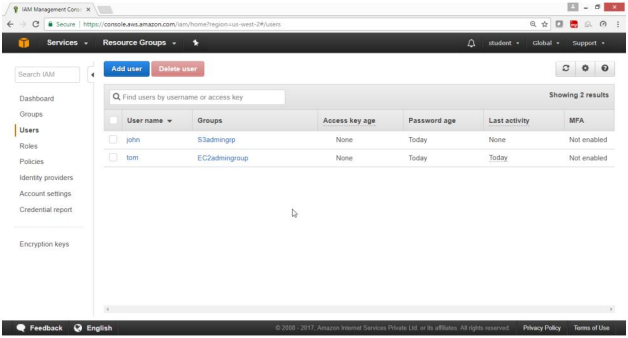


Click on **Yes, delete** button



Verification

User sai is deleted



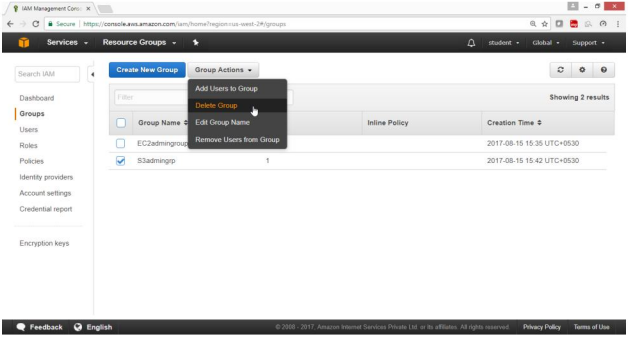
To Deleting Groups

From IAM Dashbaoard

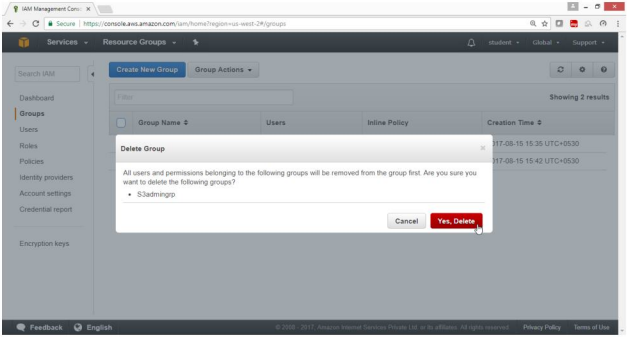
Select the **Groups**

Drop down **Group Action** button

Select **Delete Group**

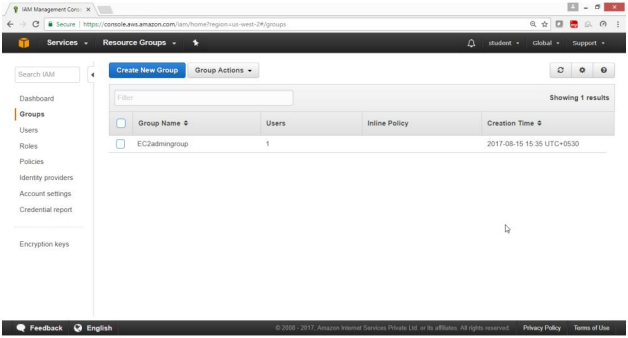


Click **Yes, Delete** button



Verification

Group is deleted



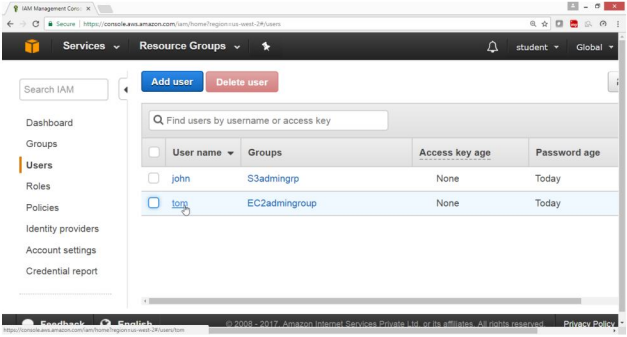
To Create Multifactor Authentication

Install Google authenticator in your Android Mobile

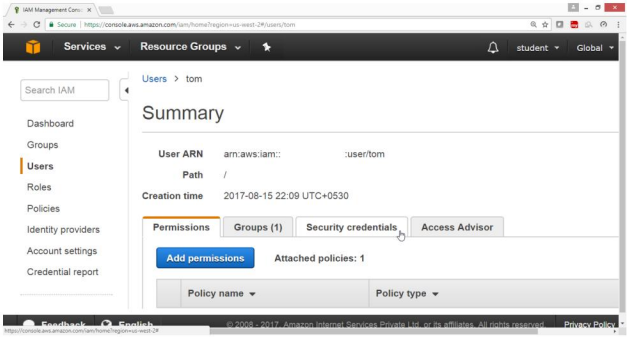
On the **IAM Dashboard** panel

Click on Users

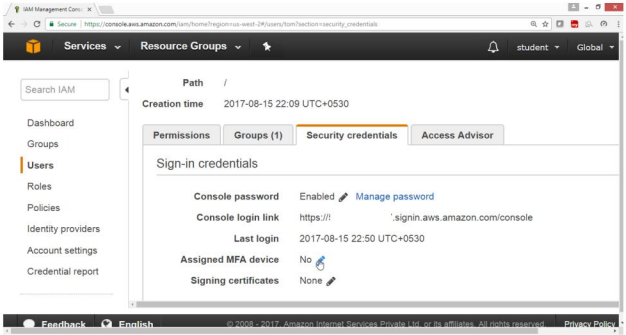
Click on the user tom



Click on Security credentials

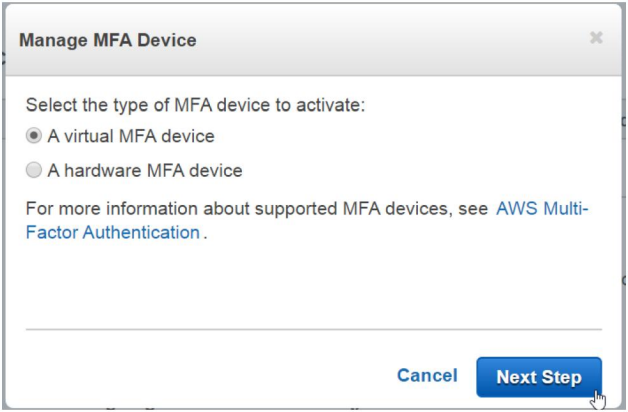


Click on pen sign for "**Assigned MFS device**"

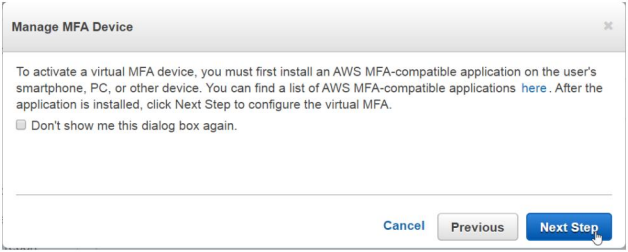


Select →**"A virtual MFS device"**

Click on **Next Step** button



Click on **Next Step** button



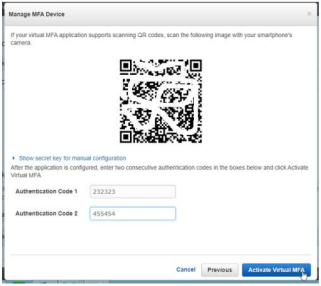
Bar code will be created

Scan this bar code from your mobile Google Authenticator application.

Now type 6 digit bar code in Authetication code 1

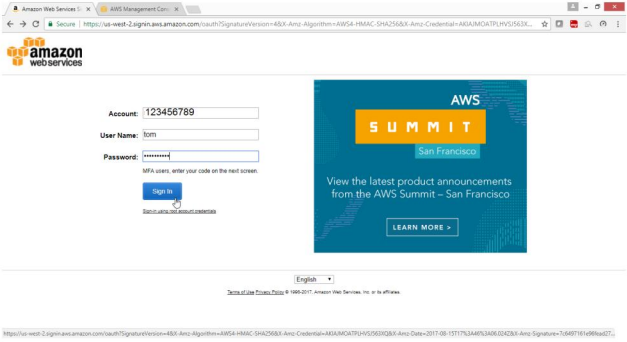
Once the bar code changes

Retype 6 digit bar code in Authetication code 2



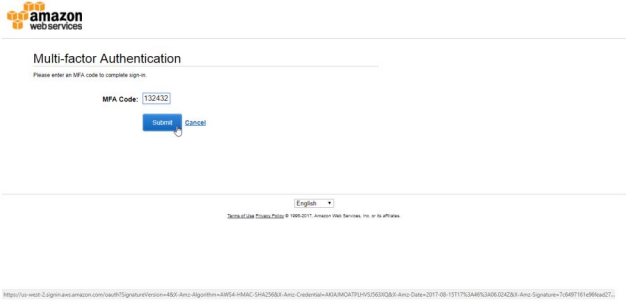
Click on Finish

Now login as tom user

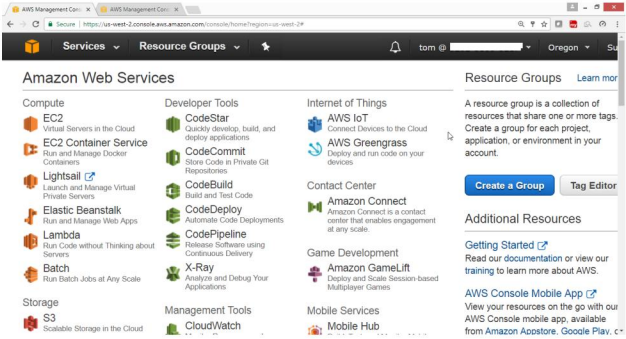


Once the user types the MFA 6 digit coder

Click on submit



Verify user had successfully logged in.

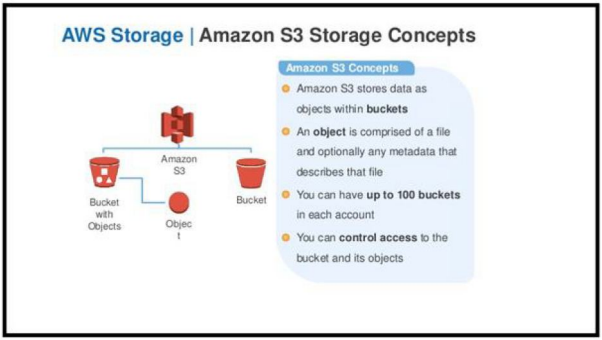


Lab 7: To Configure Amazon Simple Storage Service (Amazon S3)

OBJECTIVE

To configure and use AWS S3 service

TOPOLOGY



PRE-REQUISTES

User should have AWS account, or IAM user with AmazonS3FullAccess

To Configure S3 with following task:

Sign Up for Amazon S3

Create a Bucket

Add an Object to a Bucket

Add an folder to Bucket

View an Object

Move an Object

Delete an Object and Bucket

To empty a bucket

To delete a bucket

Hosting a Static Website on Amazon S3

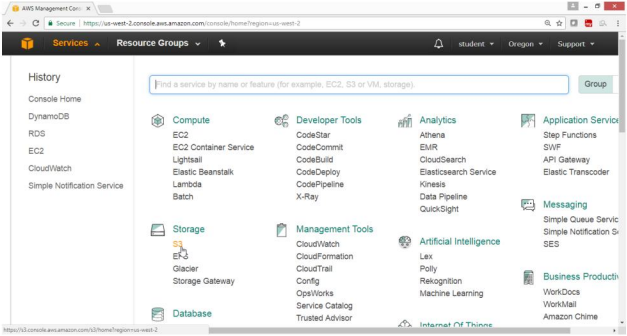
AWS user to control S3

1. To create S3 bucket for storing objects that is files and folders

Open AWS console

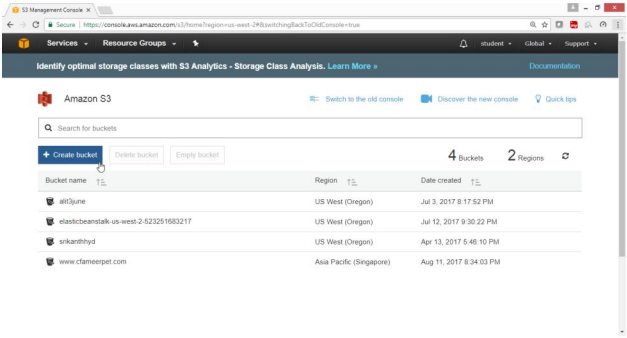
Select **"Storage"** service

Click on **S3**



On Amazon **S3** page

Click on **Create Bucket**



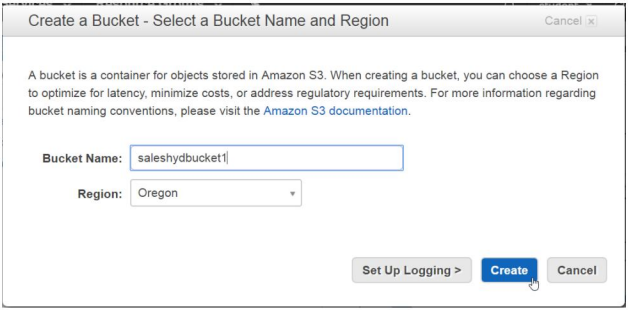
On "**Create Bucket - Select a Bucket Name and Region" box**

Provide following values

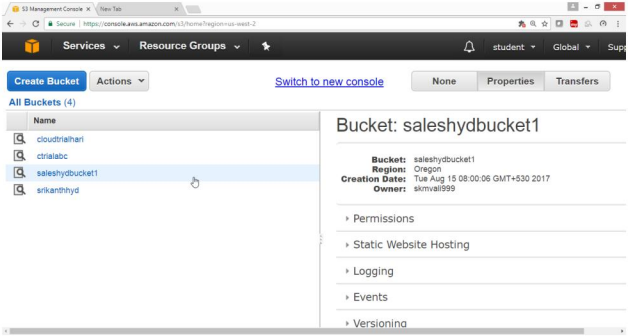
Bucket Name → saleshydbucket

Region → Oregon

Note: A bucket name in region must contain only lower case characters and should be unique in entire Amazon bucket names from all the region.



Verify that bucket is created.



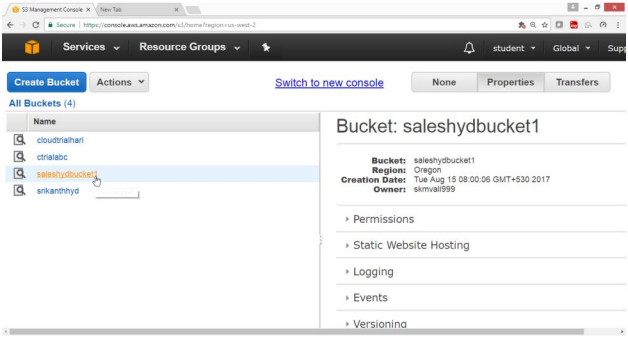
To upload files of any type

Right click in empty space, select **Upload**

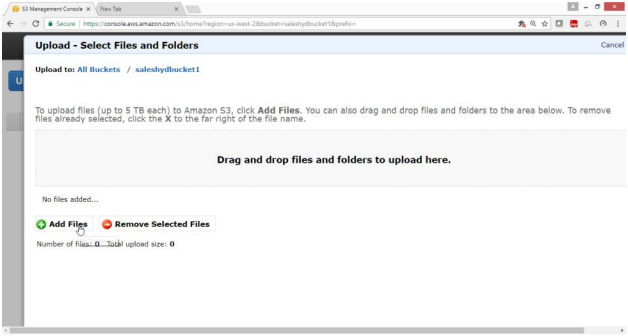
Note: 5 GB can be uploaded

It will be charged if crossed free tier usage.

Click on Created bucket



Click on **Add files**

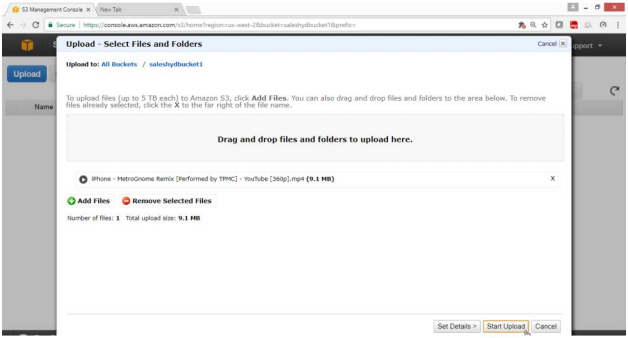


In the upload Wizard

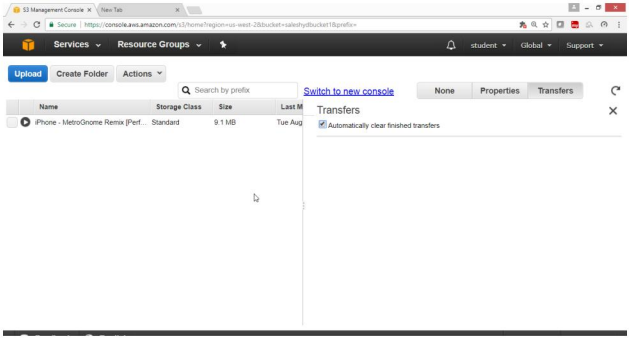
Click on **Add files**

Select some txt, pdf, video files

Click "**start upload**" button

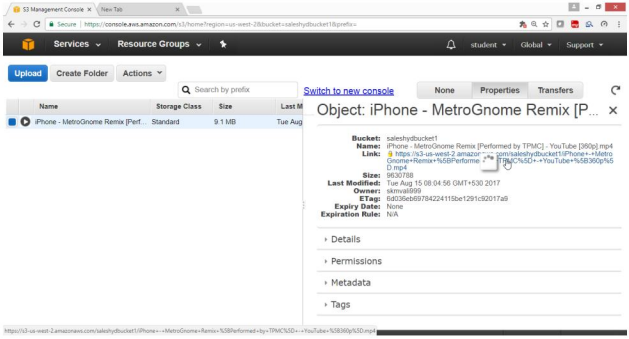


Verify that the file got uploaded.

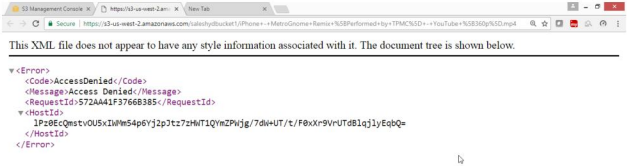


Select the file, Click on Properties on Right Panel,

Click on the **link**

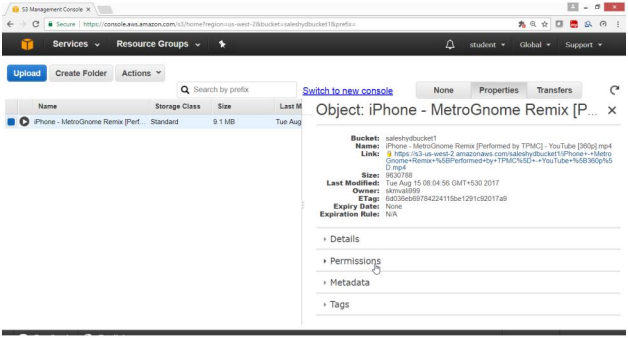


Verification : Cannot access due to lack of permission



To allow users to Download, or view give permission

Select, **Permission** tag



Click on **Plus Radio** button for **Add more permissions**

Drop down Grantee Button

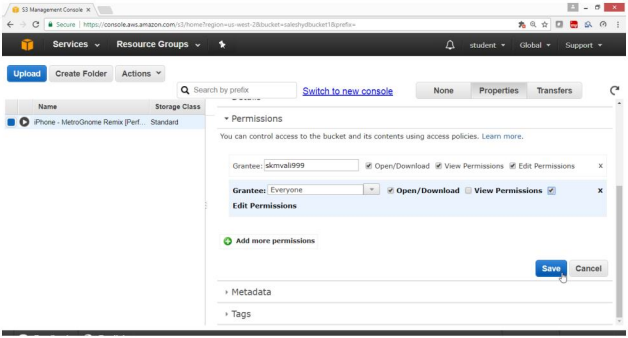
Select **Everyone** to make it public

Enable the check box to **Open/Download**

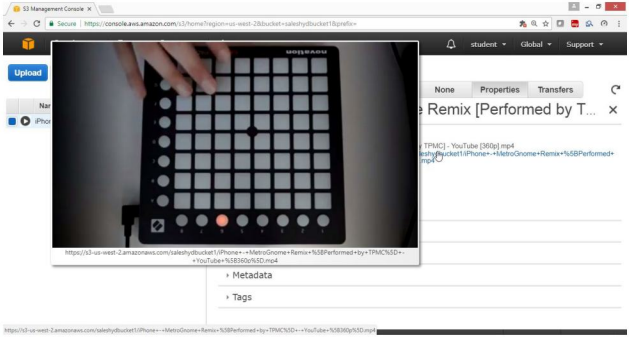
Enable the check box to **View Permission**

Enable the check box the **Edit View Permission**

Click on **Save** button



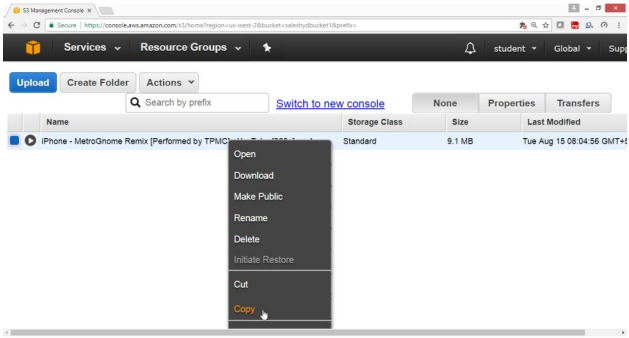
Verify file is accessible.



