

**A Practical Guide to Configuring**

**AWS**

(Amazon Web Services)

**Cloud Platform**

**Lab Manual**

# **Introduction**

We are pleased to release the practical guide to configuring AWS (Amazon Web Services). This lab manual can be used as a standalone guide or in conjunction with the AWS course.

The list of exercises ranges from the basic to the advanced, with each exercise building over the one before it. All the steps are clearly outlined with screenshots so that students can practically work through the manual by themselves.

Each of the exercises is divided into four sections:

1. Objective
2. Prerequisite
3. Topology
4. Tasks

We hope this practical guide will be a useful addition to an IT professional's collection, providing reliable step by step how-tos for general AWS configuration. Any feedback or suggestions to improve this would be gratefully accepted.

## Table of Contents

<b>Lab 1: To Launch Amazon Linux EC2 instance .....</b>	3
<b>1a ) To connect to “Amazon linux instance” from linux client operating system.....</b>	16
<b>1b ) To connect to “Amazon linux instance” from Windows Client Operating System.....</b>	19
<b>Lab 2: To Launch Windows EC2 instance in AWS.....</b>	32
<b>2a) To connect to “Windows instance” from Windows client operating system.....</b>	45
<b>2b) To connect to your Windows instance using Linux client operating system.....</b>	53
<b>Lab 3: To Configure Webserver on Amazon Linux instance with Elastic IP .....</b>	55
<b>Lab 4: To Assign Elastic IP address .....</b>	65
<b>Lab 5: To Manage Elastic Block Store (EBS).....</b>	72
<b>Lab 6: To Manage IAM Users, Groups and Policies.....</b>	101
<b>Lab 7: To Configure Amazon Simple Storage Service (Amazon S3) .....</b>	137
<b>Lab 8: To configure Amazon Glacier .....</b>	162
<b>Lab 9: To Configure Amazon Virtual Private Cloud ( VPC ) .....</b>	169
<b>1) To create your own VPC .....</b>	171
<b>2) To create public subnet .....</b>	174
<b>3) To create private subnet .....</b>	176
<b>4) Create a Internet Gateway and attach to your VPC .....</b>	178
<b>5) Create Public Routing Table, associate subnet and add routing rules .....</b>	182
<b>6) Create Private Routing Table, associate subnet and add routing rules .....</b>	189
<b>7) To launch Windows instance in Public subnet.....</b>	194
<b>8) To Launch Windows instance in Private Subnet under HYDVPC VPC .....</b>	203
<b>9) To Connect to Public subnet instance .....</b>	213
<b>10) To Connect to Private subnet instance .....</b>	221
<b>11) To connect to linux instance in private subnet .....</b>	227
<b>12) To connect to linux instance in private subnet .....</b>	236
<b>Lab 10: To Configure Amazon CloudWatch .....</b>	250
<b>Lab 11: To Configure Amazon Simple Notification Service ( SNS ) .....</b>	268
<b>Lab 12: To Configure Amazon Elastic Load Balancer.....</b>	275
<b>Lab 13: To Configure Auto Scaling With Load Balancer .....</b>	292
<b>Lab 14: To Configure an Elastic Beanstalk with Tomcat Application .....</b>	320

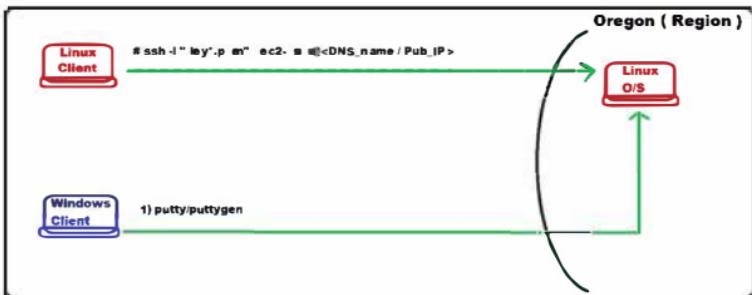
<b>Lab 15: To Configure an Amazon Relational Database Service .....</b>	<b>337</b>
<b>Lab 16: To Configure Amazon DynamoDB.....</b>	<b>360</b>
<b>Lab 17: To Configure Amazon CloudFormation.....</b>	<b>377</b>
<b>Lab 18: To Configure Amazon Simple E-Mail Service (SES).....</b>	<b>393</b>
<b>Lab 19: To Configure Amazon Simple QUEUE Service SQS.....</b>	<b>408</b>
<b>Lab 20: To Configure Amazon Route 53 .....</b>	<b>417</b>
<b>Lab 21: To configure Amazon EFS Service .....</b>	<b>435</b>
<b>Lab 22: To Configure Amazon CloudFront Service .....</b>	<b>448</b>

## Lab 1: To Launch Amazon Linux EC2 instance

### OBJECTIVE

To Launch Amazon Linux instance and to connect from linux and windows client PC.

### TOPOLOGY



**Note :** This lab helps to launch your first instance quickly, so it doesn't cover all possible options.

### PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

### TASK :

Launch Amazon Linux instance

Select Region

Select Amazon Machine Image (AMI)

Create key pair

Connect to Amazon Linux instance from linux client PC using ssh.

Connect to Amazon linux instance from from Windows client PC using putty/puttygen

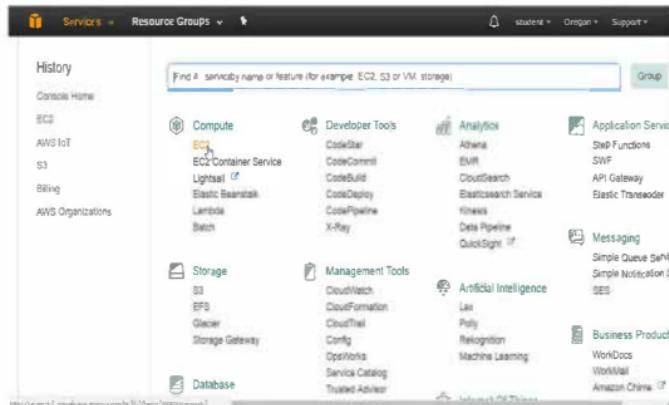
Start/stop/terminate instance

## 1. To Launch Amazon Linux instance in default VPC

Open the Amazon EC2 console

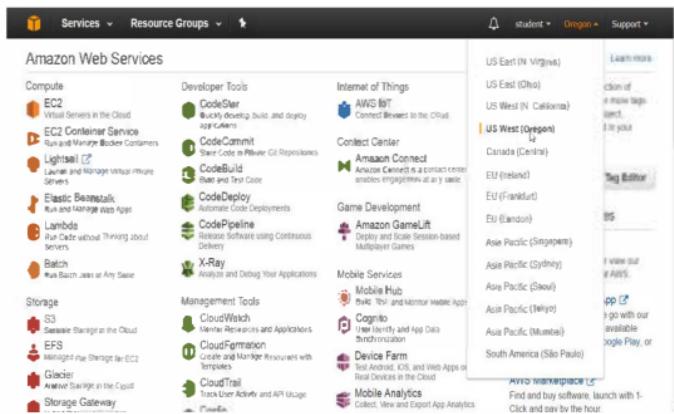
Select **Compute**

Click on **EC2 service**



Select the Region, " US West (Oregon) "

**Note:** Select the region which is nearest to your Geographical Location.



## To check Service Health

Drag down and check **Service Status&Availability Zone Status**:

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (with sub-links: Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), Images (AMIs, Bundle Tasks), and Service Health Dashboard. The main panel is titled "Service Health". It shows "Service Status: US West (Oregon): This service is operating normally". Below that is "Availability Zone Status:" with three entries: "us-west-2a: Availability zone is operating normally", "us-west-2b: Availability zone is operating normally", and "us-west-2c: Availability zone is operating normally". To the right, there's a section for "Scheduled Events" under "US West (Oregon):" which says "No events".

From the "EC2 Dashboard" panel

Select Instance

Click on "Launch Instance" button

The screenshot shows the AWS EC2 Instances page. The sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, AMIs, and Bundle Tasks. The main area is titled "Launch Instance" and shows a table of instances. There are two instances listed: "linuxvma" (Instance ID: i-04ca59221f0ac80ba, Instance Type: t2.micro, Availability Zone: us-west-2b, Status: shutting down) and "linuxvmb" (Instance ID: i-05b8f51f94d4924dd, Instance Type: t2.micro, Availability Zone: us-west-2c, Status: shutting down). Below the table, there are tabs for Description, Status Checks, Monitoring, and Tags. At the bottom, there are links for Feedback, English, and footer links for © 2006-2017 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

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

Select "Quick start"

Select "Amazon Linux AMI" and click **select** button

[Notice that this AMI is marked "Free tier eligible."]

Step 1: Choose an Amazon Machine Image (AMI)

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

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Free tier only

Amazon Linux

Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-4834a426

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

Select

64-bit

Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-0f85d0f

Red Hat Enterprise Linux version 7.3 (HVM) x86 General Purpose (SSD) Volume Type

Select

64-bit

Feedback English © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

On “Choose an Instance Type” page

Select type “t2.micro”, eligible for the free tier.

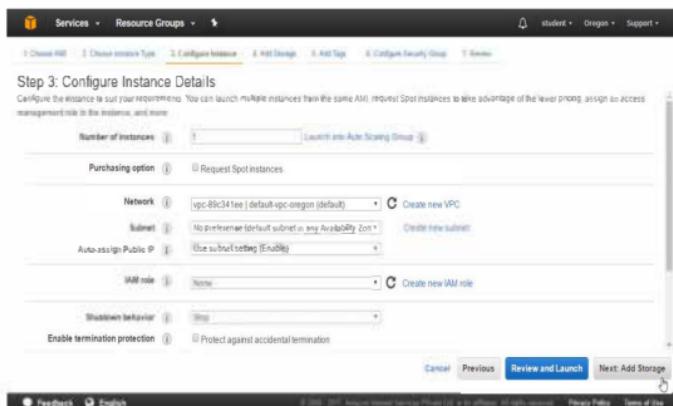
Click on “Next: Configure Instance Details” button

The screenshot shows the AWS CloudFormation console interface. At the top, there are tabs: Services, Resource Groups, and a navigation bar with student, Original, and Support. Below the tabs, a breadcrumb trail shows: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. A sub-header "Step 2: Choose an Instance Type" is displayed. A descriptive text explains that Amazon EC2 provides a wide selection of instance types optimized to fit different use cases, mentioning CPU, memory, storage, and networking capacity. It also notes the flexibility to choose the appropriate mix of resources for applications. A note states: "Currently selected: t2.micro (Variable ECUs, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GB memory, EBS only)". The main content is a table listing instance types. The columns are: Family, Type, vCPUs, Memory (GiB), Instance Storage (GiB), EBS-Optimized Available, Network Performance, and IPv6 Support. The table shows four rows: 1. General purpose (t2.nano), 2. General purpose (t2.micro, highlighted with a green border), 3. General purpose (t2.small), and 4. General purpose (t2.medium). The "Review and Launch" button is visible at the bottom right of the table area.

On "Configure Instance Details" page

Leave all values as default

Click on "Next: Add storage" button



**On “Add Storage”, page**

Leave all values as default

Click on “**Next: Tag Instance**” button

The screenshot shows the AWS Step 4: Add Storage configuration page. At the top, there is a navigation bar with tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (which is highlighted in yellow), 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the tabs, the heading "Step 4: Add Storage" is displayed, followed by a note: "Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2." A table lists the storage configuration:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Deletes on Termination	Encrypted
Root	/dev/xvda	snap-0ca97573e618bad	8	General Purpose (SSD)	100 / 3000	N/A	No	Not Encrypted

Below the table, there is a button labeled "Add New Volume". A note below the table states: "Free tier eligible customers can get up to 30 GiB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and limits." At the bottom of the page, there are several buttons: "Cancel", "Previous", "Review and Launch" (which is highlighted in blue), and "Next: Add Tags".

On "Add Tags" page

Provide following values

Key → Name

Value → linuxvmm

Click on "Next: Configure Security Group" button

The screenshot shows the AWS EC2 instance creation wizard at Step 5: Add Tags. The interface includes a navigation bar with tabs: 1. Choose All, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (highlighted in yellow), 6. Configure Security Group, and 7. Review. Below the tabs, there's a note about tags: "Step 5. Add Tags", "A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.", "A copy of a tag can be applied to volumes, instances or both.", and "Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources." A table allows adding tags with columns for Key (127 characters maximum), Value (255 characters maximum), Instances, and Volumes. One tag is listed: Name (linuxvmm). A link "Add another tag" is visible. At the bottom, there are "Cancel", "Previous", "Review and Launch" (highlighted in blue), and "Next: Configure Security Group". The footer includes links for Feedback, English, Copyright (© 2008-2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

On "Configure Security Group" page

Select → Create a new security group

Leave all values as default.

**Note:** By default for linux instance **port 22** i.e ssh is used.

Click "Review and Launch" button



On "Review Instance Launch", page

Leave all values as default.

Verify the summary, then drag down

Step 7: Review Instance Launch

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

**AMI Details**

Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-4836a428

The Amazon Linux AMI is an EBS-optimized, 64bit-supported image. The default image includes AWS command-line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

**Instance Type**

Instance Type    ECUs    vCPUs    Memory (GB)    Instance Storage (GB)    EBS-Optimized Available    Network Performance

**Security Groups**

Launch wizard-1

Type: All traffic    Protocol: TCP    Port Range: 22    Source: 0.0.0.0/0

**Launch**

Verify the summary

Click on **Launch** button

Step 7: Review Instance Launch

InstanceState: Running

**Security Groups**

Launch wizard-1

Type: All traffic    Protocol: TCP    Port Range: 22    Source: 0.0.0.0/0

**Instance Details**

**Storage**

**Tags**

**Launch**

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

Select "Create a new key pair"

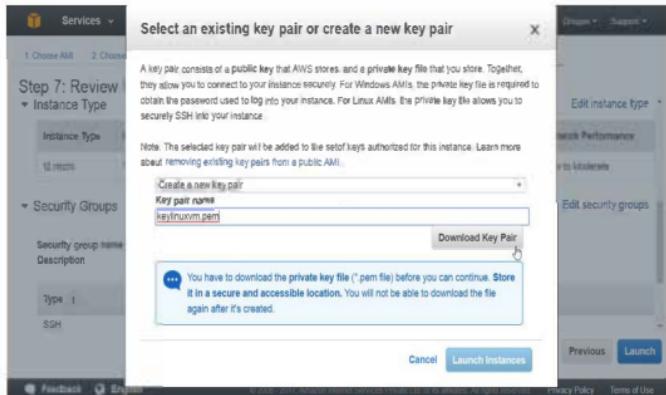
Enter Key pair name → keylinuxvm.pem

Click on "Download Key Pair"

**Note:** Store it in a secure and accessible location.

You will not be able to download the file again after it's created.

Click on "Launch an instance"



On Launch Status page, go to right bottom corner

Click on “View instances” button

The screenshot shows the AWS Launch Status page. At the top, there's a navigation bar with icons for notifications, services (dropdown), Resource Groups (dropdown), and links for Support,学生, Oxygen, and Logout. Below the navigation, the title "Launch Status" is displayed. A note says "instances will start immediately and continue to accrue until you stop or terminate your instances." Another note encourages clicking "View Instances" to monitor instance status. A section titled "While your instances are launching you can also" lists three items: "Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)", "Create and attach additional EBS volumes (Additional charges may apply)", and "Manage security groups". At the bottom right, there's a prominent blue "View instances" button.

On EC2 Dashboard panel

Click on Instances,

Select instances

Check instance status → running

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Instances (under DEDICATED), Aliases, Bundle Tasks, and Elastic Block Store (Volumes, Snapshots). The main pane shows a table with one row for an instance named 'linuxvm'. The 'Instance State' column shows a green circle with the word 'running'. A red oval highlights this green circle.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
linuxvm	i-0dad392c3195bef6	t2.micro	us-west-2b	running	Initializing	N/A

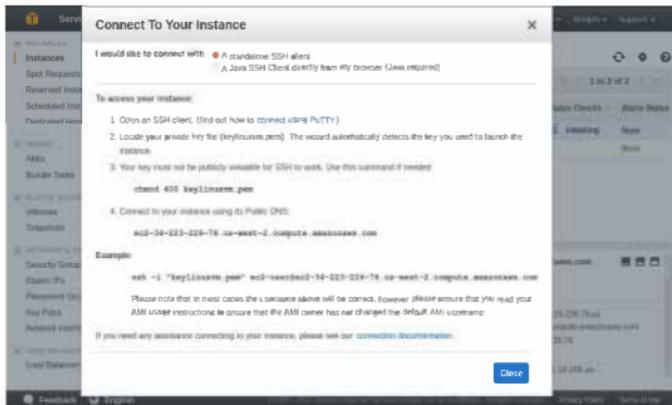
To check instance details like

Description, Status check, Monitoring, Tags

This screenshot shows the same EC2 Dashboard interface as above, but the instance details pane is expanded. It displays the instance ID, Public DNS, and Public IP. Below this, there are four tabs: 'Description' (highlighted with a red oval), 'Status Checks', 'Monitoring', and 'Tags'. The 'Description' tab shows the instance state as 'running', type as 't2.micro', and elastic IP as 'Elastic IPs'. The 'Status Checks' tab shows the public IP as 'ec2-54-149-138-51.us-west-2.compute.amazonaws.com'. The 'Monitoring' tab shows the private DNS as 'ip-172-31-23-254.us-west-2.compute.amazonaws.com'. The 'Tags' tab shows the instance has no explicit tags.

## 1a ) To connect to “Amazon linux instance” from linux client operating system.

On “Connect To Your Instance” page see the guide lines to connect to linux instance.



Login to linux client PC, Open the terminal and run following commands.

First go to the folder where your private key file \*.pem is stored.

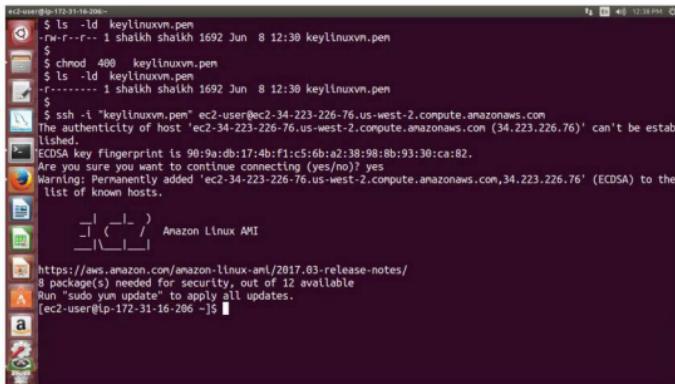
**eg : keylinuxvmm.pem**

```
# ls
```

```
# ll
```

```
# chmod 400 keylinuxvmm.pem
```

```
# ssh -i "keylinuxvmm.pem" ec2-user@ec2-54-191-200-74.us-west-2.compute.amazonaws.com
```



The screenshot shows a terminal window with a dark background and light-colored text. The session starts with the user's command to change directory and list files, followed by changing permissions on a file named 'keylinuxvmm.pem'. Then, the user runs an SSH command to connect to an Amazon EC2 instance. The terminal shows the host key fingerprint and asks for confirmation to add it to the known hosts. Finally, it displays a welcome message from the Amazon Linux AMI and a link to the release notes. The terminal ends with a prompt '[ec2-user@ip-172-31-16-206 ~]\$'.

```
ec2-user@ip-172-31-16-206:~$ ls -l keylinuxvmm.pem
-rw-r--r-- 1 shalikh shalikh 1692 Jun  8 12:30 keylinuxvmm.pem
ec2-user@ip-172-31-16-206:~$ chmod 400 keylinuxvmm.pem
ec2-user@ip-172-31-16-206:~$ ll keylinuxvmm.pem
-r----- 1 shalikh shalikh 1692 Jun  8 12:30 keylinuxvmm.pem
ec2-user@ip-172-31-16-206:~$ ssh -i "keylinuxvmm.pem" ec2-user@ec2-34-223-226-76.us-west-2.compute.amazonaws.com
The authenticity of host 'ec2-34-223-226-76.us-west-2.compute.amazonaws.com (34.223.226.76)' can't be established.
ECDSA key fingerprint is 90:9a:db:17:4b:f1:c5:6b:a2:38:98:8b:93:30:ca:82.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-34-223-226-76.us-west-2.compute.amazonaws.com,34.223.226.76' (ECDSA) to the
list of known hosts.
[ec2-user@ip-172-31-16-206 ~]$
```

**Note : ec2-user** is the default user for this instance

To know current user in linux

```
$ whoami
```

To switch to root user in linux

```
$ sudo su
```

Verify ( root user )

```
# whoami
```

To logout

```
# exit
```

```
[ec2-user@ip-172-31-17-217 ~]$ whoami  
ec2-user  
[ec2-user@ip-172-31-17-217 ~]$ sudo su  
[root@ip-172-31-17-217 ec2-user]#  
[root@ip-172-31-17-217 ec2-user]# whoami  
root  
[root@ip-172-31-17-217 ec2-user]# exit
```

I

**1b ) To connect to “Amazon linux instance” from Windows Client Operating System.**

Download **putty.exe** and **puttygen.exe** from **putty.org** website



The screenshot shows a Microsoft Edge browser window with two tabs open. The active tab displays the Putty download page at [www.putty.org](http://www.putty.org). The page title is "Download PuTTY". It contains a brief description of PuTTY as an SSH and telnet client developed by Simon Tatham for the Windows platform, noting it is open source software maintained by volunteers. A link to download Putty is provided. Below this, a note states: "Below suggestions are independent of the authors of PuTTY. They are not to be seen as endorsements by the PuTTY project." A second tab titled "Download PuTTY - archive" is visible in the background.

**Download PuTTY**

PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.

You can download PuTTY [here](#).

Below suggestions are independent of the authors of PuTTY. They are not to be seen as endorsements by the PuTTY project.

**Bitvise SSH Client**



The screenshot shows a Microsoft Edge browser window displaying the Bitvise SSH Client download page at [www.clarkgreenend.org.uk/~sgtatham/putty/download.html](http://www.clarkgreenend.org.uk/~sgtatham/putty/download.html). The page title is "Bitvise SSH Client". It describes the Bitvise SSH Client as an SSH and SFTP client for Windows, developed professionally by Bitvise. The SSH Client is robust, easy to install, and supports all features supported by PuTTY, as well as the following:

- graphical SFTP file transfer;
- single-click Remote Desktop tunneling;
- auto-reconnecting capability;
- dynamic port forwarding through an integrated proxy;
- an FTP-to-SFTP protocol bridge.

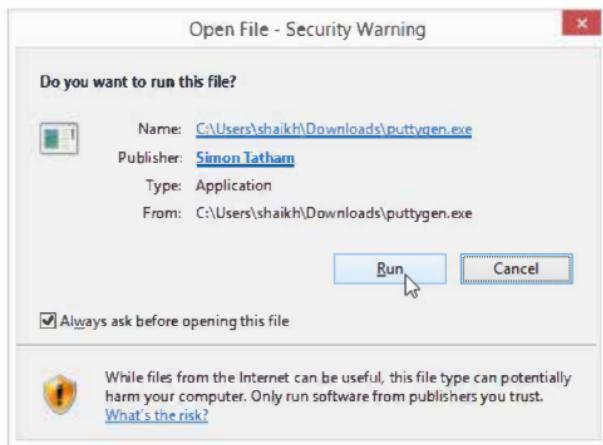
Bitvise SSH Client is **free to use**. You can [download it here](#).

**Bitvise SSH Server**

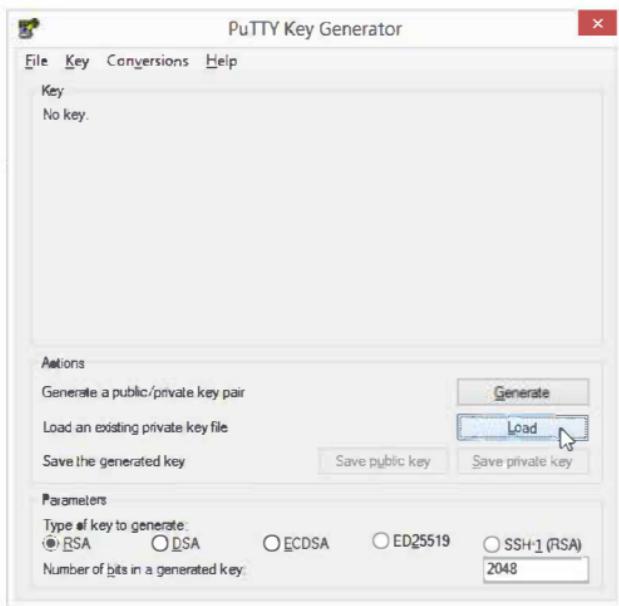
Note: Because putty cannot understand .pem file format, so use puttygen.exe to converting \*.pem file into \*.ppk format

Click on puttygen.exe file in windows operating system

Click on Run



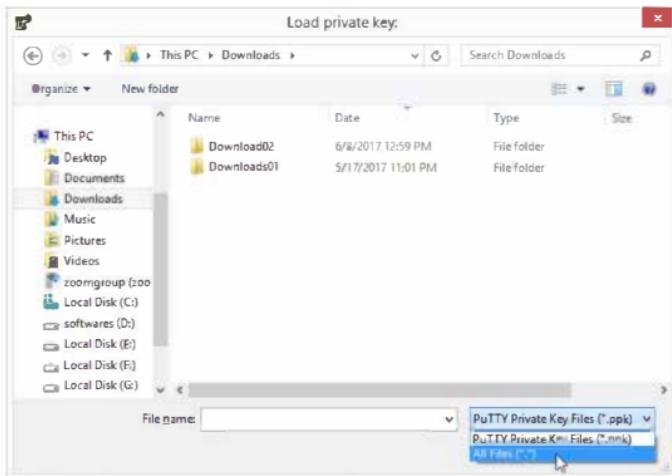
Click on Load button



**Note:** By default, PuTTYgen displays only files with the extension .ppk

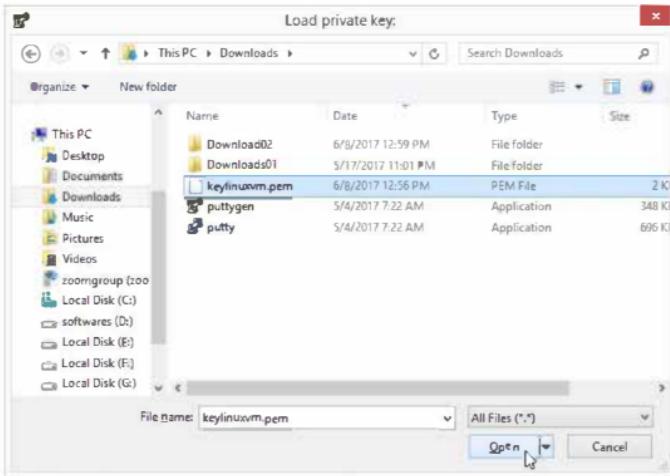
So to locate your .pem file

On file names Select →All files (\*.\*)

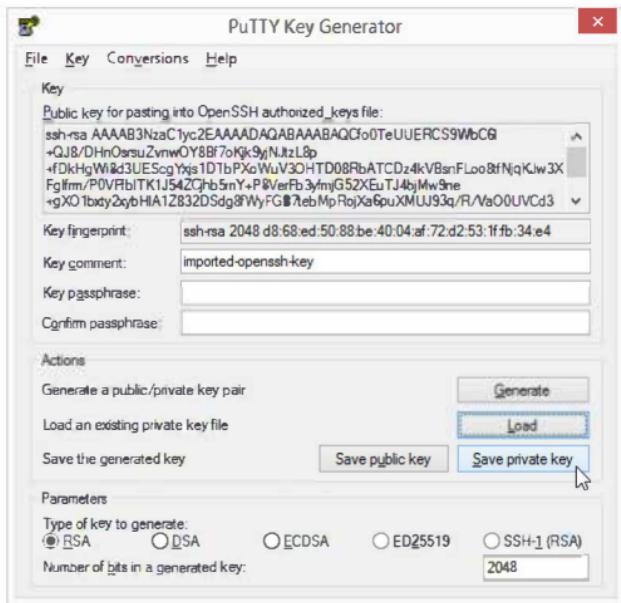


Locate keylinuxvm.pem in your folder

Click on open

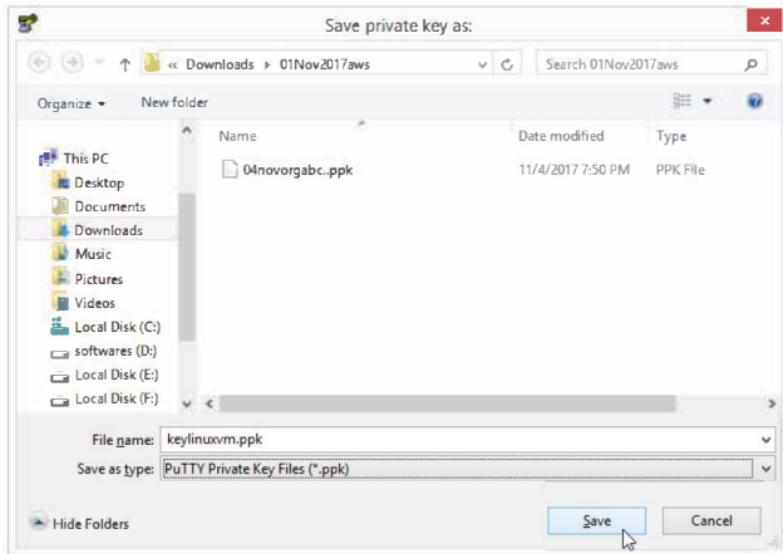


Click on "Save private key" button



Save the file → keylinuxvm.ppk

Click on Save button



To connect to linux instance Run putty.exe from windows operating system.

**Run putty.exe**

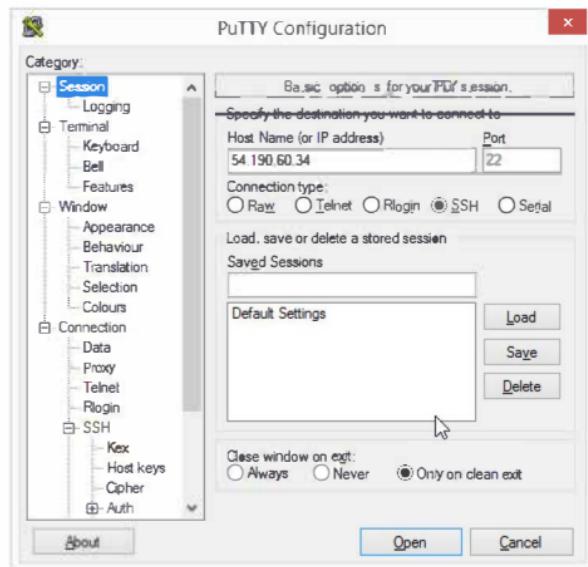
**Click on Run**



On Category page provide following values

Host Name (or IP address) → Provide public IP or DNS name of the instance

Port → 22

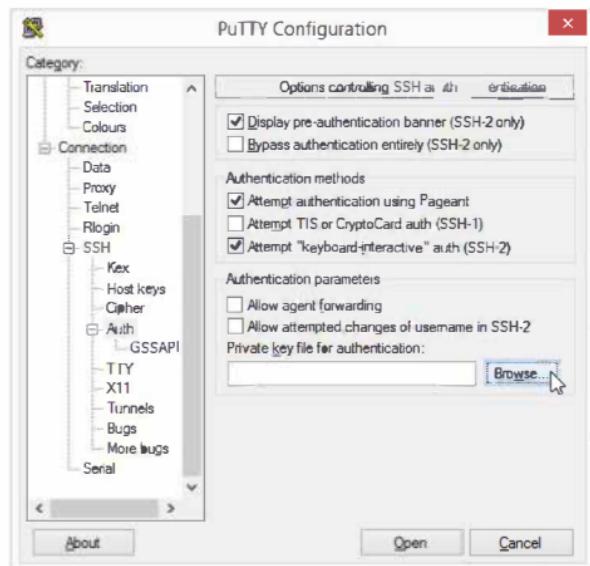


Under Connection expand

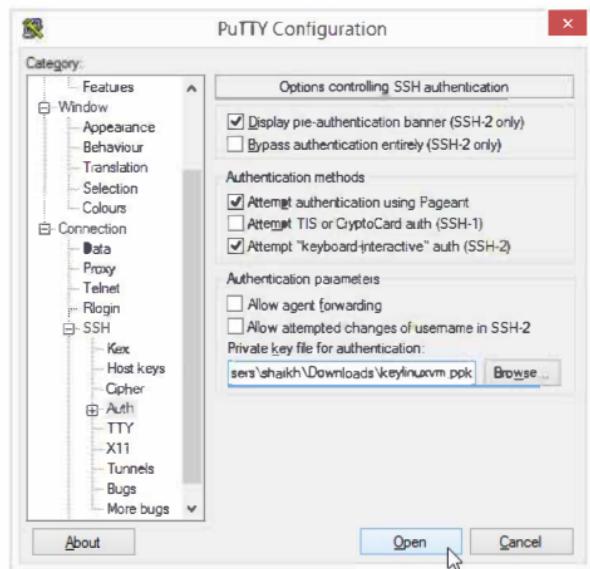
Click on SSH → Auth

Select Browse button

Provide the path of \*.ppk file



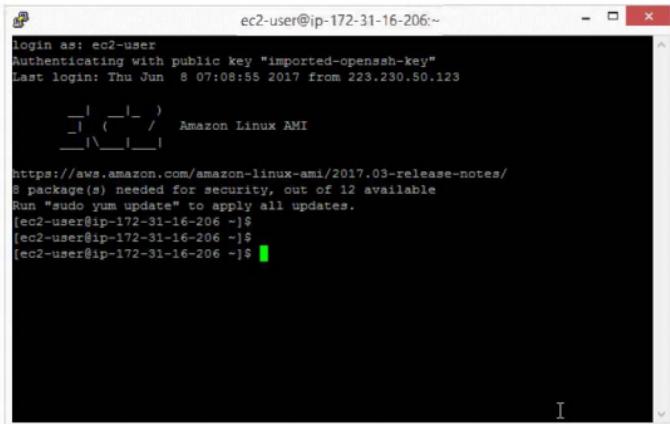
Click on Open button



## Verify

Putty login screen is for linux

Provide user name **ec2-user**



The screenshot shows a Windows-style terminal window titled "Putty". The title bar displays the session name "ec2-user@ip-172-31-16-206:~". The main window content is a black terminal session. It starts with a standard Linux login message:

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Thu Jun  8 07:08:55 2017 from 223.230.50.123
```

Below this, there is a decorative graphic consisting of several short horizontal and vertical lines forming a stylized arrow or bracket shape, followed by the text "Amazon Linux AMI".

Further down, the terminal displays a system update message:

```
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
8 package(s) needed for security, out of 12 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-16-206 ~]$
```

The command "sudo yum update" is partially typed at the end of the message.

**Now you had logged in as ec2-user in Amazon Data Center Linux Machine.**

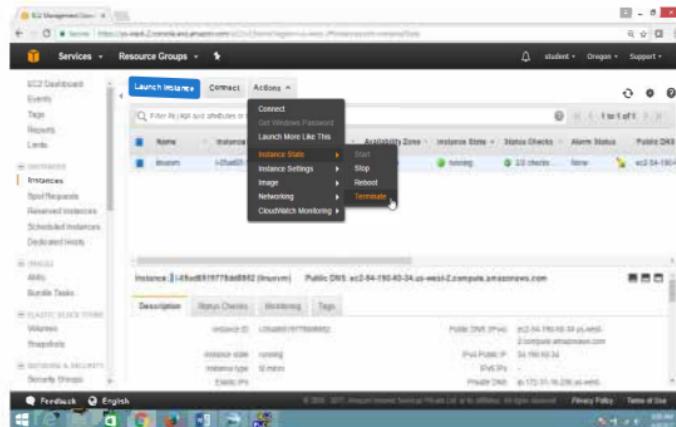
**To start/stop/terminate instance**

On Ec2 Dashboard

Select the Instance

Drop down on **Action** button

Select **Instance state to Start/Stop/Reboot//Terminate** the instances.



**Note:**

If you are not going to use the instance, terminate the instance,

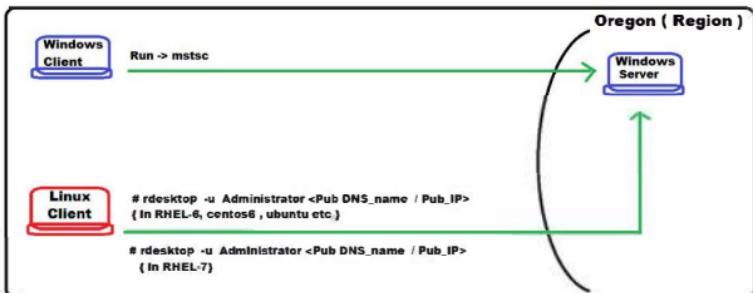
Otherwise it will be charged if the limit is over after free tier usage.

## Lab 2: To Launch Windows EC2 instance in AWS

### OBJECTIVE

To Launch Windows instance and to connect from windows and linux client PC.

### TOPOLOGY



**Note :** This lab helps to launch your first Windows instance quickly, so it doesn't cover all possible options.

### PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

### TASK :

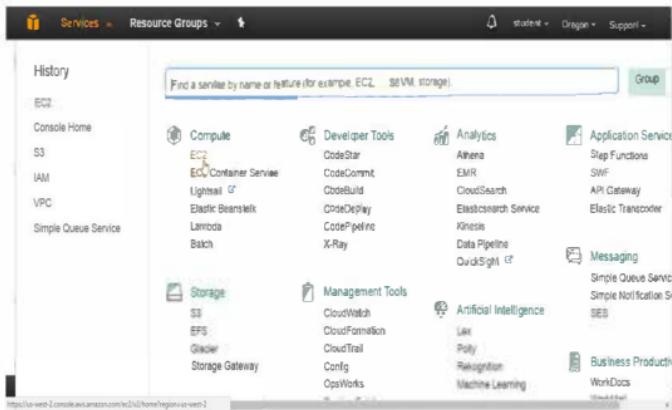
- To Launch Windows instance
- Select Region
- Select Amazon Machine Image (AMI)
- Create key pair
- Connect from Windows operating system
- Connect from Linux Operating system
- Start/stop/terminate instance

## 1. To Launch Windows instance in default VPC

Open the Amazon EC2 console

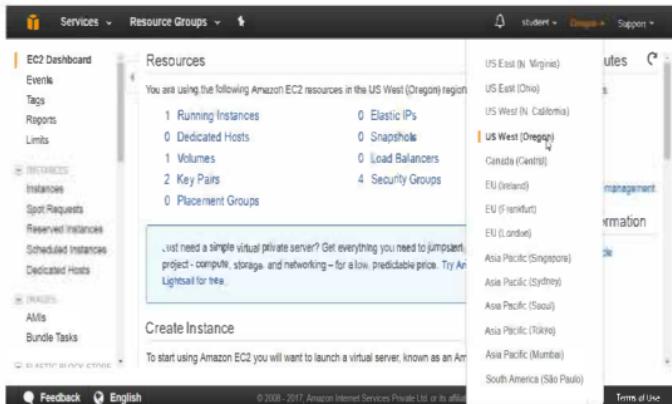
Select **Compute**

Click on **EC2 service**



Select the Region, "US West (Oregon)"

Note: Select the region which is nearest to your Geographical Location.



## To check Service Health

Drag down and check **Service Status & Availability Zone Status**:

The screenshot shows the EC2 Dashboard with the "Service Health" tab selected. On the left, there's a sidebar with links for EC2 Dashboard, Instances, Images, AMIs, and Bundle Tasks. The main content area has two sections: "Service Status" and "Availability Zone Status". Under "Service Status", it says "US West (Oregon)" and "This service is operating normally". Under "Availability Zone Status", it lists three zones: "us-west-2a", "us-west-2b", and "us-west-2c", all marked as "Availability zone is operating normally". To the right, there's a sidebar for "Scheduled Events" which is currently empty. Below the main content, there are promotional cards for "Baracuda NextGen Firewall F-Series - PAYG" and "VIArables Next-Generation Firewall Bundle 2". At the bottom, there are links for Feedback, English, and a footer with copyright information.

From the “EC2 Dashboard” panel

Select Instance

Click on “Launch Instance” button

The screenshot shows the EC2 Dashboard with the "Instances" section selected. In the center, there's a "Launch Instance" button. Below it, a table lists an instance named "linuxvm" with ID "i-05ad6519778dd8852". The instance is running in the "us-west-2b" availability zone. At the bottom, there are tabs for "Description", "Status Checks", "Monitoring", and "Tags". The "Description" tab shows detailed information: Instance ID (i-05ad6519778dd8852), Public DNS (ec2-54-190-60-34.us-west-2.compute.amazonaws.com), Instance state (running), and Instance type (t2.micro). The "Status Checks" tab shows 2/2 checks passing. The "Monitoring" and "Tags" tabs are empty. The footer includes links for Feedback, English, and a footer with copyright information.

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

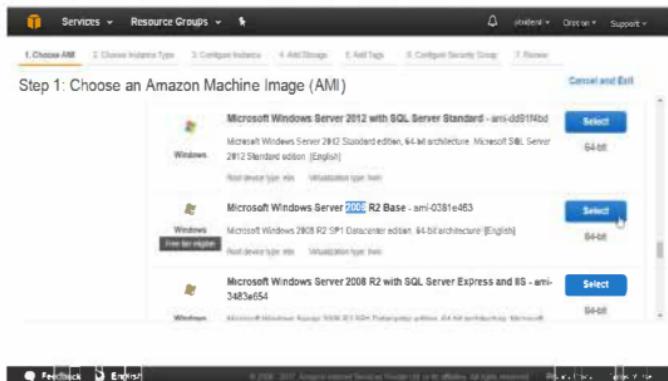
Select "Quick start"



Select "Microsoft Windows Server AMI" and click **Select** button

[Notice that this AMI is marked "**Free tier eligible.**"]

Click on **Select** button



On “Choose an Instance Type” page

Select type “t2.micro”, eligible for the free tier.

Click on “Next: Configure Instance Details” button

Family	Type	vCPUs	Memory (GB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	<b>t2.micro</b> <small>(free for usage)</small>	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

On “Configure Instance Details”, page

Leave all values as default

Click on “Next : Add storage” button

Step 3: Configure Instance Details

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

Number of Instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-89c34tee   default-vpc-oregon (default)	<input type="checkbox"/> Create new VPC
Subnet	No preference (default subnet in any Availab. My Zony)	<input type="checkbox"/> Create new subnet
Auto-assign Public IP	Use static setting (Enable)	
Domain join directory	None	<input type="checkbox"/> Create new directory

**On “Add Storage”, page**

Leave all values as default

Click on “**Next: Tag Instance**” button

The screenshot shows the 'Add Storage' step of a CloudFormation stack creation process. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'Create Stack', 'Create Resource Type', 'Configure Instance', 'Add Storage' (which is highlighted), 'Add Tags', 'Configure Security Group', and 'Review'. Below the tabs, a section titled 'Step 4: Add Storage' provides instructions: 'Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes.' A note below states: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and limits.' The main configuration table has columns: Volume Type, Device, Snapshot, Size (GB), Volume Type, IOPS, Throughput (MB/s), Delete on Termination, and Encrypted. A single row is shown for the 'Root' volume, which is an 'Amazon EBS' volume of size 30 GB, type 'General Purpose (SSD)', IOPS 100, Throughput 3000, set to delete on termination, and is not encrypted. Below the table is a 'Add New Volume' button. At the bottom of the screen, there are 'Cancel', 'Previous', 'Review and Launch' (which is blue and highlighted), and 'Next: Add Tags' buttons. The footer includes links for 'Feedback' and 'English'.

On "Add Tags" page

Provide following values

Key → Name

Value → winserver

Click on "Next: Configure Security Group" button

The screenshot shows the AWS Step 5: Add Tags configuration page. At the top, there are tabs for 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is highlighted in orange), 6. Configure Security Group, and 7. Review. Below the tabs, the heading "Step 5: Add Tags" is displayed, followed by a note: "A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = WinServer. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources." There is a table with two rows. The first row has columns for "Key" (Name) and "Value" (winserver). The second row has columns for "Instances" (1) and "Volumes" (1). Below the table, there is a button labeled "Add another tag" and a note "(Up to 50 tags maximum)". At the bottom of the page, there are buttons for "Cancel", "Previous", "Review and Launch" (which is highlighted in blue), and "Next: Configure Security Group". The footer includes links for "Feedback", "English", "© 2008-2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

On "Configure Security Group" page

Select → Create a new security group

Leave all values as default.

Note: By default for linux instance port 3389 i.e RDP is used.

Click "Review and Launch" button

The screenshot shows the AWS EC2 wizard at Step 6: Configure Security Group. The security group is named 'launch-wizard-4' and has a description of 'launch-wizard-4 created 2017-06-09T06:46:33.392+05:30'. An inbound rule is defined for RDP (Protocol: TCP, Port Range: 3389, Source: 0.0.0.0). The 'Review and Launch' button is highlighted.

Step 6: Configure Security Group

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

Assign a security group:  Create a new security group  Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
RDP	TCP	3389	Custom + 0.0.0.0

Add Rule

Cancel Previous Review and Launch

Feedback English © 2008 - 2017 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

On "Review Instance Launch", page

Leave all values as default.

Verify the summary, then drag down

**Step 7: Review Instance Launch**  
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.

**AMI Details**

Microsoft Windows Server 2008 R2 Base - ami-0381e463

Microsoft Windows 2008 R2 SP1 Datacenter edition 64-bit architecture [English]

Free tier    Read Devotee Test Drive    View details

Cancel Previous Launch

Verify the summary

Click on **Launch** button

**Step 7: Review Instance Launch**

Security Groups

Type	Protocol	Port Range	Source
UDP	TCP	3389	0.0.0.0

Instance Details    Edit instance details

Storage    Edit storage

Tags    Edit tags

Cancel Previous Launch

On "Select an existing key pair or create a new key pair", page

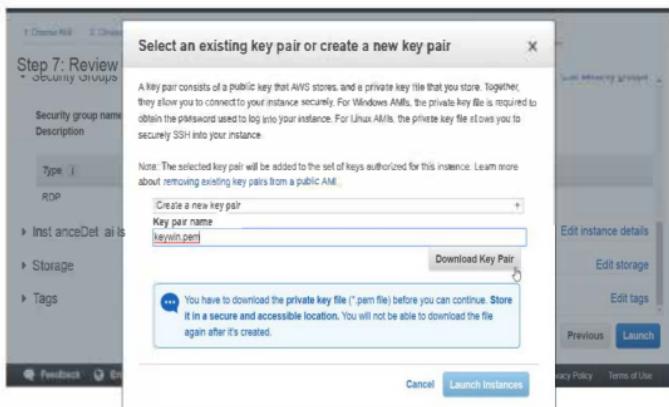
Select "Create a new key pair"

Enter Key pair name → keywin.pem

Click on "Download Key Pair"

**Note:** Store it in a secure and accessible location.

You will not be able to download the file again after it's created.

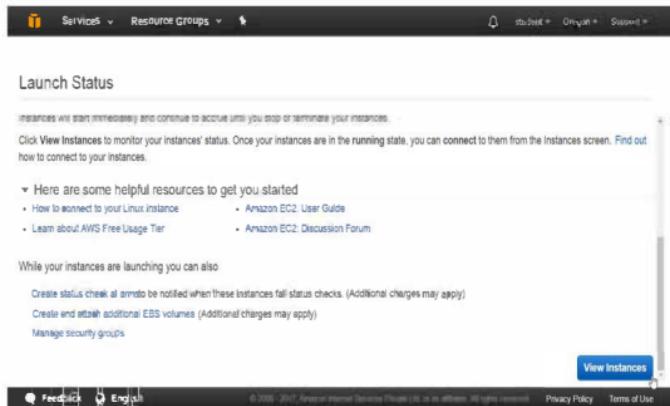


Click on "Launch an instance"



On Launch Status page, go to right bottom corner

Click "View instances" button



**On EC2 Dashboard panel**

Click on Instances

Select instances

Check instance state → pending

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links: Services, Resource Groups, EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected and highlighted in orange), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, IAMs, and Bundle Tasks. Below the sidebar, there's a Feedback link and language selection for English. The main content area has a header with 'Launch Instance', 'Connect', and 'Actions'. It includes a search bar and filters for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. There are two instances listed:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
winserver	i-096c73fb5579363	t2.micro	us-west-2b	<span style="color: red;">pending</span>	0/0 initializing	None
linunx	i-05ad951977bdd9852	t2.micro	us-west-2b	<span style="color: green;">running</span>	3/3 healthy	None

Below the instances, there's a note: "Select an instance above". At the bottom of the page, there are links for Privacy Policy and Terms of Use.

Once instance starts state is →running

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, 'Instances' is selected. The main table displays two instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
winserver	i-0a6e73f9535793e3	t2.micro	us-west-2b	running	2/2 checks ...	None
linuxvm	i-05ad951977dd8852	t2.micro	us-west-2b	running	2/2 checks ...	None

The 'winserver' instance is circled in red. Below the table, there are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Status Checks' tab is active, showing details for the 'winserver' instance.

To check instance details like

Description, Status check, Monitoring, Tags

This screenshot is identical to the one above, showing the AWS EC2 Instances page. The 'Description' tab is highlighted with a red circle. The table and instance details are the same as in the previous screenshot.

**2 a) To connect to “Windows instance” from Windows client operating system.**

Open Ec2 Dashboard Console

Go to instance

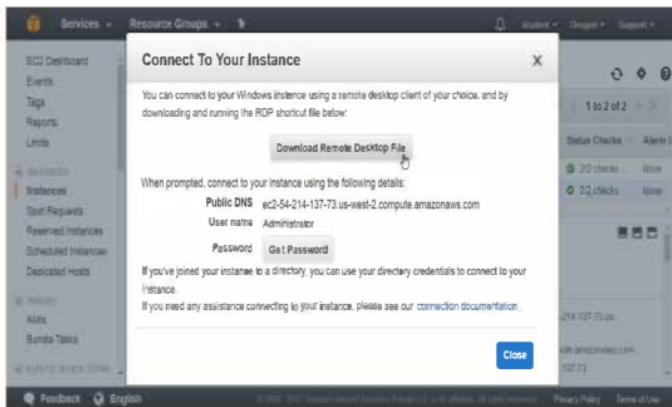
Select the instance you want to connect

Click **Connect** button

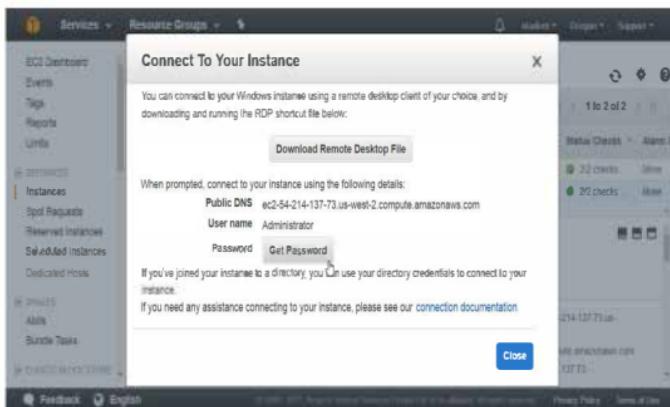
The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with links like Services, Resource Groups,学生 (student), Oregon, Support, EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected and highlighted in orange), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and Elastic Block Store. The main content area has tabs for Launch Instance, Connect (which is highlighted in blue), and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. There are two rows: "linuxvm" (Instance ID: i-05a80519778dd8852, Instance Type: t2.micro, AZ: us-west-2b, State: running, 2/2 checks, None) and "winserver" (Instance ID: i-0a6e73f953579363, Instance Type: t2.micro, AZ: us-west-2b, State: running, 2/2 checks, None). Below the table, it says "Instance: i-0a6e73f953579363 (winserver) Public DNS: ec2-54-214-137-73.us-west-2.compute.amazonaws.com". At the bottom, there are tabs for Description, Status Checks, Monitoring, and Tags. Under Status Checks, it shows "Instance ID: i-0a6e73f953579363" and "Public DNS (IPv4): ec2-54-214-137-73.us-west-2.compute.amazonaws.com". Under Monitoring, it shows "Instance state: running" and "IPv4 Public IP: 54.214.137.73". At the very bottom, there are links for Feedback, English, Copyright notice (© 2008–2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

On "Connect To Your Instance" page, see the guide lines to connect to Windows instance.

Click on "Download Remote Desktop file" button



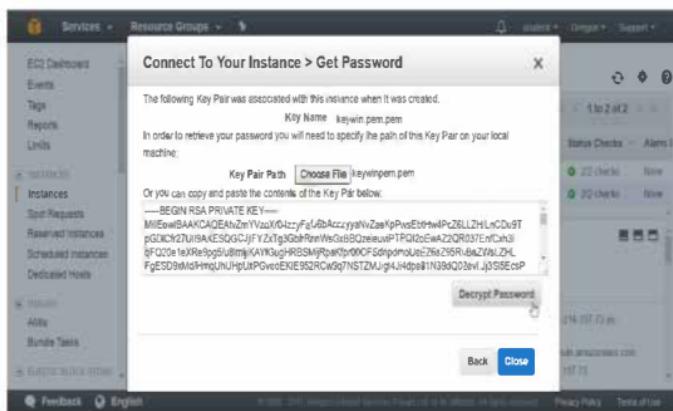
Click on "Get Password" button



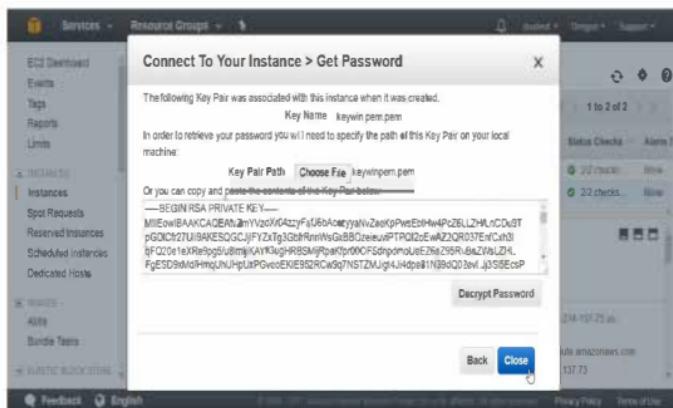
Click on "Choose file" button

Provide the path of key file

Click on "Decrypt Password" button



Click on Close button



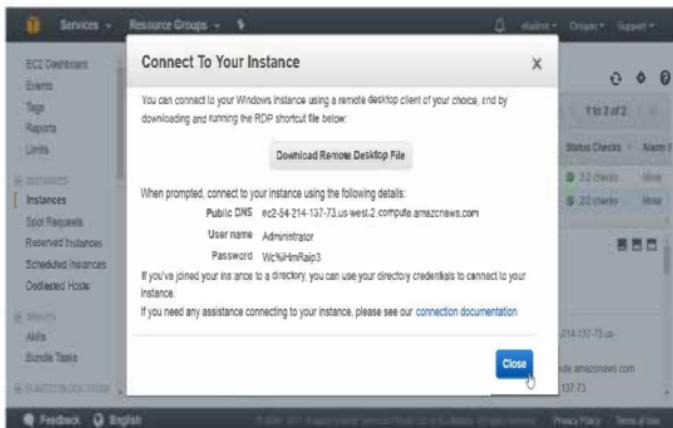
**Copy your instance Detail in Notepad**

Public DNS      ec2-54-213-234-57.us-west-2.compute.amazonaws.com

User name      Administrator

Password      \*\*\*\*\*

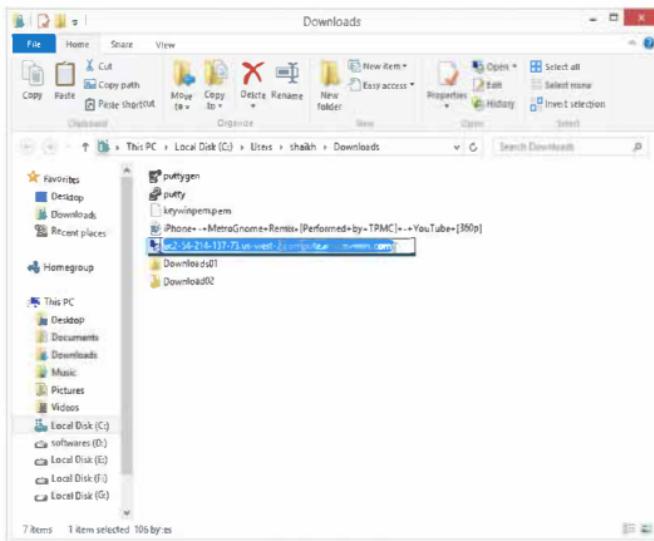
Click on **Close** button.



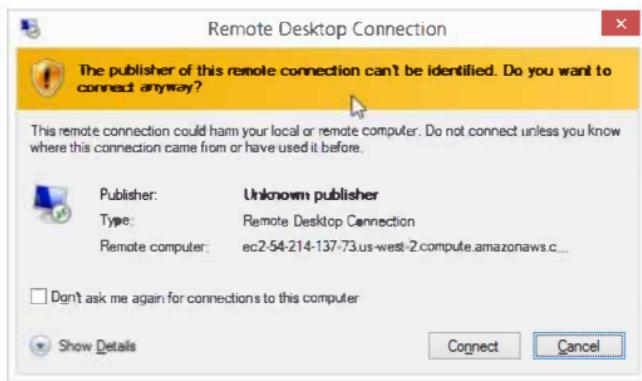
3) Now you can login to Amazon Windows instance

Double click on downloaded RDP file

Provide username as Administrator and give Password.



Click on connect



Provide username Administrator and Password

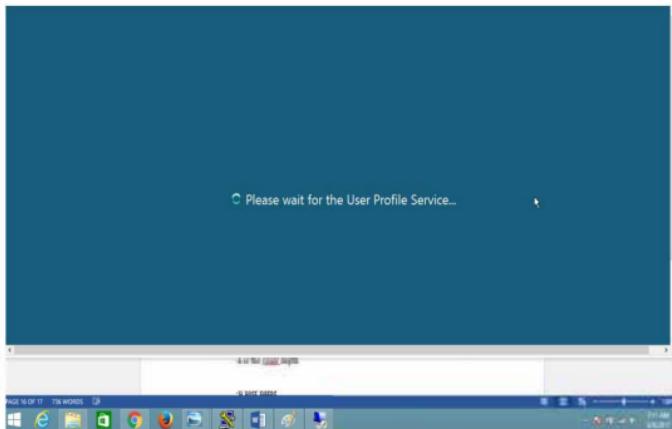
Click on OK



Click on Yes button



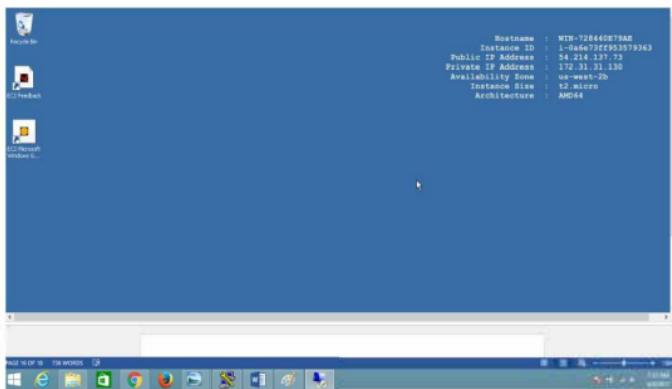
Wait for a movement



## Verify

Successfully Logged in to windows instance

Check Public and Private IP of Windows instance



2b) To connect to your Windows instance using Linux client operating system.

Login to Linux client operating system

Open linux terminal

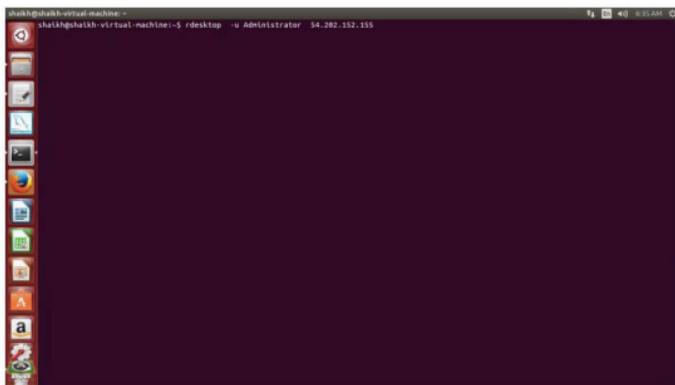
**Note: rdesktop or xfreerdp { RHEL-6,7 } package should be installed**

\$ rdesktop -u Administrator <Pub\_DNS\_name / Public\_IP>

OR

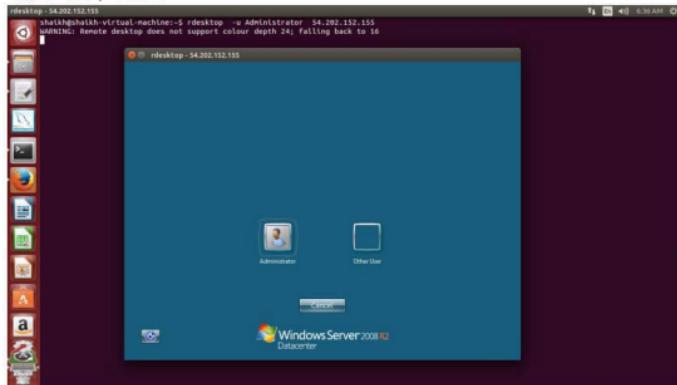
\$ xfreerdp -u Administrator <Pub\_DNS\_name / Public\_IP> { in RHEL 6,7 }

-u → user name



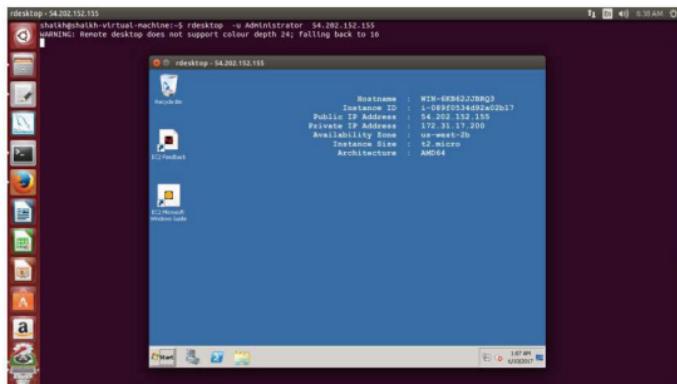
Click on Administrator

Provide the password



Verify:

Once Logged in Windows Desktop is available



Note:

If you are not going to use the instance, terminate the instance

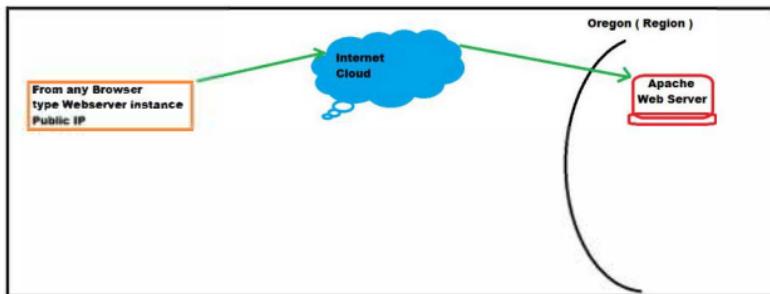
Otherwise it will be charged if the limit is over after free tier usage.

## Lab 3: To Configure Webserver on Amazon Linux instance with Elastic IP

### OBJECTIVE

To configure Webserver and to verify using Elastic public IP

### TOPOLOGY



### PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

### TASK :

- Launch linux instance in AWS
- Switch to root user
- Configure Apache Webserver
- Enable HTTP port in security Group
- Open the browser and provide public IP or DNS\_name of Webserver
- Assign an Elastic IP
- Releasing an Elastic IP

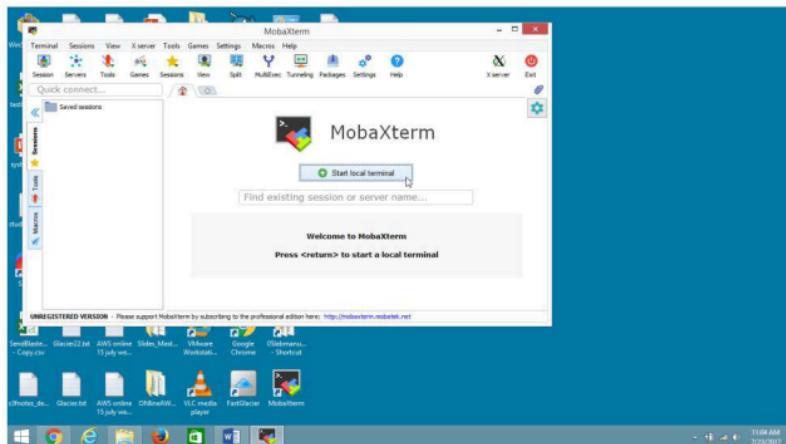
**1) Launch Amazon linux instance and login to your instance**

Refer to **Lab** [ How to configure amazon linux instance ]

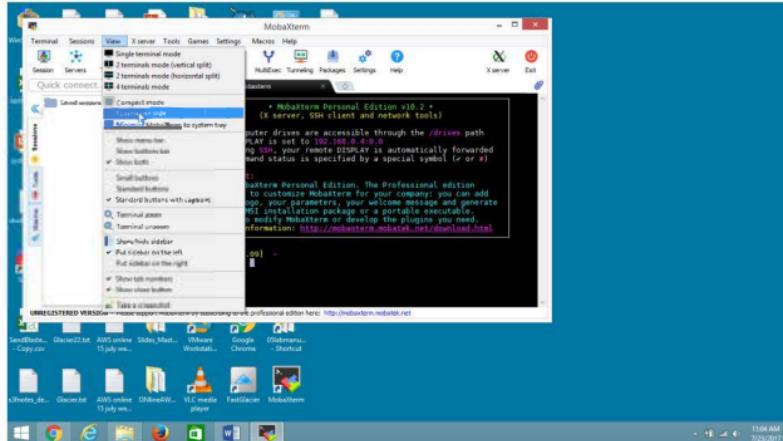
**2) Connect to linux instance from windows using MobaXterm**

Open **MobaXterm**

Click on **Start local terminal**



## Go to Full Screen mode



Navigate to the folder where key\*.pem file is stored

Eg : cd e:/awskeys

```
* MobaXterm Personal Edition v10.2 *
* EX server, SSH client and network tools*
Outer drives are accessible through the /drives path
When using SSH, your remote DISPLAY is automatically forwarded
Each command status is specified by a special symbol (> or #)

> ls
MobaXterm Personal Edition. The Professional edition
allows you to customize MobaXterm for your company: you can add
your logo, your parameters, your welcome message and generate
SSH keys. You can also install MobaXterm on a local machine and
modify MobaXterm or develop the plugins you need.
For more information: http://mobaxterm.mobatek.net/download.aspx

[15/07/2017 11:08:48] - [shashik-pc_msi] - cd e:/awskeys
```

Login to linux instance by typing the following command

```
ssh -i "keyorg123.pem" ec2-user@ec2-54-186-150-140.us-west-2.compute.amazonaws.com
```

```
[2017-07-23 09:34:47]  /drives/e/awskeys
[shaikh.pc_mas] > ssh -i "keyorg123.pem" ec2-user@ec2-54-186-150-140.us-west-2.compute.amazonaws
.com
Warning: Permanently added 'ec2-54-186-150-140.us-west-2.compute.amazonaws.com' (RSA) to the lis
t of known hosts.
X11 forwarding request failed on channel 0

 _|_(_|-_) Amazon Linux AMI
 _\|_\_|_|
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-10-246 ~]$
```

Switch to root user

Type “sudo su”

```
[ec2-user@ip-172-31-10-246 ~]$ sudo su
[root@ip-172-31-10-246 ec2-user]#
```

## **Configure Apache Webserver run following commands as shown in the screen**

```
[root@ip-172-31-10-246 ec2-user]# yum install httpd -y  
[root@ip-172-31-10-246 ec2-user]# chkconfig httpd on  
[root@ip-172-31-10-246 ec2-user]# service httpd restart  
[root@ip-172-31-10-246 ec2-user]# vi /var/www/html/index.html
```

### **To use vi editor**

Go to insert mode by typing 'i' and add following code in index.html file

Note: [ esc+shift+colon → :wq! (to save and quit in Vi editor) ]