2) To copy or move files from one bucket to another.

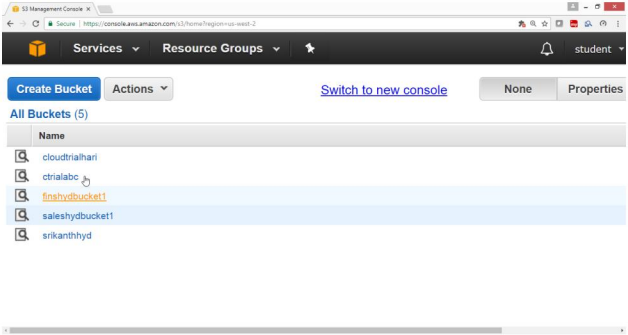
Select the file from Bucket or Folder, right click,

now select copy/cut

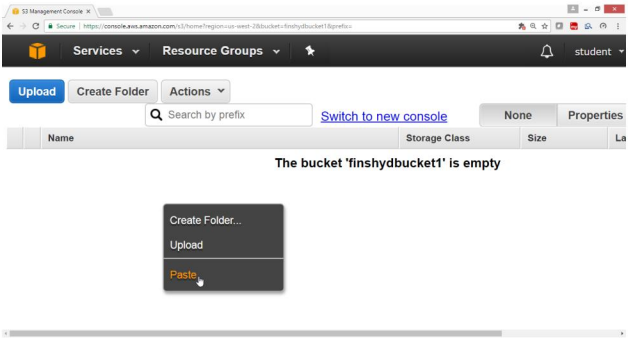


2.2 Select the Bucket or Folder, where you want to paste.

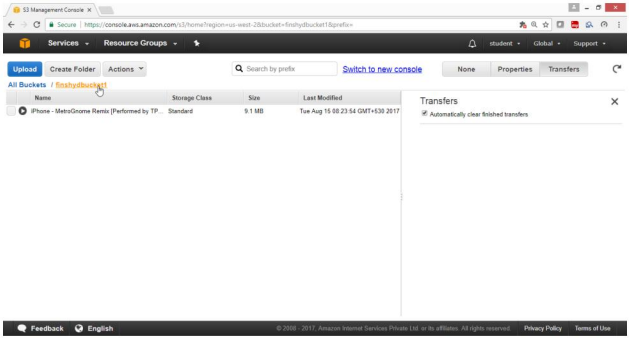
Click on the Bucket → finshydbucket1



Click on **Paste**

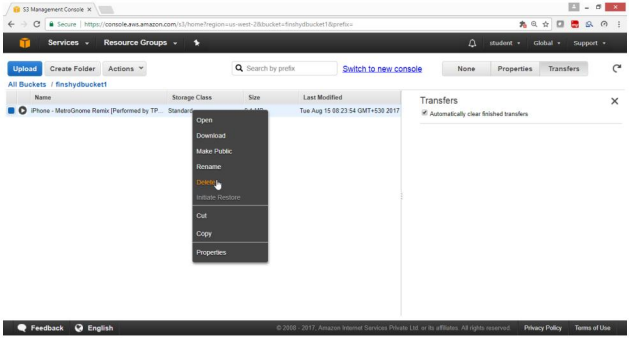


Verify that the file is copied in another bucket i.e finshydbucket1



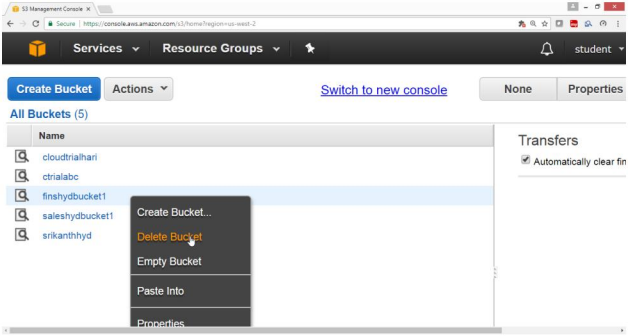
3) To **delete** a file from a bucket

Right click on it, select Delete



To Delete a bucket

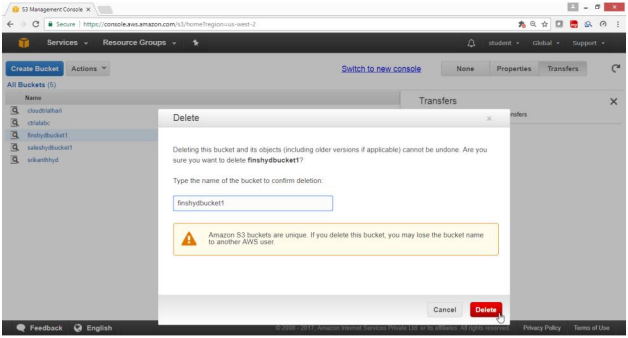
Select the bucket, right click select **Delete Bucket**



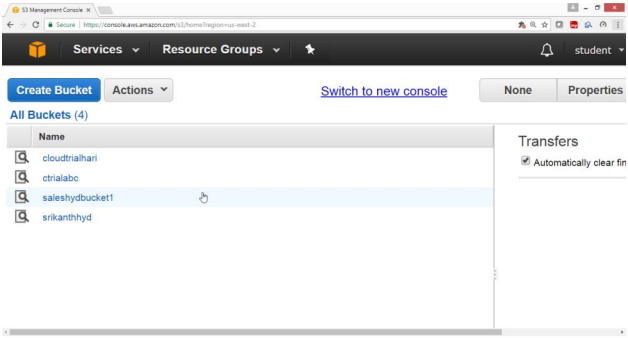
To **Delete Bucket**

Provide exact bucket name

Click on **Delete** button



Verify that the bucket **finshydbucket1** is deleted



4) To Host a Static Website using Amazon s3 Bucket

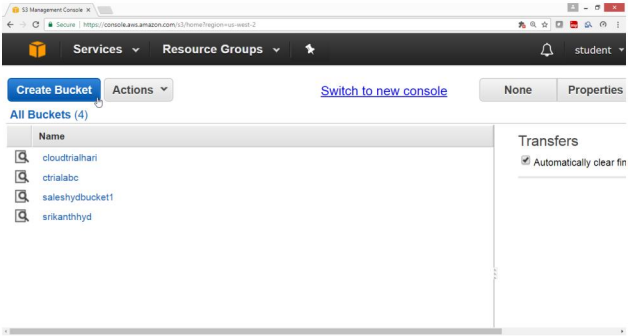
To Host a Static Website using Amazon s3 Bucket

Open AWS console

Select **Storage**

Click on **S3** service

Click on "**Create Bucket"**

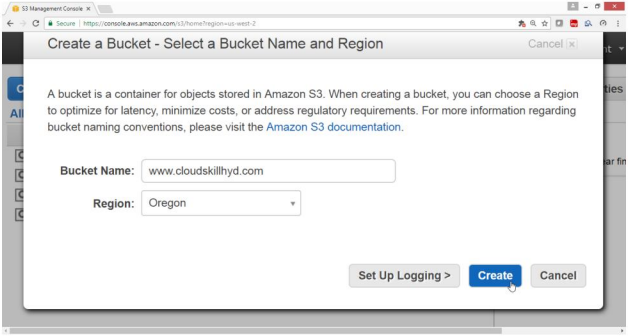


On "**Create a Bucket - Select a Bucket Name and Region"** page

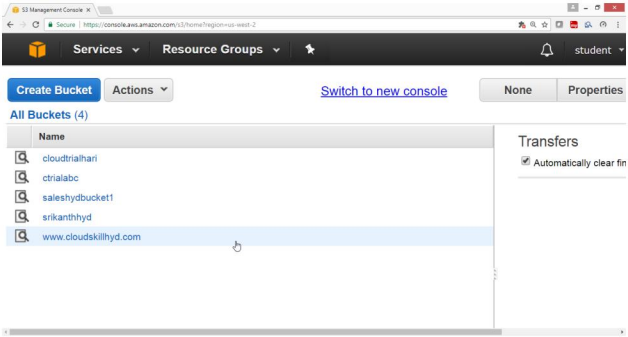
Provide following values for

Bucket Name	→	www.cloudskillhyd.com
Region	→	Oregon

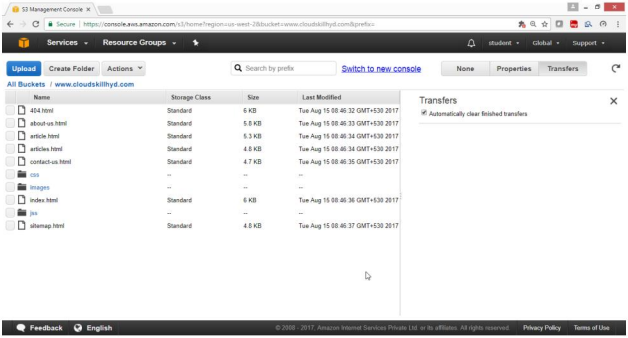
Click on **Create** button



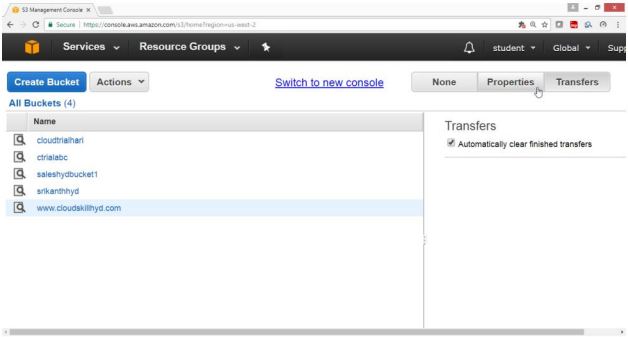
Verify Bucket got created



Upload all website contents in this bucket.



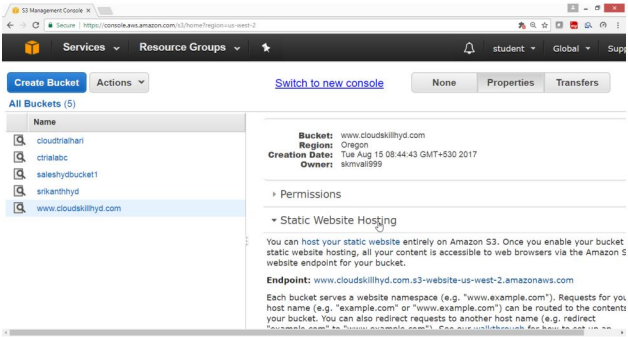
Select the bucket and click on **properties** button



On the **Properties** panel

Click **Static Website Hosting**

Drag Down



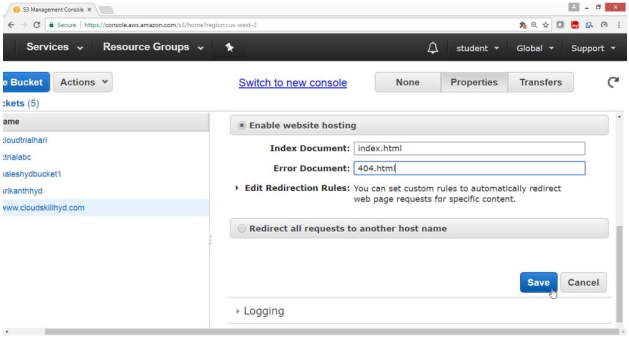
Select the **Enable website hosting**

Provide following values for

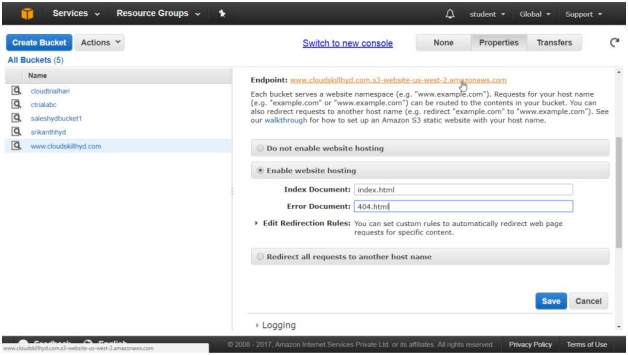
Index Document box → index.html

Error Document box → 404.html

Click on **Save** button



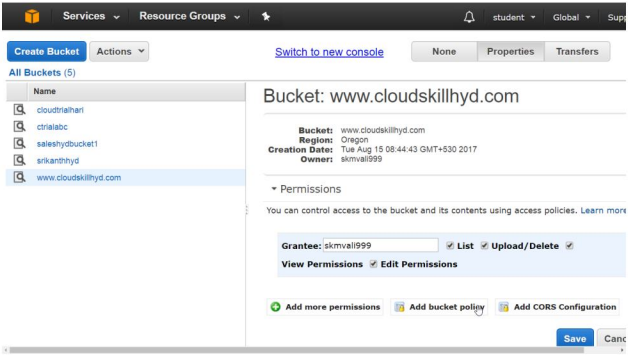
Note down the Endpoint.



2. To add a bucket policy that makes your bucket content publicly available

In the Bucket Properties, click on **Permission**

Click on **Add Bucket Policy.**



Copy the following bucket policy, and then paste it in the Bucket Policy Editor.

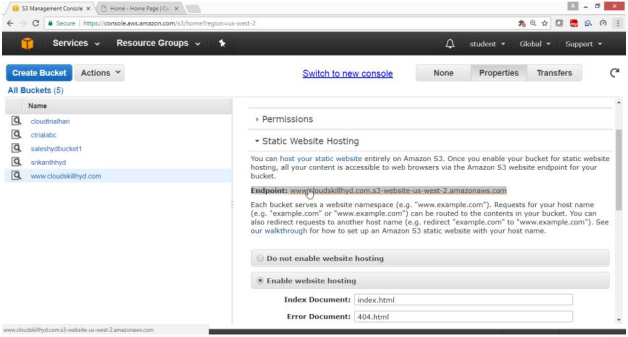
```
{
    "Version":"2012-10-17",
    "Statement":[{
          "Sid":"PublicReadForGetBucketObjects",
       "Effect":"Allow",
          "Principal": "*",
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::cloudskilllhyd.com/*"
      ]
     }
    ]
  }
```

Click on **Save** button

Verify your website

Click on Endpoint Under **Static Website Hosting**

Endpoint: www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com



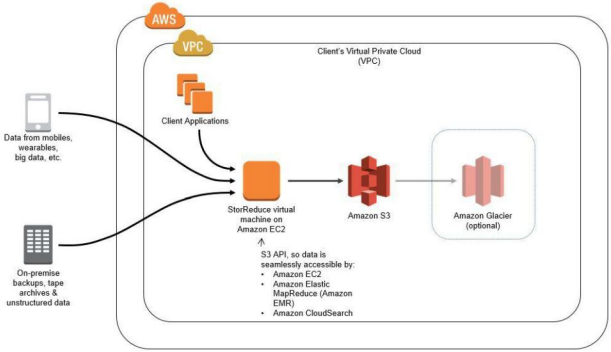
Verify the website which is coming from S3 Bucket

Lab 8: To configure Amazon Glacier

OBJECTIVE

To configure and use AWS Glacier Service.

TOPOLOGY



PRE-REQUISTES

User should have AWS account, or IAM user with AmazonGlacierFullAccess policy.

To configure Glacier with following task.

Transfer files from S3 to Glacier

Note: Amazon does not allows files to be directly loaded on Glacier

use s3 or third party tools to archive or restore.

1.Using s3 bucket & s3 lifecycle permission to archive in glacier

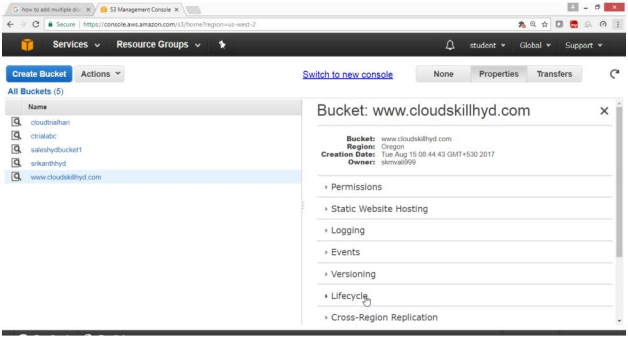
Select S3 bucket

[refer s3 topics how to create bucket and upload files]