```
<html>  
<body bgcolor=black>  
<marquee>  
    <font color=gold>  
        <h1> Welcome to Apache Webserver in AWS instance </h1>  
    </font>  
</marquee>  
</body>  
</html>  
  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
:  
:wq!
```

### 3) Create an inbound Rule to Allow http traffic on port 80.

Open the AWS console

On the **EC2 Dashboard** panel

Select the linux instance

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with navigation links like Services, Resource Groups, Events, Tags, Reports, and Links. Under Instances, it lists Sustained Instances, Reserved Instances, Scheduled Instances, and Dedicated Hosts. Below that, it lists Alarms, Alerts, and Bundled Tools. Under ELASTIC BLOCK STORE, it lists Volumes and Snapshots. The main content area is titled 'Instances' and shows a table with one row. The table columns are Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS. The instance listed is named 'Linuxwebserver', has an ID of i-09e8a71e3ce9a9561, is a t2.micro type, in us-west-2c, and is running. It has 2/2 checks and no alarms. Its Public DNS is ec2-54-186-140-140.us-west-2.compute.amazonaws.com and its Public IP is 54.186.140.140. The status bar at the bottom indicates the browser is using Google Chrome Version 77.0.3865.120 (Official Build) (64-bit).

Go to the right end

## Select Security Groups

### Click on launch-wizard-1

The screenshot shows the AWS EC2 Management Console. The left sidebar includes links for EC2 Dashboard, Events, Tag, Reports, Limits, Instances (with sub-links for Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), and various storage options like S3, Lambda, CloudWatch Metrics, CloudWatch Logs, Volumes, and Snapshots. The main content area is titled "Resource Groups" and shows a table of instances. One instance, "i-09e8a71e3ce9a9561 (Linuxwebserver)", is selected. Below the table, a detailed view of this instance is shown, including its description ("Instance ID: i-09e8a71e3ce9a9561", "Public DNS (IPv4): ec2-54-186-150-140.us-west-2.compute.amazonaws.com", "Public IP: 54.186.150.140", "Status: running", "Type: t2.micro", "Launch Time: July 25, 2017 at 9:28:59 AM"), monitoring details, and tags. At the bottom of the page, there are links for "Create New Security Group", "Inbound", "Outbound", and "Tags". The status bar at the bottom indicates "AWS Lab Manual" and "Page 1 of 1".

### Click on Inbound button

The screenshot shows the "Create Security Group" page. The left sidebar is identical to the previous screenshot. The main content area has a title "Create Security Group" and a search bar. It lists two existing security groups: "sg-6ab60510" and "launch-wizard-1". Below this, a "Security Group: sg-6ab60510" is displayed with tabs for "Inbound", "Outbound", and "Tags". The "Inbound" tab is selected. It shows a table with one rule: "Group Name: launch-wizard-1", "Group ID: sg-6ab60510", "Source: 0.0.0.0/0", "Port Range: 22", and "Protocol: TCP". At the bottom, there are buttons for "Save" and "Cancel". The status bar at the bottom indicates "AWS Lab Manual" and "Page 1 of 1".

**Click on Edit button**

The screenshot shows the AWS EC2 Management Console. The left sidebar has 'EC2 Dashboard' selected. Under 'Instances', 'Launch Wizard' is highlighted. The main content area shows a table for a security group named 'sg-4ab00510'. The 'Inbound' tab is selected. A row in the table has a 'Edit' button highlighted with a red box. The table columns are 'Name', 'Group ID', 'Group Name', 'VPC ID', and 'Description'. The row details are 'sg-4ab00510', 'sg-4ab00510', 'Launch Wizard-1', 'vpc-8fc34f8e', and 'Launch Wizard-1 Created 2017-07-23T08:23'. Below the table, there are tabs for 'Description', 'Inbound', 'Outbound', and 'Tags'. The status bar at the bottom shows 'Feedback English' and the URL 'https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#SecurityGroupsSearch=sig-4ab00510sort+groupid'.

**Click on Add Rule button**

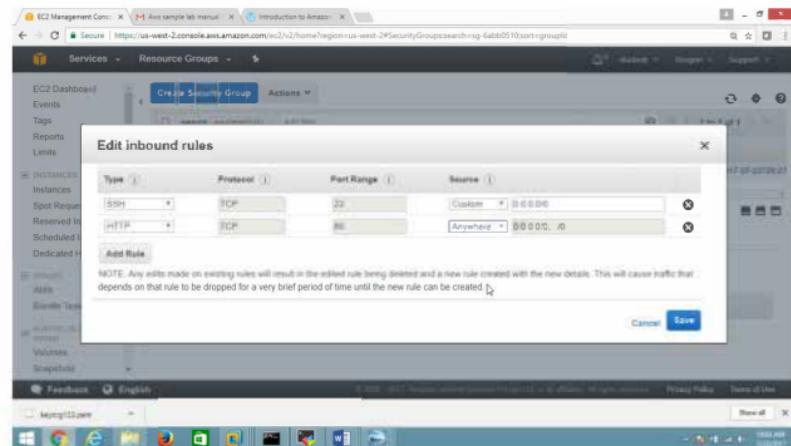
The screenshot shows the AWS EC2 Management Console with the 'Edit inbound rules' dialog open. The dialog has fields for 'Type' (SSH), 'Protocol' (TCP), 'Port Range' (22), and 'Source' (Custom, 0.0.0.0). A red box highlights the 'Add Rule' button. A note below the form states: 'NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.' At the bottom right of the dialog are 'Cancel' and 'Save' buttons. The background shows the EC2 dashboard with 'Launch Wizard' selected in the sidebar.

## Add HTTP Rule

Under **Type** column select **HTTP**

Under **Source** column select **Anywhere**

Click Save button



**4) Open Browser and provide Webserver instance DNS\_name or Public IP**

The screenshot shows the AWS EC2 Management Console. On the left, the navigation pane is open with 'Instances' selected. In the main content area, an instance named 'UbuntuServer...' is selected. The instance details panel shows the following information:

Instance ID	Public DNS (IPv4)
i-09e8a71e3ce9a9561	ec2-54-198-150-140.us-west-2.compute.amazonaws.com

Below this, a screenshot of a web browser window is displayed, showing the Apache welcome page with the text "Welcome to Apache Webserver in AWS instance".

**Verify**

Website is running



## Lab 4: To Assign Elastic IP address

### Elastic IP

**Note:** Since public IP given by AWS is not permanent, if the instance is stopped or started again, existing public IP is released by the instance, in this case users across internet again cannot visit the same website, so to have permanent Public IP, assign Elastic IP,

**Note:** If your instance is terminated or not in use, and **Elastice IP** is not released then in this case it will be charged, so be careful if you are using and running under free tier usage.

Best practise is launch an instance assign Elastic IP, and before terminating release Elastic IP then terminate the instances.

## To assigning Elastic IP to an instance

Open AWS console

On the **EC2 Dashboard** panel

Select "**Network Security**"

Click on **Elastic IP**

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links: Services (selected), Resource Groups, Network & Security, Security Groups, Basic IPs (highlighted), Placement Groups, Key Pairs, Network Interfaces, Load Balancing, Load Balancers, Target Groups, Auto Scaling, Launch Configurations, Auto Scaling Groups, Systems Manager, and Services. The main content area is titled "Instances" and shows a table with one row. The table columns are Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status Checks. The data row is for an instance named "Linuxwebserver" with Instance ID i-09e8a71e3ce9a9561, Type t2.micro, in us-west-2c, running, and 2/2 status checks. Below the table, there's a "Description" tab selected, followed by Status Checks, Monitoring, and Tags tabs. At the bottom of the page, there are links for Privacy Policy and Terms of Use, along with a timestamp of 11:45 AM 7/23/2017.

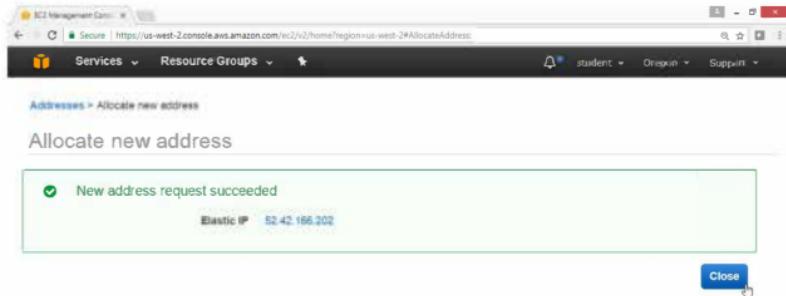
Click on Allocate new address button

The screenshot shows the AWS EC2 Management Console. The left sidebar has sections for Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups), Auto Scaling (Launch Configurations, Auto Scaling Groups), and Systems Manager Services. The 'Elastic IPs' section is currently selected. The main content area has a message: 'You don't have any Addresses in this region'. Below it is a button labeled 'Allocate new address'. The status bar at the bottom shows the URL as https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Addressessort=Public, and the date/time as 11:45 AM 7/23/2017.

Click **Allocate** button

This screenshot shows a modal dialog box titled 'Allocate new address'. It contains a single input field with the placeholder text 'Allocate a new Elastic IP address by selecting the scope in which it will be used'. To the left of the input field is a small asterisk (\*) followed by the word 'Required'. On the right side of the dialog are two buttons: 'Cancel' and 'Allocate'. The 'Allocate' button is highlighted with a red box. The status bar at the bottom shows the URL as https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#AllocateAddress, and the date/time as 11:45 AM 7/23/2017.

Click on Close button



Open your Browser and provide your instance DNS name or Elastic Public Ip

Verify website is running with elastic IP.



## To releasing Elastic IP

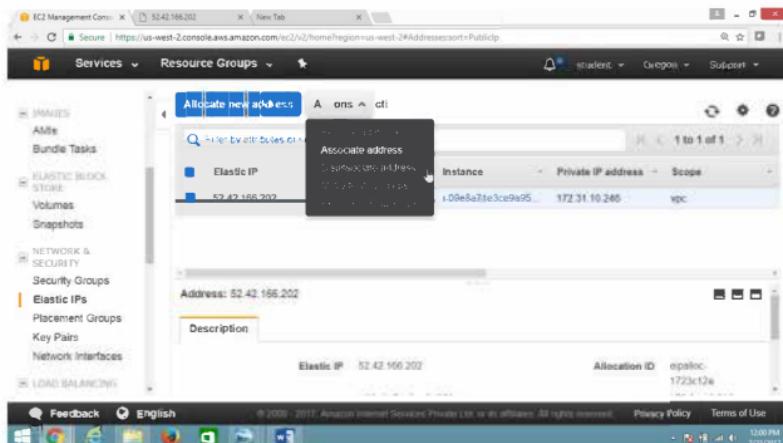
Open the console **EC2 Dashboard**

Expand "Network Security"

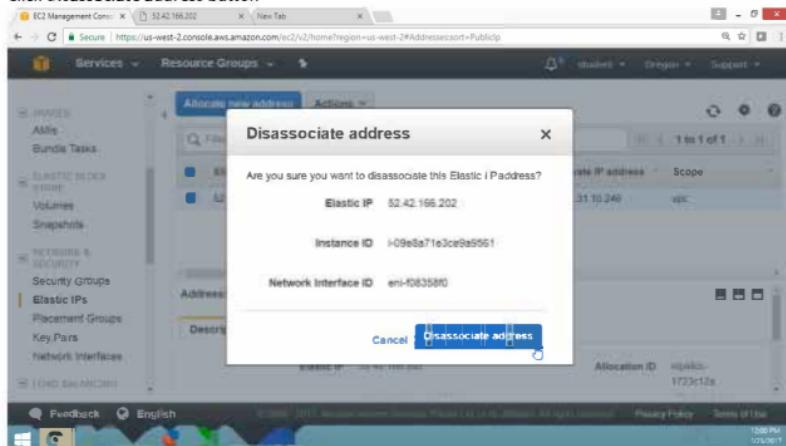
Select **Elastic IP**

Click **Action** button

Select **Disassociate Address**

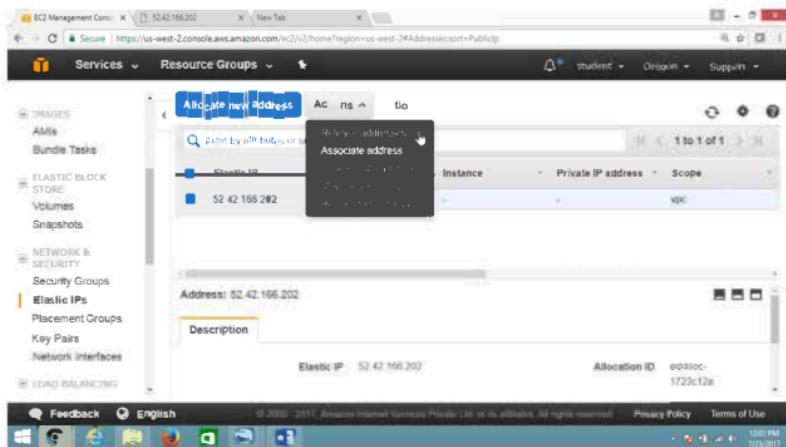


### Click Disassociate address button

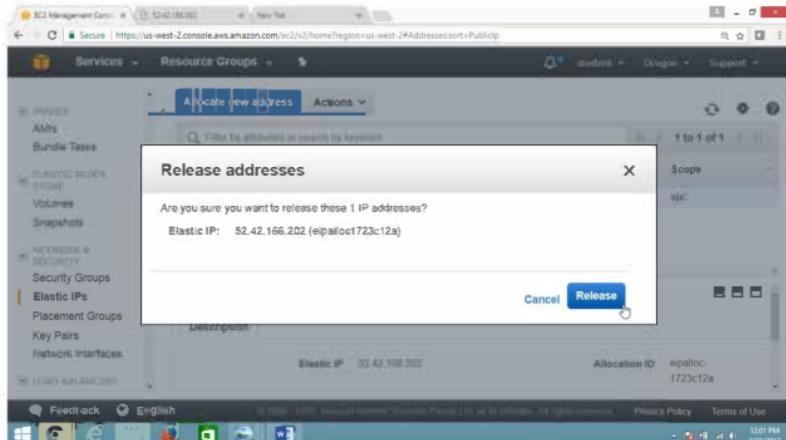


### Click Action button

#### Select Release Addresses



**Click Release button**



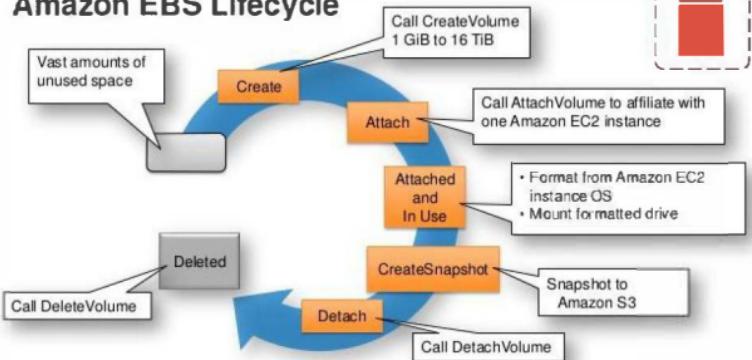
## Lab 5: To Manage Elastic Block Store (EBS)

### OBJECTIVE

To configure and use AWS EBS service

### TOPOLOGY

#### Amazon EBS Lifecycle



© 2010, Amazon Web Services Inc. or its Affiliates. All rights reserved.



### PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

User should have basic knowledge of managing partitions in Windows or Linux

### To Configure EBS With following task:

Create EBS Volume

Attaching and Detaching EBS volume.

Expanding the size of EBS volume.

Taking the snapshot of EBS volume.

## 1. To create an EBS volume

Open the Amazon console

Select **Compute**, choose **EC2** service

On the **EC2 Dashboard** panel

Choose "**ELASTIC BLOCK STORE**" click on **Volumes**

The screenshot shows the AWS EC2 Dashboard. On the left sidebar, under the "VOLUNTEERS" section, the "Volumes" option is selected. The main content area displays the following statistics:

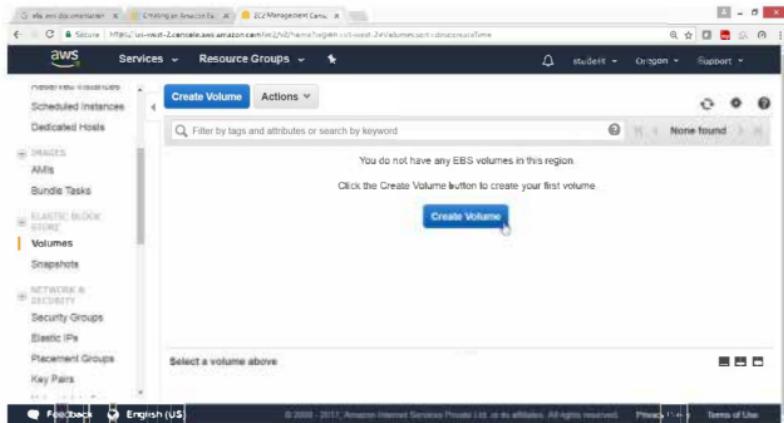
0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

Below these stats is a callout box with the text: "Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking - for a low, predictable price. Try Amazon Lightsail for free."

Under the "Create Instance" heading, there is a "Launch Instance" button. A note below it says: "Note: Your instances will launch in the US West (Oregon) region."

On the right side, there are sections for "Account Attributes" (listing Supported Platforms, VPC, Default VPC, and Resource ID length management), "Additional Information" (listing Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, and Contact Us), and "AWS Marketplace" (listing Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard. Or try these popular AMIs).

Click on Create Volumes button



**In the Create Volume dialog box,**

- Volume Type → General Purpose SSD (GP2)
- Size (GiB) → 2 GiB
- IOPS → 100 / 3000
- Throughput (MB/s) → Not Applicable
- Availability Zone → us-west-2a (as per your requirement)

Leave remaining as defaults.

Click on **Create Volume** button

The screenshot shows the 'Create Volume' dialog box on the AWS Management Console. The form fields are as follows:

- Volume Type:** General Purpose SSD (GP2)
- Size (GiB):** 2 (Min: 1 GiB, Max: 16384 GiB)
- IOPS:** 100 / 3000 (Baseline of 3 IOPS/GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Availability Zone:** us-west-2a
- Throughput (MB/s):** Not applicable
- Snapshot ID:** Select a snapshot
- Encryption:**  Encrypt this volume

Below the form, there is a 'Tags' section with a note to 'Add tags to your volume' and a 'Required' indicator. At the bottom right, there are 'Cancel' and 'Create Volume' buttons, with 'Create Volume' being highlighted.

## Verify Volume successfully created

Click **Close** button

The screenshot shows the AWS EC2 Management Console with the URL [https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2/CreateVolume](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2>CreateVolume). The page title is "Volumes > Create Volume". A green success message box contains the text "Volume created successfully" and the Volume ID "vol-0d04089fc711acee". A blue "Close" button is visible at the bottom right of the message box.

## To Monitoring the State of Your Volumes

Select Volume check state → available

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/volumes?sort=discCreateTime>. The page title is "Volumes". A table lists a single volume:

Name	Volume ID	Size	Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
	vol-08ba155bd2df3ccbc	2.00E	SSD	100 / 3000		November 16, 2017	us-west-2a	available	None

The volume is listed with the ID "vol-08ba155bd2df3ccbc", size "2.00E", type "SSD", IOPS "100 / 3000", and state "available". The "Actions" dropdown menu for this volume includes options: "Delete", "Reboot", "Mount", "Unmount", "Clone", "Copy", "Create Snapshot", and "Create Volume Copy".

In the Name column give name for your volume → 2gb2a

The screenshot shows the AWS EC2 Management Console with the 'Create Volume' tab selected. A search bar at the top right contains the text 'Filter by tags and attributes or search by keyword'. Below it is a table with the following columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, and Status. One row is visible in the table:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	Status
2gb2a	vol-08ba155bd2df3cbcc	20 GB	gp2	100 - 3000	snap-040321...	November 10, 2017...	us-west-2a	available

Below the table, there is a message: 'Volumes: vol-08ba155bd2df3cbcc'. At the bottom of the page, there are tabs for Feedback, English (US), and links to AWS Support, Privacy Policy, and Terms of Use.

## 2) To Attaching and Detaching EBS volume in Windows instance

On the EC2 Dashboard panel

Choose "ELASTIC BLOCK STORE" click on Volume

Note : The volume which you want to attach to an instance should be in same Availability zone.

Drop Down Action button,

Select Attach Volume.

Volume Type	ID/PN	Snapshot	Created	Availability Zone	State
gp2	100 / 3000	snap-04240000	November 10, 2017	us-west-2a	available
gp2	100 / 3000	snap-044d21f1	November 10, 2017	us-west-2a	available
gp2	100 / 3000	snap-044d21f1	November 10, 2017	us-west-2a	available

Select instance → Winvm1

The screenshot shows the AWS Management Console with the 'Volumes' section selected in the sidebar. A modal dialog box titled 'Attach Volume' is open. Inside the dialog, a dropdown menu is displayed under the 'Device' field, listing two options: 'i-0515c735f8fb0a071 (Winvm1) (running)' and 'i-04bd24ef0afeed12 (winvm2) (running)'. The 'Attach' button is located at the bottom right of the dialog.

Click on Attach

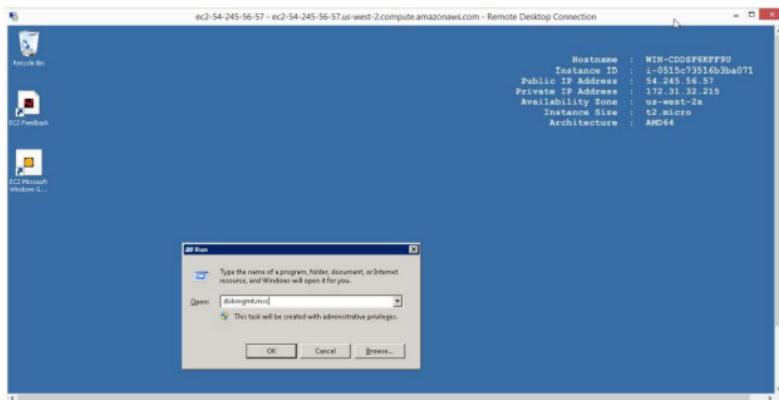
The screenshot shows the same AWS Management Console interface as the previous one, but the dropdown menu in the 'Device' field has been closed. The 'Device' field now contains the value 'xvdf'. The 'Attach' button remains at the bottom right of the dialog.

Verify the Availability of new volume

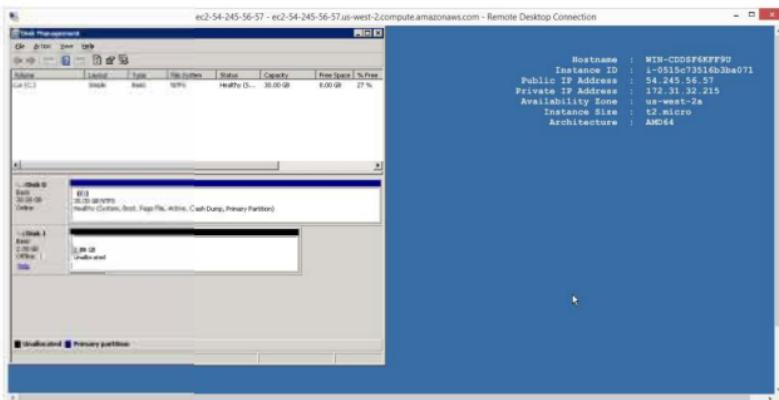
### 3. To check availability of new drive login to your Windows instance.

Login to windows instance

Run → diskmgmt.msc

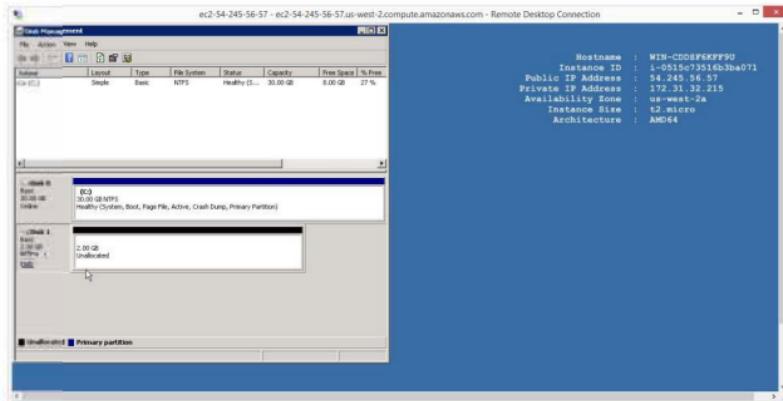


Verifies that 2 GB volume available as unallocated space

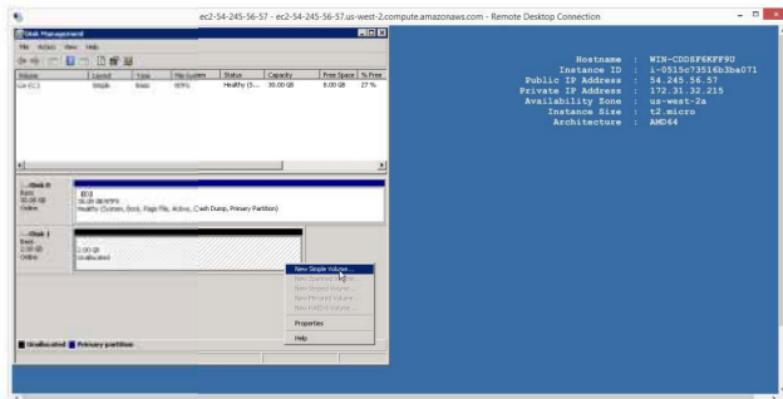


New disk is offline,

So turn it to online by right clicking and select online

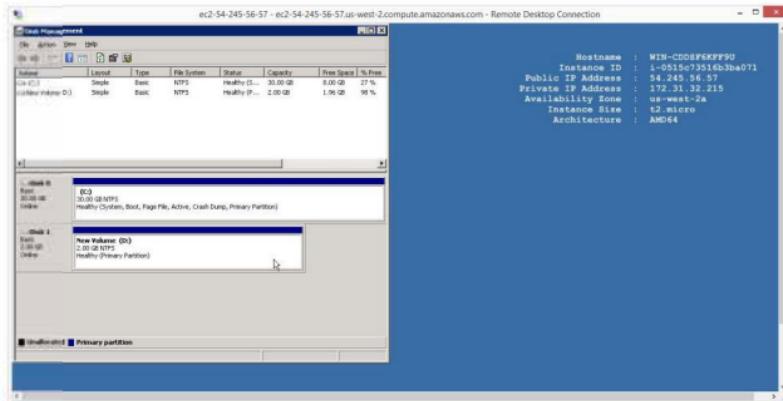


Format the unallocated disk



## Verify

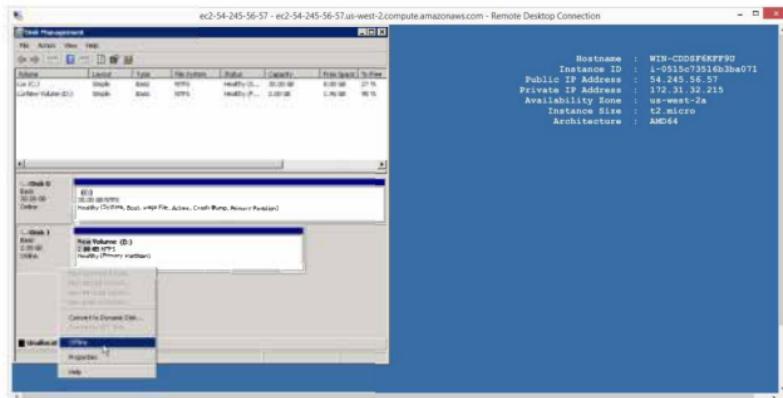
New Volume to 2GB is available to use



## 4. To Detach the volume

In Windows Select Disk 1

Right click select offline



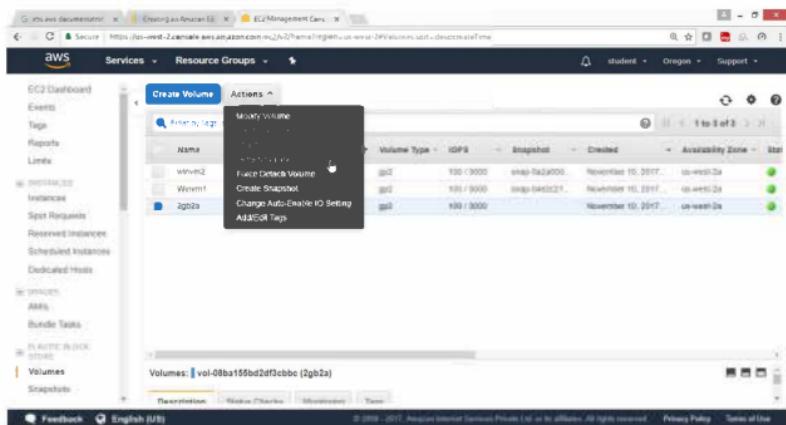
On the EC2 Dashboard panel

Choose "ELASTIC BLOCK STORE" click on Volumes

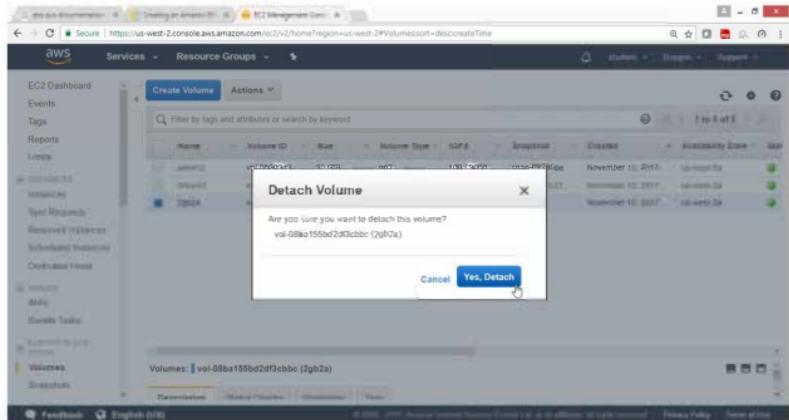
Select volume to be detached under Name column.

Drop Down Action button

Select "Detach Volume"



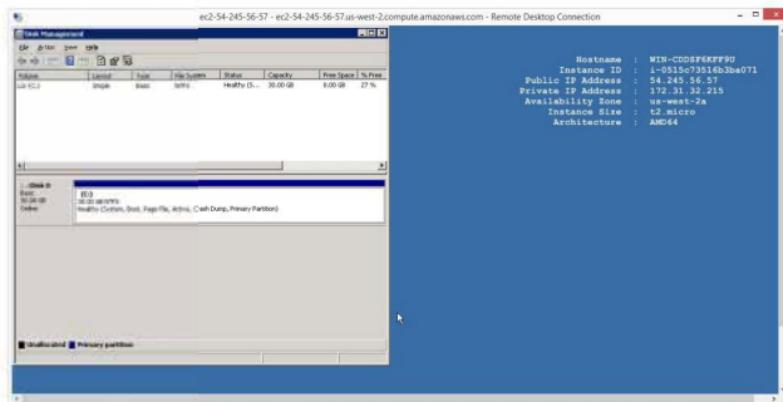
Click on "Yes, Detach" button



## Verification

Login to windows instance

Check that D: drive is removed

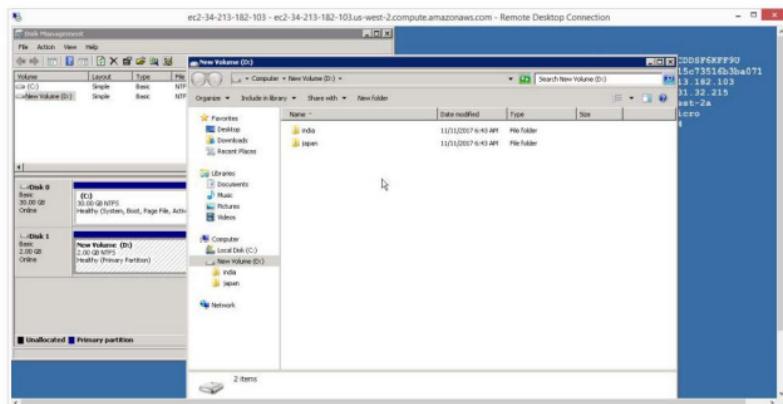


## 5. To Create Snapshot and Restore EBS volume.

### To create a snapshot

In the current D drive two folders are available

No create a snapshot of this volume



On the EC2 Dashboard panel

Click on “**ELASTIC BLOCK STORE**”, choose Volumes.

Drop down **Action** button select Create snapshot

The screenshot shows the AWS EC2 Management Console. On the left, the navigation pane is visible with sections like Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and Elastic Block Store (selected). Under EBS, there are options for Volumes and Snapshots. The main area displays a list of volumes: gp2, 100 / 3000, snap.08ba155...; gp2, 100 / 3000, snap.0fe2c21...; and gp2, 100 / 3000, snap.110... . A context menu is open over the first volume, with "Create Snapshot" highlighted. At the bottom, there's a "Create Snapshot" button.

Provide snapshot details

Click **Create** button

The dialog box is titled "Create Snapshot". It contains the following fields:

- Volume: vol-08ba155bd2df3cbcc (2gb2a)
- Name: snapvol1
- Description: snapvol1\_des
- Encrypted: No

At the bottom right are "Cancel" and "Create" buttons.

Verify that snapshot is created.

The screenshot shows the AWS Management Console with the EC2 Management Console selected. In the left sidebar, under the 'VOLUME' section, 'Snapshots' is highlighted. The main area displays a table titled 'Create Snapshot' with one item listed:

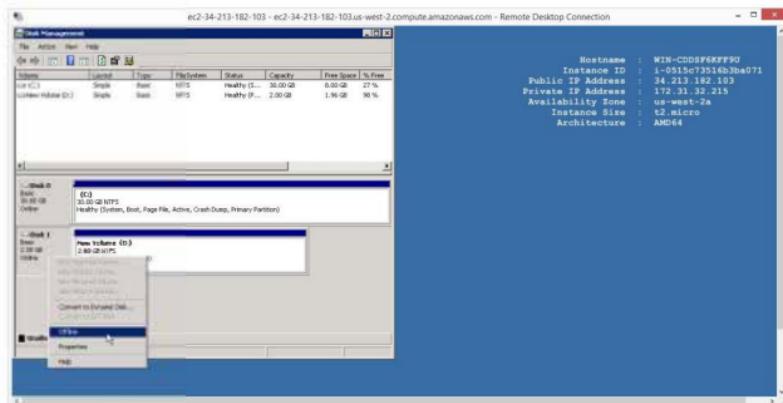
Name	Snapshot ID	Size	Description	Status
snapvol1	snap-0ff48c35456...	2 GiB	snapshot_des	Completed

Below the table, a detailed view of the snapshot is shown with tabs for 'Description', 'Permissions', and 'Tags'. The 'Description' tab contains the text: 'Snapshot: snap-0ff48c354563cba0 ( snapvol1 )'. To the right of the description, there are several small icons for managing the snapshot.

## 6) To Delete the volume.

First select the disk 1 from Disk Management

Right click select offline



On the EC2 Dashboard panel

Expand “**ELASTIC BLOCK STORE**”, choose Volumes.

Select volume to be detached under the Name column.

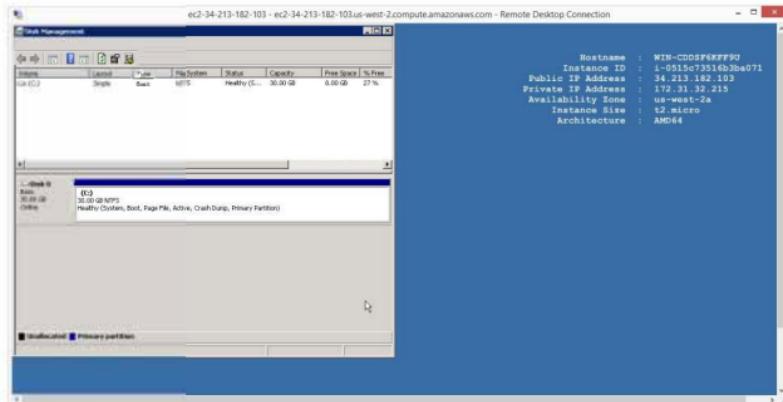
Drop Down Action button, Select “**Delete Volume**”

The screenshot shows the AWS EC2 Management Console. On the left, the navigation pane is open, showing various services like Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and **Volumes**, which is currently selected. The main content area displays a list of volumes. A context menu is open over a volume named "2gb2a". The menu is titled "Modify Volume" and includes options: Delete Volume, Attach Volume, Detach Volume (which is highlighted with a cursor), Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. Below the menu, the volume list shows three entries:

Volume Type	IOPS	Snapshot	Created
gp2	100 / 30000	snap.0e2d0ff...	November 19, 2017
gp2	100 / 30000	snap.0e9c21...	November 19, 2017
gp2	100 / 30000		November 19, 2017

Verify from windows instance open disk Management tool

Now D drive is detached



Now delete the volume

A screenshot of the AWS Management Console. The left sidebar shows 'ELASTIC BLOCK STORE' with 'Volumes' selected. In the main area, a table lists three volumes: 'g02' (100 / 3000), 'g02' (100 / 3000), and '20g2a' (100 / 3000). A context menu is open over the '20g2a' volume, with 'Delete Volume' highlighted. The top navigation bar shows 'student' and 'Create New'.

## Verify volume is deleted.

The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar navigation bar includes links for Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, Elastic Block Store, Volumes (which is the selected category), and Snapshots. Under the Volumes section, there are links for Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. At the bottom of the sidebar, there are Feedback, Language (English (US)), and Help links.

The main content area displays a table titled "Create Volume" with the heading "Actions". A search bar at the top of the table says "Filter by tags and attributes or search by keyword". The table has columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, and Created. There are two entries:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
winm2	vol-0f0004d1	30 GiB	gp2	100 / 3000	snap-0a0e00d4	November 10, 2017
Winm1	vol-0b2690e0	30 GiB	gp2	100 / 3000	snap-0a4e2c21	November 10, 2017

Below the table, a message says "Select a volume above". At the bottom right of the table area, there are three small icons: a magnifying glass, a trash can, and a refresh symbol.

## **7. To Restore the volume.**

From the console **EC2 Dashboard**

Expand “**ELASTIC BLOCK STORE**”, choose **Snapshots**

Select the snapshot

Drop Down Action button, Select **Create Volume**

The screenshot shows the AWS Management Console interface for the EC2 Dashboard. On the left, there's a sidebar with various service links like Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and others under ELASTIC BLOCK STORE. The 'Snapshots' link is highlighted. In the main content area, a list of snapshots is shown, with one named 'snapvoilt\_des' selected. A context menu is open over this snapshot, with the 'Create Volume' option highlighted. Below the menu, a detailed view of the selected snapshot is displayed, showing its ID as 'snap-08ff48c354563cba0', its name as 'snapvoilt\_des', its size as '2 GB', and its status as 'available'. There are tabs for 'Description', 'Permissions', and 'Tags'.

Accept the defaults values in wizard

Note: Check the right availability zone.

The screenshot shows the 'Create Volume' wizard on the AWS Management Console. The configuration is as follows:

- Snapshot ID:** snap-08ff48c354563cba0 (snapvol1)
- Volume Type:** General Purpose SSD (GP2)
- Size (GiB):** 2 (Min: 1 GiB, Max: 16384 GiB)
- IOPS:** 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Availability Zone:** us-west-2a
- Throughput (MB/s):** Not applicable.
- Encryption:** Not Encrypted
- Tags:** Add tags to your volume

\* Required

Cancel **Create Volume**

Feedback English (US) © 2006 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Verify Volume is created

The screenshot shows the 'Create Volume' page with the 'Actions' tab selected. It lists three volumes:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
wlmw1	vol-0cd5da3c	2 GiB	gp2	100 / 3000	snap-09ff48c3	November 11, 2017
wlmw2	vol-0f0038e1	30 GiB	gp2	100 / 3000	snap-0a2e00d1	November 10, 2017
wlmw3	vol-0f298081	30 GiB	gp2	100 / 3000	snap-04e2c211	November 10, 2017

Volumes: vol-0cd5da3c73f3a3881

Dashboard Status Checks Monitoring Tags

Feedback English (US) © 2006 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

## 7) To expanding the size of EBS volume.

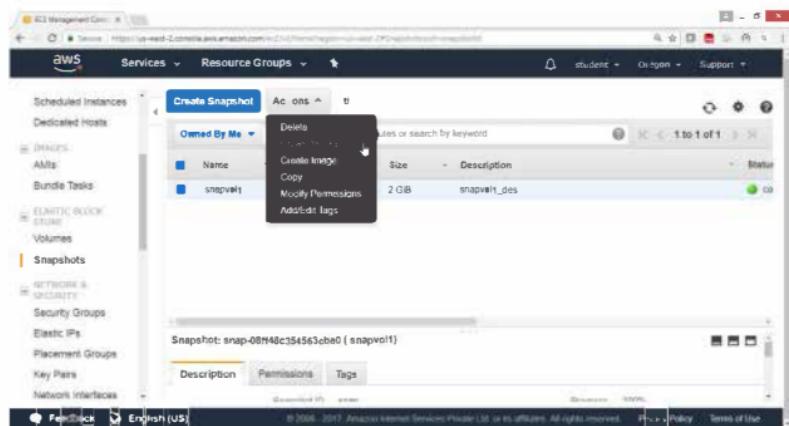
To expand EBS volume first take **snapshot**, now select the snapshot

On the **EC2 Dashboard** panel

Expand “**ELASTIC BLOCK STORE**”, choose Snapshots

Drop Down **Action** button

Select **Create Volume**



Give the required size → 4 GB

Check the right Availability Zone

click Create Volume button

The screenshot shows the 'Create Volume' step in the AWS Management Console. The configuration is as follows:

- Snapshot ID:** snap-08ff49c354563cba (snapvol1)
- Volume Type:** General Purpose SSD (GP2)
- Size (GiB):** 4 (Min: 1 GiB, Max: 16384 GiB)
- IOPS:** 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Availability Zone:** us-west-2a
- Throughput (MB/s):** Not applicable
- Encryption:** Not Encrypted

At the bottom, there is a 'Tags' section with a link to 'Add tags to your volume'. A note indicates that the volume is \* Required. On the right, there are 'Cancel' and 'Create Volume' buttons.

Verify that 4 GB is created

The screenshot shows the 'Volumes' page in the AWS Management Console. The table lists the following volumes:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
vol-024d7f00	vol-024d7f00	4 GiB	gp2	100 / 3000	snap-09ff49c3...	November 11, 2017
winnm2	vol-0f00363...	20 GiB	gp2	100 / 3000	snap-09ff49c3...	November 11, 2017
Winnm1	vol-0f2001e...	30 GiB	gp2	100 / 3000	snap-0462121...	November 10, 2017

Now attach this expanded volume to your instance.

Volume Type	ID/PN	Snapshot	Created
gp2	100 / 3000	snap-08f4fc03	November 11, 2017
gp2	100 / 3000	snap-08f4fc03	November 11, 2017
gp2	100 / 3000	snap-0a2a2008	November 10, 2017
gp2	100 / 3000	snap-04ac2c21	November 10, 2017

Select instance

Attach Volume

Volume: vol-034d7007ffcef5949 in us-west-2a

Instance: Search instance ID or Name tag in us-west-2a

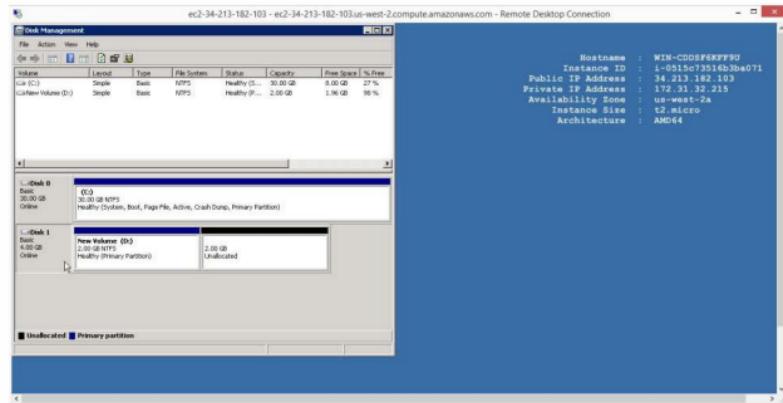
Device: i-0515c73516b3ba071 (winvm1) (running)  
i-04bd24ef0affeed12 (winvm2) (running)

Cancel Attach

Click **Attach** button

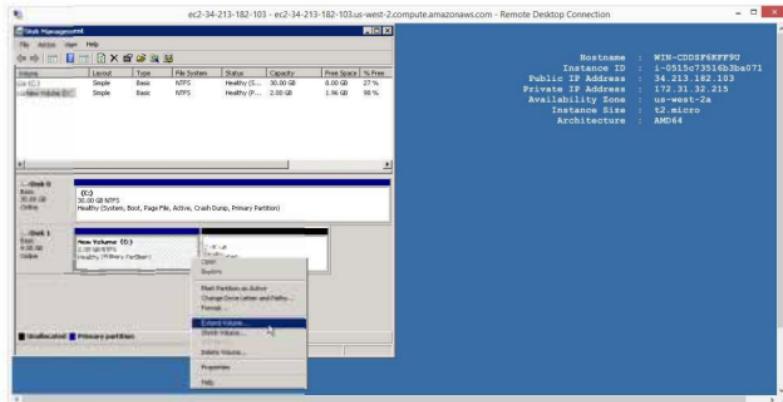


Verify 4 GB drive is available

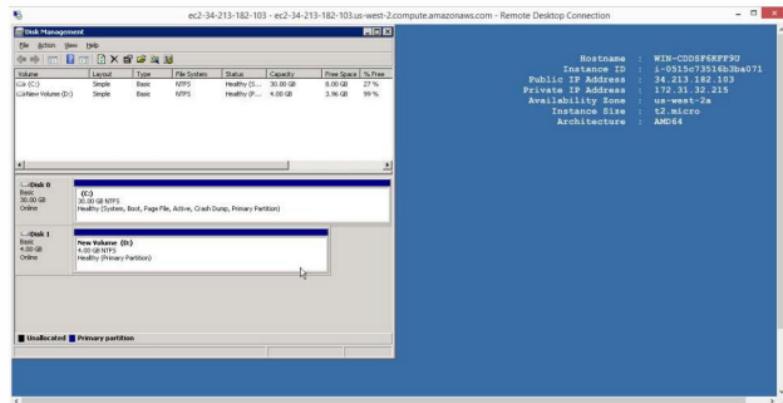


Now with respect to Windows operating system

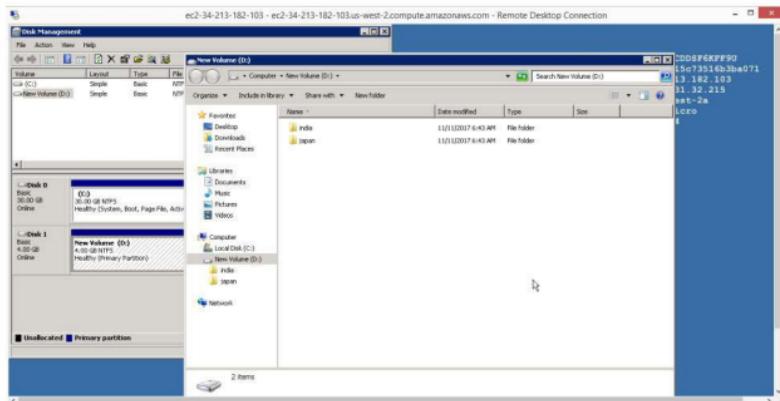
Right click on D drive extend your volume to your desired size



Verified that 4 GB volume available

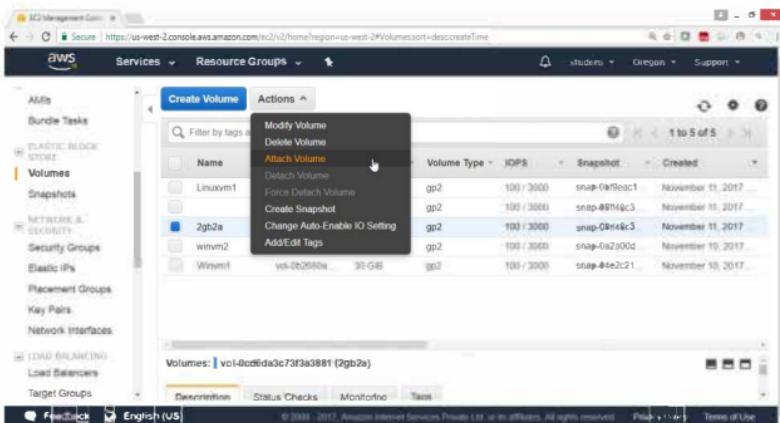


Verified that D drive contains two folders that was there in 2B drive earlier.

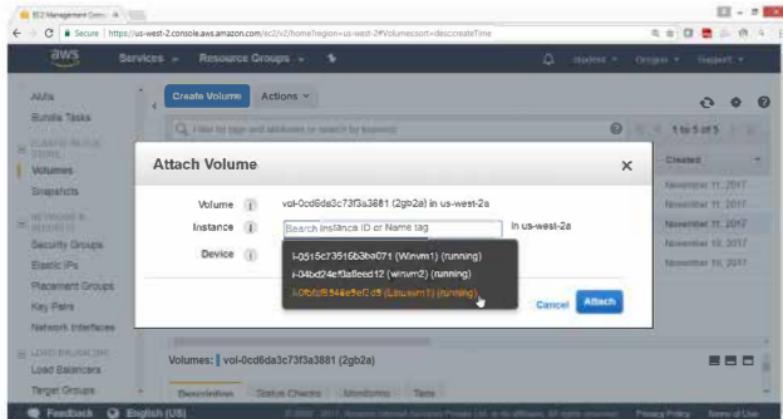


Similarly check volume in linux instance

From Action select Attach volume



## Select Linux instance



Now connect to Linux instance

```
[2017-11-11 12:58:46] /drives/e/awsskeys
[shaikh.pc_mas] > ssh -i "studentaws.pem" ec2-user@ec2-54-244-106-102.us-west-2.compute.amazonaws.com
X11 forwarding request failed on channel 0
Last login: Sat Nov 11 07:28:43 2017 from 49.206.203.114
```

Amazon Linux AMI

```
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
[ec2-user@ip-172-31-40-234 ~]$ sudo su
[root@ip-172-31-40-234 ec2-user]#
```

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]# 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 filesystem 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
```

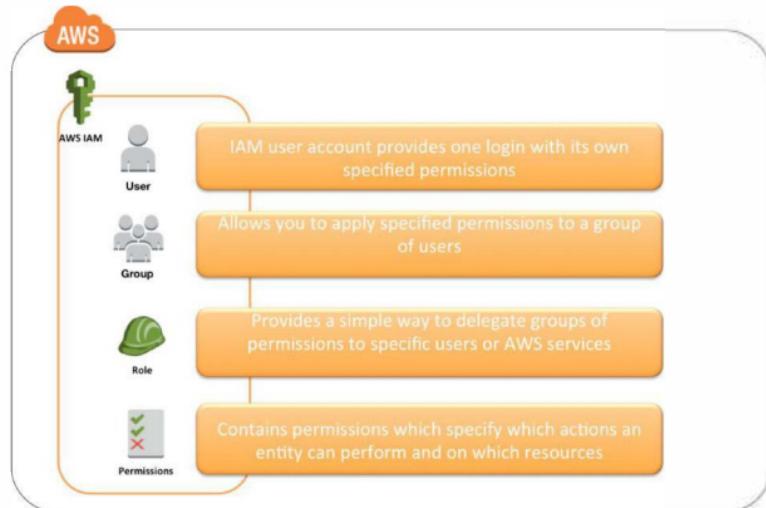
## Lab 6: To Manage IAM Users, Groups and Policies

### OBJECTIVE

To configure and use AWS IAM Service.

### TOPOLOGY

AWS IAM Identities



### PRE-REQUISITES

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.

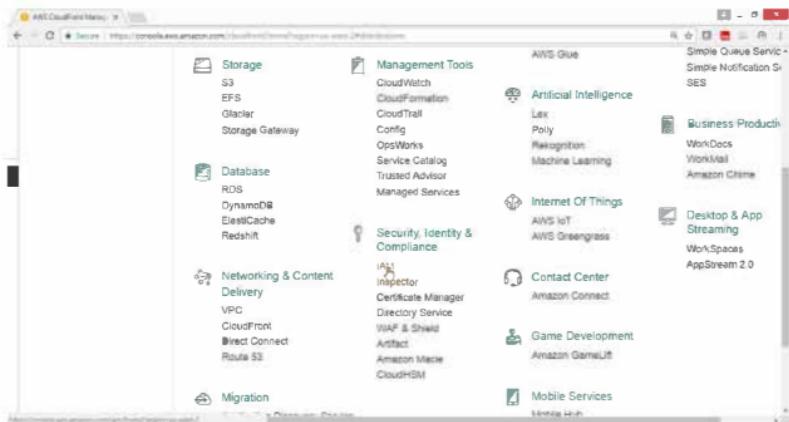
Create your own policies.

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

The screenshot shows the AWS IAM Dashboard panel. The left sidebar has a 'Search IAM' field and links for Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has a 'Welcome to Identity and Access Management' header, a 'Feature Spotlight' section with a video thumbnail, and a 'IAM Resources' section showing 0 users, 0 groups, 0 roles, and 0 customer managed policies. It also displays a 'Security Status' section with five items: 'Delete your root access keys', 'Activate MFA on your root account', 'Create individual IAM users', and 'Use groups to assign permissions'. The bottom of the page includes a footer with copyright information, a 'Feedback' link, and 'Terms of Use'.

## 2) To Mange Groups and applying policies

From IAM dashboard, select **Groups**

Click on **Create New Group** button

The screenshot shows the AWS IAM Groups page. On the left, there's a sidebar with links like Dashboard, Groups (which is selected and highlighted in yellow), Users, Roles, Policies, Identity providers, Account settings, and Credential report. Below that is an Encryption keys section. The main content area has a search bar and two buttons: 'Create New Group' (highlighted with a blue box) and 'Group Actions'. A table follows, with columns for Group Name, Users, Inline Policy, and Creation Time. The table shows 'Showing 0 results' and 'No records found'. At the bottom of the page are standard AWS navigation links: Feedback, English, Help, Terms of Use, and a copyright notice: © 2006-2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Give Group Name → EC2admingroup

Click on **Next Step** button



In Filter type → EC2f

Select check box for **AmazonEC2FullAccess**

Click on **Next Step** button

The screenshot shows the 'Attach Policy' step of the 'Create New Group Wizard'. A filter bar at the top is set to 'Policy Type: EC2f'. Below it, a table lists two policies: 'AmazonEC2FullAccess' and 'AmazonEC2FullAccess...'. The first policy has a checked checkbox next to it. At the bottom right of the table are 'Cancel', 'Previous', and 'Next Step' buttons, with 'Next Step' being highlighted.

Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/> AmazonEC2FullAccess	0	2015-02-07 00:10 UTC...	2015-02-07 00:10 ...
<input type="checkbox"/> AmazonEC2FullAccess...	0	2017-06-17 16:33 UTC...	2017-06-17 16:33 ...

Click on **Create Group**

The screenshot shows the 'Review' step of the 'Create New Group Wizard'. It displays the group name 'EC2adminGroup' and the attached policy 'arn:aws:iam::aws:policy/AmazonEC2FullAccess'. At the bottom right are 'Cancel', 'Previous', and 'Create Group' buttons, with 'Create Group' being highlighted.

## Verify

Group EC2admingrp got created with AmazonEC2FullAccess policy

The screenshot shows the AWS IAM Management Console. In the left sidebar, under 'Groups', the 'EC2admingroup' is selected. The main content area displays the group details. The 'Creation Time' is listed as 2017-08-18 18:35 UTC+0830. Below this, the 'Users' tab is selected, showing no users assigned to this group. The 'Permissions' tab is also visible. Under 'Managed Policies', it shows that the 'AmazonEC2FullAccess' policy is attached. There is a button to 'Attach Policy'. The 'Policy Name' column lists 'AmazonEC2FullAccess' and the 'Actions' column shows 'Show Policy | Detach Policy | Simulate Policy'. The 'Inline Policies' section is currently empty.

Now again create Another Group

Click on **Create Group** button

The screenshot shows the AWS IAM Management Console. In the left sidebar, under 'Groups', the 'Create New Group' button is highlighted. The main content area displays the group details. The 'Group Actions' dropdown is open, showing a table with one result: 'EC2admingroup'. The table columns are 'Group Name', 'Users', 'Inline Policy', and 'Creation Time'. The 'EC2admingroup' row shows '0' users, 'AmazonEC2FullAccess' as the inline policy, and a creation time of 2017-08-18 18:35 UTC+0830.

## To create a group With S3FullAccess

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: S3admingrp

Cancel Next Step

In Filter type → S3f

Select check box for **AmazonS3FullAccess**

Click on **Next Step** button

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ s3f Showing 2 results

Policy Name	Attached Entities	Creation Time	Edited Time
AmazonS3FullAccess	0	2015-02-07 00:10 UTC	2015-02-07 00:10 ...
AmazonS3FullAccess	0	2017-08-05 21:24 UTC	2017-08-05 21:24 ...

Cancel Previous Next Step

Click on Create Group button

Review

Review the following information, then click Create Group to proceed.

Group Name: S3admingrp [Edit Group Name](#)

Policies: arn:aws:iam::aws:policy/AmazonS3FullAccess [Edit Policies](#)

[Cancel](#) [Previous](#) [Create Group](#)

Verify EC2admingroup & S3admingrp groups got created

Search IAM

Create New Group Group Actions

Filter	Showing 2 results		
Group Name	Users	Inline Policy	Creation Time
EC2admingroup	0		2017-08-15 15:35 UTC+0530
S3admingrp	0		2017-08-15 15:42 UTC+0530

## Verify S3 policy is attached

The screenshot shows the AWS IAM Groups page. The left sidebar has a 'Groups' section selected. The main content area shows a group with the following details:

- Creation Time:** 2017-08-15 18:42 UTC+0530
- Users:** [List of users]
- Permissions** tab selected
- Managed Policies:** A table lists the attached managed policies:

Policy Name	Actions
AmazonS3FullAccess	Show Policy   Detach Policy   Simulate Policy
- Inline Policies:** [List of inline policies]

Create user tom and join to EC2admingroup

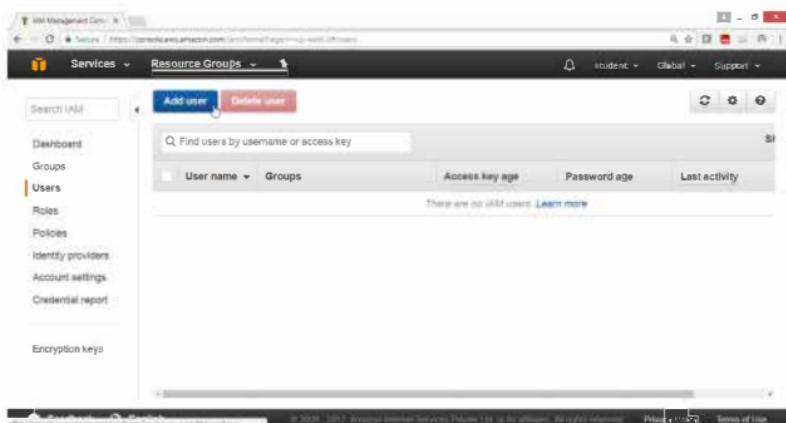
Create user john and join to S3admingroup

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

The screenshot shows the AWS IAM 'Add user' wizard. The top navigation bar includes 'Services', 'Resource Groups', and account information ('student', 'Date'). Below the header, a progress bar shows four steps: '1 Details' (highlighted in blue), '2 Permissions', '3 Review', and '4 Complete'. The main section is titled 'Set user details' with the sub-instruction 'You can add multiple users at once with the same access type and permissions. [Learn more](#)'. A 'User name\*' field contains 'tom'. There is also a radio button for 'Add another user'. The next section, 'Select AWS access type', includes the instruction 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)'. It lists two options: 'Programmatic access' (unchecked) and 'AWS Management Console access' (checked). The bottom of the page features standard AWS footer links: 'Feedback', 'English', '© 2009 - 2017 Amazon Internet Services LLC or its affiliates. All rights reserved.', 'Privacy', 'Terms of Use', and a search bar.

For Console password → \*\*\*\*\*

Click on Next Permissions button

The screenshot shows the 'AWS Management Console' interface for creating a new IAM user. The 'Services' and 'Resource Groups' tabs are visible at the top. The main area displays the 'AWS Management Console access' policy attached to the user. Below it, there's a section for setting a 'Console password'. The 'Custom password' option is selected, and a password field contains '\*\*\*\*\*'. A 'Show password' link is present. Underneath, there's a checkbox for 'Require password reset' which is unchecked. A note explains that users must create a new password at next sign-in and that they can do so if they have the IAMUserChangePassword policy. At the bottom right, there are 'Cancel', 'Previous', and 'Next: Permissions' buttons. The 'Next: Permissions' button is highlighted with a blue border.

Under Group column

Select EC2admingroup

Click on Next Review

The screenshot shows the 'AWS Management Console' interface for creating a new IAM user, specifically on the 'Next: Review' step. The 'Services' and 'Resource Groups' tabs are visible at the top. The main area displays the 'EC2admingroup' group selected under the 'Group' dropdown. The 'Attached policies' section shows two policies: 'AmazonEC2FullAccess' and 'AmazonSSMFullAccess'. At the bottom right, there are 'Cancel', 'Previous', and 'Next: Review' buttons. The 'Next: Review' button is highlighted with a blue border.

## Verify users detail

Click on **Create user** button

User details

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details	
Username	tom
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No

Permissions summary

The user shown above will be added to the following groups:

Type	Name
Group	EC2FullAccess

**Create user**

Down the .csv file

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign in at <http://523251682217.signin.aws.amazon.com/console>

**Download CSV**

User
tom

Email login instructions  
Send Email

**Close**

Click on **close** button

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-west-2#/users?newStepFinal&loginUserNames=tom&passwordType=manual&groups=EC2>. The page displays a success message: "Success: You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time." Below this message, it says "Users with AWS Management Console access can sign-in at: https://S323291883217.signin.aws.amazon.com/console". There is a "Download .csv" button, a "User" table with one item named "tom", and a "Close" button. The bottom navigation bar includes links for Feedback, English, and other AWS services.

## Scenario 2)

Create user john and join to S3admingroup

Select user

Click on Add user button

The screenshot shows the AWS IAM Management Console interface. The left sidebar has 'Users' selected. The main area displays a table with one user entry:

User name	Groups	Access key age	Password age	Last activity	MFA
John	S3admingroup	None	Today	None	Not enabled

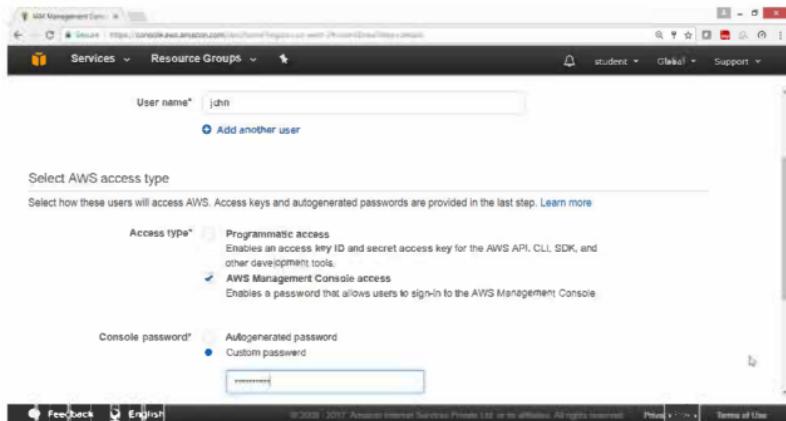
A blue 'Add user' button is visible above the table. The browser address bar shows the URL: `https://console.aws.amazon.com/iам/home?region=us-west-2#users`.

For user name → john

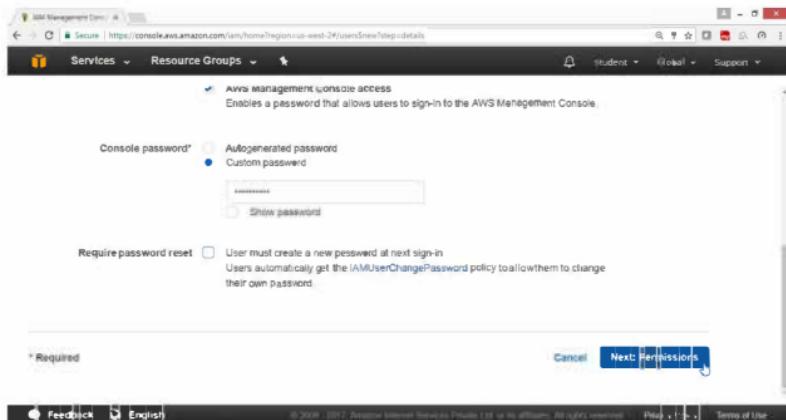
For Access type → AWS Management Console access

For console password → \*\*\*\*\*

Drag down



Click on Next Permission button



Select S3admingrp

Click on **Next Review** button

The screenshot shows the IAM Management Console with the 'Resource Groups' tab selected. In the 'Attached policies' section, the 'AmazonS3FullAccess' policy is listed under the 'S3admingrp' group. A blue selection bar highlights this row. At the bottom right of the page, there are 'Cancel', 'Previous', and 'Next Review' buttons, with 'Next Review' being the active button.

Verify user details

Click on **Create user** button

The screenshot shows the 'Create user' step of the IAM wizard. It displays the 'User details' section with a username of 'john'. Below it, the 'Permissions summary' section shows that the user will be added to the 'S3admingrp' group. At the bottom right, there are 'Cancel', 'Previous', and 'Create user' buttons, with 'Create user' being the active button.

**Download .csv file**

**Click on Close button**

The screenshot shows the AWS Management Console interface for creating a new user. At the top, there's a navigation bar with tabs like 'Services', 'Resource Groups', and 'student'. Below the navigation bar, a progress bar indicates four steps: 'Details' (step 1), 'Permissions' (step 2), 'Review' (step 3), and 'Complete' (step 4, highlighted with a blue circle). A green 'Success' message box is displayed, stating: 'You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.' It lists a user named 'jake'. Below the message box are buttons for 'Download .csv' (with a small CSV icon) and 'Email login instructions' (with an envelope icon). There are also 'Send email' and 'Close' buttons. At the bottom of the page, there are links for 'Feedback', 'English', and other AWS policies.

### 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

The screenshot shows the AWS IAM console interface. On the left, there's a sidebar with navigation links: Dashboard, Groups, Users (which is selected and highlighted in orange), Roles, Policies, Identity providers, Account settings, and Credential report. Below that is an Encryption keys section. The main content area has a search bar at the top labeled "Find users by username or access key". Below it is a table titled "Showing 2 results". The table has columns: User name, Groups, Access key age, Password age, Last activity, and MFA. Two users are listed: "john" and "sai". Both users belong to the "S3amazing" group. Their access keys and passwords are both "None". Their last activity was "Today". MFA is "Not enabled" for both.

User name	Groups	Access key age	Password age	Last activity	MFA
john	S3amazing	None	Today	None	Not enabled
sai	S3amazing	None	Today	None	Not enabled

- For User name → sai  
For Access type → AWS Management Console access  
For Console password → \*\*\*\*\*

Drag Down

User name\*  Add another user

Select AWS access type  
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more.

Access type\*  **Programmatic access**  
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.  
 **AWS Management Console access**  
Enables a password that allows users to sign-in to the AWS Management Console.

Console password\*  Autogenerated password  Custom password

Feedback English | [Help](#) | [Terms of Use](#)

Click on Next permission button

over development tools:  
 **AWS Management Console access**  
Enables a password that allows users to sign-in to the AWS Management Console.

Console password\*  Autogenerated password  Custom password  
  
 Show password

Require password reset  User must create a new password at next sign-in  
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

\* Required Cancel **Next: Permissions**

Feedback English | [Help](#) | [Terms of Use](#)

Click on Attach existing policies directly box

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-west-2#/users/new?step=permissions&loginUserNames=sai&passwordType=manual>. The top navigation bar includes 'Services', 'Resource Groups', 'student', 'Support', and 'Feedback'. Below the navigation is a progress bar with four steps: 'Details' (step 1), 'Permissions' (step 2, highlighted in blue), 'Review' (step 3), and 'Create user' (step 4). The main content area is titled 'Add user' and 'Set permissions for sai'. It features three options: 'Add user to group' (with a plus icon and three people icon), 'Copy permissions from existing user' (with a cloud and person icon), and 'Attach existing policies directly' (with a document icon). A note below says: 'Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more'. At the bottom are 'Feedback', 'English', and 'Terms of Use' buttons.

In Filter type search for ec2f

Select AmazonEC2FullAccess check box

The screenshot shows the 'Attach existing policies directly' step of the IAM wizard. The URL is <https://console.aws.amazon.com/iam/home?region=us-west-2#/users/new?step=permissions&loginUserNames=sai&passwordType=manual>. The top navigation bar and progress bar are identical to the previous screenshot. The main content area has a note: 'Attach one or more existing policies directly to the user or create a new policy. Learn more'. It includes 'Create policy' and 'Refresh' buttons. A search bar is set to 'ec2f'. A table lists policies: 'AmazonEC2FullAccess' (AWS managed, checked) and 'AmazonEC2FullAccess...' (Customer managed, unchecked). The table has columns: Policy name, Type, Attachments, and Description. At the bottom are 'Feedback', 'English', and 'Terms of Use' buttons.

In Filter type search for s3f

Select AmazonS3FullAccess check box

Click on **Next Review** button

The screenshot shows the AWS IAM Management Console. A new policy named 'AmazonS3FullAccess' is being created. The policy is listed under 'AWS managed' and has a detailed description: 'Provides full access to all buckets via the AWS Management Console'. At the bottom of the screen, there are 'Cancel', 'Previous', and 'Next Step' buttons.

Verify users detail

Click on Create user button

The screenshot shows the AWS IAM Management Console. A new user named 'saif' is being created. The user details include: User name 'saif', AWS access type 'AWS Management Console access - with a password', Console password type 'Custom', and Require password reset 'No'. In the Permissions summary section, it is noted that the following policies will be attached to the user: 'AmazonEC2FullAccess' and 'AmazonS3FullAccess'. At the bottom of the screen, there are 'Cancel', 'Previous', and 'Create user' buttons, with the 'Create user' button being the target of a cursor click.

**Download .csv file**

**Click on Close button**

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-west-2#/users/new?step=final&loginType=sso&passwordType=manual&permission...>. The page title is "Add user". A progress bar at the top shows four steps: 1. Details, 2. Permissions, 3. Review, and 4. Complete (highlighted with a blue circle).  
**Success:**  
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.  
Users with AWS Management Console access can sign-in at: <http://52.32.51.68:3217> sign-in aws.amazon.com/console  
  
A "Download .csv" button is highlighted with a red box. Other buttons include "Email login inst.", "Send email", and "Close".  
  
Feedback English © 2018 - 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

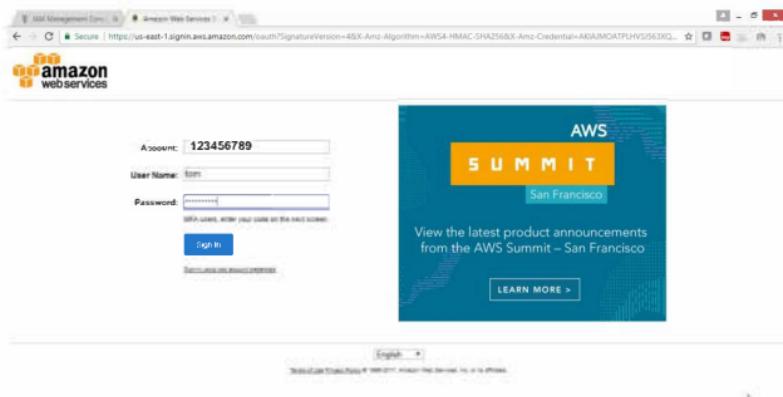
To verify whether users can access particular Service

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

The screenshot shows the AWS Management Console Services page. The left sidebar lists services: Console Home, S3, IAM, CloudFront, VPC, and EC2. The main area is divided into several sections: Compute (EC2, EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, Batch), Storage (EFS, Glacier), Developer Tools (CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, X-Ray), Management Tools (CloudWatch, CloudFormation, CloudTrail), Analytics (Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, Data Pipeline, QuickSight, AWS Glue), and Artificial Intelligence (Lex). A search bar at the top right says "Find a service by name or feature (for example, EC2, S3 or VPC, storage)".

## Verification

Error Access Denied

The screenshot shows the AWS S3 console. The top navigation bar includes "Services", "Resource Groups", and "Oregon". The main content area has a heading "Identify optimal storage classes with S3 Analytics - Storage Class Analysis" with a "Learn More" link. Below this, there's a "Create bucket" button and tabs for "Create bucket", "Create queue", and "Create private". A large red-bordered box contains an "Error" message: "Access Denied". There are also "Switch to the old console", "Discover the new (2019)", "Quick tips", "Buckets", and "Regions" links.

## Now select EC2 service

The screenshot shows the AWS Management Console navigation bar at the top. Below it is a sidebar titled "History" containing links for S3, Console Home, IAM, CloudFront, VPC, and ECE. The main area displays a grid of service icons and names. The "Compute" section includes EC2, Lambda, and Batch. The "Storage" section includes S3, EBS, Glacier, and Storage Gateway. The "Database" section includes RDS and DynamoDB. The "Developer Tools" section includes CodeStar, CodeCommit, CodeBuild, CodeDeploy, and CodePipeline. The "Management Tools" section includes CloudWatch, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Trusted Advisor, and Managed Services. The "Analytics" section includes Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, Data Pipeline, Quicksight, and AWS Glue. The "Application Services" section includes Step Functions, SWF, API Gateway, and Elastic Transcoder. The "Messaging" section includes Simple Queue Service, Simple Notification Service, and SES. The "Business Products" section includes WorkDocs, WorkMail, and Amazon Chime. The "Internet Of Things" section includes AWS IoT. The "Desktop & App" section includes AWS Device Farm. A search bar at the top right says "Filter by service key name or resource. For example: EC2, S3 or Lambda." A "Group" button is also present.

## Verification

User tom can access EC2 service.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with "Services" dropdown set to "EC2", "Resource Groups" dropdown set to "Oregon", and "Sup" link. Under "INSTANCES", it lists Instances, Spot Requests, Reserved Instances, Scheduled Instances, and Dedicated Hosts. Under "IMAGES", it lists AMIs. At the bottom, there are "Feedback" and "English" buttons. The main content area has three main sections: "Resources" (listing 1 Running Instances, 0 Dedicated Hosts, 1 Volumes, 3 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 1 Snapshots, 0 Load Balancers, 6 Security Groups), "Account Attributes" (listing Supported Platforms, VPC, Default VPC, vpc-89c341ee, Resource ID length management), and "Additional Information" (links to Getting Started Guide and Documentation). At the very bottom, there are "Privacy Policy" and "Terms of Use" links, along with a copyright notice: "© 2008 - 2017, Amazon Internet Services Private Ltd. All rights reserved."