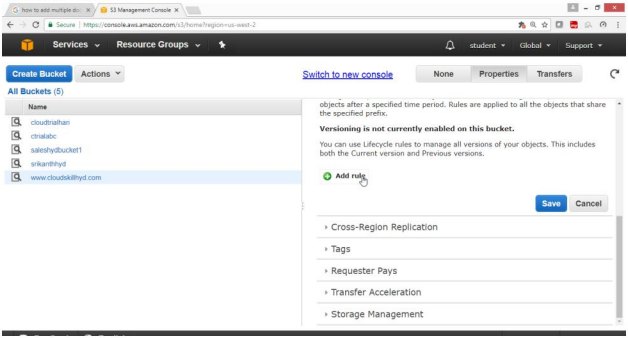
Select the bucket,

Go to properties

Click on **Lifecycle**



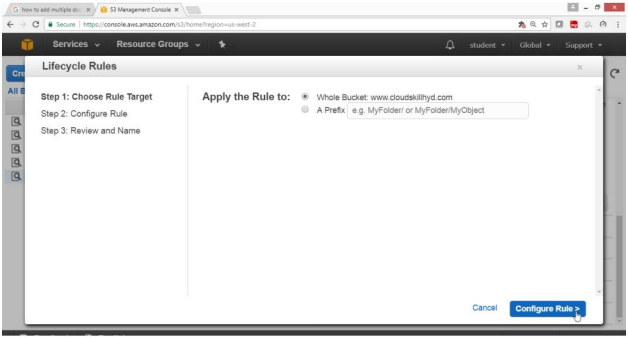
Click on **Add rule**



Under Lifecycle Rules

select **Choose Rule Target**

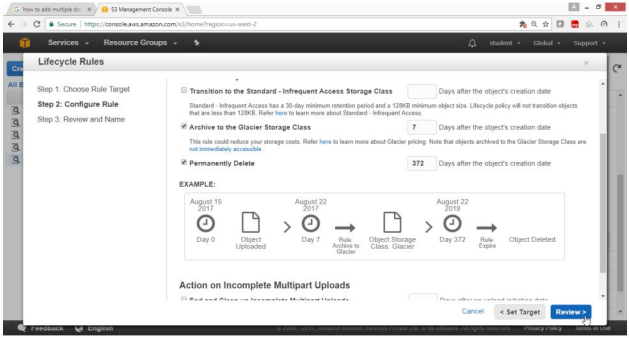
Apply the Rule to → Whole Bucket



Select check box **Archieve to the Glacier Storage Class**→ 7

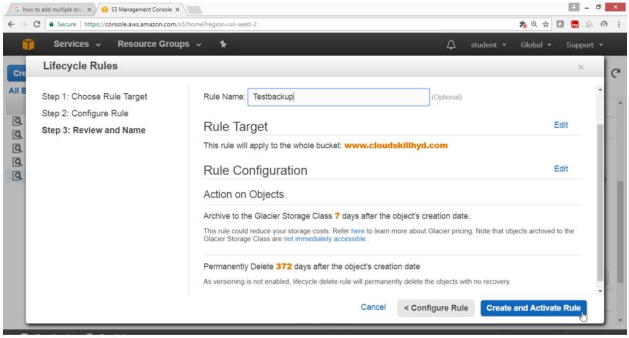
Select the check box **Permanently Delete → 372**

click on **Review**

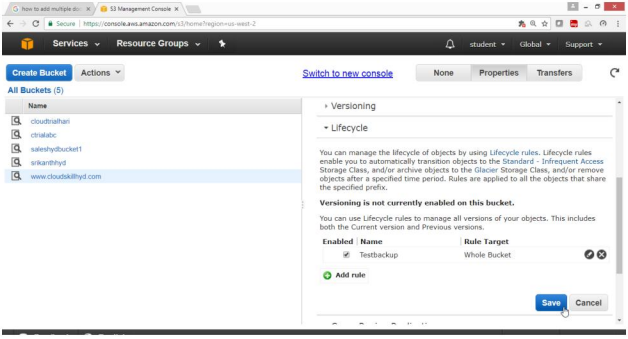


Provide Rule Name → Testbackup

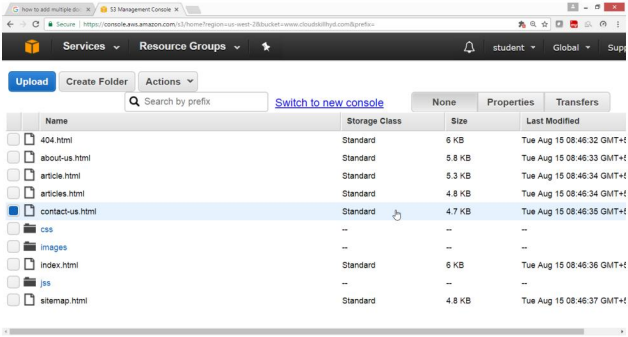
click on **"Create and Activate Rule"** button



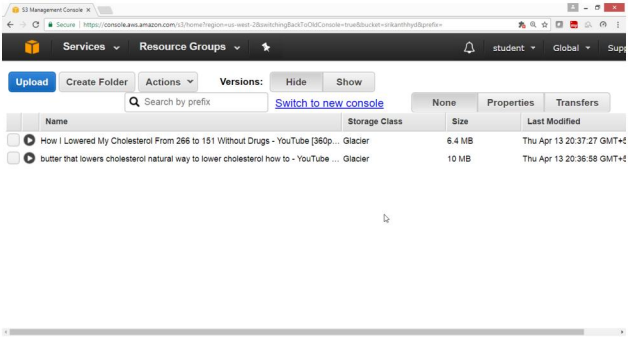
Click on **Save** button



Verify Storage Class is **Standard**

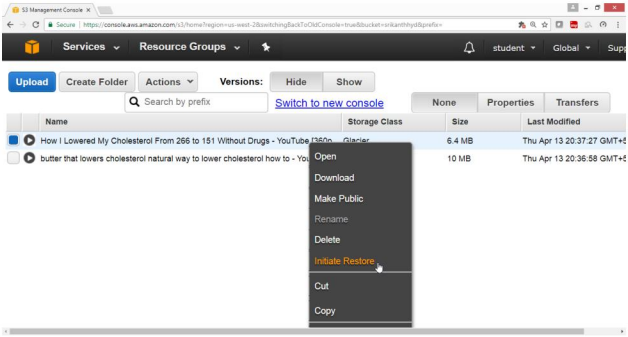


Verify Once the file goes to Glacier then Storage Class is **Glacier**



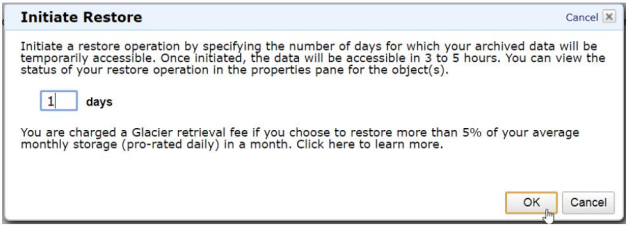
To Restore go to the bucket select the file

Right click and select **Initiate Restore**



Provide number of days → 1

Click on **OK**



Verify

File will get restored after 1 Day

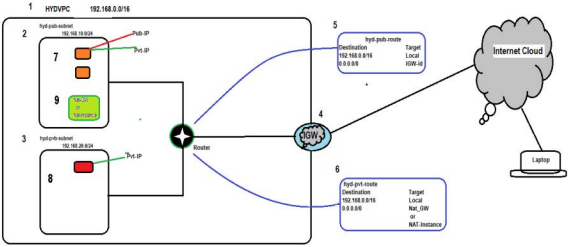
Storage class will become Standard.

Lab 9: To Configure Amazon Virtual Private Cloud (VPC)

OBJECTIVE

To configure Amazon Virtual Private Cloud with public and private subnet

TOPOLOGY



PRE-REQUISTES

User should have AWS account, or IAM user with VPCfullaccess

TASK

Create your own VPC

Create Public subnet

Create Private subnet

Create Internet Gateway

Attach Internet Gateway to your VPC

Create Public Routing Table, associate subnet and add routing rules

Create Private Routing table, associate subnet and add routing rules

Launch an instance in Public network

Launch an instance in Private network

Create Nat Gateway

Connect to public instance and check internet connectivity

Connect to private instance and check internet connectivity

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

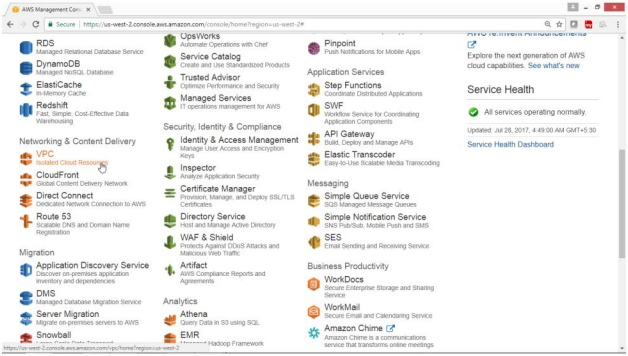
1) To create your own VPC

Open AWS console

Click on **Services**

Select **Networking and Content Delivery**

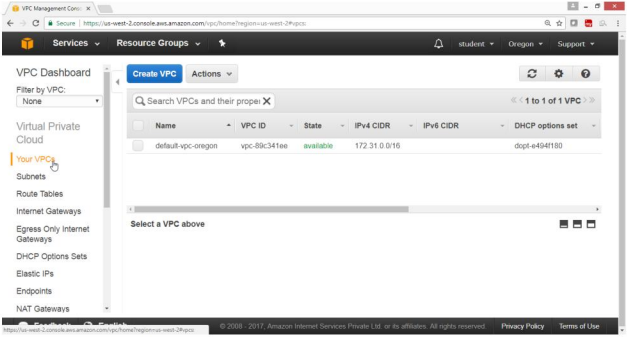
Click on **VPC**



On **VPC Dashboard** panel

Click on **Your VPC**

Click on **Create VPC** button



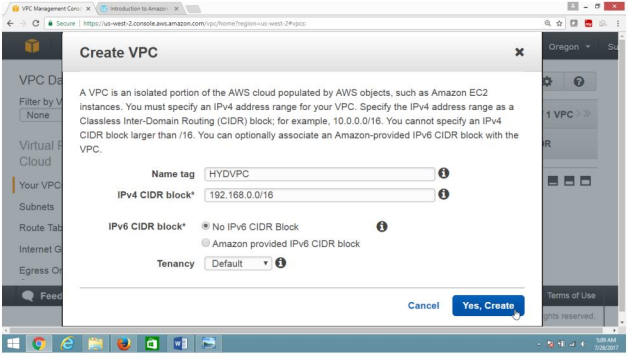
On "**Create VPC"**, page

For **Name tag→HYDVPC**

For **IPv4 CIDR block→192.168.0.0/16**

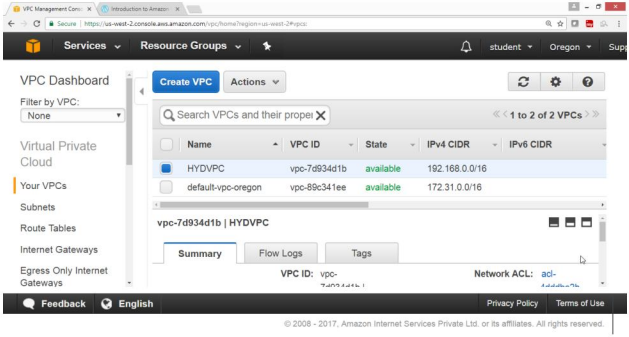
Leave remaining field as default

Click on "**Yes Create"** button



Verify

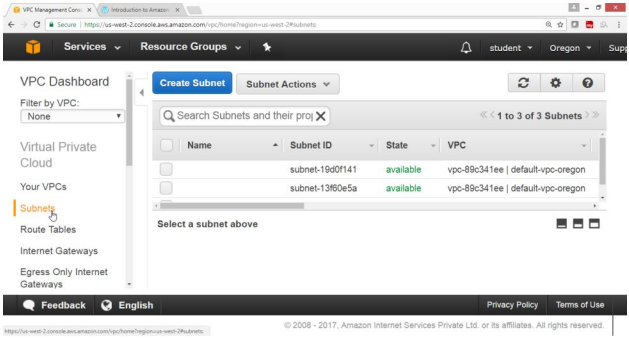
HYDVPC is created



2) To create public subnet

Click on **Subnet**

Click on **Create Subnet** button



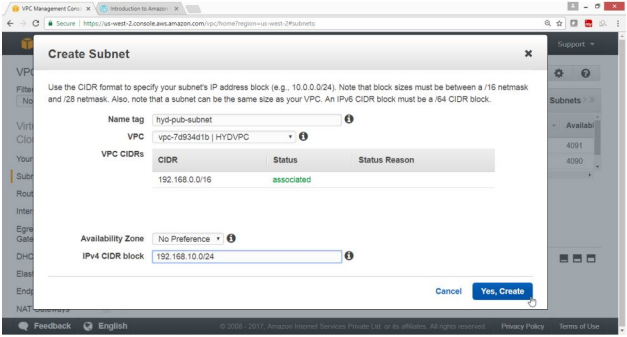
On **Create Subnet**, page

For **Name tag** → **hyd-pub-subnet**

For **VPC** → **HYDVPC**

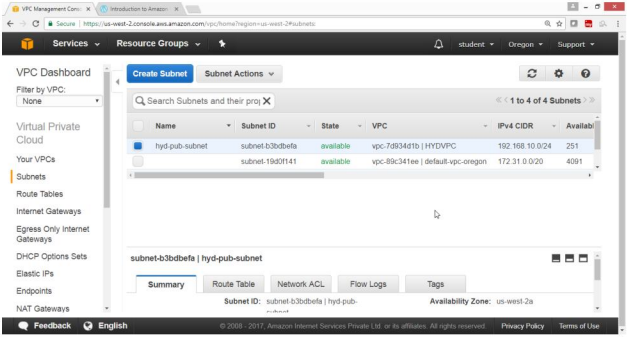
For **IPv4 CIDR block** → **192.168.10.0/24**

Click on **Yes Create** button



Verify

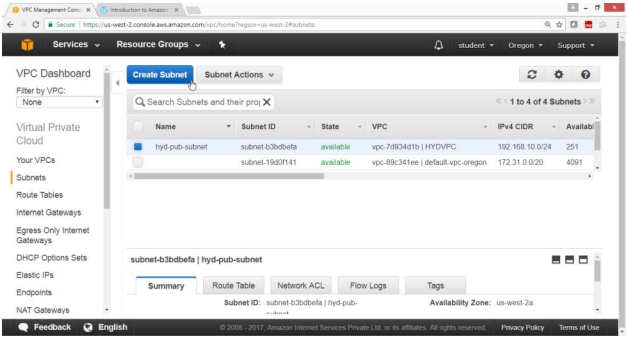
hyd-pub-subnet got created



3) To create private subnet

Click on **Subnet**

Click on **Create Subnet** button



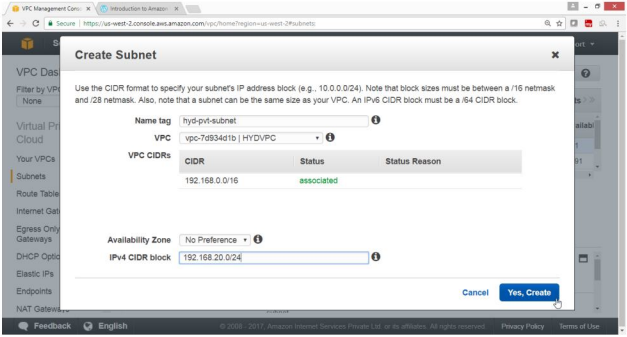
On **Create Subnet**, page

For **Name tag** → **hyd-pvt-subnet**

For **VPC** → **HYDVPC**

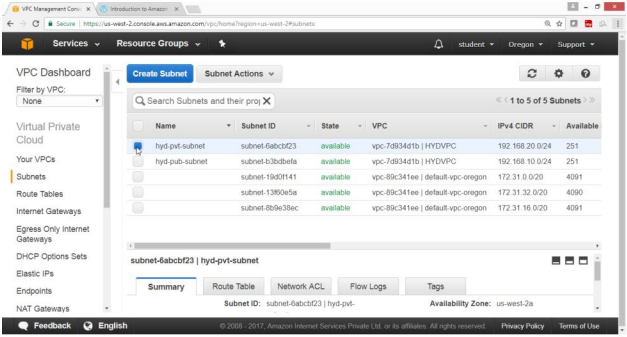
For **IPv4 CIDR block** → **192.168.20.0/24**

Click on **Yes Create** button



Verify

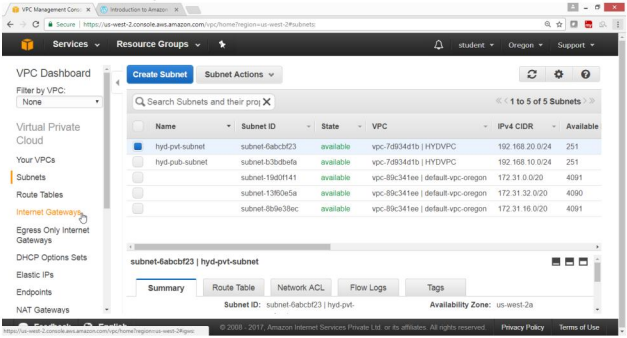
hyd-pvt-subnet got created



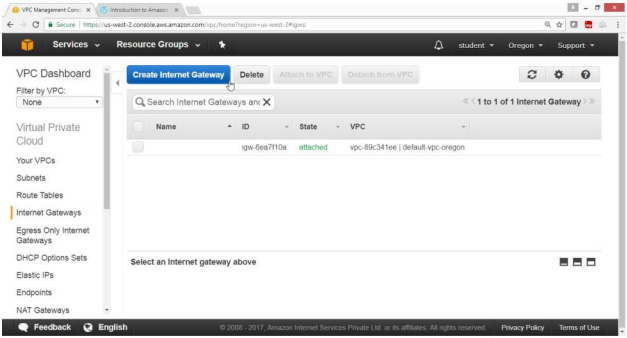
4) Create a Internet Gateway and attach to your VPC.

In VPC **Dashboard** panel

Click on **Internet Gateway**



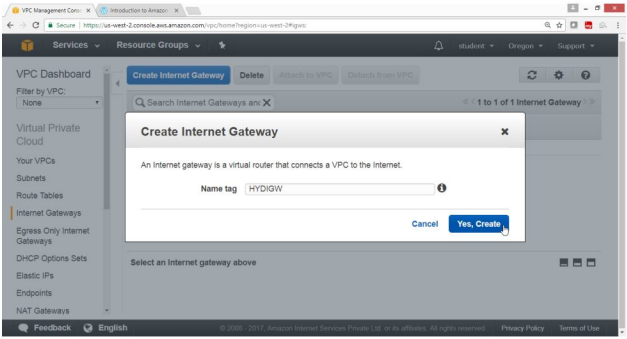
Click on **Create Internet Gateway** button



In **Create Internet Gateway**, box

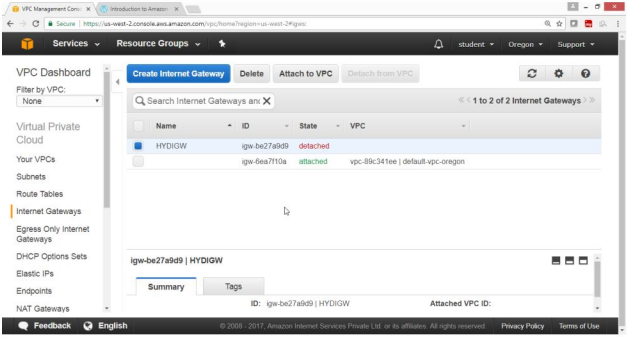
For **Name tag → HYDIGW**

Click on "**Yes, Create"** button



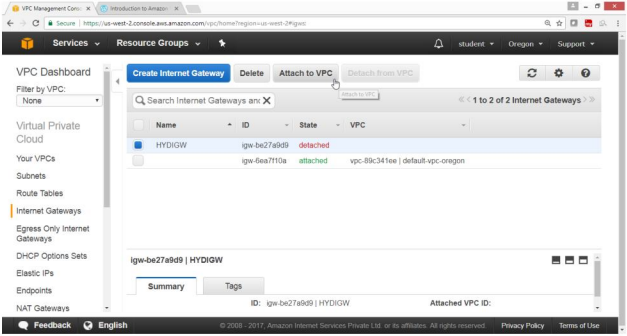
Verify

Internet gateway is created



Select HYDIGW

Click **"Attach to VPC"**



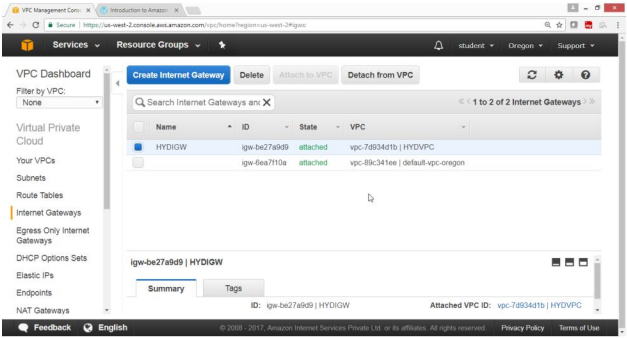
In **"Attach to VPC"** box

For VPC →**HYDVPC**

click on **"Yes, Attach"** button

Verify

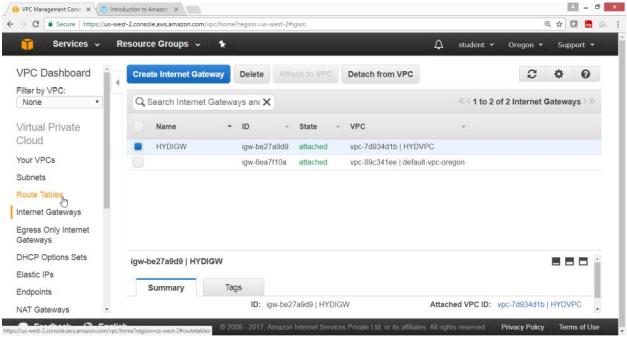
Internet gateway is connected to your VPC