Similarly check for user john

To Delete users and groups

From IAM dashboard, select **Users**

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

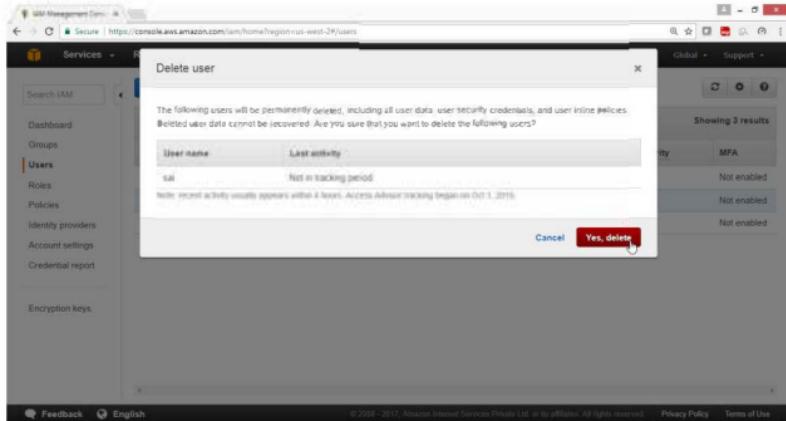
Click on **Delete Users** button

The screenshot shows the AWS IAM service dashboard under the 'Services' tab. On the left, a sidebar lists 'Dashboard', 'Groups', 'Users' (which is selected), 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Encryption keys'. The main content area is titled 'Users' and shows a table with three rows. The columns are 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. The users listed are:

User name	Groups	Access key age	Password age	Last activity	MFA
john	S3AdminGroup	None	Today	None	Not enabled
bob	None	None	Today	None	Not enabled
sam	EC2AdminGroup	None	Today	Today	Not enabled

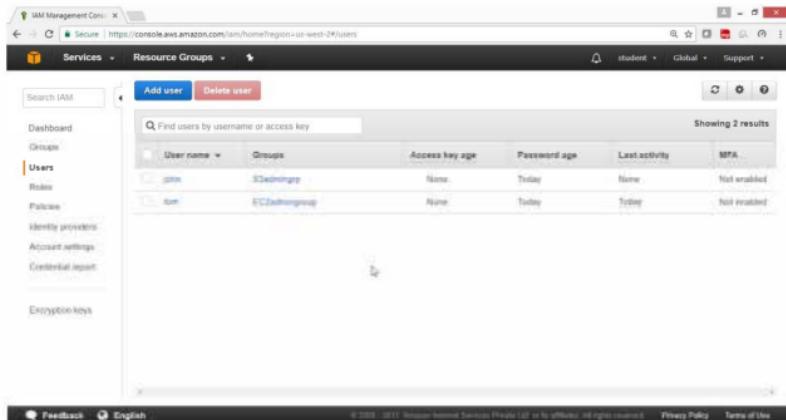
At the top of the table, there are buttons for 'Add user' and 'Delete user'. A search bar at the top says 'Find users by username or access key'.

Click on Yes, delete button



## Verification

User sai is deleted



## To Deleting Groups

From IAM Dashboard

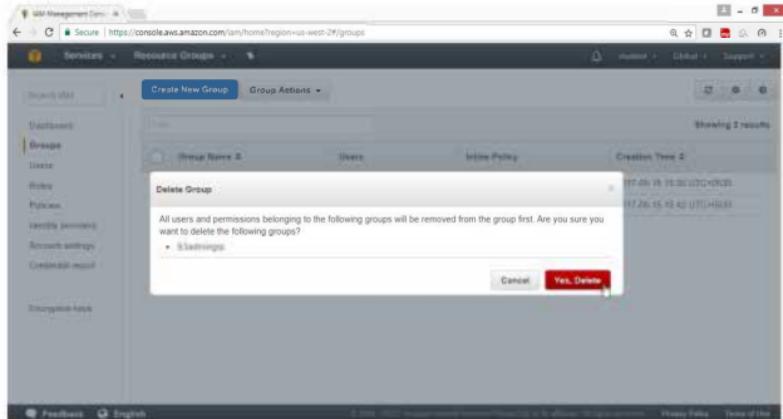
Select the Groups

Drop down Group Action button

Select Delete Group

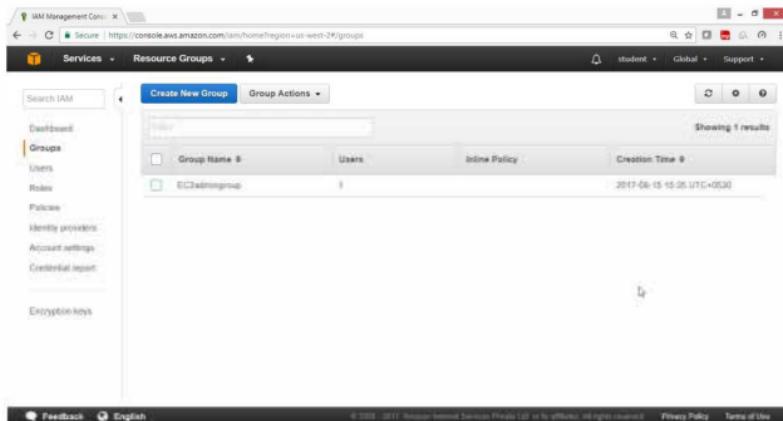
The screenshot shows the AWS IAM Groups page. On the left, there's a sidebar with links like Dashboard, Groups (which is selected), Users, Roles, Policies, Identity providers, Account settings, and Credential report. Below that is a section for Encryption keys. The main area has a search bar and a table with three results. The first row shows a checkbox, a group name 'EC2AdminGroup', and two users. The second row shows a checkbox and a user 'SAdministrator'. A context menu is open over the first row, with the 'Delete Group' option highlighted. The menu also includes 'Add Users to Group', 'Edit Group Name', and 'Remove Users from Group'. The table has columns for 'Group Actions', 'Group Name', 'Users', 'Inline Policy', and 'Creation Time'.

**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

The screenshot shows the AWS IAM Dashboard. On the left, there is a sidebar with navigation links: Dashboard, Groups, Users (which is selected and highlighted in orange), Roles, Policies, Identity providers, Account settings, and Credential report. The main content area has tabs for 'Add user' (blue) and 'Delete user' (red). Below these tabs is a search bar labeled 'Find users by username or access key'. A table lists two users: 'john' and 'tom'. The table columns are 'User name', 'Groups', 'Access key age', and 'Password age'. The 'john' row shows 'S3admingrp' under 'Groups', 'None' under 'Access key age', and 'Today' under 'Password age'. The 'tom' row shows 'EC2admingroup' under 'Groups', 'None' under 'Access key age', and 'Today' under 'Password age'. At the bottom of the page, there are links for 'Feedback', 'English', and a copyright notice: '© 2006-2017, Amazon Web Services, Inc., or its affiliates. All rights reserved.' and 'Privacy Policy'.

User name	Groups	Access key age	Password age
john	S3admingrp	None	Today
tom	EC2admingroup	None	Today

Click on Security credentials

The screenshot shows the AWS IAM Management Console. The URL is <https://console.aws.amazon.com/iam/home?region=us-east-1#user-summary:username=tom>. The top navigation bar includes 'Services', 'Resource Groups', 'student', and 'Global'. On the left, a sidebar menu lists 'Dashboard', 'Groups', 'Users' (which is selected), 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. The main content area is titled 'Summary' for user 'tom'. It displays the User ARN (arn:aws:iam::123456789012:user/tom), Path (/), and Creation time (2017-08-15 22:09 UTC+0530). Below this, there are tabs for 'Permissions', 'Groups (1)', 'Security credentials' (which is highlighted in orange), and 'Access Advisor'. Under 'Attached policies: 1', it shows a single policy named 'Policy name' with a dropdown arrow and 'Policy type' with a dropdown arrow. At the bottom of the page, there are 'Feedback' and 'English' buttons, and a copyright notice: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' and 'Privacy Policy'.

Click on pen sign for "Assigned MFS device"

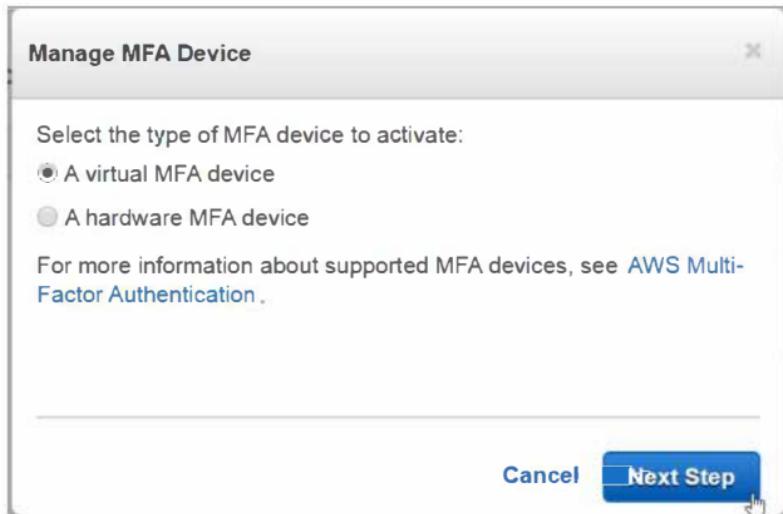
This screenshot is from the same AWS IAM Management Console as the previous one, showing the user 'tom'. The URL is <https://console.aws.amazon.com/iam/home?region=us-east-1#user-summary:username=tom>. The 'Security credentials' tab is selected. The 'Sign-in credentials' section shows the following details:

Setting	Value	Action
Console password	Enabled	
Console login link	<a href="https://signin.aws.amazon.com/console">https://signin.aws.amazon.com/console</a>	
Last login	2017-08-15 22:50 UTC+0530	
Assigned MFA device	No	
Signing certificates	None	

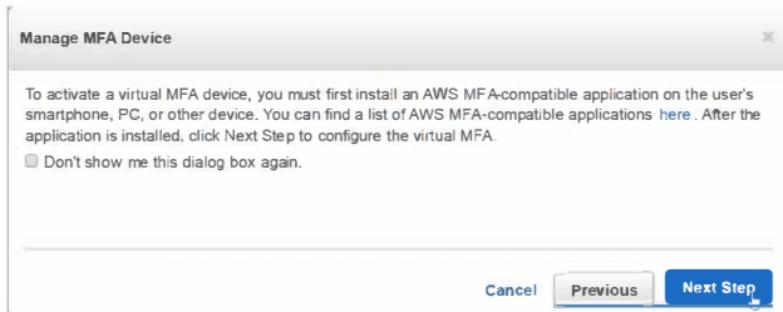
At the bottom of the page, there are 'Feedback' and 'English' buttons, and a copyright notice: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' and 'Privacy Policy'.

Select ➔ “A virtual MFA 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 Authentication code 1

Once the bar code changes

Retype 6 digit bar code in Authentication code 2



Click on Finish



Now login as tom user

A screenshot of a web browser displaying the AWS login page at https://us-west-2.signin.aws.amazon.com/. The page features the Amazon Web Services logo. On the left, there are input fields for "Account" (123456789), "User Name" (tom), and "Password". Below these fields is a note: "MFA users: enter your code on the next screen." A "Sign in" button is centered below the password field. To the right of the login form is a large, dark blue advertisement for the "AWS SUMMIT San Francisco". The ad features the AWS logo and the text "View the latest product announcements from the AWS Summit – San Francisco". At the bottom of the ad is a "LEARN MORE &gt;" button. The browser's address bar shows the URL, and the status bar at the bottom displays the full URL and some security information.

Once the user types the MFA 6 digit code

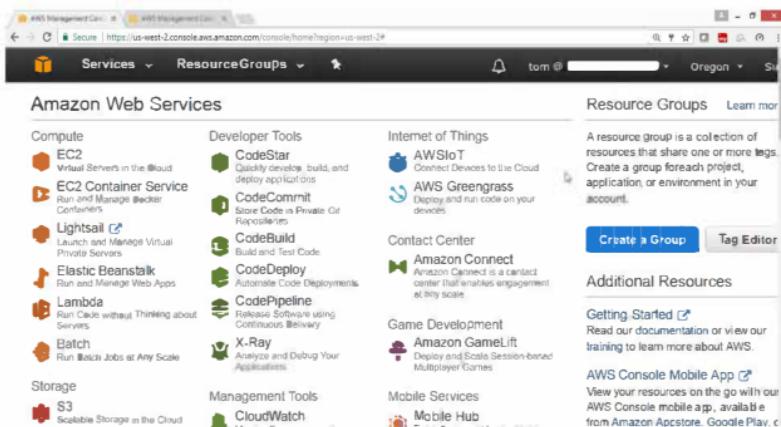
Click on submit



MFA Code: 123456

Submit Cancel

Verify user had successfully logged in.



Services    ResourceGroups

## Amazon Web Services

Compute

- EC2 Virtual Servers in the Cloud
- EC2 Container Service Run and Manage Docker Containers
- Lightsail Launch and Manage Virtual Private Servers
- Elastic Beanstalk Run and Manage Web Apps
- Lambda Run Code without Thinking about Servers
- Batch Run Batch Jobs at Any Scale

Storage

- S3 Scalable Storage in the Cloud

Developer Tools

- CodeStar Quickly develop, build, and deploy applications
- CodeCommit Host your Git Repository in a Private Git Repository
- CodeBuild Build and Test Code
- CodeDeploy Automate Code Deployments
- CodePipeline Release Software using Continuous Delivery
- X-Ray Analyze and Debug Your Applications

Internet of Things

- AWS IoT Connect Devices to the Cloud
- AWS Greengrass Deploy and run code on your devices

Contact Center

- Amazon Connect Amazon Connect is a contact center that enables engagement at any scale

Game Development

- Amazon GameLift Deploy and Scale Session-based Multiplayer Games

Management Tools

- CloudWatch

Mobile Services

- Mobile Hub

Resource Groups [Learn more](#)

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

[Create a Group](#) [Tag Editor](#)

### Additional Resources

[Getting Started](#) Read our documentation or view our training to learn more about AWS.

[AWS Console Mobile App](#) View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, etc.

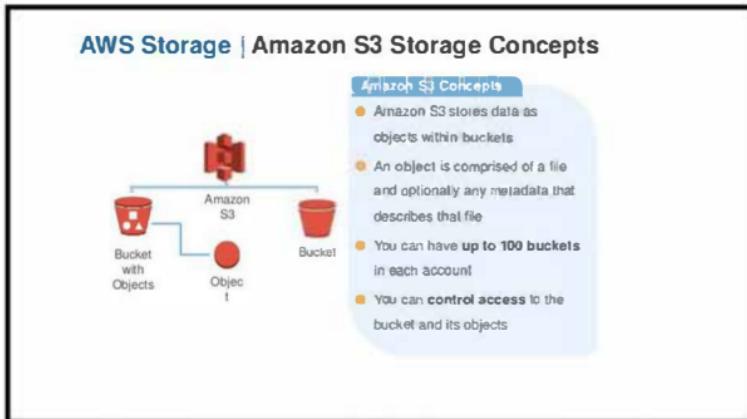
[AWS Lab Manual](#)

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

### OBJECTIVE

To configure and use AWS S3 service

### TOPOLOGY



### PRE-REQUISITES

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

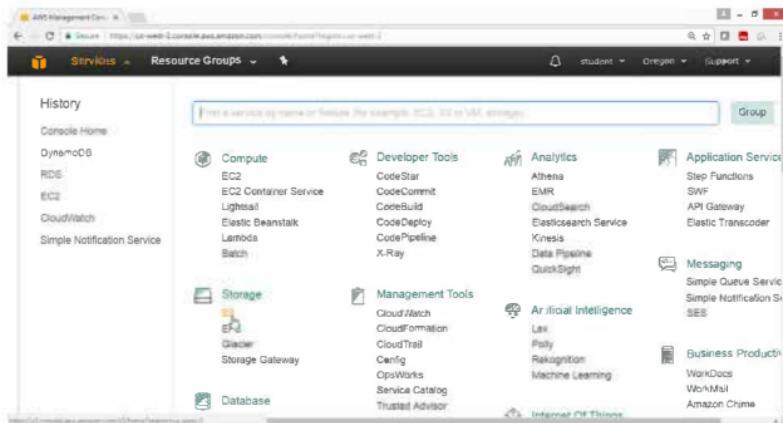
AWS user to control S3

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

Open AWS console

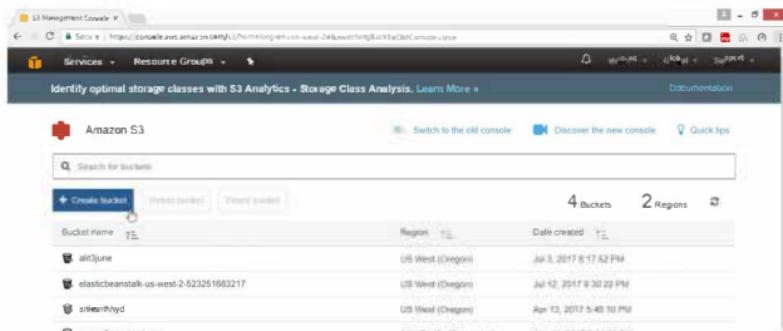
Select “**Storage**” service

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.

Create a Bucket - Select a Bucket Name and Region

A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the Amazon S3 documentation.

Bucket Name: saleshydbucket1

Region: Oregon

[Set Up Logging >](#) [Create](#) [Cancel](#)

Verify that bucket is created.

S3 Management Console | New Tab | <https://console.aws.amazon.com/s3/home?region=us-west-2>

Services | Resource Groups | [Switch to new console](#) | student | Global | Support

[Create Bucket](#) [Actions](#) | None Properties Transfers

All Buckets (4)

Name
cloudtrialhari
ctrilabc
<b>saleshydbucket1</b>
srikanthhyd

**Bucket: saleshydbucket1**

Bucket: saleshydbucket1  
Region: Oregon  
Creation Date: Tue Aug 15 08:00:06 GMT+530 2017  
Owner: srihavalis99

[Permissions](#)  
[Static Website Hosting](#)  
[Logging](#)  
[Events](#)  
[Versioning](#)

## 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

The screenshot shows the AWS S3 Management Console interface. In the top navigation bar, there are tabs for 'Services', 'Resource Groups', and 'Actions'. Below the navigation bar, there are buttons for 'Create Bucket', 'Actions', 'Switch to new console', 'None', 'Properties', and 'Transfers'. A dropdown menu labeled 'All Buckets (4)' is open, listing four buckets: 'cloudtrialhari', 'ctrilabc', 'saleshydbucket1', and 'srikanthhyd'. The 'saleshydbucket1' bucket is highlighted with a blue selection bar. To the right of the list, a detailed view of the selected bucket is displayed. The bucket name is 'Bucket: saleshydbucket1'. Below it, the details are listed: 'Bucket: saleshydbucket1', 'Region: Oregon', 'Creation Date: Tue Aug 15 08:00:06 GMT+530 2017', and 'Owner: skmvali@99'. On the far right of the bucket details, there are five expandable sections: 'Permissions', 'Static Website Hosting', 'Logging', 'Events', and 'Versioning'.

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.

The screenshot shows the AWS S3 Management Console interface. In the left sidebar, 'Services' and 'Resource Groups' are visible. The main area displays a table with one item: 'iPhone - MetroGnome Remix [Perf...' under the 'Name' column, 'Standard' under 'Storage Class', and '9.1 MB' under 'Size'. A 'Last M.' column shows 'Tue Aug 1'. On the right side, there are tabs for 'Transfers' and 'Properties'. Below the table, a note says 'Automatically clear finished transfers.'

Select the file, Click on Properties on Right Panel,

Click on the link

The screenshot shows the AWS S3 Management Console interface, similar to the previous one, but with the file properties expanded. The 'Properties' tab is selected. The 'Object' section shows the file 'iPhone - MetroGnome Remix [P...'. Under the 'Bucket' section, it lists 'saleshybucket1'. The 'Name' is 'iPhone - MetroGnome Remix [Performed by TPMC] - YouTube [360p].mp4'. The 'Link' field contains a URL: 'https://s3.us-west-2.amazonaws.com/saleshybucket1/iPhone - MetroGnome Remix [Performed by TPMC] - YouTube [360p].mp4'. Other properties listed include 'Size: 9.10 MB', 'Last Modified: 2017-08-15 08:04:56 GMT +530 2017', 'Owner: skmvai@999', 'ETag: 6d036eb69784224115be1291c92017a9', 'Expiration Date: None', and 'Expiration Rule: N/A'. Below the properties, there are sections for 'Details', 'Permissions', 'Metadata', and 'Tags'.

## Verification : Cannot access due to lack of permission

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>572AA41P376663B5</RequestId>
<HostId>
1Px9EcQestvOUsxIWMm54p6Yj2p7tz7zHNT1QYmZPwgj/7dw+UT/t/F0xkr9VrUTd8lq3lyEqbQ=
</HostId>
</Error>
```

To allow users to Download, or view give permission

Select, Permission tag

Object: iPhone - MetroGnome Remix [P... x

Name	Type	Last Modified
iPhone - MetroGnome Remix [Per...	Standard	9:1 MB

Bucket: s3nghybucket1  
Name: iPhone - MetroGnome Remix [Performed by TPMC] - YouTube [360].mp4  
Link: [https://s3.us-west-2.amazonaws.com/s3nghybucket1/iPhone+-+MetroGnome+Remix+\[360\].mp4?Expires=1603544158&Signature=1291692181769](https://s3.us-west-2.amazonaws.com/s3nghybucket1/iPhone+-+MetroGnome+Remix+[360].mp4?Expires=1603544158&Signature=1291692181769)  
Size: 9530788  
Last modified: Tue Aug 18 06:54:00 PDT 2017  
Owner: s3nghybucket1  
ETag: 6d035444784204158e1291692181769  
Expiry Date: None  
Expiration Rule: None

Details  
Permissions  
Metadata  
Tags

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

Drop down Grantee Button

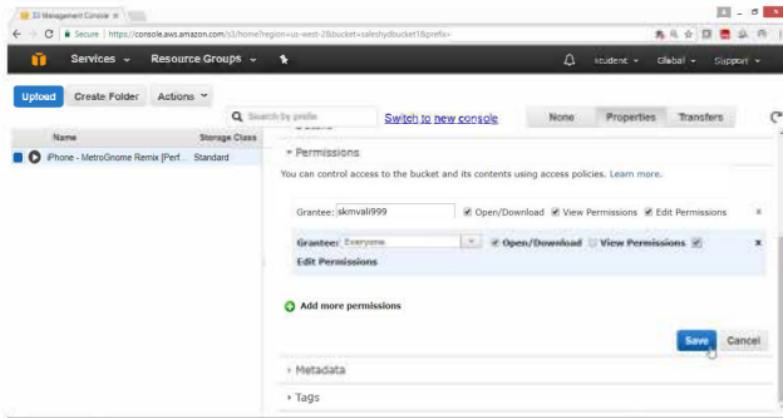
Select **Everyone** to make it public

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

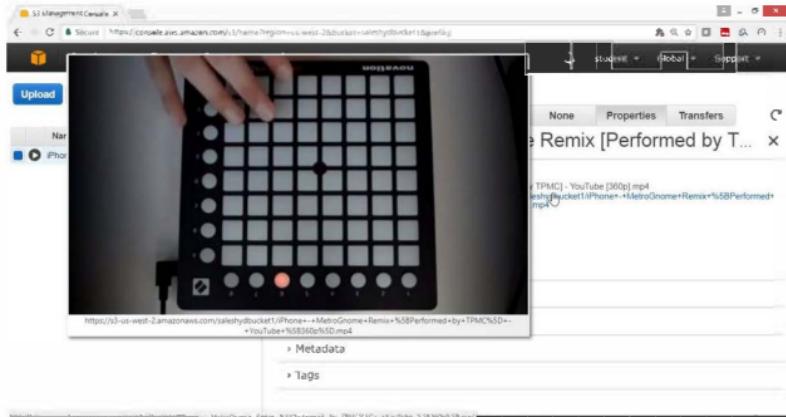
Enable the check box to **View Permission**

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

**Click on Save button**



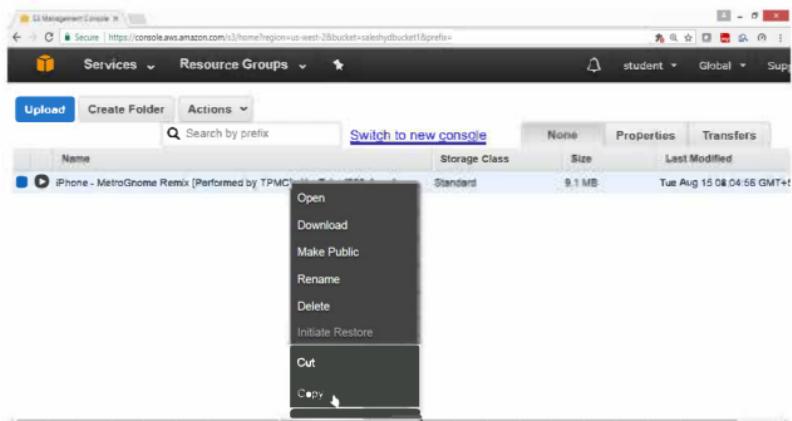
Verify file is accessible.



## 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

The screenshot shows the AWS S3 Management Console. At the top, there's a navigation bar with tabs for 'Services' and 'Resource Groups'. Below the navigation bar, there's a search bar and two buttons: 'None' and 'Properties'. A link 'Switch to new console' is also present. The main area is titled 'All Buckets (5)' and contains a table with a single column labeled 'Name'. The buckets listed are: cloudtrialhari, ctrialabc, finshydbucket1, saleshydbucket1, and srikanthhyd. The bucket 'finshydbucket1' is highlighted with a blue selection bar at the bottom of its row.

Click on Paste

The screenshot shows the AWS S3 Management Console with the same interface as the previous one. The 'Actions' dropdown menu is open, revealing three options: 'Create Folder...', 'Upload', and 'Paste'. The 'Paste' option is highlighted with a black background and white text. Below the dropdown, a message states 'The bucket 'finshydbucket1' is empty.'

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

The screenshot shows the AWS S3 Management Console interface. In the left sidebar, 'All Buckets' is selected, and 'finshydbucket' is chosen. The main area displays a single object: 'iPhone - MotoGame Remix [Performed by TP...' with a size of 9.1 MB and a last modified date of Tue Aug 15 08:23:54 GMT+530 2017. A context menu is open over this file, with the 'Delete' option highlighted in yellow.

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

Right click on it, select Delete

This screenshot is identical to the one above, showing the AWS S3 Management Console with the 'finshydbucket' bucket selected. The same file ('iPhone - MotoGame Remix [Performed by TP...') is selected, and the context menu is open with 'Delete' highlighted.

## To Delete a bucket

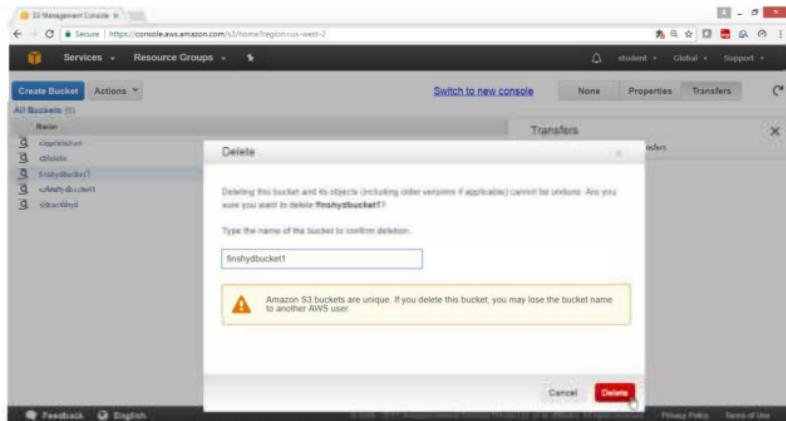
Select the bucket, right click select **Delete Bucket**

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with links for 'Management Console', 'Secure', and the URL 'https://console.aws.amazon.com/s3/home?region=us-west-2'. Below the navigation bar, the main header includes 'Services' (with a dropdown arrow), 'Resource Groups' (with a dropdown arrow), and a user dropdown set to 'student'. On the left, there's a sidebar with 'Create Bucket' and 'Actions' dropdown menus, and buttons for 'Switch to new console', 'None', and 'Properties'. The main content area is titled 'All Buckets (5)' and lists five buckets: 'cloudtrialhari', 'ctrialabc', 'finshydbucket1', 'saleshydbucket1', and 'srikanthhyd'. A context menu is open over the 'finshydbucket1' bucket, listing options: 'Create Bucket...', 'Delete Bucket' (which is highlighted in yellow), 'Empty Bucket', 'Paste Into', and 'Properties'. To the right of the bucket list, there's a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'.

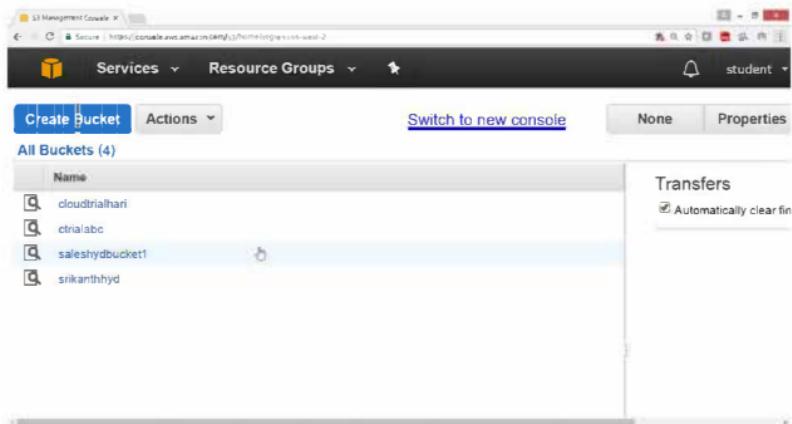
## To Delete Bucket

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"

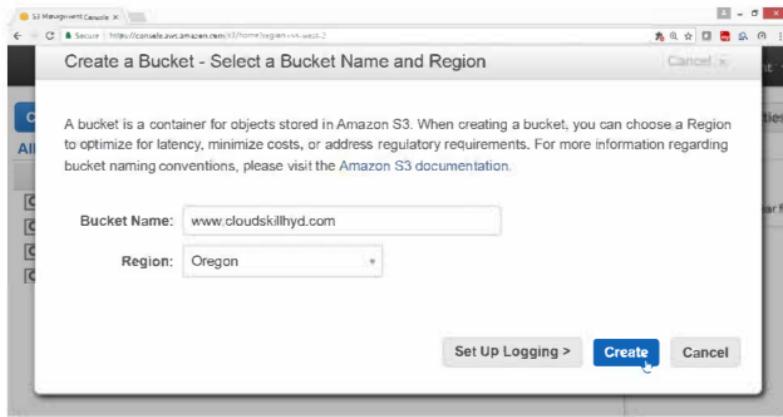
The screenshot shows the AWS Management Console interface for the S3 service. At the top, there's a navigation bar with links for Services, Resource Groups, and a user icon labeled 'student'. Below the navigation bar, there are two main buttons: 'Create Bucket' (which is highlighted in blue) and 'Actions'. To the right of these buttons is a link to 'Switch to new console'. Further to the right are 'None' and 'Properties' buttons. The main content area is titled 'All Buckets (4)' and lists four buckets: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1', and 'srikanthyd'. Each bucket entry includes a small icon and a delete button. To the right of the bucket list is a sidebar titled 'Transfers' with a single option: 'Automatically clear finished transfers' with a checked checkbox.

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

The screenshot shows the AWS S3 Management Console. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a sub-navigation bar has 'Create Bucket' highlighted in blue. To the right are 'Actions', 'Switch to new console', 'None', and 'Properties' buttons. The main area is titled 'All Buckets (4)'. A table lists four buckets: 'cloudnathari', 'ctrilabc', 'saleshydbucket1', and 'www.cloudskillhyd.com'. The last bucket is currently selected, indicated by a blue highlight. On the right side, there's a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'.

## Upload all website contents in this bucket.

The screenshot shows the AWS S3 Management Console with the 'www.cloudskillhyd.com' bucket selected. The left sidebar shows 'Upload', 'Create Folder', and 'Actions'. The main area displays a list of objects within the bucket. The objects are:

Name	Storage Class	Size	Last Modified
404.html	Standard	8 KB	Tue Aug 15 08:46:32 GMT+530 2017
about-us.html	Standard	5.8 KB	Tue Aug 15 08:46:33 GMT+530 2017
article.html	Standard	5.3 KB	Tue Aug 15 08:46:34 GMT+530 2017
articles.html	Standard	4.8 KB	Tue Aug 15 08:46:34 GMT+530 2017
contact-us.html	Standard	4.7 KB	Tue Aug 15 08:46:35 GMT+530 2017
css	—	—	—
images	—	—	—
index.html	Standard	8 KB	Tue Aug 15 08:46:36 GMT+530 2017
js	—	—	—
sitemap.html	Standard	4.9 KB	Tue Aug 15 08:46:37 GMT+530 2017

On the right, there's a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'.

Select the bucket and click on properties button

S3 Management Console | Services | Resource Groups | student | Global | None | Properties | Transfers

Create Bucket Actions Switch to new console

All Buckets (4)

Name
cloudskillhyd
crmlab0c
saleshydbucket1
srikanthyd
www.cloudskillhyd.com

Transfers

Automatically clear finished transfers

On the **Properties** panel

Click **Static Website Hosting**

Drag Down

S3 Management Console | Services | Resource Groups | student | Global | None | Properties | Transfers

Create Bucket Actions Switch to new console

All Buckets (5)

Name
cloudskillhyd
crmlab0c
saleshydbucket1
srikanthyd
www.cloudskillhyd.com

Bucket: www.cloudskillhyd.com  
Region: Oregon  
Creation Date: Tue Aug 15 08:44:43 GMT+530 2017  
Owner: skmval999

> Permissions

> Static Website Hosting

You can host your static website entirely on Amazon S3. Once you enable your bucket static website hosting, all your content is accessible to web browsers via the Amazon S3 website endpoint for your bucket.

**Endpoint:** [www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com](http://www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com)

Each bucket serves a website namespace (e.g., "www.example.com"). Requests for your host name (e.g. "example.com" or "www.example.com") can be routed to the contents of your bucket. You can also redirect requests to another host name (e.g. redirect

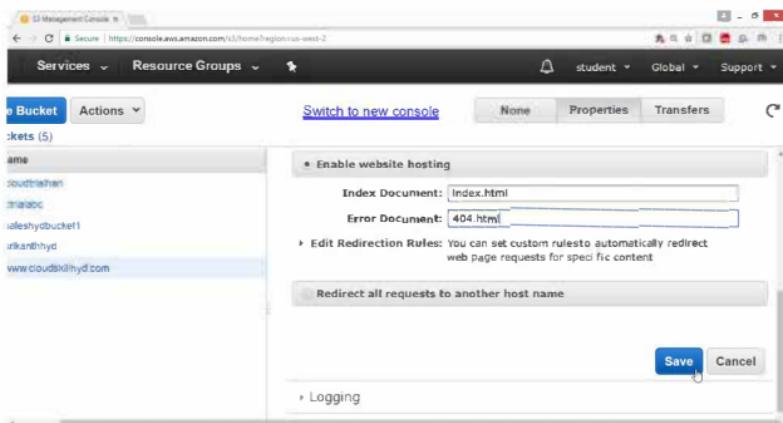
Select the **Enable website hosting**

Provide following values for

Index Document box → index.html

Error Document box → 404.html

Click on **Save** button



Note down the Endpoint.

The screenshot shows the AWS S3 console with the 'Static Website Hosting' tab selected. On the left, a list of buckets is shown, including 'cloudnathan', 'criralabc', 'saleshybucket1', 'srikanthyd', and 'www.cloudskylhyd.com'. The 'www.cloudskylhyd.com' bucket is currently selected. The main pane displays the configuration for this bucket's endpoint, which is set to `www.cloudskylhyd.com.s3-website-us-east-2.amazonaws.com`. A detailed description explains that each bucket serves a website namespace and can be routed to its contents. Below this, there are three sections: 'Do not enable website hosting' (disabled), 'Enable website hosting' (selected), and 'Edit Redirection Rules'. Under 'Enable website hosting', the 'Index Document' is set to 'index.html' and the 'Error Document' is set to '404.html'. At the bottom right, there are 'Save' and 'Cancel' buttons, and a 'Logging' section is visible below them.

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**.

The screenshot shows the AWS S3 console. In the top navigation bar, 'Services' is selected. On the left sidebar, 'Create Bucket' and 'Actions' dropdown are visible. The main area shows 'All Buckets (5)' with a list of buckets: 'cloudnat1', 'ctrlabc', 'saleshydbucket1', 'srikanthhyd', and 'www.cloudskillhyd.com'. The 'www.cloudskillhyd.com' bucket is selected. The top right shows 'student', 'Global', and 'Sup...'. Below the bucket list, tabs for 'None', 'Properties', and 'Transfers' are present. The main content area displays the bucket details: Bucket: www.cloudskillhyd.com, Region: Oregon, Creation Date: Tue Aug 15 08:44:43 GMT+530 2017, Owner: skmvai999. A 'Permissions' section is expanded, showing a grantee 'Grantee: skmvai999' with checkboxes for 'List' and 'Upload/Delete'. Buttons for 'View Permissions' and 'Edit Permissions' are shown. At the bottom, there are links for 'Add more permissions', 'Add bucket policy' (which is highlighted with a blue border), and 'Add CORS Configuration'. A 'Save' button is at the bottom right.

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:::cloudskillhyd.com/*"  
        ]  
    ]  
}
```

---

---

Click on **Save** button



## Verify your website

Click on Endpoint Under Static Website Hosting

Endpoint: [www.cloudskilhyd.com.s3-website-us-west-2.amazonaws.com](http://www.cloudskilhyd.com.s3-website-us-west-2.amazonaws.com)

The screenshot shows the AWS S3 Management Console. In the left sidebar, under 'All Buckets (5)', the 'www.cloudskilhyd.com' bucket is selected. On the right, under 'Static Website Hosting', the 'Enable website hosting' option is selected. The 'Index Document' field is set to 'index.html' and the 'Error Document' field is set to '404.html'. A note at the top right explains that you can host a static website on an Amazon S3 bucket by enabling static website hosting and providing an endpoint.