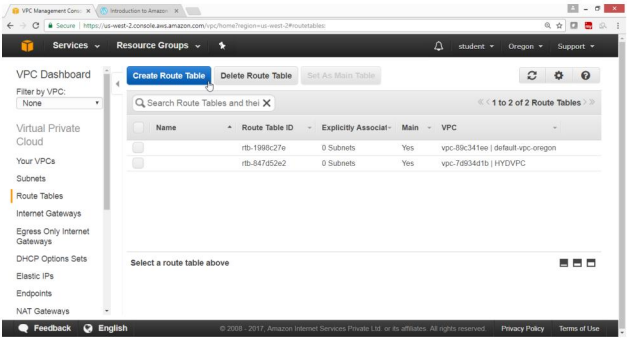
5) Create Public Routing Table, associate subnet and add routing rules

On **VPC Dashboard** panel

Click on **Route Table**



Click on **"Create Route table"** button

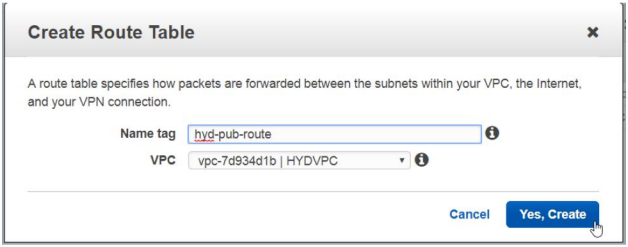


On "**Create Route Table"** box

For **Name tag**→ hyd-pub-route

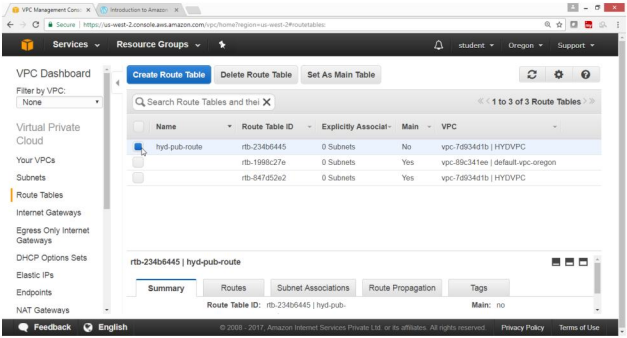
For VPC → HYDVPC

Click on "**Yes, Create"** button

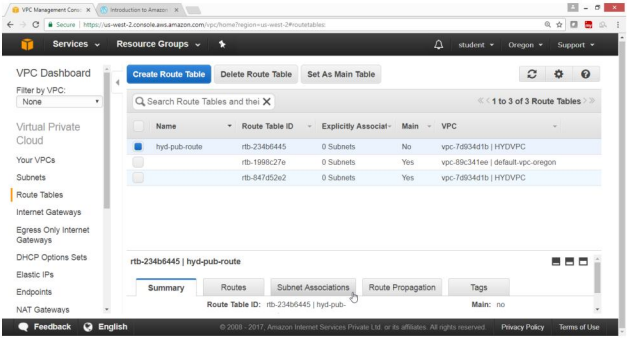


Verify

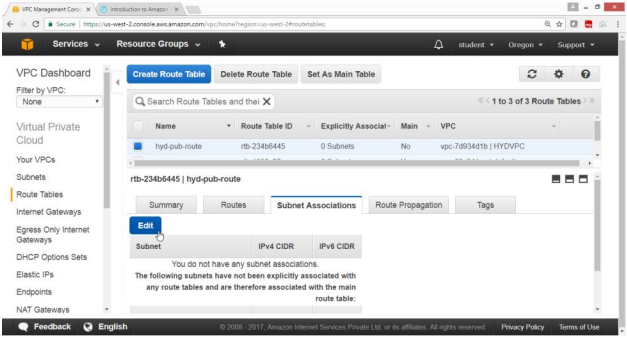
hyd-pub-route table is created



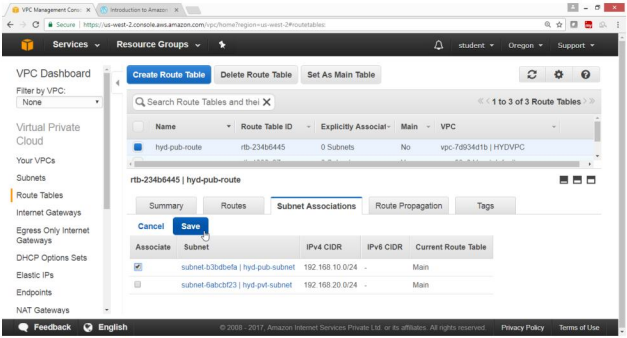
Click on **"Subnet Association"** button



Click on **Edit** button

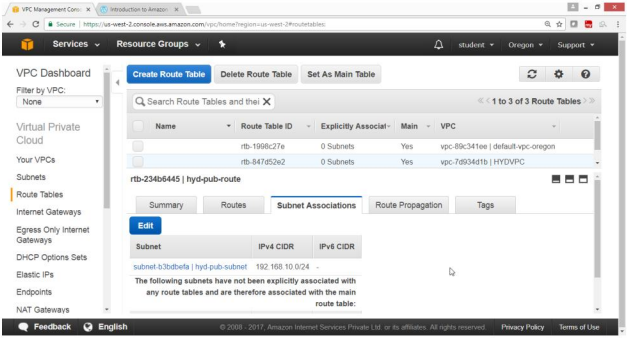


Select check box of hyd-pub-subnet → 192.168.10.0/24



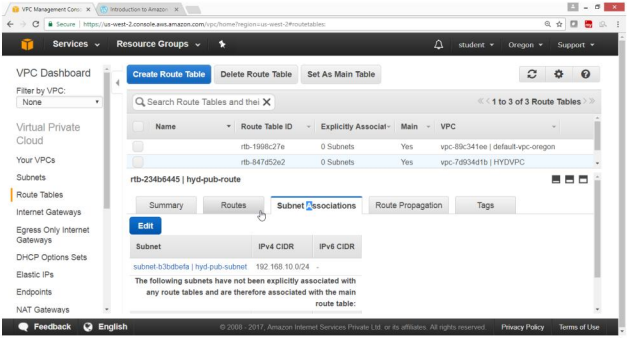
Verify

hyd-pub-subnet is associated with routing table

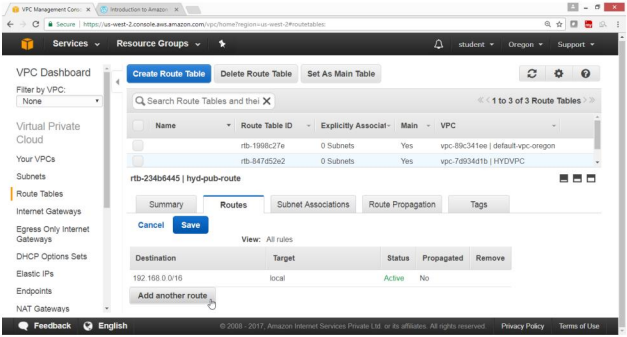


Click on **Route** Button

Click on **Edit** button



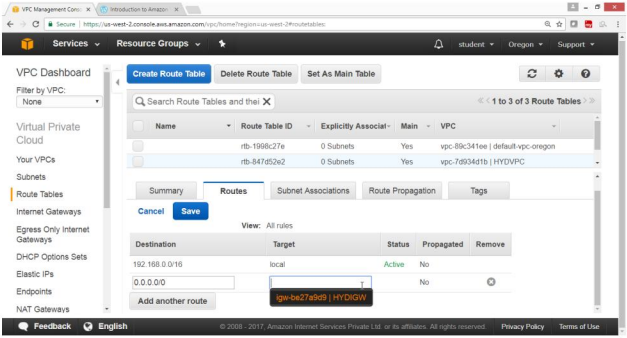
Click on **"Add another route"** button



For Destination → 0.0.0.0/0

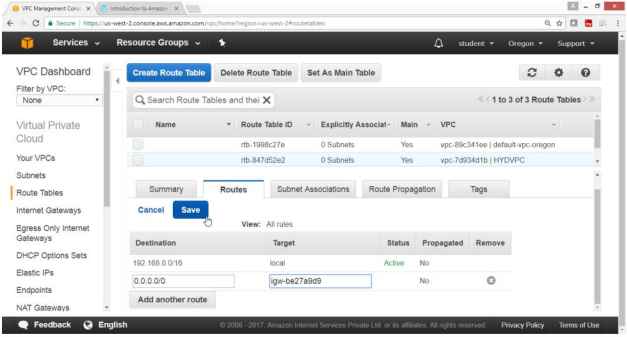
For Target → select HYDIGW

Click on **Save** button



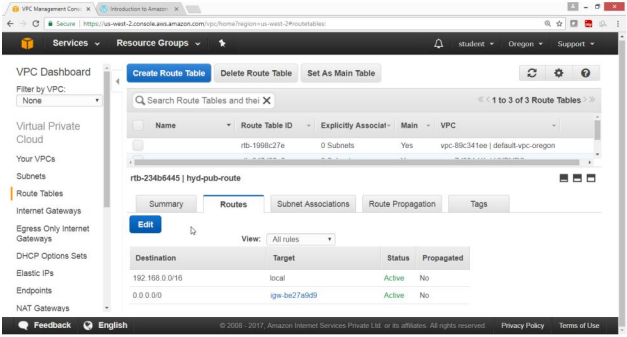
Verification

Public route is added through internet gateway



Verify

Status column show Active

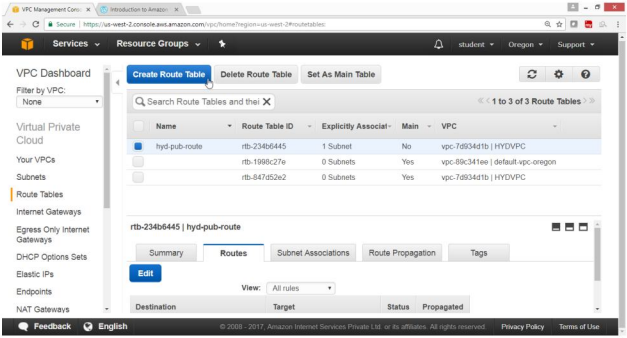


6) Create Private Routing Table, associate subnet and add routing rules

On **VPC Dashboard** panel

Select **Route Tables**

Click on **" Create Route Table"**

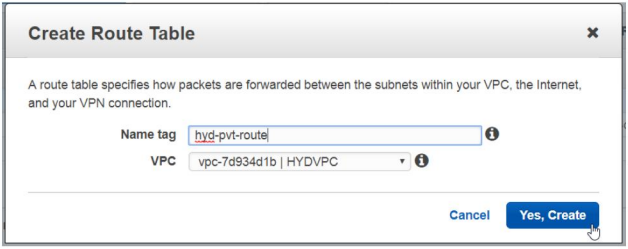


On "**Create Route Table"** box

For **Name tag**→ hyd-pvt-route

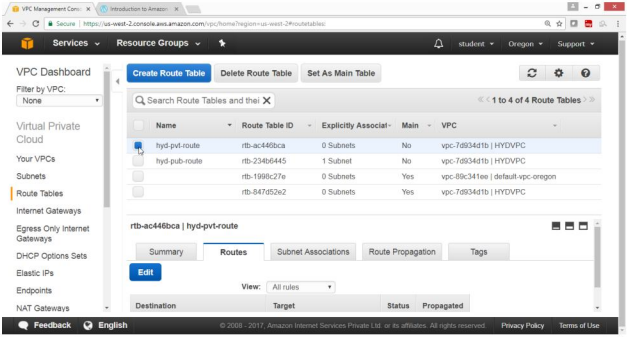
For VPC → HYDVPC

Click on "**Yes, Create"** button

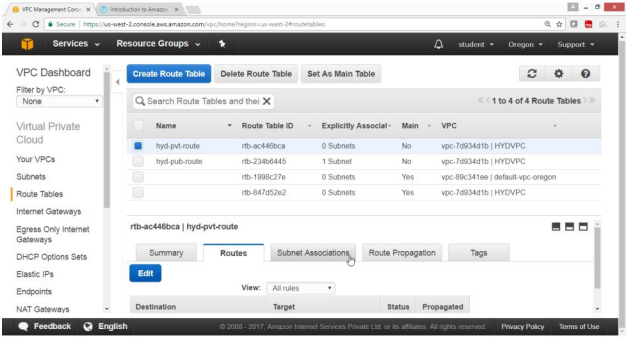


Verify

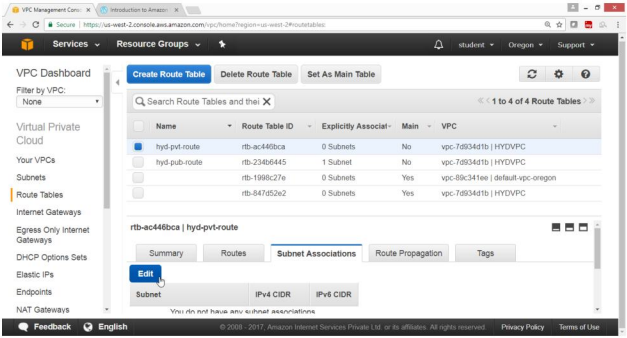
hyd-pvt-route table is create



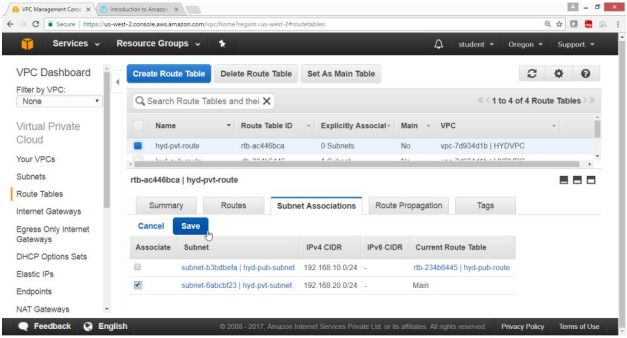
Click on **Subnet Association** button



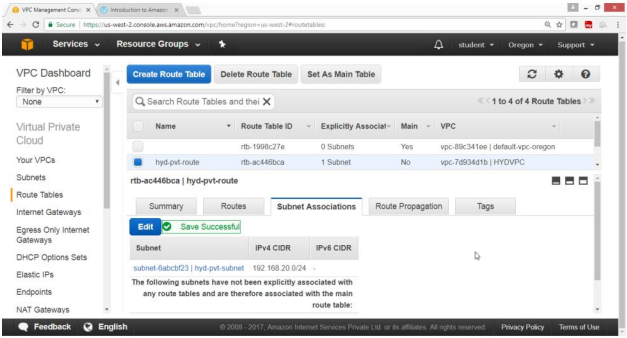
Click on **Edit** button



Select check box hyd-pvt-subnet → 192.168.20.0/24

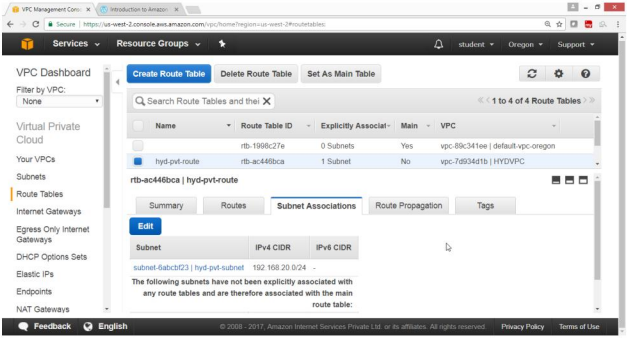


Click on **Save** button

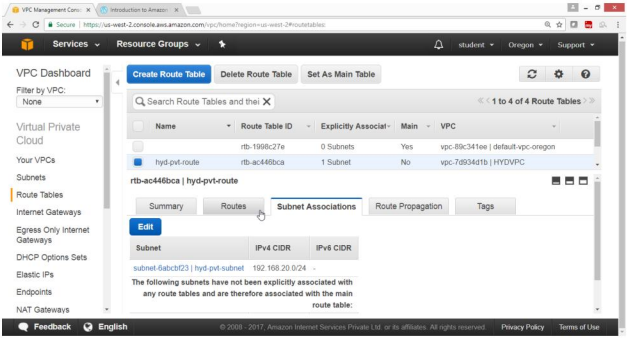


Verify

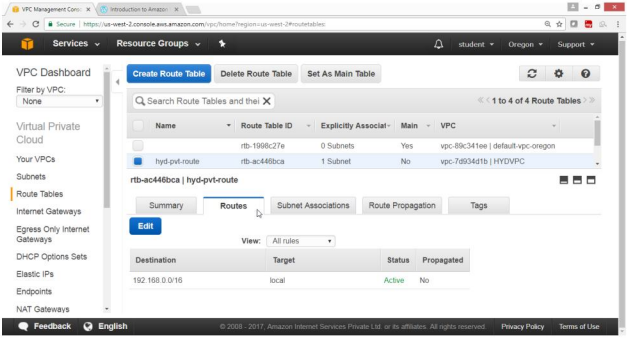
Hyd-pvt-subnet is associated with hyd-pvt-route table



Click on **Route** button



Note: No need to add IGW in pvt route

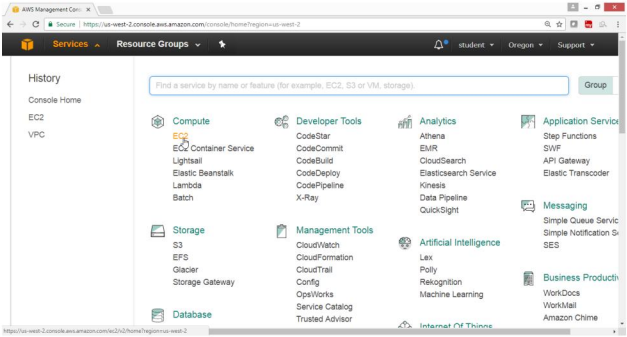


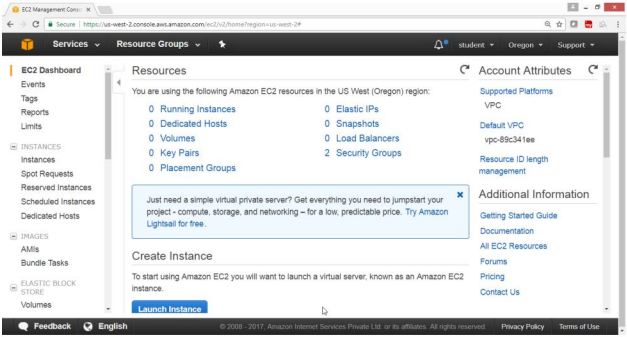
7) To launch Windows instance in Public subnet

Open the AWS console

Click on Services

Click on Ec2 services

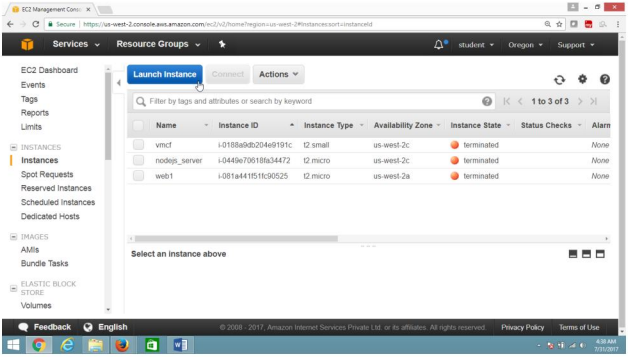




On the EC2 dashboard panel

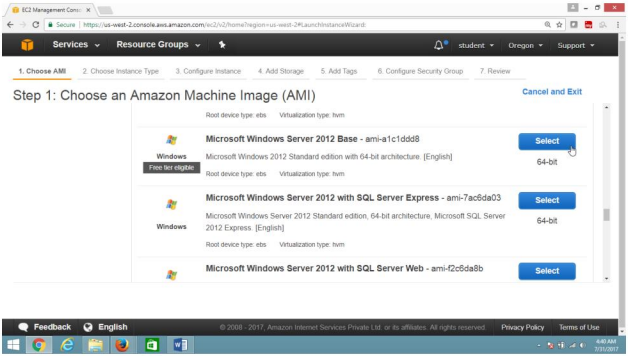
Click on **instance**

Click on **Launch instance** button



Select AMI **"Microsoft Windows Server 2012 Base** - ami-a1c1ddd8"

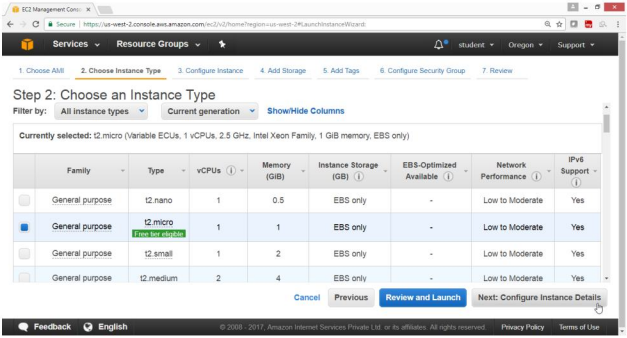
Free tier elegible



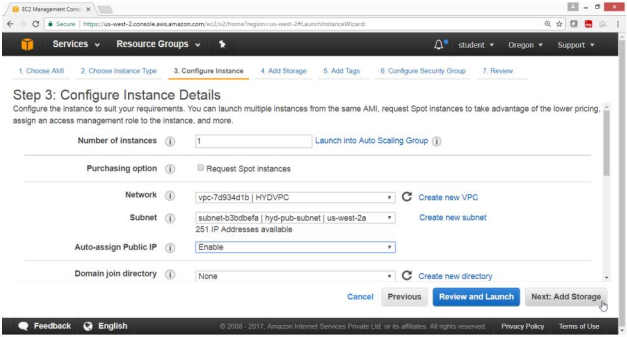
On the **"Choose an Instance Type"** page

Select "**General purposet2.micro"**

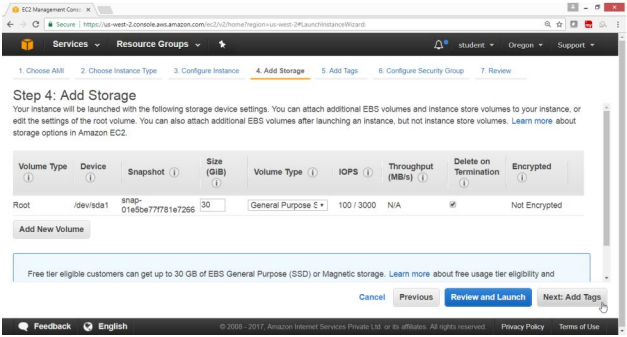
Click on **"Next Configure Instance Details"** button



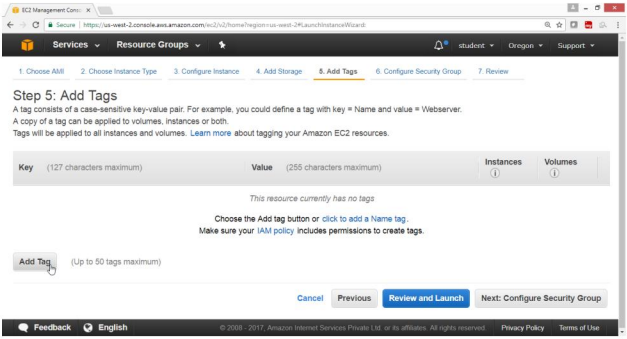
On the **"Configuration Instance Details"** page
For "Number of instances" → 1
For "Network" → HYDVPC
For "Subnet" → hyd-pub-subnet
For "Auto-assign Public IP" → Enable
Click on **"Next: Add Storage"** button



On the **"Add Storage"** page
Take default values
Click on **"Next: Add tags"** button



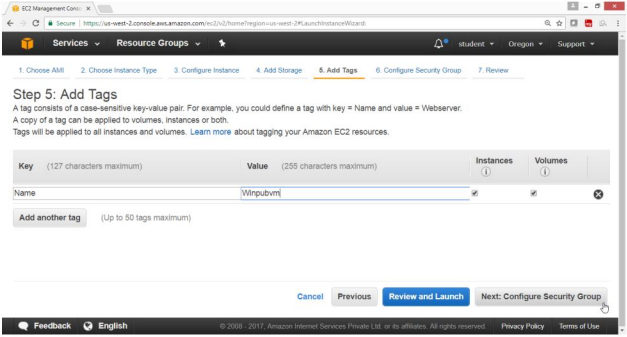
Click on **"Add tag"** button



For “Key” → Name

For Value → Winpubvm

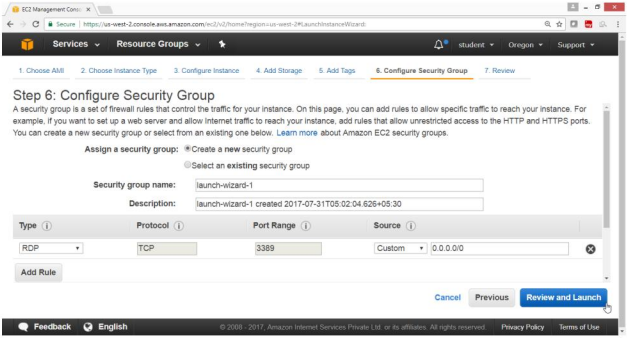
Click on **“Next: Configure Security Group”**



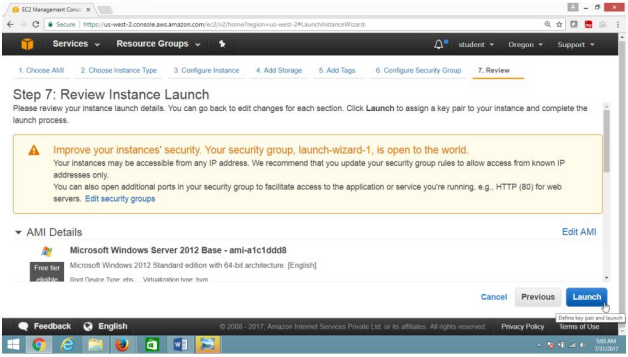
On the “Configure Security Group” page

Take Default Values

Click on **“Review and Launch”** button



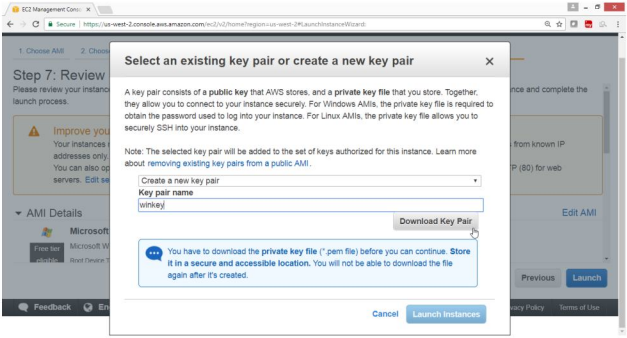
Click on **“Launch”** button



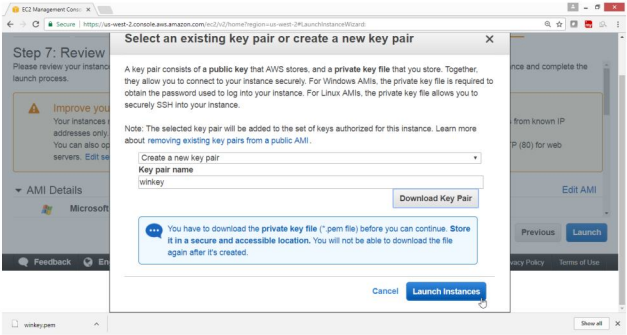
Select **"Create a new key pair"**

For **"Key pair name" → winkey**

Click on **"Download Key Pair"** button

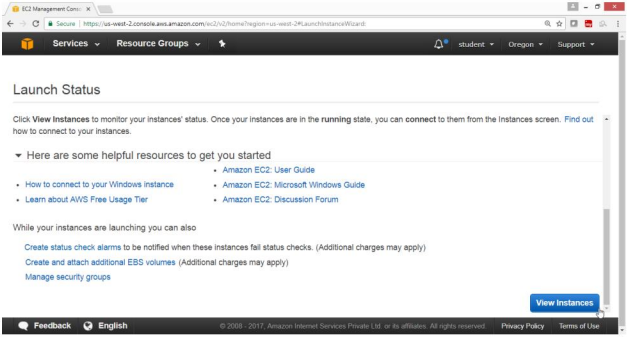


Click on **"Launch Instance"** button

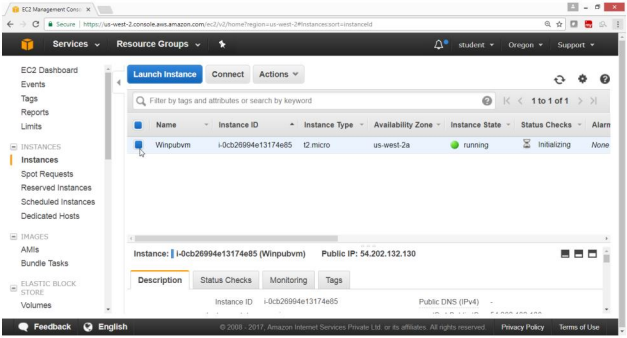


Check summary, Drag down

Click on **"View Instance"** button



Verify that instance is Running

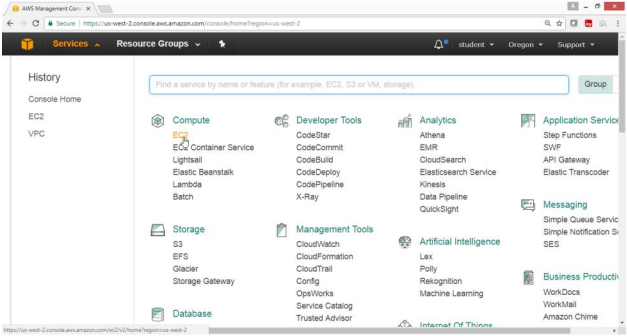


8) To Launch Windows instance in Private Subnet under HYDVPC VPC

Open the AWS console

Click on Services

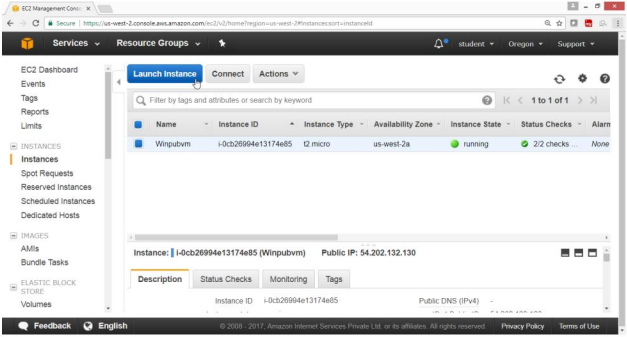
Click on **Ec2** services



On the **EC2 Dashboard** panel

Click on **Instance**

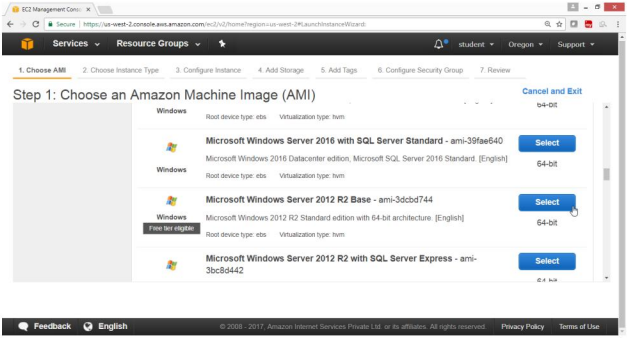
Click on "**Launch instance"** button



On the **"Choose an Amazon Machine Image (AMI) "** page

Select AMI **"Microsoft Windows Server 2012 R2 Base** - ami-a1c1ddd8"

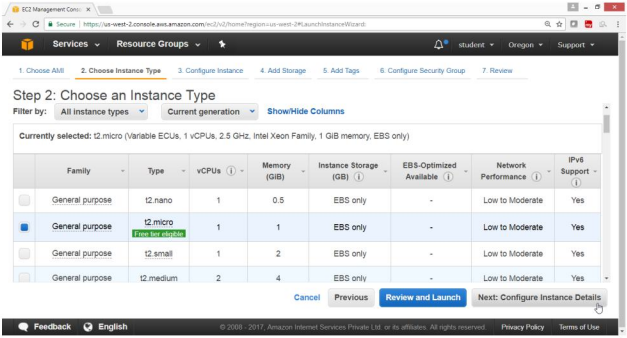
Free tier elegible



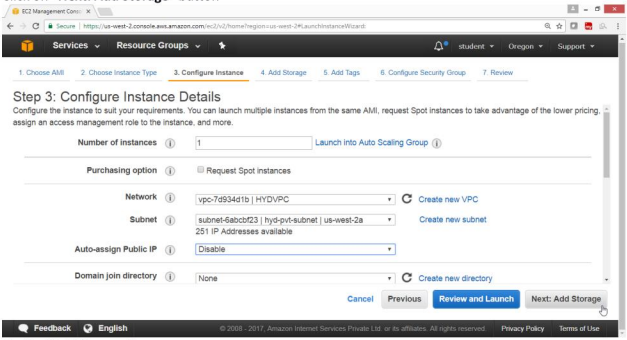
On the **"Choose an Instance Type"** page

Select "**General purposet2.micro"**

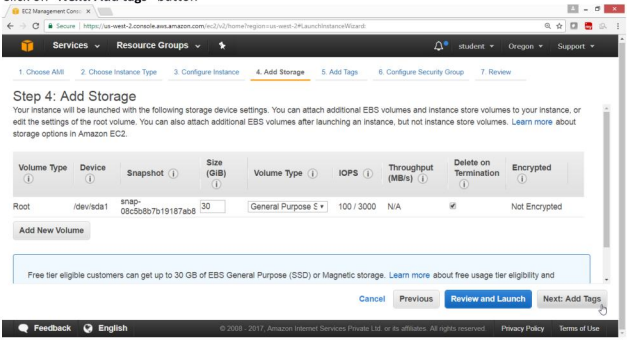
Click on **"Next Configure Instance Details"** button



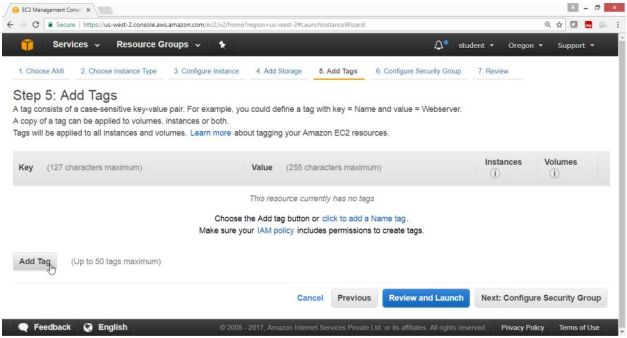
On the **"Configuration Instance Details"** page
For "Number of instances" → 1
For "Network" → HYDVPC
For "Subnet" → hyd-pvt-subnet
For "Auto-assign Public IP" → Disabled
Click on **"Next: Add Storage"** button



On the **"Add Storage"** page
Take default values
Click on **"Next: Add tags"** button



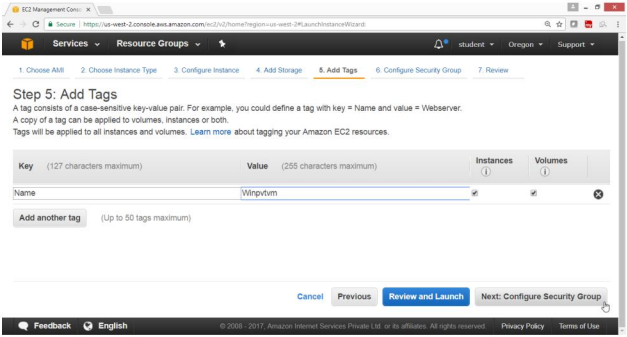
Click on **"Add tag"** button



For "Key" → Name

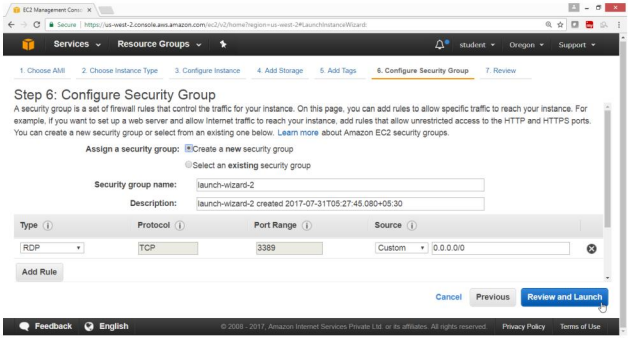
For Value → Winpvtvm

Click on **"Next: Configure Security Group"** button



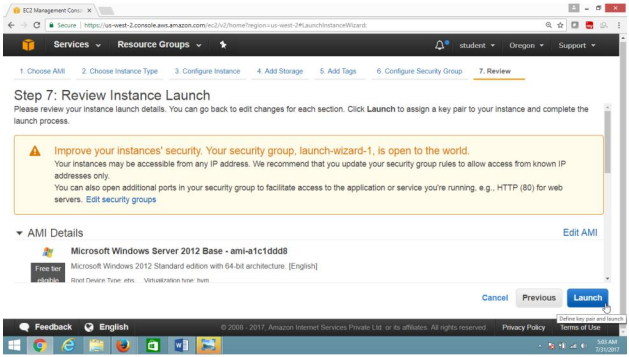
Take Default Values

Click on **"Review and Launch"** button



Drag down

Click on **"Launch"** button

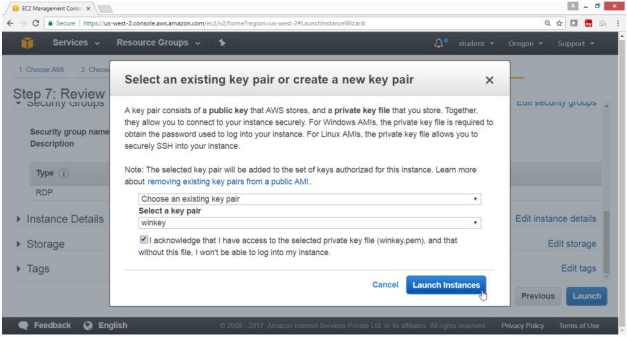


Select **"Choose an existing key pair"**

For **"Key pair name" → winkey**

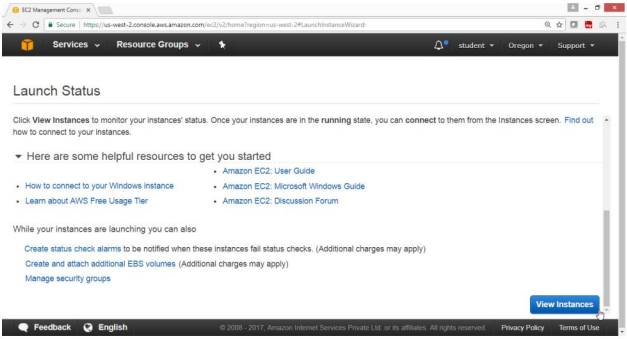
Select I acknowledge check box

Click on **"Launch Instance"** button

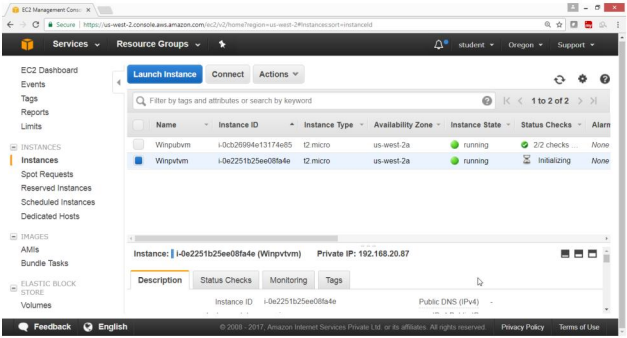


Check summary, Drag down

Click on **"View Instance"** button

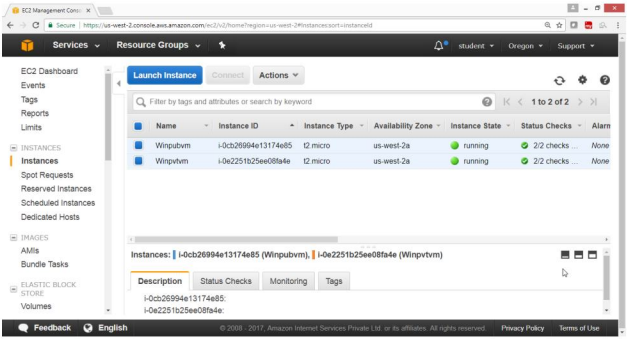


Verify that instance is Running

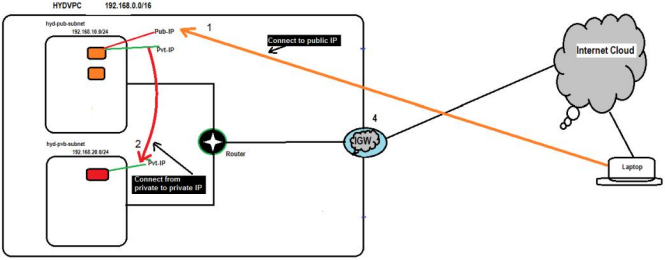


Verification

Output shows that both instances in public & private subnet are running.