Verify the website which is coming from S3 Bucket

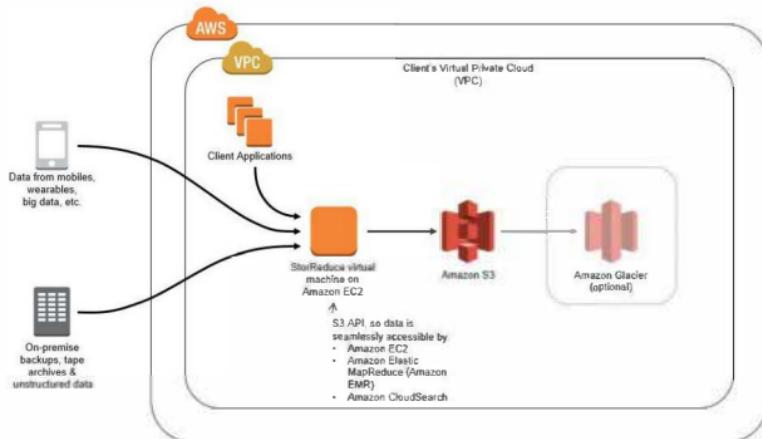
The screenshot shows a website template titled 'Car Club'. The header features a purple navigation bar with links for HOME, ABOUT, ARTICLES, CONTACTS, SITE MAP, Help, and FAQ. Below the header is a large banner image of a purple sports car. The main content area includes a 'Latest News' section with two items and a 'Welcome to Our Club' section. The 'Latest News' items are: '10.06.2010 Sed ut perspiciatis unde omnis iste natus error sit voluptate.' and '03.08.2010 Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet.'. The 'Welcome to Our Club' section contains a brief description of the template and a list of features: 'Aliquam poset et accumsan et velut', 'Ode sedemus delectus, qui', 'Etiamque presentium voluntatum', 'Dicitur aliquip enimque', 'Cupiditate non proident, similique', and 'Sunt in culpa qui officia deserunt'.

## Lab 8: To configure Amazon Glacier

### OBJECTIVE

To configure and use AWS Glacier Service.

### TOPOLOGY



### PRE-REQUISITES

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**

The screenshot shows the AWS S3 Management Console interface. In the top navigation bar, the URL is https://console.aws.amazon.com/s3/home?region=us-west-2. The main menu includes Services (selected), Resource Groups, and other options like学生 (student), Global, and Support. Below the menu, there are buttons for Create Bucket, Actions, and Switch to new console. A dropdown menu shows 'None' selected. On the left, a sidebar lists 'All Buckets (5)' with names: cloudmahan, crialabc, saleshydbucket1, srikanthyd, and www.cloudskillhyd.com. The 'www.cloudskillhyd.com' bucket is currently selected. The main content area displays the properties for this bucket. The 'Bucket' field is set to 'www.cloudskillhyd.com'. Under the 'Lifecycle' section, there is a table with one item:

Rule ID	Prefix	Transitions	Expiration
1		From Standard to Glacier	Never

Below the table, there are several tabs: Permissions, Static Website Hosting, Logging, Events, Versioning, Lifecycle (which is currently selected), and Cross-Region Replication.

Click on Add rule

The screenshot shows the AWS S3 Management Console. On the left, there's a sidebar with 'Create Bucket' and 'Actions'. Below it, a list of buckets: 'cloudmathan', 'crababc', 'saileshybucket1', 'srikanthhyd', and 'www.cloudskilhyd.com'. The main area has tabs for 'None', 'Properties', and 'Transfers'. A 'Switch to new console' link is at the top right. A tooltip says 'Versioning is not currently enabled on this bucket.' Below it, a note says 'You can use Lifecycle rules to manage all versions of your objects. This includes both the Current version and Previous versions.' A green 'Add rule' button is highlighted with a cursor. At the bottom right are 'Save' and 'Cancel' buttons.

### Under Lifecycle Rules

select **Choose Rule Target**

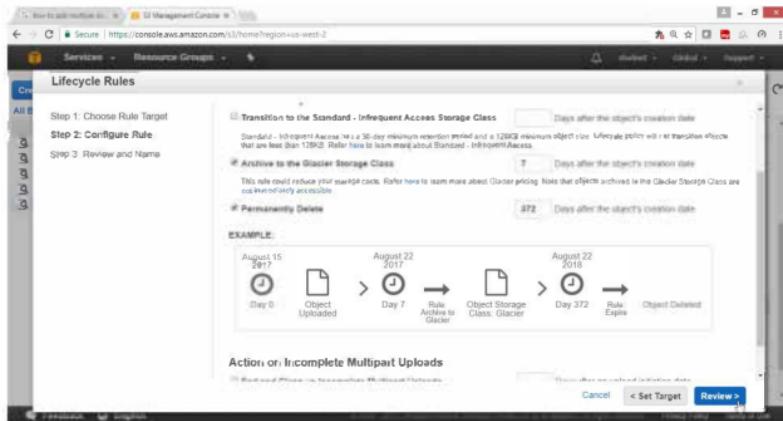
Apply the Rule to → Whole Bucket

The screenshot shows the 'Lifecycle Rules' configuration dialog. It has three steps: 'Step 1: Choose Rule Target', 'Step 2: Configure Rule', and 'Step 3: Review end Name'. Step 1 is active, showing 'Apply the Rule to: Whole Bucket www.cloudskilhyd.com'. Step 2 shows a dropdown menu with 'A Prefix', 'e.g. MyFolder/ or MyFolder/MyObject'. Step 3 is partially visible. At the bottom right are 'Cancel' and 'Configure Rule >' buttons, with the latter being highlighted by a cursor.

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

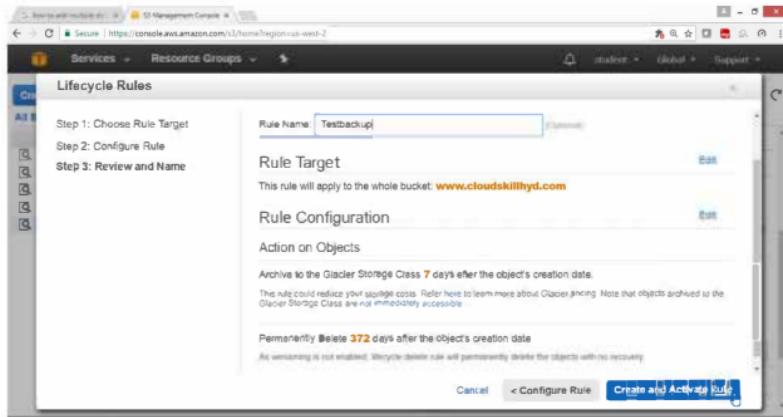
Select the check box **Permanently Delete** → 372

click on **Review**



Provide Rule Name → Testbackup

click on “Create and Activate Rule” button



Click on Save button

The screenshot shows the AWS Management Console for S3 buckets. On the left, a sidebar lists buckets: cloudmihai, cristic, saleshybucket1, srikanthy, and www.cloudskilthy.com. The main area is titled 'Lifecycle' under 'Versioning'. It explains how lifecycle rules manage object versions. A specific rule, 'TestBackup', is highlighted. The rule is enabled and targets the whole bucket. The 'Save' button at the bottom right is circled in red.

Verify Storage Class is Standard

The screenshot shows the AWS Management Console for an S3 folder named 'contact-us.html'. The table lists several files with their storage classes, sizes, and last modified dates. All files are listed as 'Standard' storage class.

Name	Storage Class	Size	Last Modified
404.html	Standard	6 KB	Tue Aug 15 08:46:32 GMT+01:00 2015
about-us.html	Standard	5.8 KB	Tue Aug 15 08:46:33 GMT+01:00 2015
article.html	Standard	5.3 KB	Tue Aug 15 08:46:34 GMT+01:00 2015
articles.html	Standard	4.8 KB	Tue Aug 15 08:46:34 GMT+01:00 2015
contact-us.html	Standard	4.7 KB	Tue Aug 15 08:46:35 GMT+01:00 2015
css	-	-	-
images	-	-	-
index.html	Standard	6 KB	Tue Aug 15 08:46:36 GMT+01:00 2015
js	-	-	-
sitemap.html	Standard	4.8 KB	Tue Aug 15 08:46:37 GMT+01:00 2015

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

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with 'Services' (selected), 'Resource Groups', and other account-related options like 'student', 'Global', and 'Sup...'. Below the navigation is a toolbar with 'Upload', 'Create Folder', 'Actions' (with dropdown options 'Versions', 'Hide', and 'Show'), and a search bar labeled 'Search by prefix' with a magnifying glass icon. To the right of the search bar are buttons for 'None', 'Properties', and 'Transfers'. A 'Switch to new console' link is also present. The main area displays a table of uploaded files:

Name	Storage Class	Size	Last Modified
How I Lowered My Cholesterol From 266 to 151 Without Drugs - YouTube [360p]	Glacier	6.4 MB	Thu Apr 13 20:37:27 GMT+0
butter that lowers cholesterol natural way to lower cholesterol how to - YouTube	Glacier	10 MB	Thu Apr 13 20:36:58 GMT+0

To Restore go to the bucket select the file

Right click and select **Initiate Restore**

The screenshot shows the AWS S3 Management Console. A context menu is open over a file named "How I Lowered My Cholesterol From 266 to 151 Without Drugs - YouTube'Brien - Glacier". The menu options include Open, Download, Make Public, Rename, Delete, Initiate Restore, Cut, and Copy. The "Initiate Restore" option is highlighted with a yellow arrow.

Provide number of days → 1

Click on OK

The screenshot shows the "Initiate Restore" dialog box. It contains the following text:  
Initiate a restore operation by specifying the number of days for which your archived data will be temporarily accessible. Once initiated, the data will be accessible in 3 to 5 hours. You can view the status of your restore operation in the properties pane for the object(s).  
A text input field shows "1" days selected. Below it is a note: You are charged a Glacier retrieval fee if you choose to restore more than 5% of your average monthly storage (pro-rated daily) in a month. Click here to learn more.  
At the bottom are "OK" and "Cancel" buttons, with "OK" being highlighted.

Verify

File will get restored after 1 Day

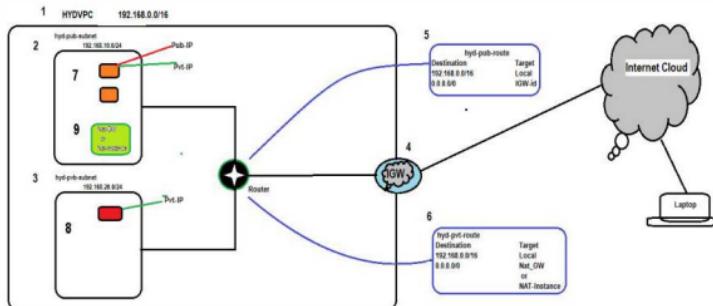
Storage class will become Standard.

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

### OBJECTIVE

To configure Amazon Virtual Private Cloud with public and private subnet

### TOPOLOGY



### PRE-REQUISITES

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.

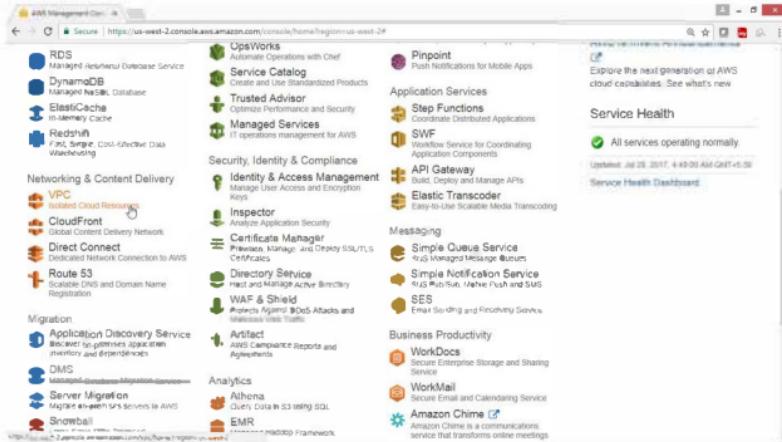
## 1) To create your own VPC

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

The screenshot shows the AWS VPC Management Dashboard. On the left, there's a sidebar with various VPC-related options like Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The 'My VPCs' option is selected and highlighted with a yellow box. In the main content area, there's a search bar at the top labeled 'Search VPCs and their properties'. Below it is a table with one row of data:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
default-vpc-oregon	vpc-80c341ee	available	172.31.0.0/16		dhcp-options-set-10

Below the table, there's a message: 'Select a VPC above.' At the bottom of the page, there's a footer with links for 'AWS Home', 'AWS Support', 'AWS Marketplace', 'AWS Documentation', 'AWS API Reference', and 'AWS Terms of Use'.

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

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Feedback English

Privacy Policy Terms of Use

© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

2) To create public subnet

Click on Subnet

Click on Create Subnet button

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Feedback English

Privacy Policy Terms of Use

© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

### 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

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like Services, Resource Groups, VPC Dashboard, and Subnets (which is selected). The main area is titled 'Create Subnet' and shows a table of subnets. One row is highlighted: 'hyd-pub-subnet' with Subnet ID 'subnet-b3bdbefb'. The table includes columns for Name, Subnet ID, State, VPC, IPv4 CIDR, and Available. Below the table, a detailed view of 'subnet-b3bdbefb | hyd-pub-subnet' is shown with tabs for Summary, Route Table, Network ACL, Flow Logs, and Tags. The summary tab displays the Subnet ID, Availability Zone (us-west-2a), and other basic details.

### 3) To create private subnet

Click on Subnet

Click on Create Subnet button

This screenshot is similar to the previous one but shows a different state for the subnets. The 'hyd-pub-subnet' is now listed as 'available' with Subnet ID 'subnet-b3bdbefb'. A new subnet, 'Hyd-pvt-subnet', has been created and is listed below it with Subnet ID 'subnet-19d9f141'. The rest of the interface is identical, showing the detailed view for the newly created private subnet.

### 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

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The 'Subnets' option is selected. The main area is titled 'Create Subnet' and 'Subnet Actions'. A search bar says 'Search Subnets and their pro: X'. Below it is a table with columns: Name, Subnet ID, State, VPC, IPv4 CIDR, and Available. The table shows five subnets, including the newly created 'hyd-pvt-subnet' which is in the 'available' state. The table also lists other subnets from different VPCs and regions. At the bottom, there's a summary for 'subnet-6abcbf23 | hyd-pvt-subnet' with tabs for Summary, Route Table, Network ACL, Flow Logs, and Tags. It shows the Subnet ID, Availability Zone (us-west-2a), and the fact that it's attached to a default route table.

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

In VPC Dashboard panel

Click on Internet Gateway

This screenshot is identical to the previous one, showing the AWS VPC Management Console. The difference is that the 'Internet Gateways' option in the sidebar is highlighted with a mouse cursor, indicating the next step in the process.

**Click on Create Internet Gateway button**

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with navigation links: VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways (which is selected), Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main content area has a search bar at the top labeled "Search Internet Gateways and X". Below it is a table with columns: Name, ID, State, and VPC. One row is visible: "igw-0aa7f1f0a" with state "attached" and VPC "vpc-80c341ee | default-vpc-oregon". Below the table, there's a message "Select an Internet gateway above" and a "Create Internet Gateway" button. At the bottom of the page, there are links for Feedback, English, and Terms of Use.

In **Create Internet Gateway**, box

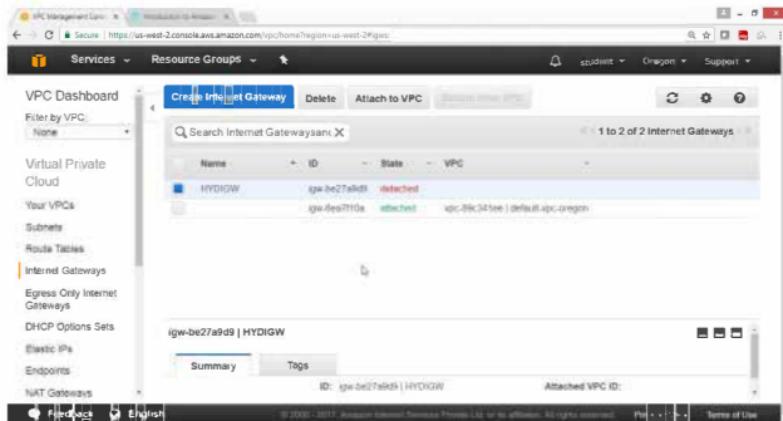
For **Name tag** → HYDIGW

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

This screenshot shows the "Create Internet Gateway" dialog box. It contains a brief description: "An Internet gateway is a virtual router that connects a VPC to the Internet." Below this is a "Name tag" input field containing "HYDIGW". At the bottom right of the dialog are two buttons: "Cancel" and "Yes, Create". The background shows the same VPC Management Console interface as the previous screenshot, with the "Create Internet Gateway" button highlighted in blue.

## Verify

Internet gateway is created



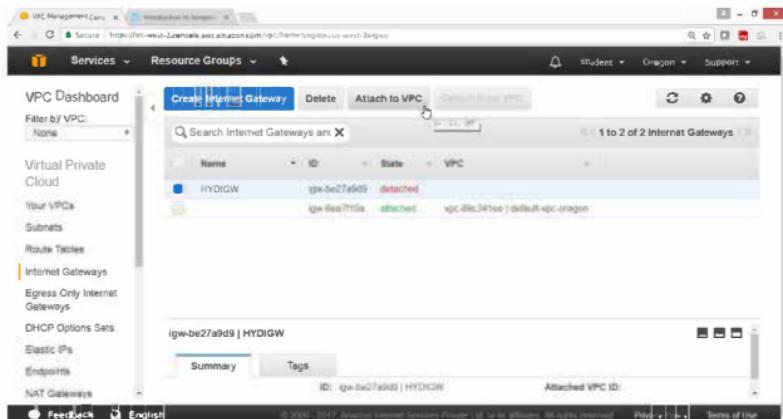
The screenshot shows the AWS VPC Management Console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#igw>. The left sidebar navigation includes: Services, Resource Groups, VPC Dashboard, Filter by VPC (None), Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways (selected), Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main content area displays a table titled 'Internet Gateways' with one entry:

Name	ID	State	VPC
HYDIGW	igw-be27a9d9	detached	

A modal window titled 'igw-be27a9d9 | HYDIGW' is open, showing the 'Summary' tab with the ID 'igw-be27a9d9 | HYDIGW' and the 'Attached VPC ID' field empty. The 'Tags' tab is also visible.

Select HYDIGW

Click "Attach to VPC"



The screenshot shows the same AWS VPC Management Console interface. The table in the main content area now shows the 'HYDIGW' entry with the 'Attached to VPC' status changed to 'attached':

Name	ID	State	VPC
HYDIGW	igw-be27a9d9	attached	vpc-8fc343ee   default-vpc-oregon

The modal window for 'igw-be27a9d9 | HYDIGW' is still open, showing the 'Summary' tab with the attached VPC information.

In "Attach to VPC" box

For VPC → HYDVPC

click on "Yes, Attach" button



## Verify

Internet gateway is connected to your VPC

The screenshot shows the AWS VPC Dashboard. The left sidebar lists services: VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways (which is selected), Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main content area displays a table of Internet Gateways. One row is selected, showing details for 'igw-be27a9d9 | HYDIGW'. The table includes columns for Name, ID, State, and VPC. The 'State' column shows 'attached' for both rows. The 'VPC' column shows 'vpc-7d934d1b | HYDVPC' for the first row and 'vpc-6fc341ee | default vpc oregon' for the second row. Below the table, a summary card for 'igw-be27a9d9 | HYDIGW' shows its ID and Attached VPC ID.

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

On VPC Dashboard panel

Click on Route Table

The screenshot shows the AWS VPC Management Console. On the left sidebar, under the 'Route Tables' section, there is a blue highlighted button labeled 'Create Route Table'. The main content area displays a table of existing route tables:

Name	ID	State	VPC
HYDIGW	igw-be27af9d	attached	vpc-7d934d1b   HYDVPC
	igw-be27af9d	attached	vpc-89c341ee   default-vpc-oregon

Below the table, a specific route table is selected: 'igw-be27af9d | HYDIGW'. The 'Summary' tab is active, showing the ID 'igw-be27af9d | HYDIGW' and the 'Attached VPC ID' 'vpc-7d934d1b | HYDVPC'. At the bottom of the page, there are links for 'Price' and 'Terms of Use'.

Click on "Create Route table" button

The screenshot shows the 'Create Route Table' dialog box. At the top, there is a 'Create Route Table' button. Below it, a table lists existing route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
(E-)199fc27e	(E-)199fc27e	0 Subnets	No	vpc-89c341ee   default-vpc-oregon
(E-)847d52e2	(E-)847d52e2	0 Subnets	Yes	vpc-7d934d1b   HYDVPC

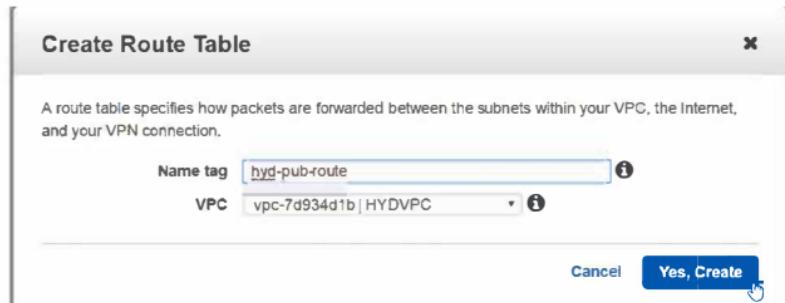
Below the table, a message says 'Select a route table above.' At the bottom of the dialog, there are 'Feedback' and 'English' buttons, along with copyright information: '© 2006 - 2017 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.'

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

The screenshot shows the AWS VPC Management Console with the 'Route Tables' section selected. The left sidebar lists various VPC components like Virtual Private Cloud, Your VPCs, Subnets, and Route Tables. The main area displays a table of route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	No	No	vpc-7d934d1b   HYDVPC
	rtb-199c27e	No	Yes	vpc-7f9341ee   default.vpc.oregon
	rtb-847d5262	No	Yes	vpc-7d934d1b   HYDVPC

Below the table, a detailed view for the first route table (rtb-234b6445) is shown with tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags. The Summary tab is selected, showing the Route Table ID as 'rtb-234b6445 | hyd-pub-route'.

Click on "Subnet Association" button

VPC Dashboard  
Filter by VPC:  
None

Virtual Private Cloud  
Your VPCs  
Subnets  
Route Tables  
Internet Gateways  
Egress Only Internet Gateways  
DHCP Options Sets  
Elastic IPs  
Endpoints  
NAT Gateways

Services Resource Groups

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	No	No	vpc-7d934d1b   HYD-VPC
	rtb-1509c27e	No	Yes	vpc-48c341ee   default-vpc-oregon
	rtb-847d52e2	No	Yes	vpc-7a934d1b   HYD-VPC

rtb-234b6445 | hyd-pub-route

Summary Routes Subnet Associations Route Propagation Tags

Main: rtb-234b6445 | hyd-pub-route

Edit English

Click on Edit button

VPC Dashboard  
Filter by VPC:  
None

Virtual Private Cloud  
Your VPCs  
Subnets  
Route Tables  
Internet Gateways  
Egress Only Internet Gateways  
DHCP Options Sets  
Elastic IPs  
Endpoints  
NAT Gateways

Services Resource Groups

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	No	No	vpc-7d934d1b   HYD-VPC

rtb-234b6445 | hyd-pub-route

Summary Routes Subnet Associations Route Propagation Tags

**Edit**

Subnet IPv4 CIDR IPv6 CIDR

You do not have any subnet associations.  
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Feedback English

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

VPC Dashboard

Services Resource Groups

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

1 to 3 of 3 Route Tables

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	0 Subnets	No	vpc-748544fb   HYDAPC

rtb-234b6445 | hyd-pub-route

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

Associate Subnet

IPv4 CIDR IPv6 CIDR Current Route Table

subnet-630db6fa | hyd-pub-subnet 192.168.10.0/24 Main

subnet-64fcf2f2 | hyd-pub-subnet 192.168.10.0/24 Main

Feedback English

© 2016 - 2017 Amazon Internet Services LLC or its affiliates. All rights reserved. Privacy Terms of Use

## Verify

hyd-pub-subnet is associated with routing table

VPC Dashboard

Services Resource Groups

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

1 to 3 of 3 Route Tables

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-1986c2fe	rtb-1986c2fe	0 Subnets	Yes	vpc-ff9c54ee   default-vpc-oregon
rtb-0f1652e2	rtb-0f1652e2	0 Subnets	Yes	vpc-748544fb   HYDAPC

rtb-234b6445 | hyd-pub-route

Summary Routes Subnet Associations Route Propagation Tags

Edit

Subnet IPv4 CIDR IPv6 CIDR

subnet-630db6fa | hyd-pub-subnet 192.168.10.0/24

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table.

Feedback English

© 2016 - 2017 Amazon Internet Services LLC or its affiliates. All rights reserved. Privacy Terms of Use

Click on **Route** Button

Click on **Edit** button

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like VPC Dashboard, Virtual Private Cloud, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The 'Route Tables' section is selected. In the main area, there's a table titled '1 to 3 of 3 Route Tables'. One row is selected, showing 'rtb-234b6445 | hyd-pub-route'. Below the table, there are tabs for Summary, Routes, Subnet Associations (which is active), Route Propagation, and Tags. Under 'Subnet Associations', there's a 'Edit' button. A cursor is hovering over this 'Edit' button.

Click on "Add another route" button

This screenshot is from the same VPC Management Console as the previous one, but it shows a different state. The 'Subnet Associations' tab is still active, but the 'Edit' button is now replaced by a 'Save' button. At the bottom of the 'Subnet Associations' section, there's a link labeled 'View... All rules.' followed by a button labeled 'Add another route'. A cursor is hovering over this 'Add another route' button.

For Destination → 0.0.0.0/0

For Target → select HYDIGW

Click on **Save** button

The screenshot shows the AWS VPC Management Console with the 'Create Route Table' dialog open. The 'Routes' tab is selected. A new route is being added with the following details:

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	igw-ec27a8d9   HYDIGW	Active	No	(Delete)

At the bottom right of the dialog, there is a blue 'Save' button.

## Verification

Public route is added through internet gateway

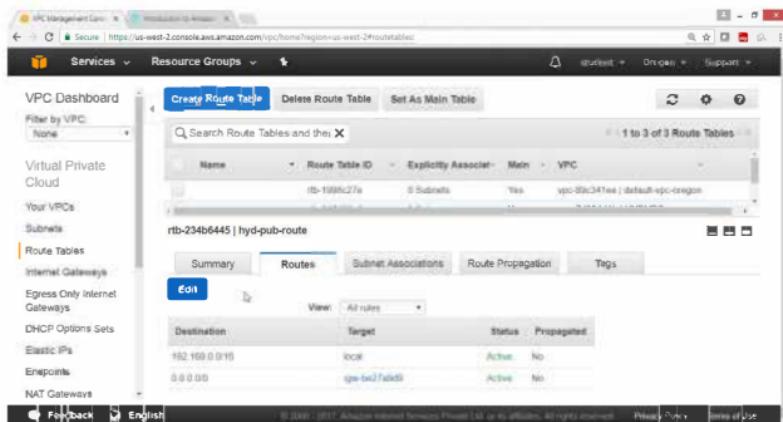
The screenshot shows the AWS VPC Management Console with the 'Create Route Table' dialog open. The 'Routes' tab is selected. The previously added route is listed:

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	igw-be27a8d9	Active	No	(Delete)

At the bottom right of the dialog, there is a blue 'Save' button.

## Verify

Status column show Active



The screenshot shows the AWS VPC Management Console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#routetables>. The left sidebar is collapsed, and the main area displays the 'Route Tables' section. A single route table, 'rtb-234b6445 | hyd-pub-route', is listed. The 'Routes' tab is selected, showing two entries:

Destination	Target	Status	Propagated
10.169.0.0/16	IGRP	Active	No
0.0.0.0	gw-ec27add8	Active	No

**6) Create Private Routing Table, associate subnet and add routing rules**  
On VPC Dashboard panel

Select Route Tables

Click on "Create Route Table"

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like Services, Resource Groups, VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables (which is selected), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main area shows a list of Route Tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	(rt-234b6445)	1 Subnet	No	vpc-7d934d1b   HYDVPC
	(rt-1986c27e)	2 Subnets	Yes	vpc-86c341ee   default-vpc-oregon
	(rt-847d5262)	8 Subnets	Yes	vpc-7d934d1b   HYDVPC

Below this, a specific route table is selected: "rtb-234b6445 | hyd-pvt-route". It has tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags. The Routes tab is active, showing one entry: "Destination: 0.0.0.0/0 Target: 172.31.1.1 Status: Propagated". At the bottom of this section, there are buttons for Feedback, English, and a license notice.

On "Create Route Table" box

For Name tag → hyd-pvt-route

For VPC → HYDVPC

Click on "Yes, Create" button

The dialog box is titled "Create Route Table". It contains a descriptive text: "A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection." Below this, there are two input fields: "Name tag" with the value "hyd-pvt-route" and "VPC" with the value "vpc-7d934d1b | HYDVPC". At the bottom right, there are "Cancel" and "Yes, Create" buttons, with "Yes, Create" being highlighted.

## Verify

hyd-pvt-route table is created

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Electric IPs

Endpoints

NAT Gateways

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b   HYDVPCC
hyd-pub-route	rtb-204b6445	1 Subnet	No	vpc-7d934d1b   HYDVPCC
	rtb-1889c2fe	0 Subnets	Yes	vpc-88c341ee   default-vpc-oregon
	rtb-0f89c2fe	0 Subnets	Yes	vpc-7d934d1b   HYDVPCC

rtb-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit View: All rules

Destination Target Status Propagated

Click on Subnet Association button

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Electric IPs

Endpoints

NAT Gateways

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b   HYDVPCC
hyd-pub-route	rtb-204b6445	1 Subnet	No	vpc-7d934d1b   HYDVPCC
	rtb-1889c2fe	0 Subnets	Yes	vpc-88c341ee   default-vpc-oregon
	rtb-0f89c2fe	0 Subnets	Yes	vpc-7d934d1b   HYDVPCC

rtb-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit View: All rules

Destination Target Status Propagated

Click on Edit button

The screenshot shows the AWS VPC Management Console. On the left sidebar, under 'Route Tables', 'hyd-pvt-route' is selected. In the main area, a table lists four route tables. The 'hyd-pvt-route' row is selected. Below the table, tabs for 'Summary', 'Routes', 'Subnet Associations', 'Route Propagation', and 'Tags' are visible. The 'Subnet Associations' tab is active, and the 'Edit' button is highlighted with a mouse cursor.

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b   HYD-VPC
hyd-pub-route	rtb-234b445	1 Subnet	No	vpc-7d934d1b   HYD-VPC
	rtb-199c27e	0 Subnets	Yes	vpc-68341ee   default-vpc-oregon
	rtb-847b52e	0 Subnets	Yes	vpc-7d934d1b   HYD-VPC

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

The screenshot shows the 'Subnet Associations' tab for the 'hyd-pvt-route' route table. It lists two subnets: 'subnet-83bcbf0a | hyd-pvt-subnet' (selected) and 'subnet-8abcbf23 | hyd-pvt.subnet'. The 'Associate' column has checkboxes for both. The 'IPv4 CIDR' and 'IPv6 CIDR' columns show '192.168.20.0/24' and '-' respectively. The 'Current Route Table' column shows 'rtb-234b445 | hyd-pub-route' for the first subnet and 'Main' for the second. The 'Save' button is highlighted with a mouse cursor.

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-83bcbf0a   hyd-pvt-subnet	192.168.20.0/24	-	rtb-234b445   hyd-pub-route
<input checked="" type="checkbox"/>	subnet-8abcbf23   hyd-pvt.subnet	192.168.20.0/24	-	Main

Click on Save button

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables (which is selected), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main area is titled 'Create Route Table' and shows a table of route tables. One row is selected: 'hyd-pvt-route' (Route Table ID: rtb-ac446bca). Below the table, there are tabs for Summary, Routes, Subnet Associations (which is selected), Route Propagation, and Tags. At the bottom, there's an 'Edit' button and a green 'Save Successful' message. The message says: 'The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table: subnet-6aacb23 | hyd-pvt-subnet | 192.168.20.0/24'.

## Verify

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

This screenshot is from the same VPC Management Console as the previous one. The sidebar and the 'Create Route Table' section are identical. The 'Subnet Associations' tab is selected under the 'hyd-pvt-route' table. It shows a single entry: 'subnet-6aacb23 | hyd-pvt-subnet | 192.168.20.0/24'. The message below it states: 'The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:'.

## Click on Route button

The screenshot shows the AWS VPC Management Console with the 'Route Tables' section selected. A specific route table, 'hyd-pvt-route', is selected. The 'Subnet Associations' tab is active, showing one association for subnet 'subnet-ac446bc3' with a target of '192.168.20.0/24'. Below this, a note states: 'The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table.'

Note: No need to add IGW in pvt route

The screenshot shows the same AWS VPC Management Console interface, but the 'Routes' tab is now active. It displays a single route entry: '192.168.0.0/16' pointing to the target '0.0.0.0/0'. The status is 'Active' and 'Propagated'.

## 7) To launch Windows instance in Public subnet

Open the AWS console

Click on Services

Click on Ec2 services

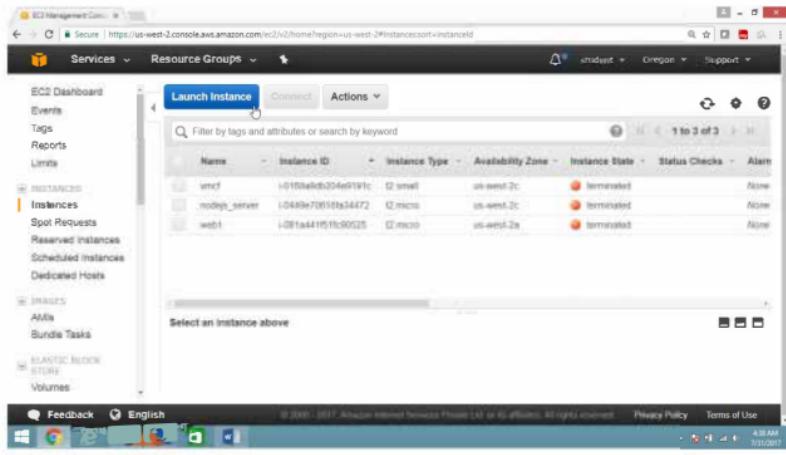
The screenshot shows the AWS Management Console with the Services menu open. The EC2 icon is highlighted, indicating it is selected. Other services listed include VPC, Storage (with S3, EBS, and Glacier), and Database (with Amazon RDS, Amazon Redshift, and Amazon DynamoDB). To the right, there are sections for Developer Tools, Analytics, Application Services, Management Tools, Artificial Intelligence, Messaging, Business Products, and Account Attributes.

The screenshot shows the AWS Management Console EC2 Dashboard. On the left, there are navigation links for Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, AMIs, and Volumes. The main area displays EC2 resources: 0 Running Instances, 0 Dedicated Hosts, 0 Volumes, 0 Key Pairs, 0 Elastic IPs, 0 Snapshots, 0 Load Balancers, and 2 Security Groups. A callout box provides information about Amazon Lightsail. Below this, there is a "Create Instance" section with a "Launch Instance" button. On the right, there are sections for Account Attributes (Supported Platforms: VPC, Default VPC: vpc-09c34fee, Resource ID length management) and Additional Information (Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us).

On the EC2 dashboard panel

Click on **instance**

Click on **Launch instance** button



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

Free tier eligible

The screenshot shows the AWS Lambda Management Console interface. The user is on Step 1: Choose an Amazon Machine Image (AMI). They have selected the 'Microsoft Windows Server 2012 Base - ami-a1c1ddd8' option, which is described as 'Microsoft Windows 2012 Standard edition with 64-bit architecture [English]'. The 'Select' button is highlighted. Other options listed are 'Microsoft Windows Server 2012 with SQL Server Express - ami-7ac8da03' and 'Microsoft Windows Server 2012 with SQL Server Web - ami-f2cd1d8b', each with their own 'Select' button.

On the "Choose an Instance Type" page

Select "General purpose t2.micro"

Click on "Next Configure Instance Details" button

The screenshot shows the AWS Lambda Management Console interface. The user is on Step 2: Choose an Instance Type. They have selected the 't2.micro' instance type from the 'General purpose' family. The 'Free tier eligible' status is shown next to the 't2.micro' entry. The 'Review and Launch' button is highlighted at the bottom of the table.

On the “Configuration Instance Details” page

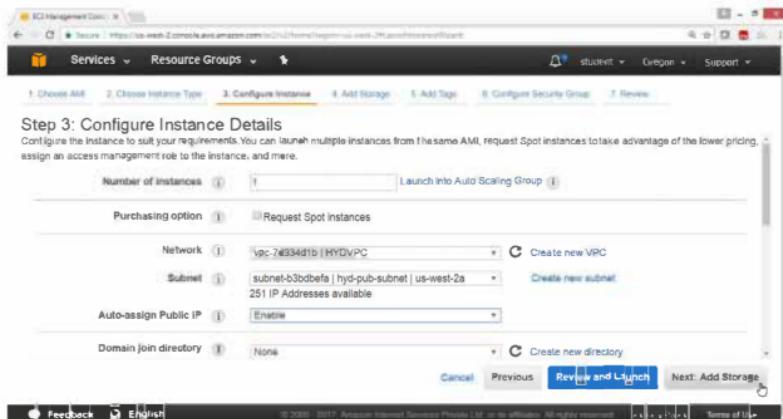
For “Number of instances” → 1

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

Step 4: Add Storage

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (Mbps)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-01e5be77f781e7266	30	General Purpose EBS	100 / 3000	N/A	Yes	Not Encrypted

Add New Volume

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

Cancel Previous Review and Launch Next: Add Tags

Click on “Add tag” button

Step 5: Add Tags

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

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
This resource currently has no tags					

Choose the Add tag button or click to add a Name tag.  
Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

For "Key" → Name

For Value → Winpubvm

Click on "Next: Configure Security Group"

The screenshot shows the 'Add Tags' step of the EC2 instance creation process. At the top, there are tabs for '1. Choose AMI', '2. Choose Instance Type', '3. Configure Instances', '4. Add Storage', '5. Add Tags' (which is highlighted in yellow), '6. Configure Security Group', and '7. Review'. Below the tabs, a note says: 'A tag consists of a case-sensitive key/value pair. For example, you could define a tag with key = Name and value = Webserver.' It also states: 'A copy of a tag can be applied to volumes, instances or both.' A note at the bottom says: 'Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.' The main form has 'Key' set to 'Name' and 'Value' set to 'Winpubvm'. There are 'Instances' and 'Volumes' dropdowns. Below the input fields is a button 'Add another tag' with the note '(Up to 50 tags maximum)'. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is blue), and 'Next: Configure Security Group'. The status bar at the bottom includes links for 'Feedback', 'English', and 'AWS Support'.

On the “Configure Security Group” page

Take Default Values

Click on “Review and Launch” button

Step 6: Configure Security Group

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

Assign a security group:  Create a new security group.  Select an existing security group

Security group name: launch-wizard-1

Description: launch-wizard-1 created 2017-07-31T05:02:04.626+05:00

Type	Protocol	Port Range	Source
RDP	TCP	3389	Custom 0.0.0.0/0

Add Rule

Cancel Previous Review and Launch

Click on “Launch” button

Step 7: Review Instance Launch

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

**⚠ Improve your instances' security. Your security group, launch-wizard-1, is open to the world.**

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.

You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details

Microsoft Windows Server 2012 Base - aml-a1c1ddd8

Free tier Microsoft Windows 2012 Standard edition with 64 bit architecture [English]

Review instance type, AMI, and configuration now

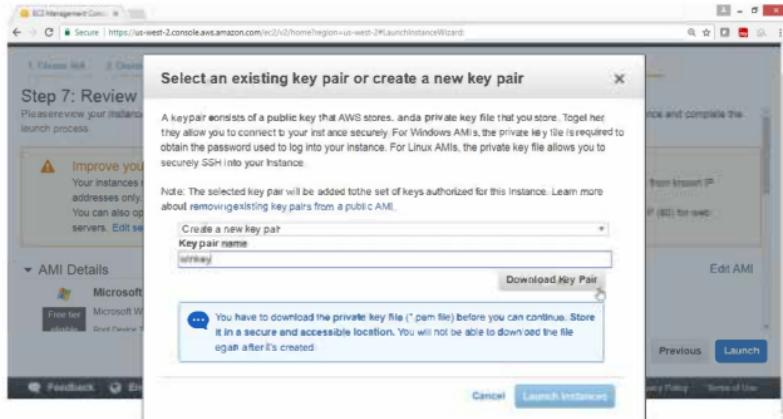
Cancel Previous Launch

Define key pair and launch Terms of Use

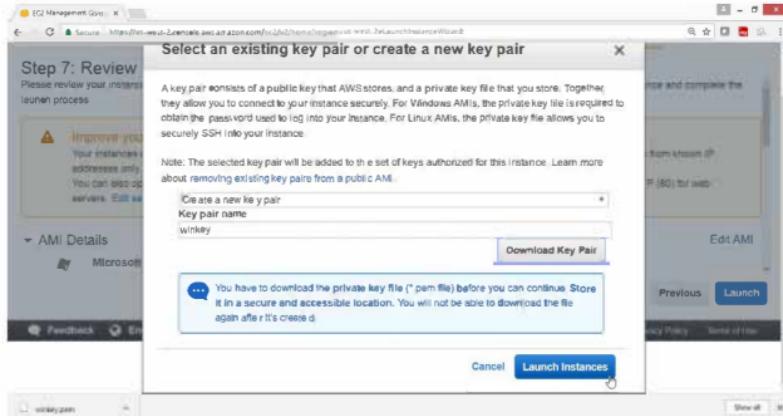
Select "Create a new key pair"

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

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#launchInstanceWizard>. The page title is "Launch Status". A sub-header says "Click View Instances to monitor your instances' status. Once your instances are in the running state, you can connect to them from the Instances screen. Find out how to connect to your instances." Below this, a section titled "Here are some helpful resources to get you started" lists links to the Amazon EC2 User Guide, Amazon EC2 Microsoft Windows Guide, and the Amazon EC2 Discussion Forum. Further down, under "While your instances are launching you can also", there are three links: "Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)", "Create and attach additional EBS volumes (Additional charges may apply)", and "Manage security groups". At the bottom right is a blue "View Instances" button.

Verify that instance is Running

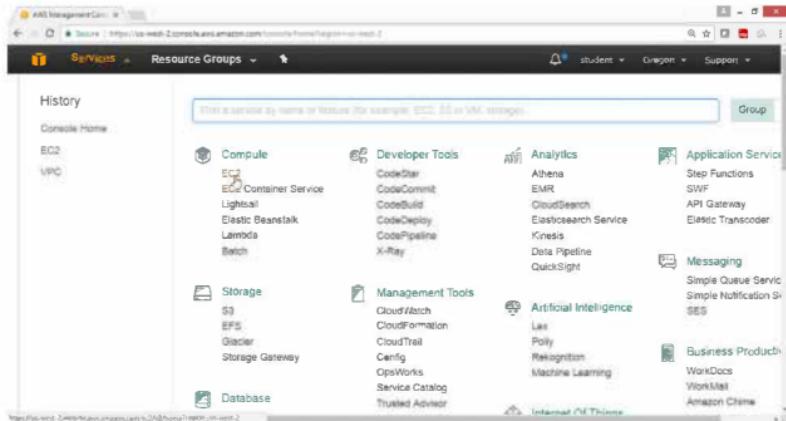
The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instances>. The left sidebar has sections for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Instances Requests, Reserved Instances, Scheduled Instances, and Dedicated Hosts. The Instances section shows a table with one row. The table columns are Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. The single row contains "Winpubvm", "i-0cb26994e13174e85", "t2.micro", "us-west-2a", "running", "running", and "None". Below the table, a detailed view for "Instance: i-0cb26994e13174e85 (Winpubvm)" is shown. It includes tabs for Description, Status Checks, Monitoring, and Tags. Under Description, it shows Public IP: 54.202.132.130, Instance ID: i-0cb26994e13174e85, and Public DNS (IPv4). At the bottom right of the main content area are "View" and "Edit" buttons, and a "Feedback" link at the bottom left.

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

Open the AWS console

Click on Services

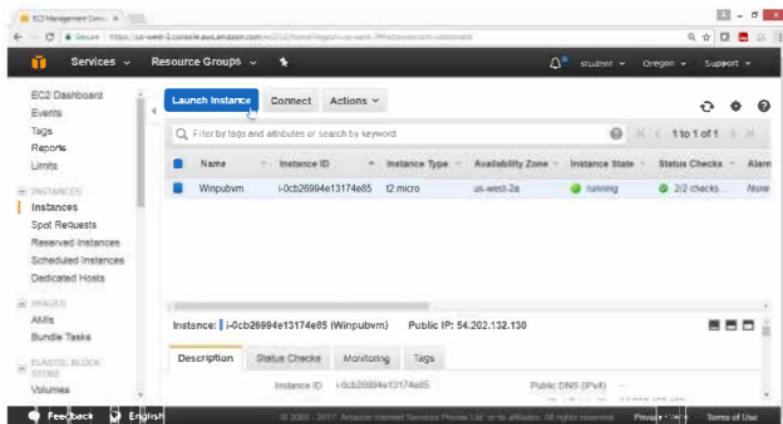
Click on EC2 services



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 eligible

The screenshot shows the AWS Management Console interface for launching a new EC2 instance. The top navigation bar includes 'Services' (selected), 'Resource Groups', and tabs for 'Launch Instance Wizard' (step 1: Choose AMI, currently active), 'Choose Instance Type', 'Configure Instance', 'Add Storage', 'Add Tags', 'Configure Security Group', and 'Review'. Below the tabs, the heading 'Step 1: Choose an Amazon Machine Image (AMI)' is displayed. A search bar is present above the list of AMIs. The list shows four Windows-based AMIs:

- Microsoft Windows Server 2016 with SQL Server Standard - ami-39fae640**: 64-bit, Select button.
- Microsoft Windows 2016 Datacenter edition - Microsoft SQL Server 2016 Standard [English]**: 64-bit, Select button.
- Microsoft Windows Server 2012 R2 Base - ami-3dccb744**: 64-bit, Select button.
- Microsoft Windows Server 2012 R2 with SQL Server Express - ami-3bc8d442**: 64-bit, Select button.

At the bottom of the page, there are links for 'Feedback', 'English', and '© 2006-2017 Amazon Internet Services Process LLC or its affiliates. All rights reserved. Privacy Policy | Terms of Use'.

On the “Choose an Instance Type” page

Select “General purpose t2.micro”

Click on “Next Configure Instance Details” button

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'student' and 'Oregon'. Below the navigation is a breadcrumb trail: '1. Choose AMI' → '2. Choose Instance Type' (which is underlined in blue) → '3. Configure Instance' → '4. Add Storage' → '5. Add Tags' → '6. Configure Security Group' → '7. Review'. A dropdown menu 'Filter by:' is set to 'All Instance types' and 'Current generation'. The main content area is titled 'Step 2: Choose an Instance Type' with a sub-instruction 'Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz. Intel Xeon Family, 1 GiB memory, EBS only)'. A table lists available instance types:

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	<b>t2.micro</b> <small>Free tier eligible</small>	1	1	EBS only	+	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

At the bottom of the table are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is highlighted in blue), and 'Next: Configure Instance Details'.

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

The screenshot shows the 'Add Storage' step of the EC2 instance creation wizard. It displays configuration options for a single instance:

- Number of instances:** 1
- Purchasing option:** Request Spot Instances
- Network:** vpc-7d934d1b | HYDVPC
- Subnet:** subnet-6abccb23 | hyd-pvt-subnet | us-west-2a
- Auto-assign Public IP:** Disabled
- Domain join directory:** None

At the bottom right, there are 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Add Storage' buttons.

On the "Add Storage" page

Take default values

Click on "Next: Add tags" button

The screenshot shows the 'Add Tags' step of the EC2 instance creation wizard. It displays storage settings for the instance:

Volume Type	Device	Snapshot	Size (GB)	Volume Type	IDP	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snapshot-08c5bb7b19187abb	30	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/> Not Encrypted

Below the table, there is a note about free tier usage and a 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Add Tags' button at the bottom right.

Click on “Add tag” button

This screenshot shows the 'Add Tag' step in the EC2 Launch Instance Wizard. It displays a table for adding key-value pairs. A tooltip says: "This resource currently has no tags. Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags." Below the table is a large 'Add Tag' button with the placeholder "(Up to 50 tags maximum)". At the bottom are 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Configure Security Group' buttons.

For “Key” → Name

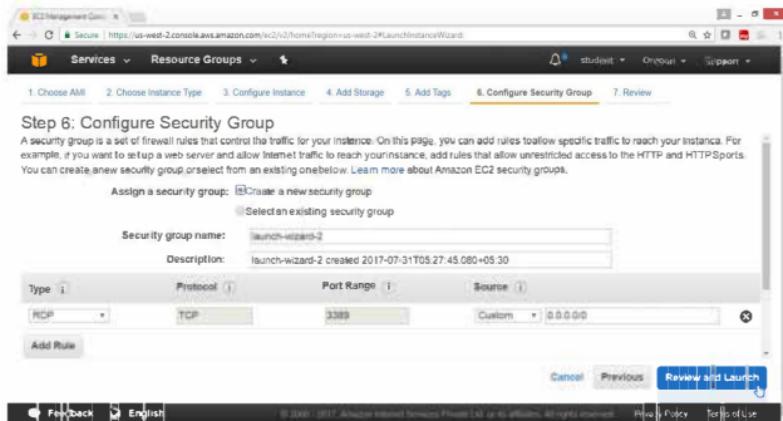
For Value → Winpvttvm

Click on “Next: Configure Security Group” button

This screenshot shows the 'Add Tag' step again, but now with a tag named 'Name' and a value of 'Winpvttvm' entered. The 'Value' field placeholder '(Up to 50 tags maximum)' is still visible. The 'Review and Launch' button is highlighted in blue at the bottom.

## Take Default Values

Click on “Review and Launch” button



Step 6: Configure Security Group

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

Assign a security group:  Create a new security group  
 Selected an existing security group

Security group name: launch-wizard-2

Description: launch-wizard-2 created 2017-07-31T05:27:45.080+05:30

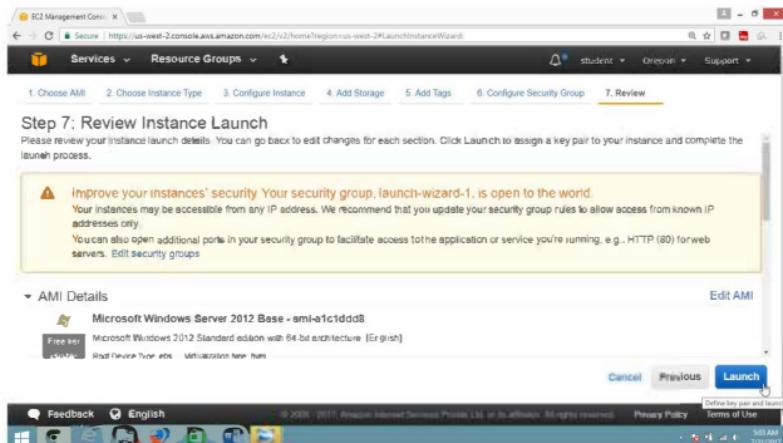
Type	Protocol	Port Range	Source
RDP	TCP	3389	Custom <input type="radio"/> 0.0.0.0/0

Add Rule

Cancel Previous Review and Launch

Drag down

Click on “Launch” button



Step 7: Review Instance Launch

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

**⚠ Improve your instances' security Your security group, launch-wizard-1, is open to the world.**  
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.  
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details

Microsoft Windows Server 2012 Base - ami-a1c1dd08

Free tier Microsoft Windows 2012 Standard edition with 64-bit architecture (English)

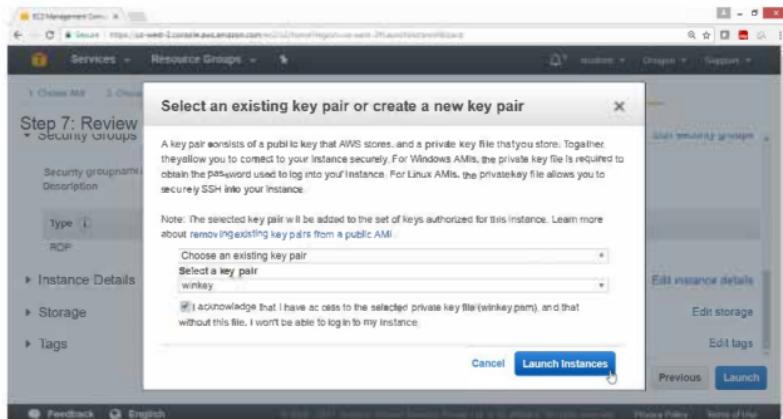
Launch

Select "Choose an existing key pair"

For "Key pair name" → winkey

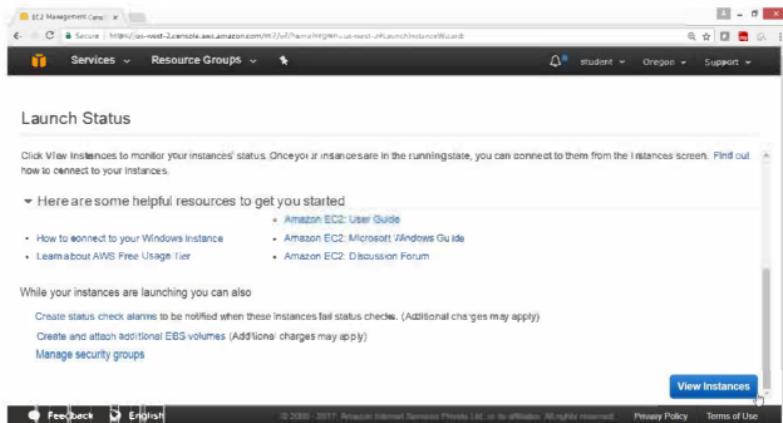
Select I acknowledge check box

Click on "Launch Instance" button



Check summary, Drag down

Click on "View Instance" button



## Verify that instance is Running

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Feedback, and English. The main content area has tabs for Launch Instance, Connect, and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Two instances are listed:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Winpubvm	i-0cb26994e13174e85	t2.micro	us-west-2a	running	2/2 checks	None
Winnpvtvm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks	None

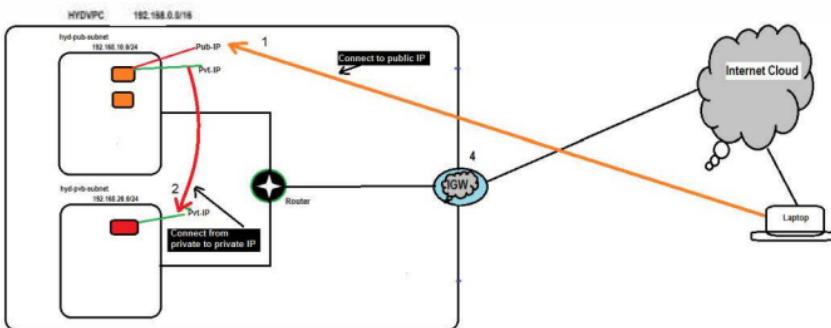
Below the table, a specific instance is selected: Instance: i-0e2251b25ee08fa4e (Winnpvtvm) Private IP: 192.168.20.87. There are tabs for Description, Status Checks, Monitoring, and Tags. Under Description, the instance ID is i-0e2251b25ee08fa4e and the Public DNS (IPv4) is listed as well.

## Verification

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

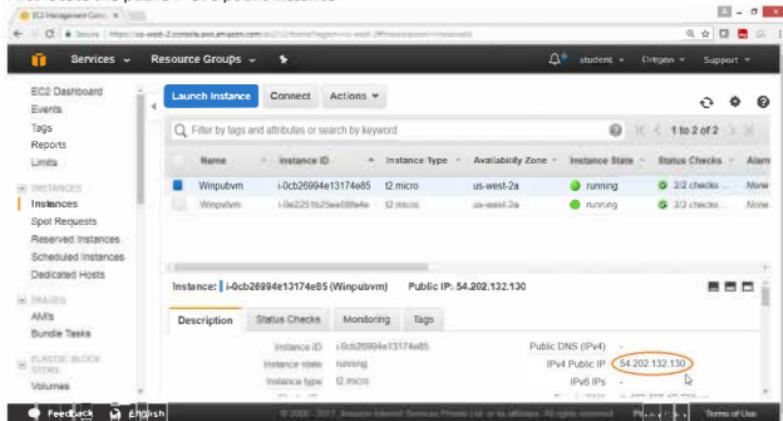
This screenshot is identical to the one above, showing the AWS EC2 Management Console. The sidebar and main content area are the same, displaying the status of two instances: Winpubvm and Winnpvtvm, both of which are running in the us-west-2a availability zone.

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



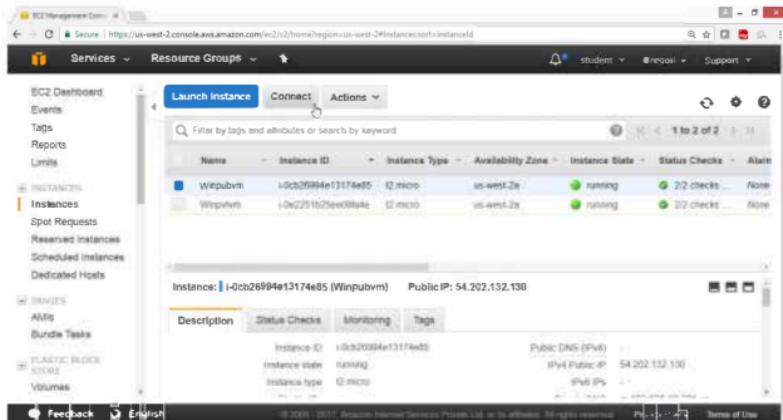
## 9) To Connect to Public subnet instance

First locate the public IP of a public instance



The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with navigation links like Services, Resource Groups, Instances, Images, and Volumes. The main area displays a table of running instances. One instance, 'Winpubvm' with Instance ID i-0cb26994e13174e85, is highlighted. Below the table, a detailed view for this instance shows its Public IP address: 54.202.132.130. This IP address is circled in red.

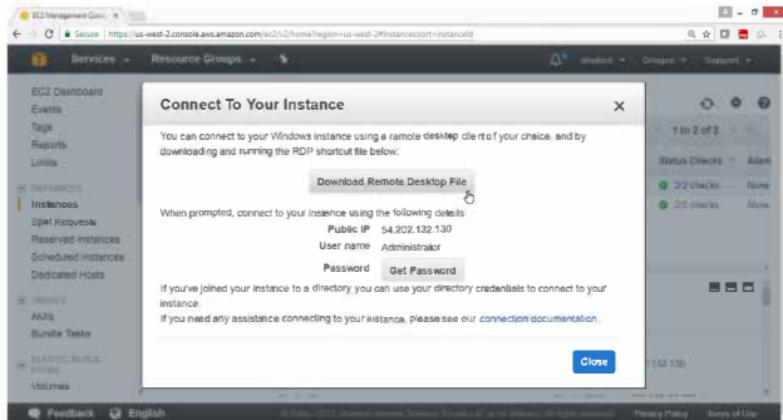
Click on “Connect” button



This screenshot is identical to the one above, showing the EC2 Management Console Instances page. The 'Connect' button in the top navigation bar is highlighted with a red circle. The rest of the interface, including the list of instances and the detailed view for 'Winpubvm', remains the same.

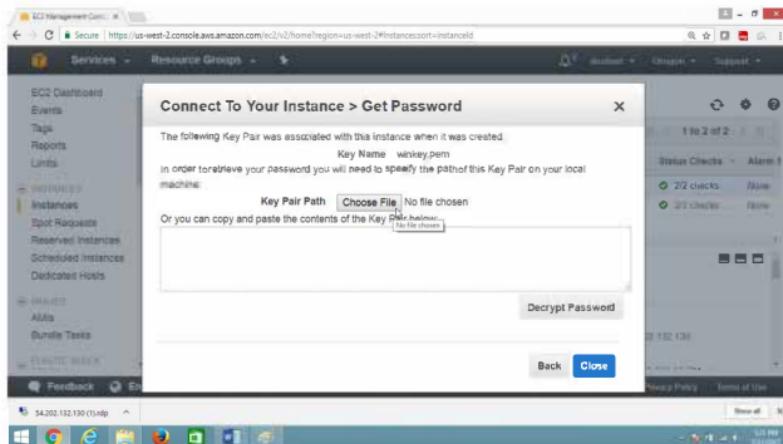
Click on "Download Remote Desktop file"

Click on "Get Password"



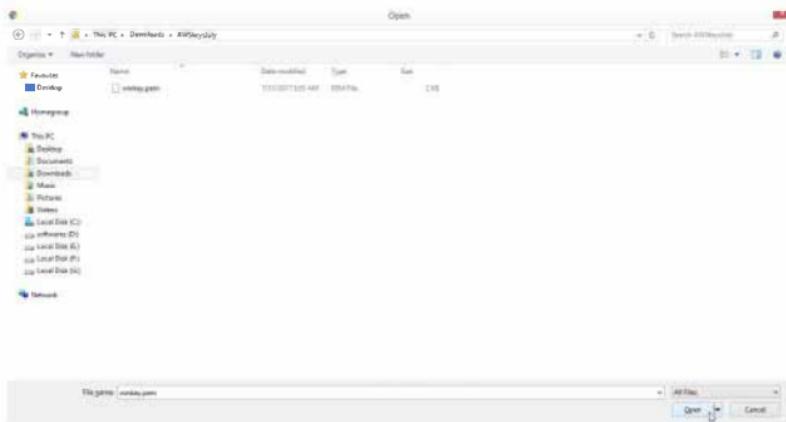
Provide the path of key file

Click on Choose file button

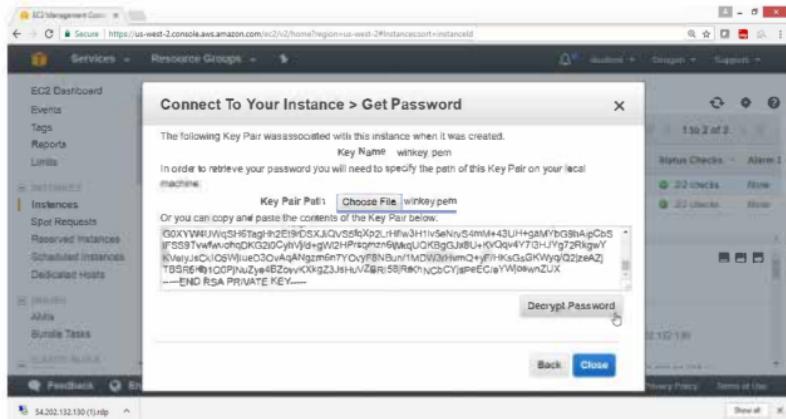


## Select the key file

Click on **Open** button



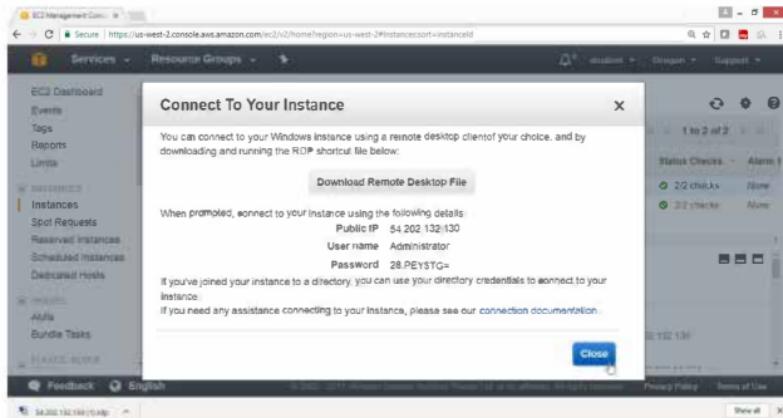
Now click on "Decrypt Password" button



## Verification

Password is generated copy in notepad

Click on **Close** button



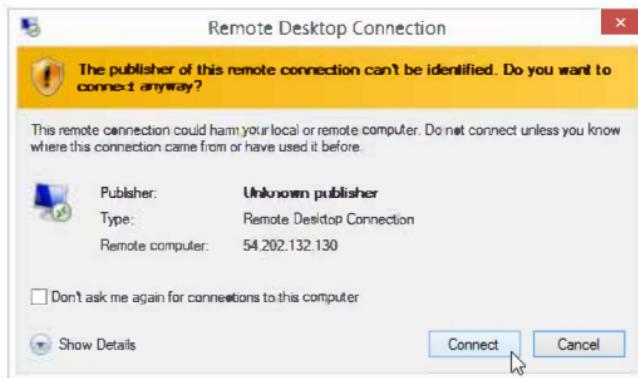
Double Click on RDP file

Provide Windows Username → Administrator

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

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with links for Services, Resource Groups, and various EC2-related categories like Instances, Images, and Elastic Block Store. The main area is titled 'Launch Instance' and shows a table of instances. One instance, 'Winpubvm', is highlighted. Below the table, a detailed view of 'Winpubvm' is shown with tabs for Description, Status Checks, Monitoring, and Tags. The 'Description' tab is active, displaying the instance ID, state, and type. The status checks tab shows 2/2 checks green. The monitoring tab indicates no metrics are being collected. The tags tab shows no tags. At the bottom of the page, there's a feedback section and a language selector set to English. The browser's taskbar at the bottom has two entries for '54.202.132.130 (1) [rdp]'.

Click on “Connect” button

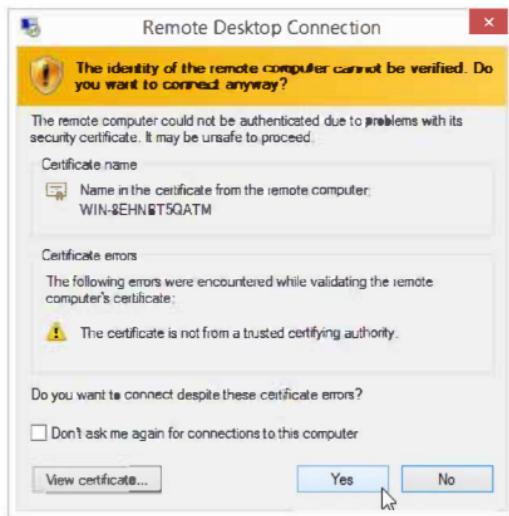


Paste the password

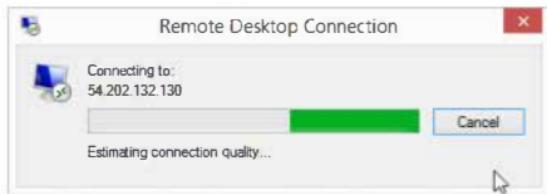
Click on **OK** button



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

EC2 Management Console <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instanceId=instanceId> student Oregon Support

Services Resource Groups

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Winpubvm	i-0cb20994e131f4e85	12 micro	us-west-2a	running	2/2 checks	None
Wnpvpm	i-0e2251a25ed0f8e	12 micro	us-west-2a	running	2/2 checks	None

Elastic IPs Availability zone: us-west-2a Private DNS: ip-192-168-20-87.us-west-2.compute.internal  
Security group: launch-wizard-2 - view Private IPs: 192.168.20.87  
Inbound rules Secondary private IPs:  
Scheduled events: No scheduled events VPC ID: vpc-7d934d10  
AMI ID: Windows Server Subnet ID: subnet-4ecbb83

Feedback English

Click on Connect button

EC2 Management Console <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instanceId=instanceId> student Oregon Support

Services Resource Groups

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Winpubvm	i-0cb20994e131f4e85	12 micro	us-west-2a	running	2/2 checks	None
Wnpvpm	i-0e2251a25ed0f8e	12 micro	us-west-2a	running	2/2 checks	None

Elastic IPs Availability zone: us-west-2a Private DNS: ip-192-168-20-87.us-west-2.compute.internal  
Security group: launch-wizard-2 - view Private IPs: 192.168.20.87  
Inbound rules Secondary private IPs:  
Scheduled events: No scheduled events VPC ID: vpc-7d934d10  
AMI ID: Windows Server Subnet ID: subnet-4ecbb83

Feedback English

To get the password

Click on “Get Password” button



Click on "Decrypt Password"

### Connect To Your Instance > Get Password

The following Key Pair was associated with this instance when it was created.