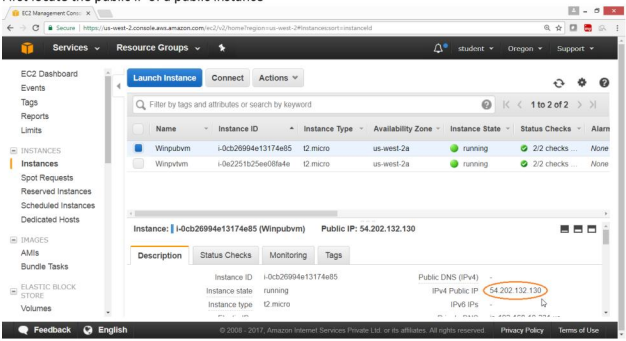


Now to connect an instance in private subnet first connect an instance in public network then from there connect to an instance in private subnet as shown in diagram

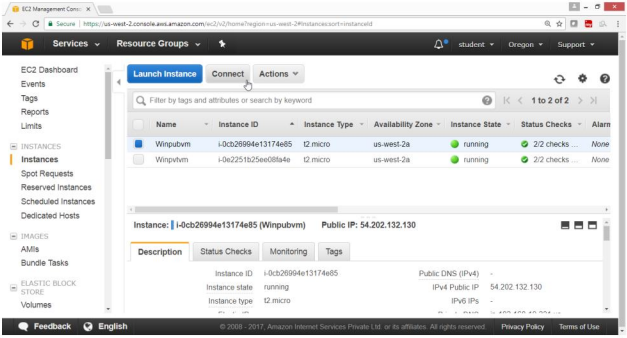


9) To Connect to Public subnet instance

First locate the public IP of a public instance

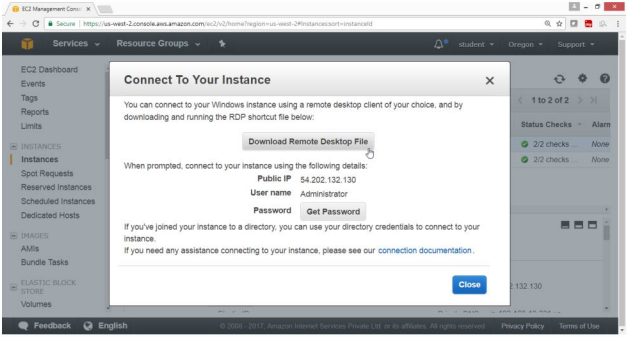


Click on **"Connect"** button



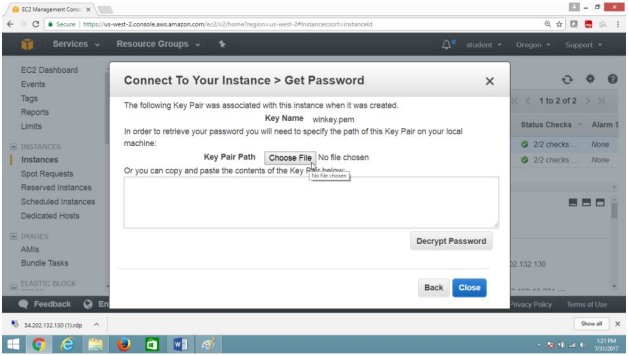
Click on **"Download Remote Desktop file"**

Click on **"Get Password"**



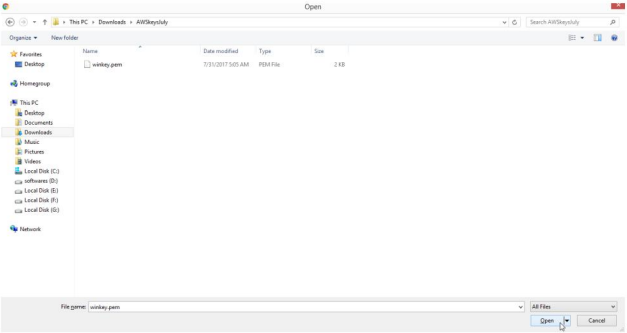
Provide the path of key file

Click on **Choose file** button

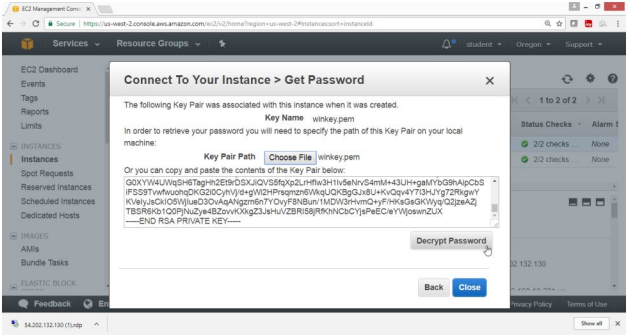


Select the key file

Click on **Open** button



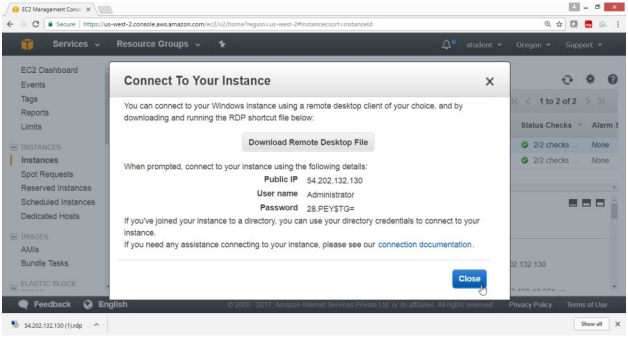
Now click on **"Decrypt Password"** button



Verification

Password is generated copy in notepad

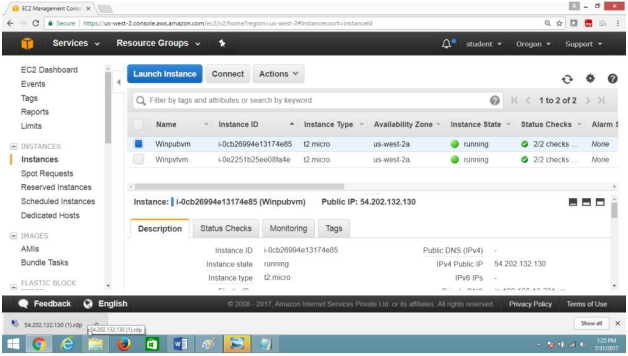
Click on **Close** button



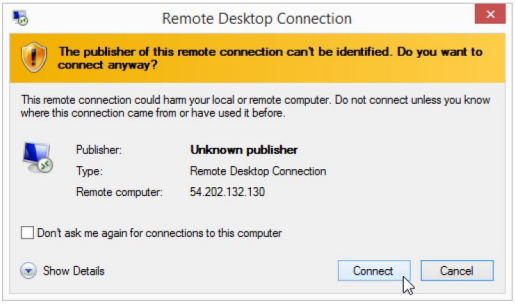
Double Click on RDP file

Provide Windows Username → Administrator

Password → "28.PEY$TG=" , as shown above

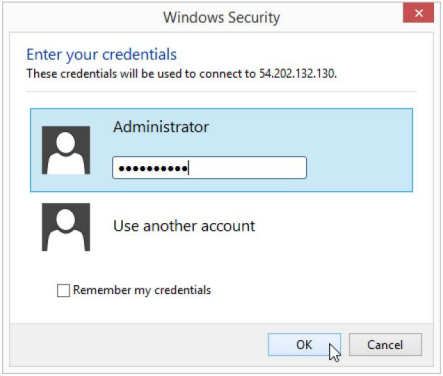


Click on **"Connect"** button

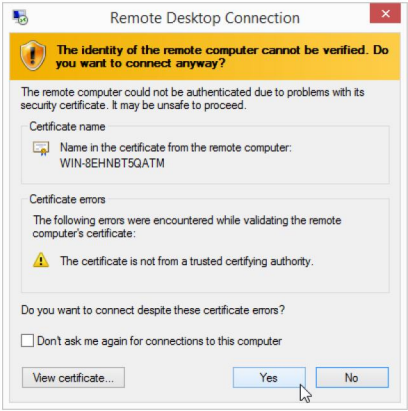


Paste the password

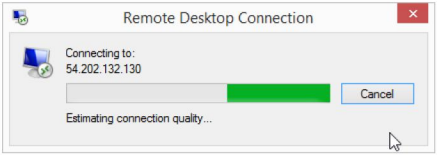
Click on **OK** button



Click on **Yes** button



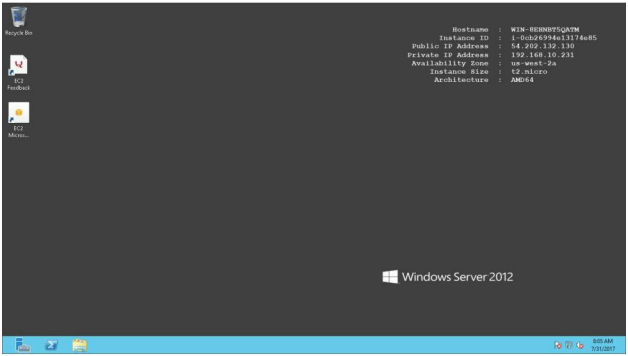
Verify



Verification

Now you are connected to Windows Public instance

On Windows Desktop public and private both IP's are displayed

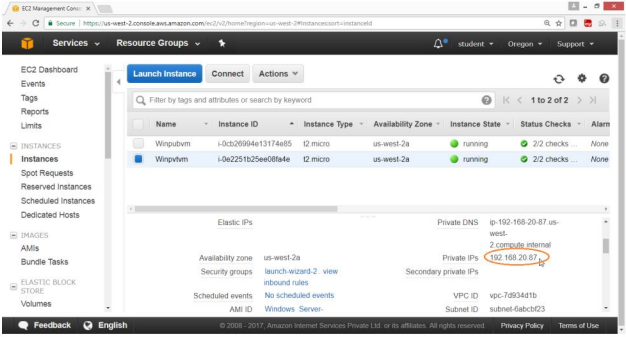


10) To Connect to Private subnet instance

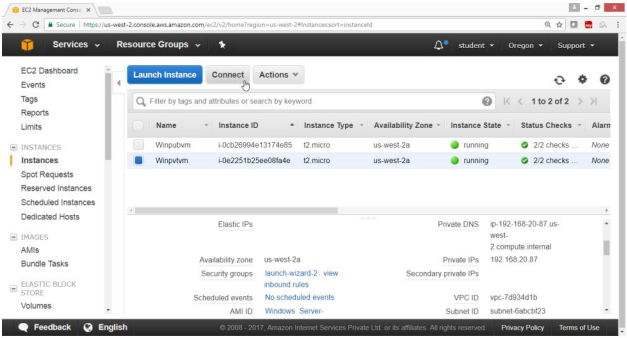
Go to Ec2 Dashboard

Select private instance

Get the private IP of the instance

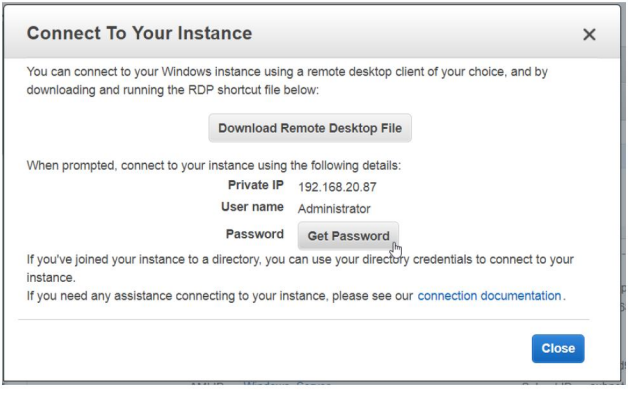


Click on **Connect** button

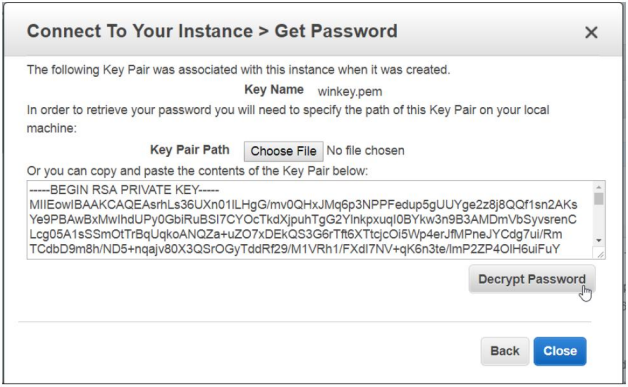


To get the password

Click on **"Get Password" button**

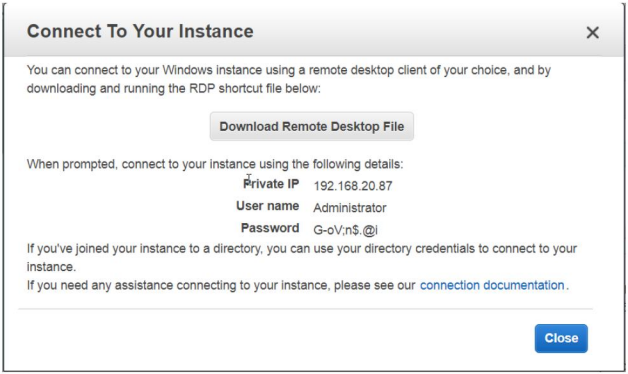


Click on **"Decrypt Password"**



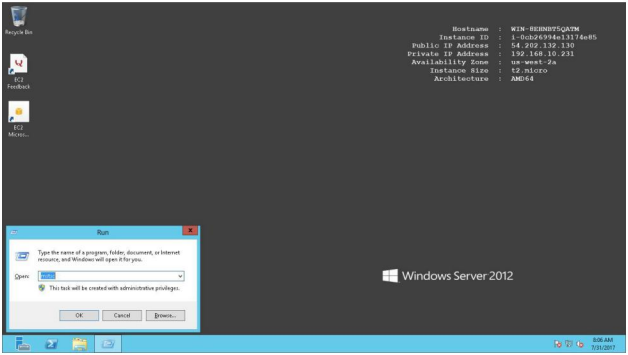
Verify

IP and password of private subnet instance is provided



Now logging to public instance

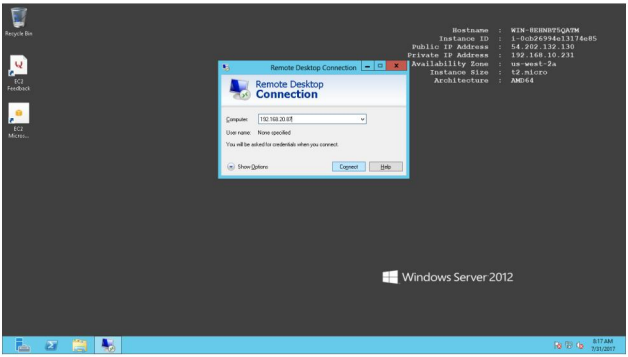
Open Run and type mstsc to connect to window private instance



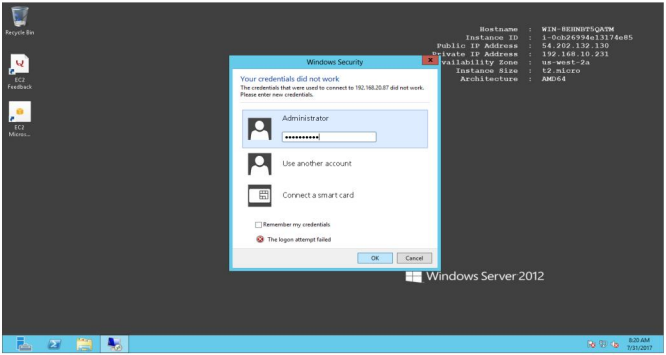
Provide private instance

Private IP →192.168.20.87
Username → Adminsitrator

Password →G-oV;n$.@i



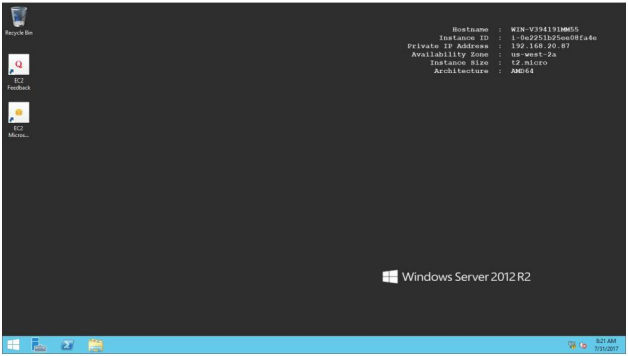
Now Provide Username & password



Verification

Check private IP at Right top corner

Now you are connected to windows private instance.



11) To connect to linux instance in private subnet

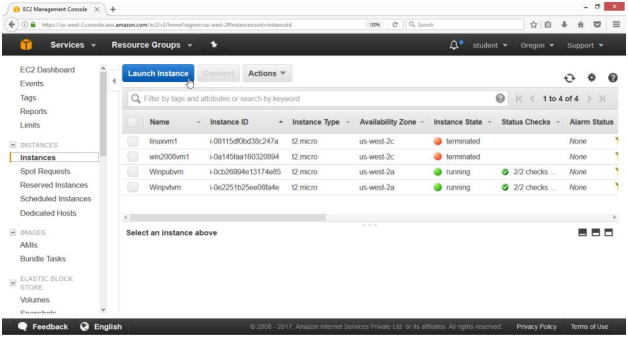
Launch linux instance in public subnet → hyd-pub-subnet

Open the AWS console

Click on Services

Click on Instance

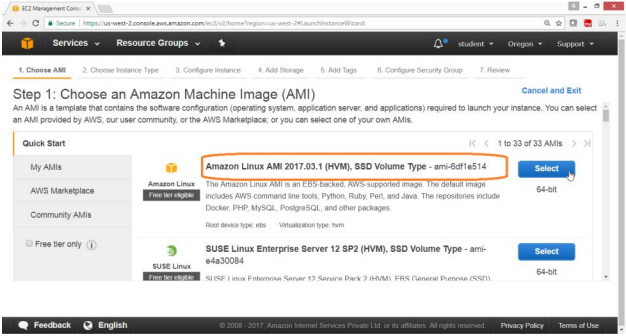
Click on **"Launch Instance"** button



On the **"Choose an Amazon Machine Image (AMI)"** page

Select AMI **"Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type** - ami-6df1e514

Click on **Select** button

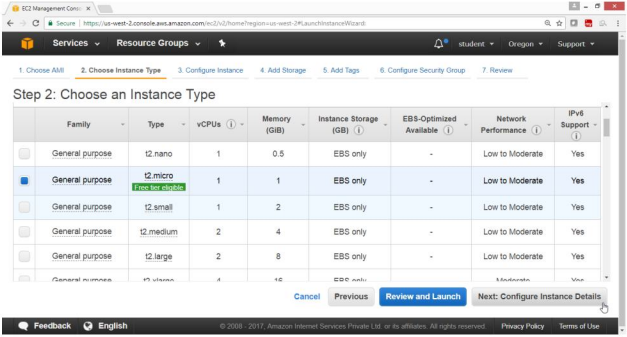


On the **"Choose an Instace Type"** page

Select **"General purpose"**

Type →**t2.micro**

Click on **"Next: Configure Instance Details"**



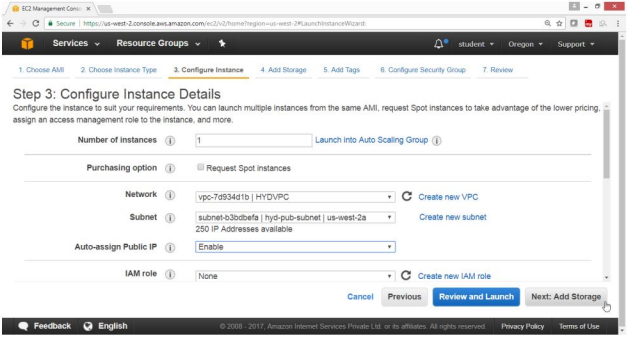
On the **"Configure Instance Details" page**

Number of instance → 1

Network → HYDVPC

Subnet → hyd-pub-subnet

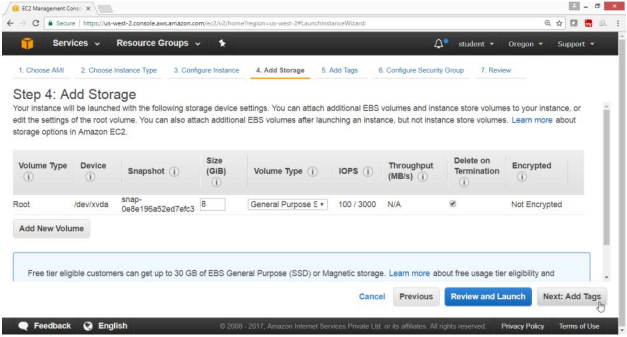
Auto-assign Public IP → Enable



On the **"Add Storage"** page

Leave the values as default

Click on **"Next: Add Tags"** button

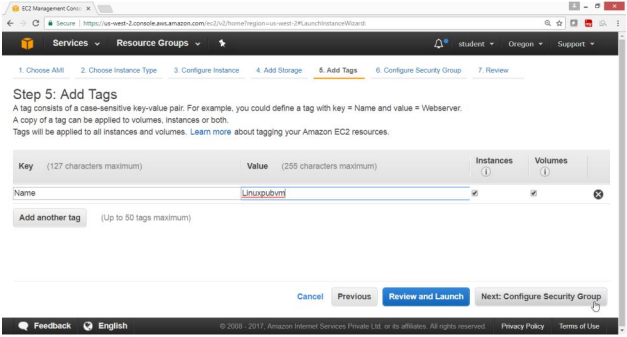


On the **"Add Tags"** page

Key → Name

Value → Linuxpubvm

Click on **"Next: Configure Security Group"** button

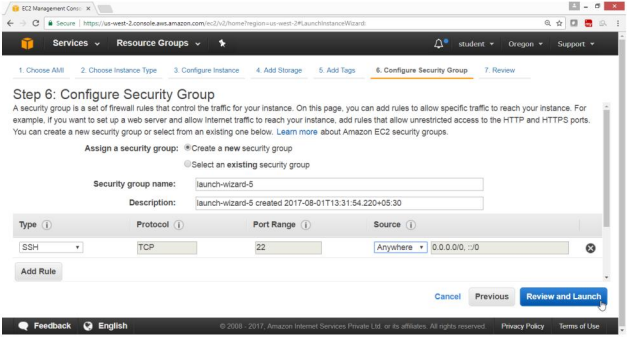


On the **"Configure Security Group"** page

Assign a security group → Create a new security group

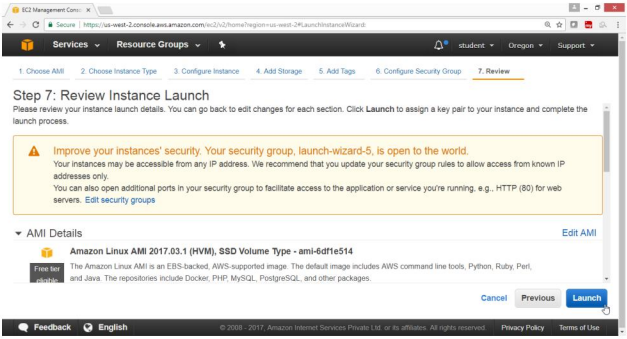
Leave remaining values as default

Click on **Review and Launch** button



On the **"Review Instance Launch"** page

Click on **Launch** button

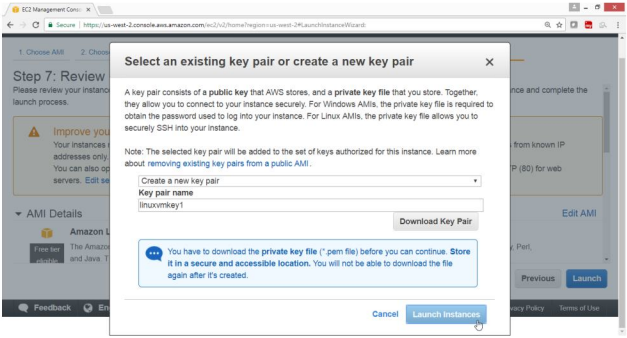


On the “Select an existing key pair or create a new key pair” page

Select **Create a new key pair**

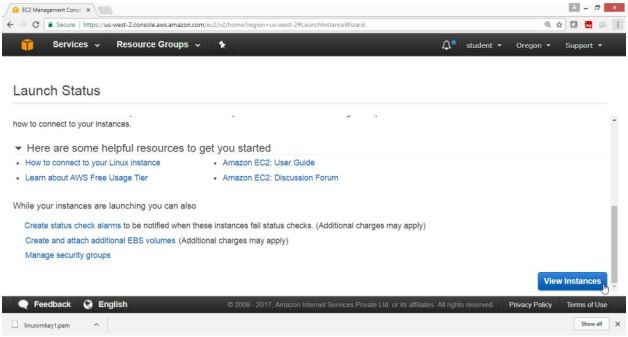
Key pair name → linuxvmkey1

Click on **“Launch Instance”** button



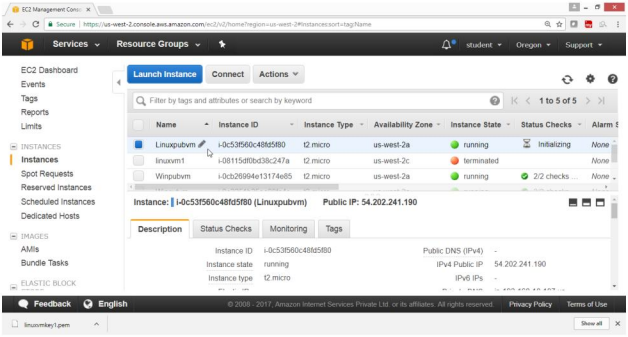
Check the summary

Click on **View Instance** button



Verification

Linux instance in public subnet is launched



12) To connect to linux instance in private subnet

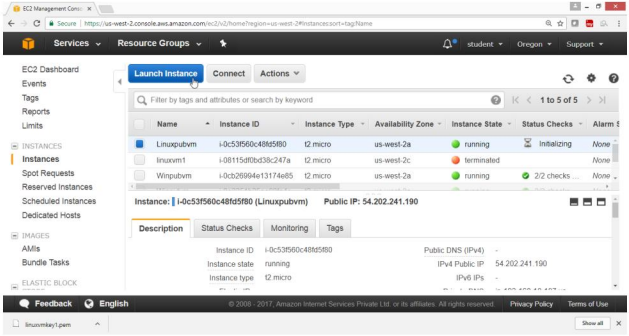
Launch linux instance in private subnet → hyd-pvt-subnet

Open the AWS console

Click on Services

Click on Instance

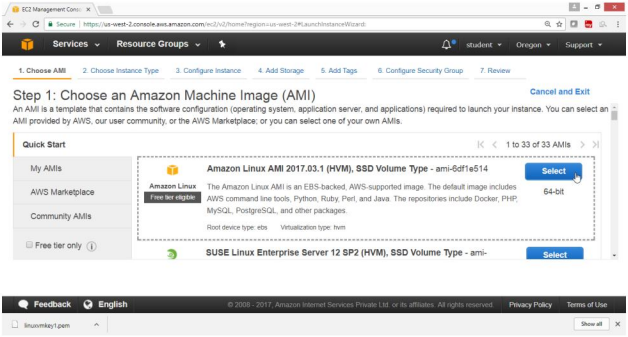
Click on **"Launch Instance"** button



On the **"Choose an Amazon Machine Image (AMI)"** page

Select AMI **"Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type** - ami-6df1e514

Click on **Select** button

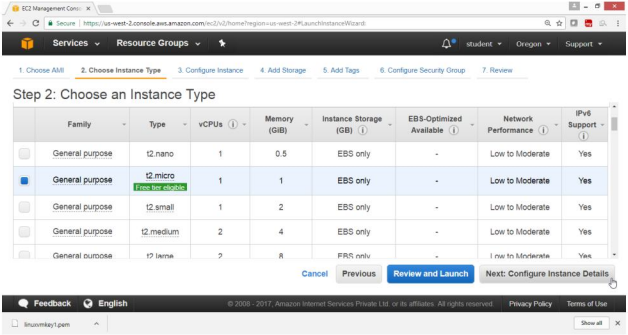


On the **"Choose an Instace Type"** page

Select **"General purpose"**

Type →**t2.micro**

Click on **"Next: Configure Security Group"** button



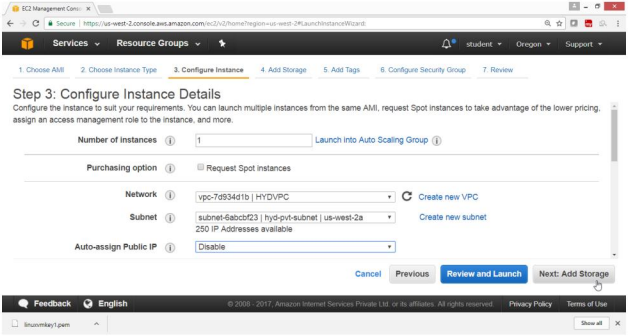
On the **"Configure Instance Details" page**

Number of instance → 1

Network → HYDVPC

Subnet → hyd-pvt-subnet

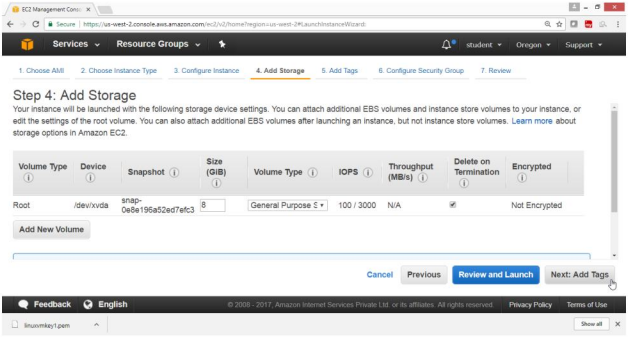
Auto-assign Public IP → Disable



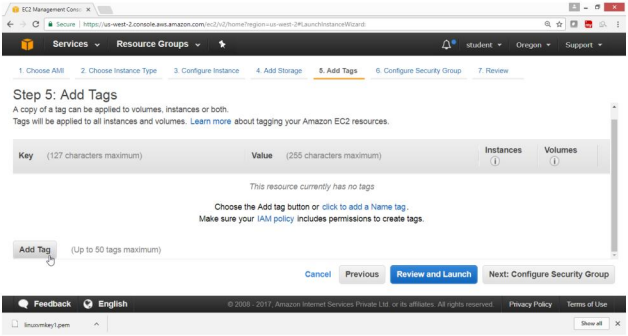
On the **"Add Storage"** page

Leave the values as default

Click on **"Next: Add Tags"** button



Click on **Add Tag**

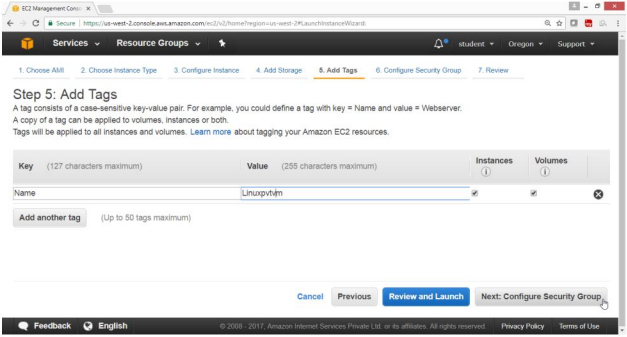


On the **"Add Tags"** page

Key → Name

Value → Linuxpvtvm

Click on **"Next: Configure Security Group"** button

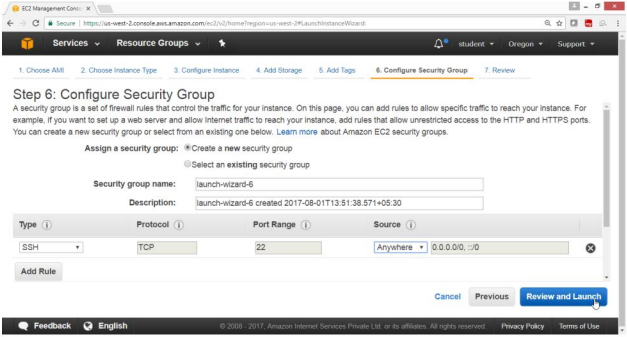


On the **"Configure Security Group"** page

Assign a security group → Create a new security group

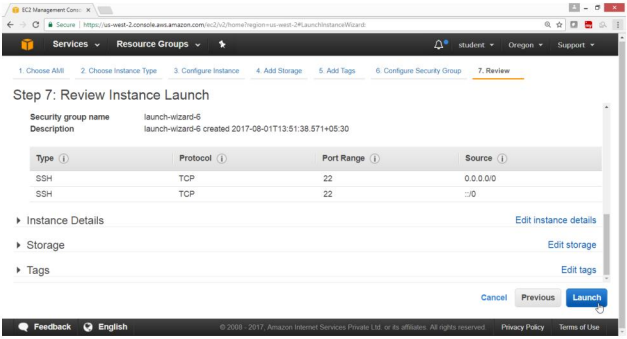
Leave remaining values as default

Click on **"Review and Launch"** button



On the **"Review Instance Launch"** page

Click on **Launch** button

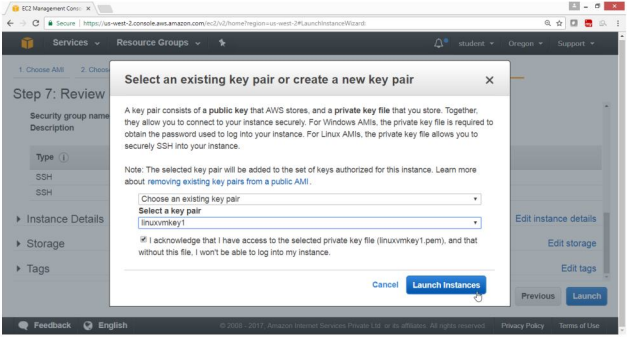


On the **"Select an existing key pair or create a new key pair"** box

Select **Create a new key pair**

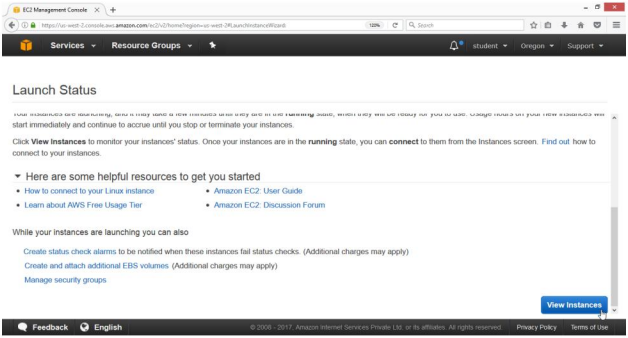
Key pair name → linuxvmkey1

Click on **"Launch Instance"** button



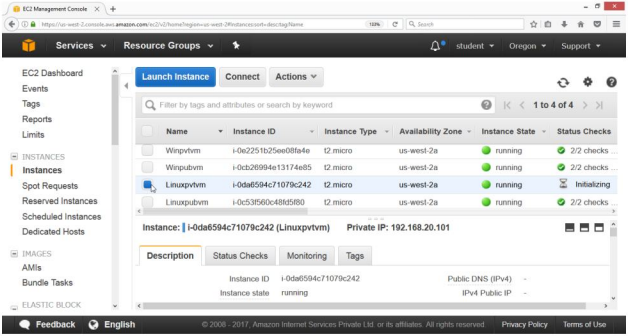
Check the summary

Click on **View Instance** button



Verification

Linux instance in public subnet is launched



To connect to linux private instance

First copy the key to linux instance in public subnet

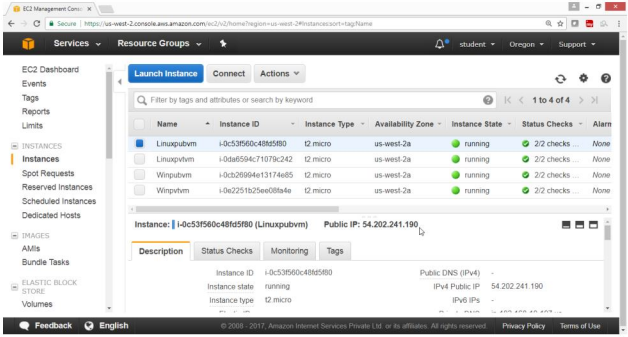
Now connect to linux instance in public

Then connect to linux instance in private

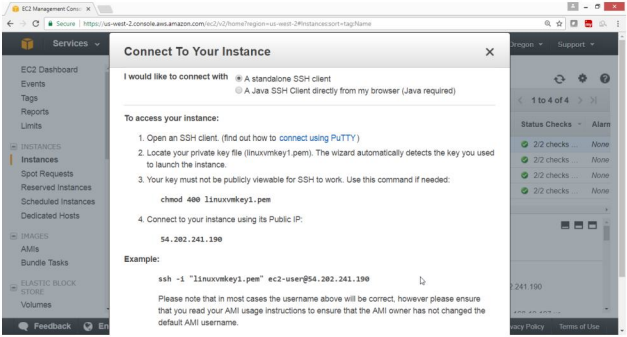
Open Mobaxterm

Coping *.pem file to linux instance in public

Select public linux instance click on connect

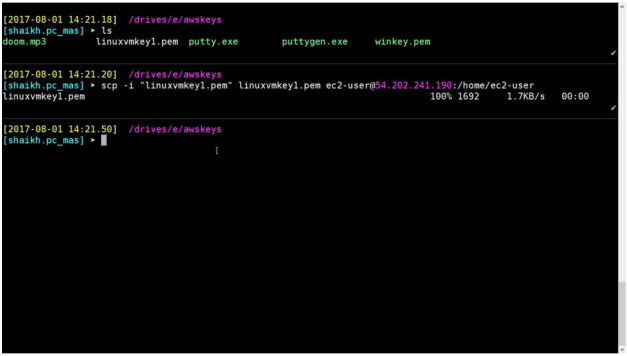


View the guide lines



Use the above public ip of linux instance in mobaxterm

Copy *.pem file to pun linux instance using scp command



Verify

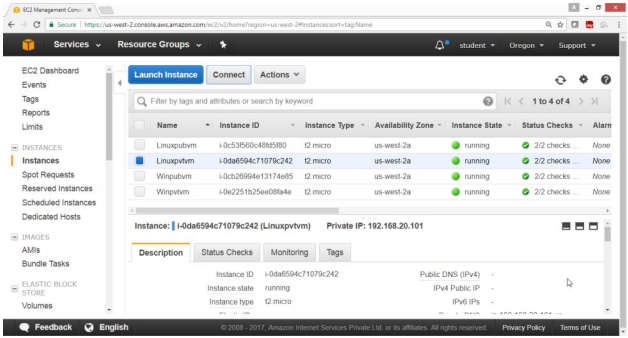
Use commands , pwd, ls to check *.pem file

```
2. /drives/e/awskeys
Re-attach  Fullscreen  Stay on top  Duplicate  Hide toolbar  Close

[2017-08-01 14:22.27]  /drives/e/awskeys
[shaikh.pc_mas] ➤ pwd
/drives/e/awskeys

[2017-08-01 14:22.29]  /drives/e/awskeys
[shaikh.pc_mas] ➤ ls
doom.mp3        linuxvmkey1.pem  putty.exe        puttygen.exe     winkey.pem

[2017-08-01 14:22.30]  /drives/e/awskeys
[shaikh.pc_mas] ➤
```

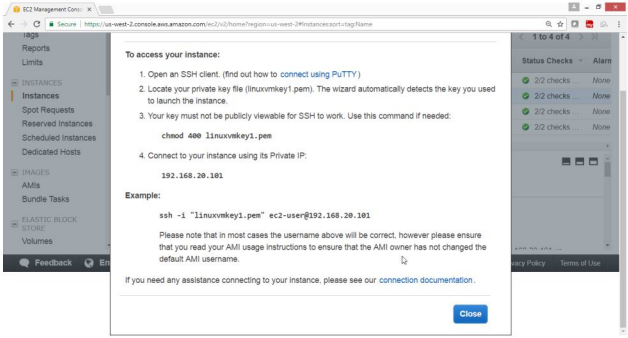
Now connect to public instance using ssh command

```
2. ec2-user@ip-192-168-10-197:~
Re-attach  Fullscreen  Stay on top  Duplicate  Hide toolbar  Close

[2017-08-01 14:22.43]  /drives/e/awskeys
[shaikh.pc_mas] ➤ ssh -i "linuxvmkey1.pem" ec2-user@54.202.241.190
X11 forwarding request failed on channel 0
Last login: Tue Aug  1 08:50:19 2017 from 183.82.211.216

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
1 package(s) needed for security, out of 3 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-10-197 ~]$
```

Select private instance and get private ip



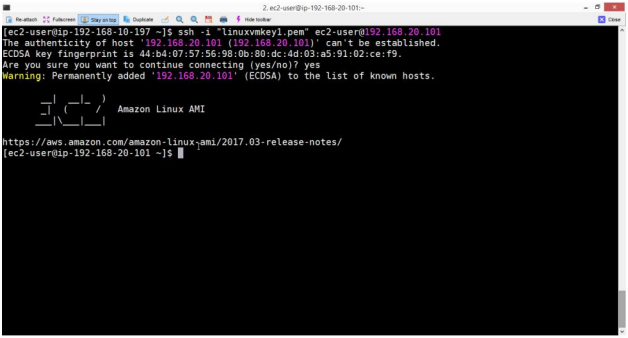
View the details of private instance



Verification

Run ssh command to login to private instance

Now you are connected to private instance in private subnet

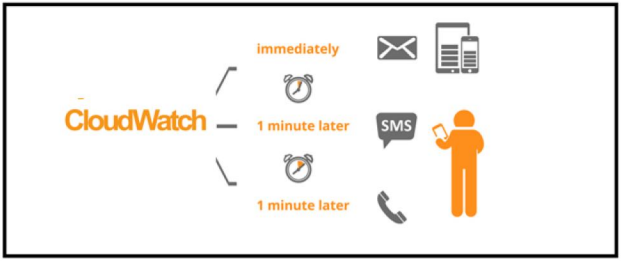


Lab 10: To Configure Amazon CloudWatch

OBJECTIVE

To configure CloudWatch to monitor CPU Utilization

TOPOLOGY



PRE-REQUISTES

User should have AWS account, or IAM user with EC2fullaccess

TASK :

Creating Alarm

Select Notification

Check mail to verify

1) To Configure Amazon CloudWatch Service

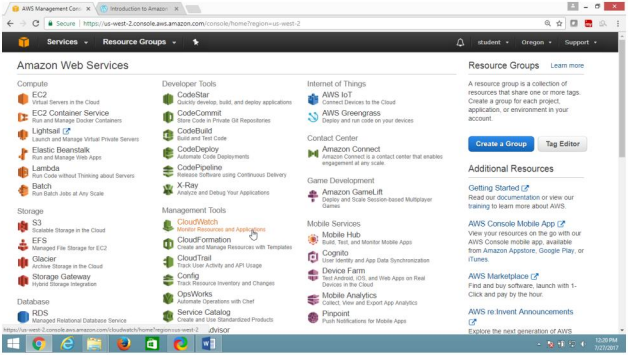
Launch a Amazon linux instance, then

Open **AWS** Console

Click on **Services**

In the **Management Tools** section

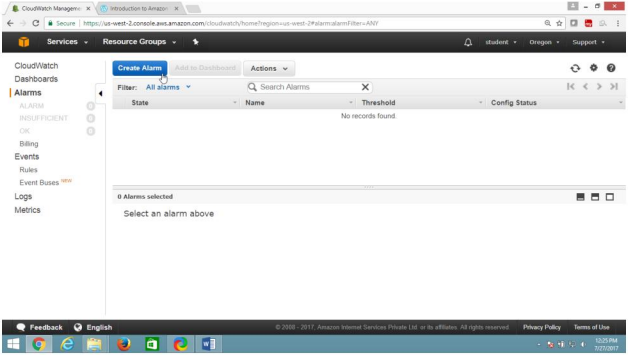
Click on **CloudWatch**



On "**CloudWatch"**, panel

Select **Alarms**

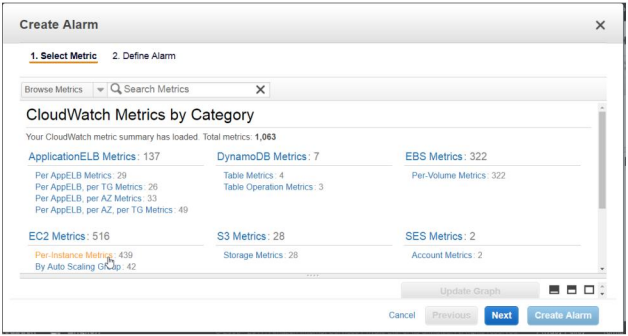
Click on "**Create Alaram"** button



In **“Create Alarm”** page

Select **“EC2 Metrics”**

Click on **“Per-instance Metrics”**



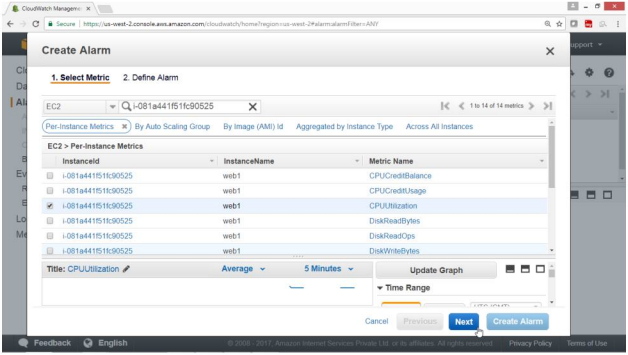
From **"Create Alarm"** page

Select **"1. Select Metric"**

In search box provide instance ID or Name

Under Metric Name, select **CPUUtilization** checkbox

Click on **Next** button



On **Create Alarm** page

Select " **2. Define Alarm**"

Under Alarm Threshold

Name → testcpuuitlization

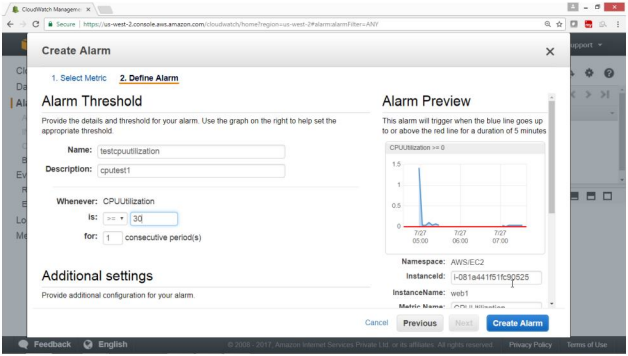
Description→ cputest

Under Whenever CPUUtilization

is >= **30**

for **1** consecutive periods

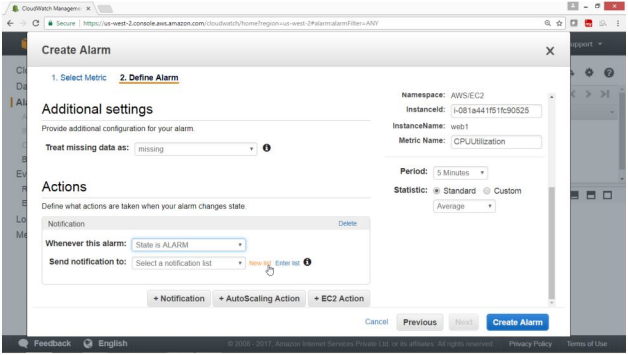
Drag Down



Under Actions

Whenever this alarm → State is Alaram

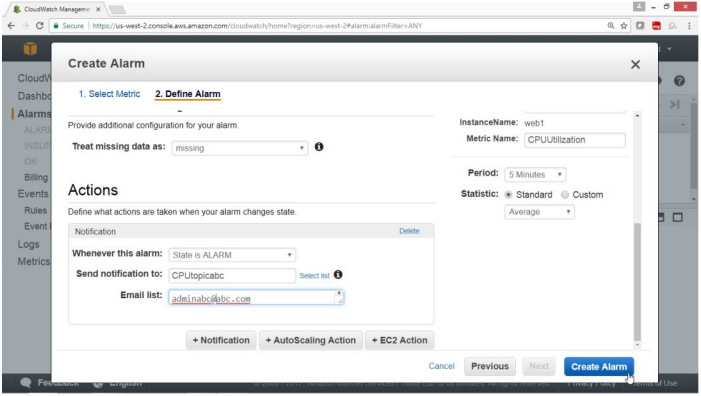
Send notification to → Click on New list



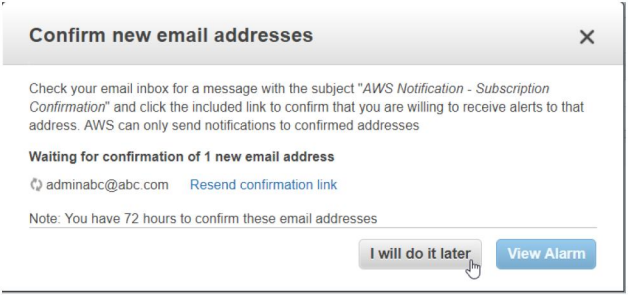
Send notification to → CPUtopicabc

Email → adminabc@abc.com

Click on **"Create Alaram"** button



Click on "**I will do it Later"** button.

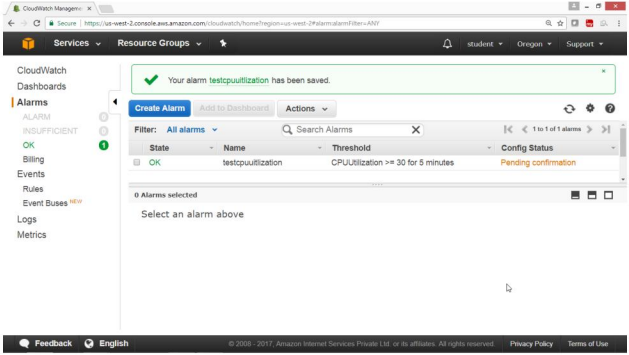


Go to your Email account and check the Mail

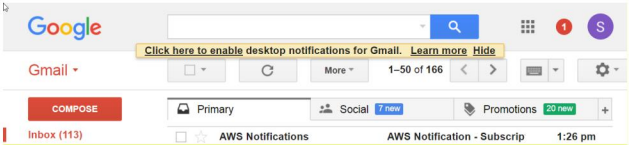
Once mail is been checked

Config status → Pending confirmation

Verify the link from your Email

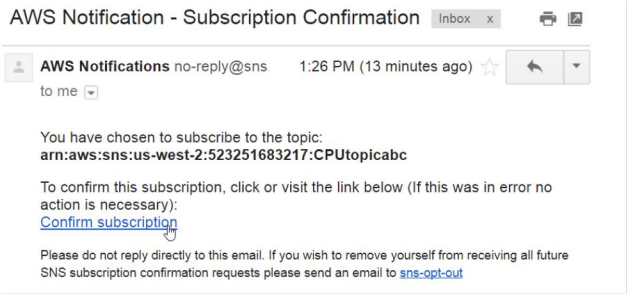


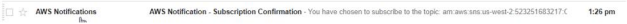
Open your email



Click on **"Confirm subscription"**

==========

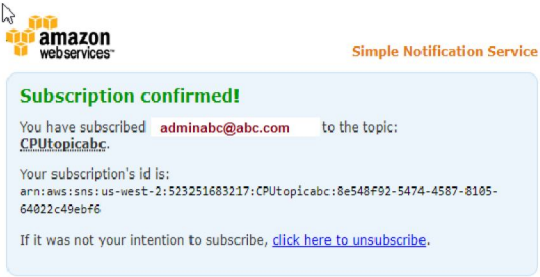




==========

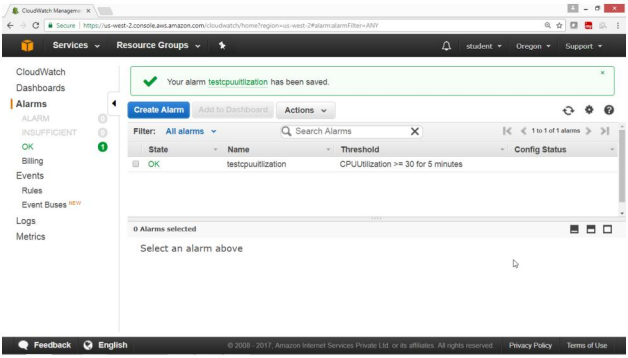
Verified by this output

==========



==========

After confirmation from email **Config status** has become blank



Now login to Instance using mobaxterm

```
[2017-07-27 14:19.15]  ~
[shaikh.pc_mas] ➤ cd e:awskeys
```

```
[2017-07-27 14:19.55]  /drives/e/awskeys
[shaikh.pc_mas] ➤ ssh -i "25july2017masorg.pem" ec2-user@ec2-54-191-150-199.us-w
est-2.compute.amazonaws.com
```

Switch to root user and install stress command

```
[ec2-user@ip-172-31-40-129 ~]$ sudo su
[root@ip-172-31-40-129 ec2-user]# yum install stress -y
```

Login to another terminal-2

Run top command

```
[root@ip-172-31-40-129 ec2-user]# top
```

Verify output

CPU status is 100% idle

```
top - 08:56:26 up  1:53,  2 users,  load average: 0.00, 0.00, 0.00
Tasks:  94 total,   1 running,  93 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1017372k total,   166080k used,   851292k free,     9224k buffers
Swap:        0k total,        0k used,        0k free,    90380k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      20   0 19628 2420 2108 S  0.0  0.2   0:00.90 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kworker/0:0
    5 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kworker/0:0H
    6 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kworker/u30:0
    7 root      20   0     0    0    0 S  0.0  0.0   0:00.03 rcu_sched
    8 root      20   0     0    0    0 S  0.0  0.0   0:00.00 rcu_bh
    9 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
   10 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 lru-add-drain
   11 root      20   0     0    0    0 S  0.0  0.0   0:00.00 cpuhp/0
   12 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kdevtmpfs
   13 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 netns
   16 root      20   0     0    0    0 S  0.0  0.0   0:00.01 xenwatch
   17 root      20   0     0    0    0 S  0.0  0.0   0:00.02 kworker/u30:2
   21 root      20   0     0    0    0 S  0.0  0.0   0:00.00 xenbus
  139 root      20   0     0    0    0 S  0.0  0.0   0:00.00 khungtaskd
  140 root      20   0     0    0    0 S  0.0  0.0   0:00.00 oom_reaper
  141 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 writeback
  143 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kcompactd0
  144 root      25   5     0    0    0 S  0.0  0.0   0:00.00 ksmd
  145 root      39  19     0    0    0 S  0.0  0.0   0:00.00 khugepaged
  146 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 crypto
  147 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kintegrityd
```

Run this command in terminal -1 which will increase the load

 # stress --cpu 40 --timeout 1000

```
[root@ip-172-31-40-129 ec2-user]# stress  --cpu  40  --timeout 1000
stress: info: [3095] dispatching hogs: 40 cpu, 0 io, 0 vm, 0 hdd
```

Now check the status in another terminal-2 by running top command

 # top

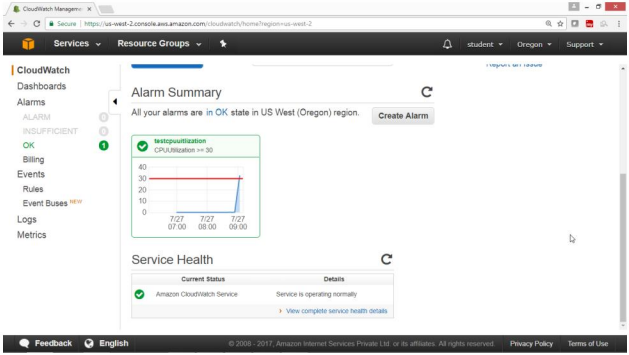
Verify the output

Cpu load is 100%

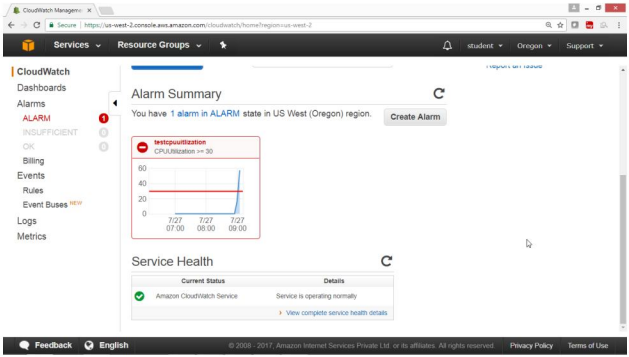
```
top - 09:07:11 up  2:04,  3 users,  load average: 16.16, 6.55, 2.88
Tasks: 144 total,  41 running, 103 sleeping,   0 stopped,   0 zombie
Cpu(s):100.0%us,  0.0%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1017372k total,   179324k used,   838048k free,     9460k buffers
Swap:        0k total,        0k used,        0k free,    90760k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 3143 root      20   0  7260   96    0 R  2.7  0.0   0:00.73 stress
 3147 root      20   0  7260   96    0 R  2.7  0.0   0:00.73 stress
 3179 root      20   0  7260   96    0 R  2.7  0.0   0:00.73 stress
 3141 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3142 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3144 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3145 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3146 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3148 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3149 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3150 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3151 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3152 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3153 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3154 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3155 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3156 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3157 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3158 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3159 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3160 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3161 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3162 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
 3163 root      20   0  7260   96    0 R  2.3  0.0   0:00.72 stress
```

Go to CloudWatch service

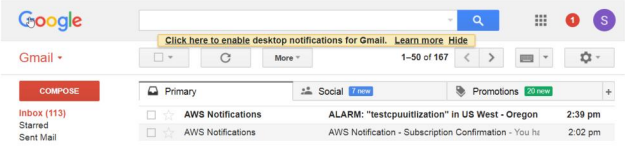
Check the status



After 5 minutes Alarm is generated



Go to email and check mail



Click on mail

Verify output

==========

AWS Notifications no-reply@sns.a 2:39 PM (2 minutes ago)

to me

You are receiving this email because your Amazon CloudWatch Alarm "testcpuuitlization" in the US West - Oregon region has entered the ALARM state, because "Threshold Crossed: 1 datapoint [46.236000000000004 (27/07/17 09:04:00)] was greater than or equal to the threshold (30.0)." at "Thursday 27 July, 2017 09:09:58 UTC".

View this alarm in the AWS Management Console:
https://console.aws.amazon.com/cloudwatch/home?region=us-west-2#s=Alarms&alarm=testcpuuitlization

Alarm Details:
- Name: testcpuuitlization
- Description: cputest
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [46.236000000000004 (27/07/17 09:04:00)] was greater than or equal to the threshold (30.0).
- Timestamp: Thursday 27 July, 2017 09:09:58 UTC

- Timestamp: Thursday 27 July, 2017 09:09:58 UTC
- AWS Account: 523251683217

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 30.0 for 300 seconds.

Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-081a441f51fc90525]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-west-2:523251683217:CPUtopicabe]
- INSUFFICIENT_DATA:

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-west-2:523251683217:CPUtopicabe]
- INSUFFICIENT_DATA:

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:523251683217:CPUtopicabe:e8d238f8-8e77-46ec-8b2f-609f9ba26876&Endpoint= adminabc@abc.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support

========== **END OF OUTPUT** ==========