Key Name `winkey.pem`

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path  No file chosen

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEAsrhLs36UXn01ILHgG/mv0QHxJMq6p3NPPFedList5gUU  
Yge2z8j8QQf1sn2AKsYe9PBAwBxIwlhdUpy0GbIRuBSI7CYCtKdXjpuhTg2Y  
Inkpxuql0BYKw3n9B3AMDmVbSyvrenC  
Lcg05A1sSSm0tTr8qUjqkoANQZa+uZO7xDEkQS3G6rTf6XTtcjOl5Wp4erJf  
MPneJYCdg7ui/RmTCdbD9m8h/ND5+nqajv80X3QSrOGyTddRf29/M1VRh1/F  
XdI7NV+qK6n3te/lmP2ZP4OIH6lFuY
```

Verify

IP and password of privatesubnetinstance is provided

### Connect To Your Instance

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

Private IP `192.168.20.87`

User name `Administrator`

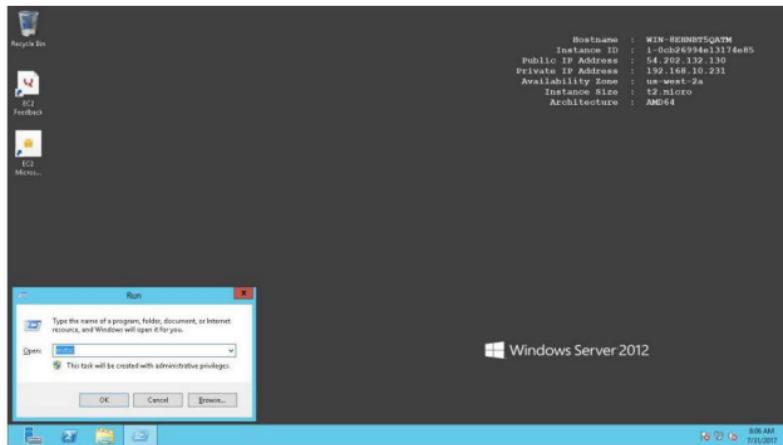
Password `G-oV:$@!`

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Now logging to public instance

Open Run and type mstsc to connect to window private instance

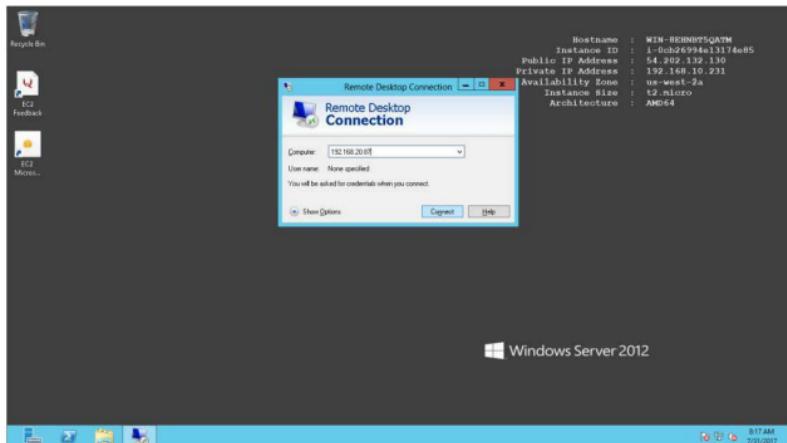


### Provide private instance

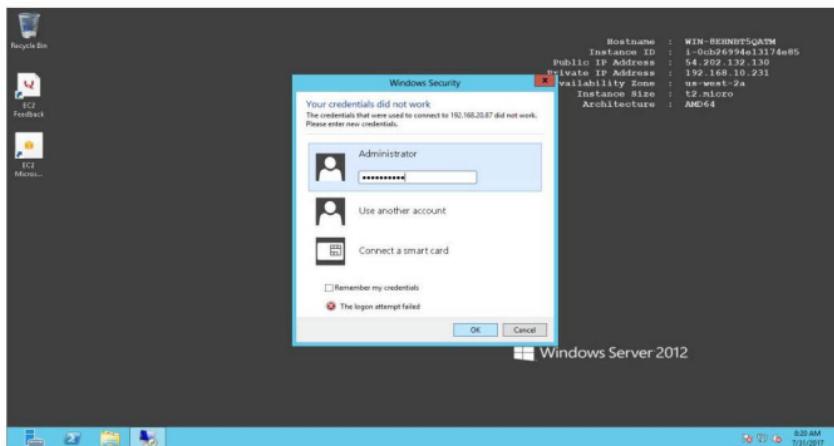
Private IP → 192.168.20.87

Username → Adminsitrator

Password → G-oV;n\$.(@)



### 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

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Instances1	i-0f15e9bd50c247e	t2.micro	us-west-2c	terminated	None	None
wip2008m1	i-0a140aaef160320894	t2.micro	us-west-2c	terminated	None	None
Wipapdm	i-0d25949e4c317465	t2.micro	us-west-2a	running	3/2 checks	None
Wipahm	i-0e275fb25ee090e	t2.micro	us-west-2a	running	3/2 checks	None

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

Step 1: Choose an Amazon Machine Image (AMI)

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

Quick Start

My AMIs

Amazon Linux Free tier eligible

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

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

Select

64-bit

Free tier only

SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-e4a30084

Select

64-bit

Free tier eligible

SUSE Linux Enterprise Server 12 Service Pack 2 (HVM) FBS Central Processor (SSD)

Feedback English

© 2006-2017 Amazon.com, Inc. or its affiliates. All rights reserved. Privacy | Help | Terms of Use

On the “Choose an Instance Type” page

Select “General purpose”

Type →t2.micro

Click on “Next: Configure Instance Details”

The screenshot shows the AWS Management Console interface for creating a new instance. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'student' and 'Oregon'. Below the navigation is a progress bar with steps: 1. Choose AMI, 2. Choose Instance Type (which is highlighted in orange), 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review.

**Step 2: Choose an Instance Type**

A table lists various instance types under the 'General purpose' family. The 't2.micro' row is selected, indicated by a blue border and the text 'Free tier eligible' in green. Other rows include t2.nano, t2.small, t2.medium, and t2.large. Each row displays columns for Family, Type, vCPUs, Memory (GiB), Instance Storage (GiB), EBS-Optimized Available, Network Performance, and IPv6 Support.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	<b>t2.micro</b> Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
(Customized, m1.small)	m1.small	1	1.0	EBS only	-	Medium	Yes

At the bottom of the page are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is highlighted in blue), and '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

The screenshot shows the AWS Launch Wizard Step 3: Configure Instance Details. The page has a header with tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (which is selected), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review.

**Step 3: Configure Instance Details**

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

Number of Instances: 1 | Launch into Auto Scaling Group

Purchasing option: Request Spot Instances

Network: vpc-7d34d1b | HYDVPC | Create new VPC

Subnet: subnet-63dbdefa | hyd-pub-subnet | us-west-2a | Create new subnet  
250 IP Addresses available

Auto-assign Public IP: Enable

IAM role: None | Create new IAM role

Buttons at the bottom: Cancel, Previous, Review and Launch (highlighted with a red circle), Next: Add Storage

On the “Add Storage” page

Leave the values as default

Click on “Next: Add Tags” button

Step 4: Add Storage

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

Volume Type	Device	Snapshot	Size (GB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snapshot-0e8e196a52ed7efc3	8	General Purpose	100	N/A	Yes	Not Encrypted

Add New Volume

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

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

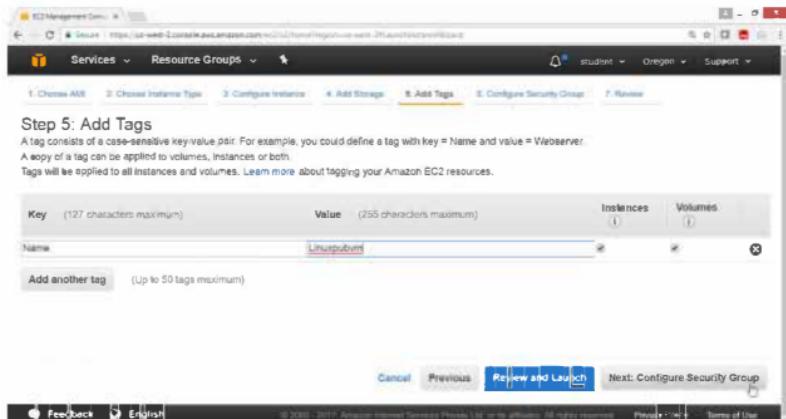
[Feedback](#) [English](#)

On the “Add Tags” page

Key → Name

Value → Linuxpubvbm

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

Step 6: Configure Security Group

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

Assign a security group:  Create a new security group  Select an existing security group

Security group name: launch-wizard-5

Description: launch-wizard-6 created 2017-08-01T13:31:54.220+05:30

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere (0.0.0.0/0)

Add Rule

Cancel Previous Review and Launch

## On the “Review Instance Launch” page

Click on **Launch** button

Step 7: Review Instance Launch

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

**⚠ Improve your instances' security. Your security group, launch-wizard-5, is open to the world.**  
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.  
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details

**AmazonLinux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514**

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

Cancel Previous Launch

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

The screenshot shows the 'Launch Status' step of the EC2 Launch Instance Wizard. It includes a note about connecting to instances, a list of helpful resources (Amazon EC2 User Guide, Learn about AWS Free Usage Tier), and links to status checks, EBS volumes, and security groups. A 'View Instances' button is located at the bottom right.

## Verification

Linux instance in public subnet is launched

The screenshot shows the EC2 Management Console's 'Launch Instance' results page. It displays three instances: 'Linuxpubvm' (running, micro, us-west-2a), 'Windows1' (terminated, m4.2xlarge, us-west-2c), and 'Windows2' (running, micro, us-west-2a). The 'Linuxpubvm' instance is selected. The 'Description' tab shows detailed information like Instance ID, State, and Public IP (54.202.241.190).

## 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

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (selected), AMIs, Bundle Tasks, and Elastic Block Store. The main content area has tabs for Launch Instance, Connect, and Actions. A search bar says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. The table shows three instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Linuxpubvm	i-0c53f560c48fd5f80	t2.micro	us-west-2a	running	1/2 checks	None
Insunvm1	i-08115db8b35c247a	t2.micro	us-west-2c	terminated	0/0 checks	None
Wingpubvm	i-0cb0994e1317a8b5	t2.micro	us-west-2a	running	0/2 checks	None

Below the table, a specific instance is highlighted: Instance: i-0c53f560c48fd5f80 (Linuxpubvm). It shows Public IP: 54.202.241.190. There are tabs for Description, Status Checks, Monitoring, and Tags. Under Description, it shows Instance ID: i-0c53f560c48fd5f80, Instance state: running, and Instance type: t2.micro. Under Status Checks, it shows Public DNS (IPv4): 54.202.241.190 and IPv6 IP: -.

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

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'Launch Instance Wizard' (Step 1: Choose AMI, Step 2: Choose Instance Type, Step 3: Configure Instance, Step 4: Add Storage, Step 5: Add Tags, Step 6: Configure Security Group, Step 7: Review). The main content area is titled 'Step 1: Choose an Amazon Machine Image (AMI)'. It displays a list of 33 AMIs, with 'Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514' selected. This item is described as an EBS-backed AWS-supported image with Docker, PHP, MySQL, PostgreSQL, and Java installed. The 'Select' button is highlighted in blue. Other options shown include 'Amazon Linux Free tier eligible', 'SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-...', and 'Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-...'. The bottom of the screen shows the AWS footer with links for Feedback, English, Terms of Use, and a link to insurancemyaws.com.

On the “Choose an Instance Type” page

Select “General purpose”

Type →t2.micro

Click on “Next: Configure Security Group” button

The screenshot shows the AWS Management Console EC2 service interface. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'student', 'Urgeon', and 'Support'. Below the tabs, a progress bar indicates the steps: 1. Choose AMI, 2. Choose Instance Type (which is currently selected), 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review.

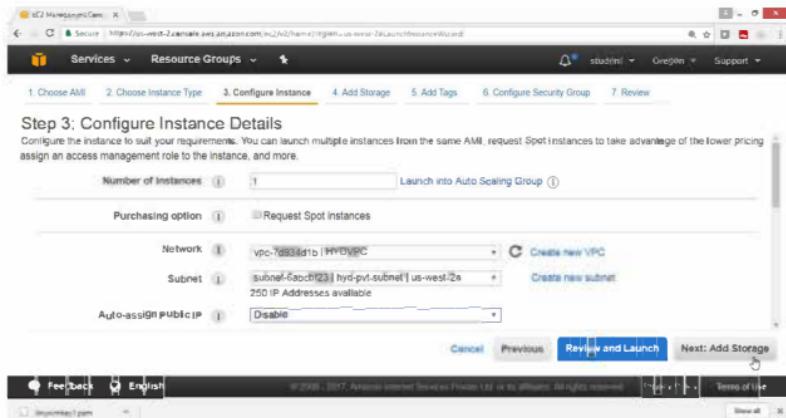
**Step 2: Choose an Instance Type**

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

Buttons at the bottom include 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Configure Instance Details'.

**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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (Mbps)	Delete on Termination	Encrypted
Root	/dev/xvda	snapshot-0e8e196a52ed7fc3	8	General Purpose	100 / 3000	N/A	Not Encrypted	

Add New Volume

Cancel Previous Review and Launch Next: Add Tags

Click on Add Tag

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
Name	(Up to 50 tags maximum)	Lab1			

This resource currently has no tags.

Choose the Add tag button or click to add a Name tag.  
Make sure your IAM policy includes permissions to create tags.

Add Tag

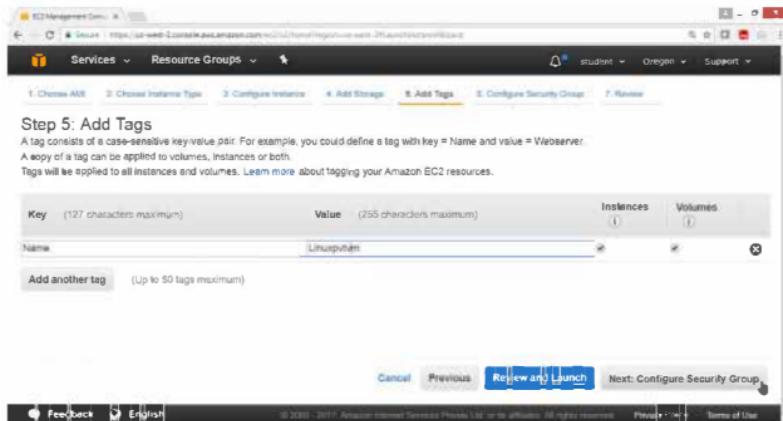
Cancel Previous Review and Launch Next: Configure Security Group

On the “Add Tags” page

Key → Name

Value → Linuxpvvm

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

Step 6: Configure Security Group

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

Assign a security group:  Create a new security group  Select an existing security group

Security group name: launch-wizard-6

Description: launch-wizard-6 created 2017-08-01T13:51:38.571+05:30

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere (0.0.0.0/0)

Add Rule

Cancel Previous Review and Launch

## On the “Review Instance Launch” page

Click on Launch button

Step 7: Review Instance Launch

Security group name: launch-wizard-6

Description: launch-wizard-6 created 2017-08-01T13:51:38.571+05:30

Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0

Instance Details Edit instance details

Storage Edit storage

Tags Edit tags

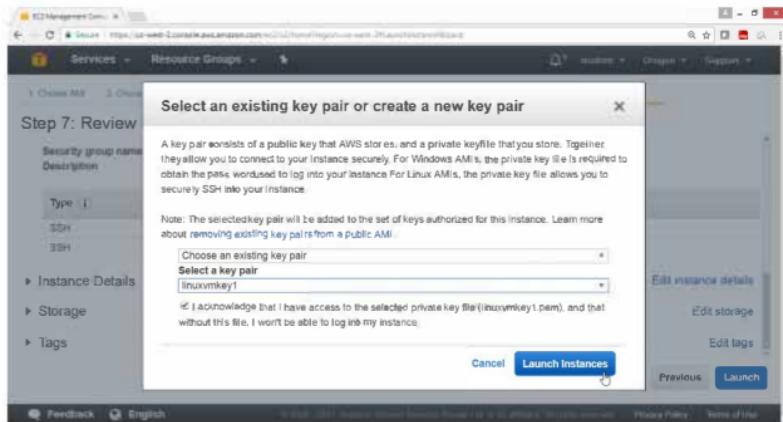
Cancel Previous Launch

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

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchProgress:status>. The page title is "Launch Status". It displays a summary of the launch process, including the instance type (t2.micro), region (us-west-2), and availability zone (us-west-2a). A progress bar indicates the status is "In Progress". Below the summary, there's a section titled "Here are some helpful resources to get you started" with links to the User Guide and Discussion Forum. Further down, there are sections for "Create status check alarms" and "Create and attach additional EBS volumes". At the bottom right, there's a "View Instances" button.

## Verification

Linux instance in public subnet is launched

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:all>. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, and Elastic Network. The main content area shows a table of instances. One row is highlighted for a Linux instance named "Linuxpvtvm" with Instance ID i-0da6594c71079c242. The instance is listed under the "Running" status. At the bottom of the table, it says "Instance: i-0da6594c71079c242 (Linuxpvtvm) Private IP: 192.168.20.101". Below the table, there are tabs for Description, Status Checks, Monitoring, and Tags. The Status Checks tab shows "2/2 checks" for the instance. The Public DNS (IPv4) and IPv4 Public IP fields are also visible.

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

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Linuxpubvm	i-0c53f560c48fd5f80	t2.micro	us-west-2a	running	2/2 checks	None
Linuxpvvm	i-0da6594c71079c242	t2.micro	us-west-2a	running	2/2 checks	None
Winpubvm	i-0cb20894e31794dd0	t2.micro	us-west-2a	running	2/2 checks	None
Wingvmm	i-0e223fb252ee0fffe	t2.micro	us-west-2a	running	2/2 checks	None

## View the guide lines

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instancessort=tagName>. A modal window titled "Connect To Your Instance" is open. It asks "I would like to connect with:" and provides two options: "A standard SSH client" (selected) and "A Java SSH Client directly from my browser (Java required)". Below this, it says "To access your instance:" and lists the following steps:

1. Open an SSH client. (Find out how to connect using PuTTY)
2. Locate your private key file (linuxvmkey1.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:  
chmod 400 linuxvmkey1.pem
4. Connect to your instance using its Public IP:  
54.202.241.198

Below these steps, there is an "Example:" section with the command:

```
ssh -i "linuxvmkey1.pem" ec2-user@54.202.241.198
```

Notes say: "Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username."

In the background, the main EC2 dashboard shows 4 instances, all in the "Running" state, with 0/2 checks passed and 0/2 alarms.

Use the above public ip of linux instance in mobaxterm

Copy \*.pem file to run linux instance using scp command

```
[2017-08-01 14:21.18] /drives/e/awskeys
[shaikh_pc_mas] > ls
doom.mp3      linuxvmkey1.pem  putty.exe      puttygen.exe  winkey.pem

[2017-08-01 14:21.20] /drives/e/awskeys
[shaikh_pc_mas] > scp -i "linuxvmkey1.pem" linuxvmkey1.pem ec2-user@54.202.241.198:/home/ec2-user
linuxvmkey1.pem                                         100% 1692      1.7KB/s   00:00

[2017-08-01 14:21.50] /drives/e/awskeys
[shaikh_pc_mas] >
```

## Verify

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

```
[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] > [REDACTED]
```

Now connect to public instance using ssh command

```
2. ec2-user@ip-192-168-10-197:~
```

```
[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
[REDACTED]
[REDACTED] | (   )  Amazon Linux AMI
[REDACTED] \_\_|_\_|_\_|
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 ~]$ [REDACTED]
```

## Select private instance and get private ip

The screenshot shows the AWS EC2 Management Console. On the left sidebar, under the 'Instances' section, the 'Linuxpriv' instance is selected. The main pane displays a table of instances with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. The 'Linuxpriv' instance is highlighted with a blue box. Below the table, the instance details are shown: Instance ID: i-0da6594c71079c242, Instance State: running, Instance Type: t2.micro. The Private IP is listed as 192.168.20.101.

## View the details of private instance

The screenshot shows the 'To access your instance' modal dialog. It contains the following text:

**To access your instance:**

1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (linuxvmkey1.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:  
chmod 400 linuxvmkey1.pem
4. Connect to your instance using its Private IP:  
192.168.20.101

**Example:**

```
ssh -i "linuxvmkey1.pem" ec2-user@192.168.20.101
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

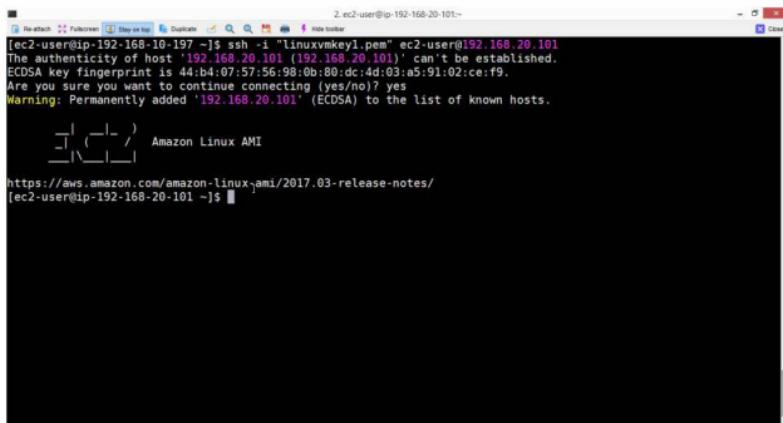
If you need any assistance connecting to your instance, please see our connection documentation.

**Close**

## Verification

Run ssh command to login to private instance

Now you are connected to private instance in private subnet



The screenshot shows a terminal window titled "2. ec2-user@ip-192-168-20-101~". The window contains the following text:

```
[ec2-user@ip-192-168-10-197 ~]$ ssh -i "Linuxvmkey1.pem" ec2-user@192.168.20.101
The authenticity of host '192.168.20.101 (192.168.20.101)' can't be established.
ECDSA key fingerprint is 44:bc:07:57:56:98:0b:80:dc:4d:03:a5:91:02:ce:f9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.20.101' (EDSA) to the list of known hosts.
```

Below this, the terminal shows the URL <https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/> and the command [ec2-user@ip-192-168-20-101 ~]\$.

## Lab 10: To Configure Amazon CloudWatch

### OBJECTIVE

To configure CloudWatch to monitor CPU Utilization

### TOPOLOGY



### PRE-REQUISITES

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

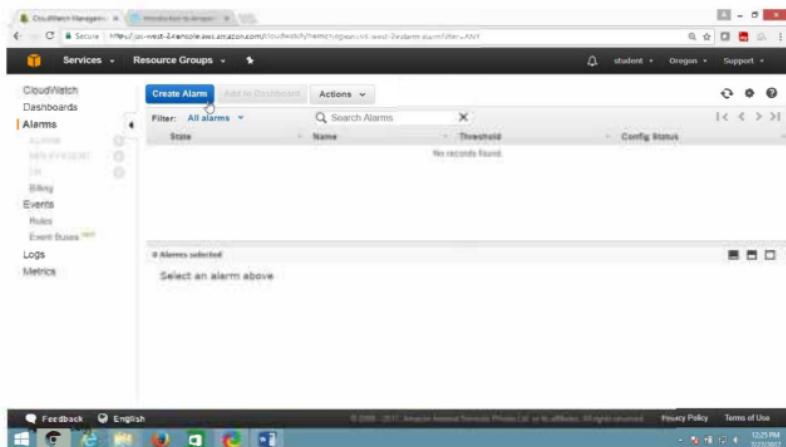
Click on CloudWatch

The screenshot shows the AWS Management Console with the URL <https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2>. The left sidebar lists various services under 'Amazon Web Services' such as Compute, Storage, Databases, and Management Tools. Under 'Management Tools', 'CloudWatch' is selected, which is highlighted in blue. The main content area displays the CloudWatch service page with sections like 'Developer Tools' (CodeStar, Gradle, CodeBuild, CodePipeline, X-Ray), 'Internet of Things' (AWS IoT, AWS Greengrass), 'Contact Center' (Amazon Connect), 'Game Development' (Amazon GameLift), 'Mobile Services' (Mobile Hub, Cognito, Device Farm, Mobile Analytics, Pinpoint), and 'Additional Resources' (AWS Concierge, AWS Marketplace). A 'Resource Groups' sidebar on the right allows users to create and manage resource groups.

On "CloudWatch" panel

Select Alarms

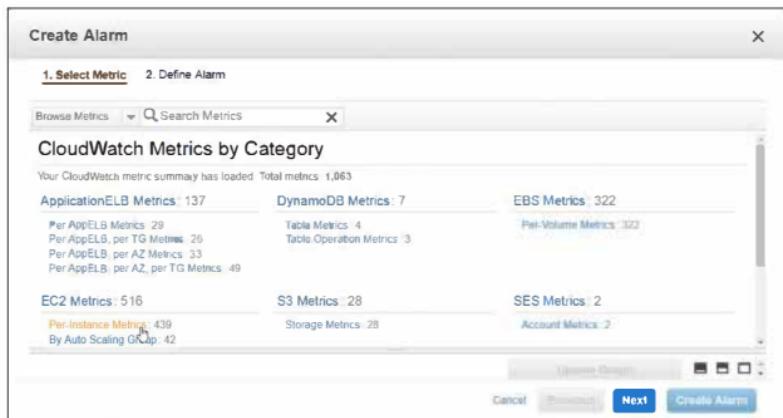
Click on "Create Alaram" button



In "Create Alarm" page

Select "EC2 Metrics"

Click on "Per-instance Metrics"



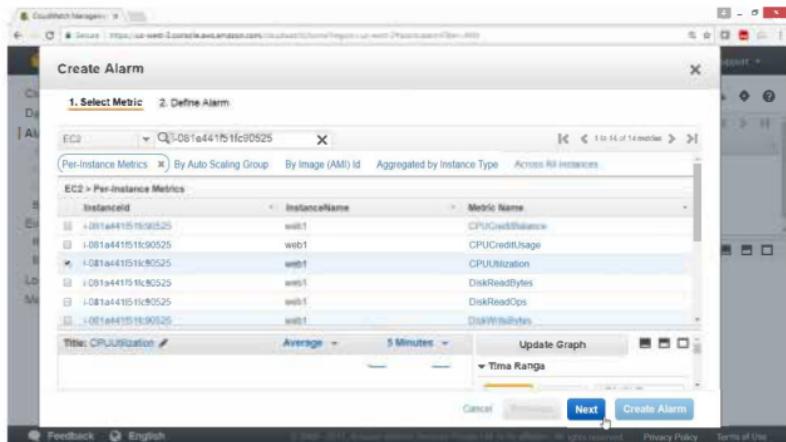
From "Create Alarm" page

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** → testcpuutilization

**Description**→ cputest

Under Whenever CPUUtilization

is  $\geq$  30

for 1 consecutive periods

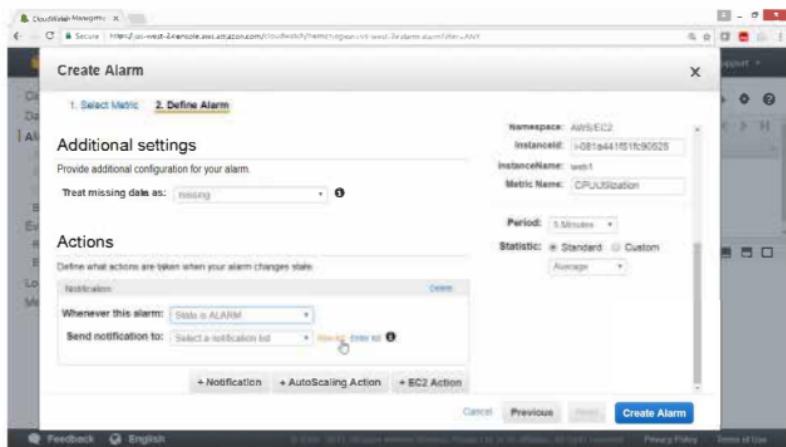
Drag Down

The screenshot shows the 'Create Alarm' wizard on the 'Define Alarm' step. The 'Name' field is set to 'testcpuutilization' and the 'Description' field is set to 'cputest'. Under 'Whenever: CPUUtilization', the 'is' dropdown is set to ' $\geq$ ' and the value is '30', with 'for' set to '1 consecutive period(s)'. On the right, the 'Alarm Preview' section shows a graph titled 'CPUUtilization  $\geq 0$ ' with a sharp spike reaching above the red threshold line at approximately 1.5. The preview includes details like Namespace: AWS/ECS, InstanceID: i-081a441f5fc9526, and InstanceName: vvv1. At the bottom, there are 'Cancel', 'Previous', 'Next', and 'Create Alert' buttons.

## Under Actions

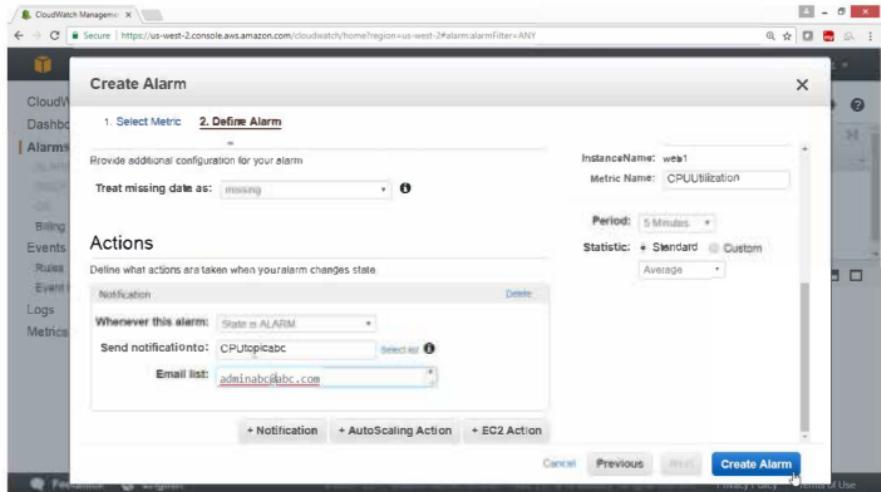
Whenever this alarm → State is Alaram

Send notification to → Click on New list

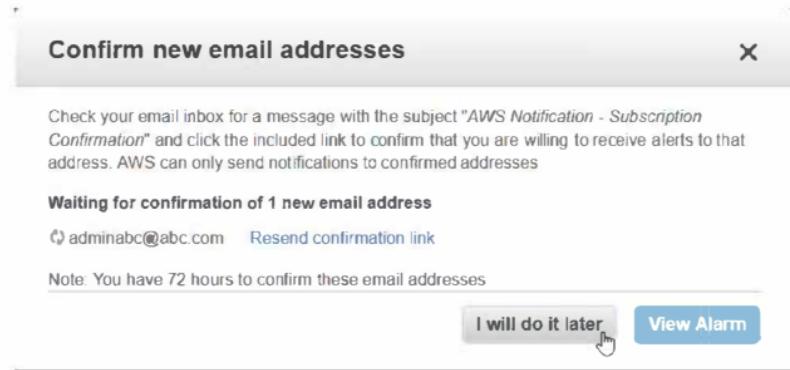


Send notification to → CPUpicabc  
Email → adminabc@abc.com

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

The screenshot shows the AWS CloudWatch Metrics Metrics Explorer interface. On the left sidebar, under the 'Alarms' section, 'testcpuutilization' is listed as 'OK'. In the main pane, a success message says 'Your alarm testcpuutilization has been saved.' Below it, a table lists the alarm details: Name is 'testcpuutilization', Threshold is 'CPUUtilization >= 30 for 5 minutes', and Config Status is 'Pending confirmation'. A note at the bottom says 'Select an alarm above'.

Open your email

The screenshot shows a Gmail inbox with 113 messages. The top navigation bar includes 'Gmail', 'Compose', and a red notification badge with the number '1'. Below the inbox, there are tabs for 'Primary', 'Social', 'Promotions', and 'AWS Notifications'. An email from 'AWS Notification - Subscri...' with the subject 'AWS Notification' is visible in the inbox, along with other messages from 'AWS Notifications'.

Click on "Confirm subscription"

=====

AWS Notification - Subscription Confirmation Inbox x

AWS Notifications no-reply@sns 1:26 PM (13 minutes ago) Star

to me

You have chosen to subscribe to the topic:  
**arn:aws:sns:us-west-2:523251683217:CPUtopicabc**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):  
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

AWS Notifications no-reply@sns 1:26 PM (13 minutes ago) 1:26 PM

=====

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-west-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): 0.0us, 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	5	0.0	0.2	0:00.00	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	xthreadd
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	kwworker/0:0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kwworker/0:0H
6	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kwworker/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	cphup/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	kwworker/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	writelback
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: 16G Total, 179324k used, 83048k free, 960k 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

The screenshot shows the AWS CloudWatch Metrics Management interface. On the left, a sidebar lists various services: CloudWatch (selected), Dashboards, Alarms, Metrics, and others like Billing, Events, Rules, Logs, and Metrics. The main area displays the 'Alarm Summary' section, which indicates that all alarms are in 'OK' state in the US West (Oregon) region. It features a chart titled 'testcpuutilization' showing CPU utilization over time, with a sharp spike reaching approximately 80% at 09:00. Below the chart, the 'Service Health' section shows the 'Amazon CloudWatch Service' in 'Current Status' as 'Service is operating normally'. At the bottom, there are links for 'Feedback', 'English', and legal notices.

After 5 minutes Alarm is generated

This screenshot is identical to the one above, but it is taken 5 minutes later. The 'CloudWatch' sidebar remains the same. In the 'Alarm Summary' section, it now states 'You have 1 alarm in ALARM state in US West (Oregon) region.' The chart for 'testcpuutilization' shows the utilization spike has continued to rise, reaching its peak of 100% at 09:00. The 'Service Health' section remains unchanged, showing the service is operating normally. The footer links are also present.

Go to email and check mail

The screenshot shows a Gmail inbox with the following details:

- Inbox (113)**: The inbox contains 113 messages.
- Starred**: There are no starred messages.
- Sent Mail**: There are no sent messages.
- Compose**: A red button for composing a new email.
- Primary**: The selected filter.
- Social**: A filter for social media posts.
- New**: A filter for new messages.
- Promotions**: A filter for promotional emails.
- 1-50 of 167**: The total number of messages in the inbox.
- Search bar**: A search bar with a magnifying glass icon.
- Notifications**: A purple circle with the number 1, indicating one unread message.
- Settings**: A gear icon.
- Compose**: A blue icon with a pencil.
- Reply**: A blue icon with an arrow pointing left.
- Forward**: A blue icon with an arrow pointing right.
- Trash**: A blue icon with a trash can.
- Archive**: A blue icon with a folder.
- Details**: A blue icon with a magnifying glass.
- Help**: A blue icon with a question mark.

**AWS Notifications** (2 messages):

- ALARM: "testcpuitilization" in US West - Oregon 2:39 pm
- AWS Notification - Subscription Confirmation - You're invited 2:02 pm

Click on mail

Verify output

=====  
AWS Notifications no-reply@sns.eu-west-2.amazonaws.com 2:39 PM (2 minutes ago)   
to me

You are receiving this email because your Amazon CloudWatch Alarm "testcpuitilization" 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#Alarms&alarm=testcpuitilization>

Alarm Details:

- Name: testcpuitilization
- 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?](https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:523251683217:CPUtopicabe&e8d238fb-8e77-46ec-8b2f-609f9ba26876&Endpoint=adminabc@abc.com)  
SubscriptionArn=arn:aws:sns:us-west-2:523251683217:CPUtopicabe&e8d238fb-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>

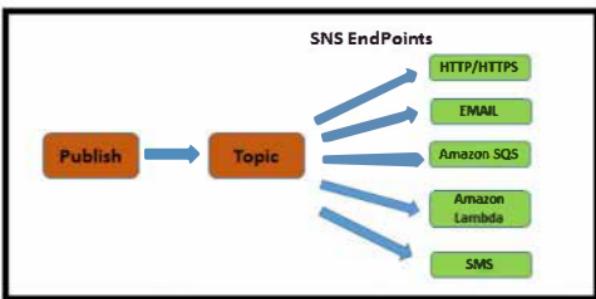
===== END OF OUTPUT =====

## Lab 11: To Configure Amazon Simple Notification Service ( SNS )

### OBJECTIVE

To configure Amazon Simple Service (SNS)

### TOPOLOGY



### PRE-REQUISITES

User should have AWS account, or IAM user with AmazonSNSFullAccess

### TASK :

Create a Topic

Subscribe your topic

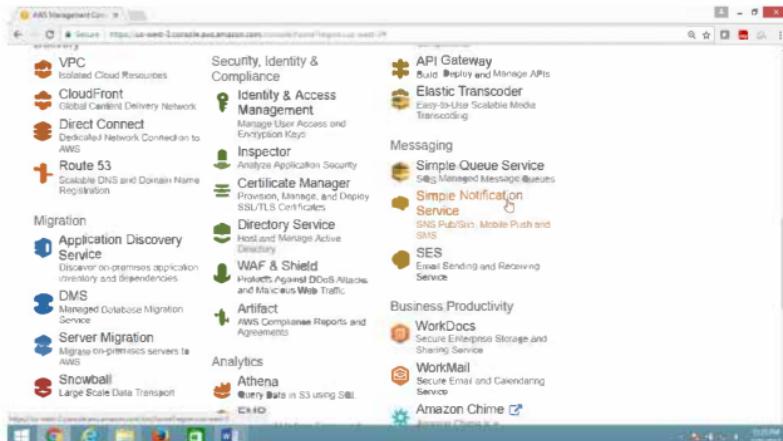
Veriy in your mail account

## 1) To configure Amazon Simple Notification Service ( SNS )

Open AWS console

Select "Messaging" service

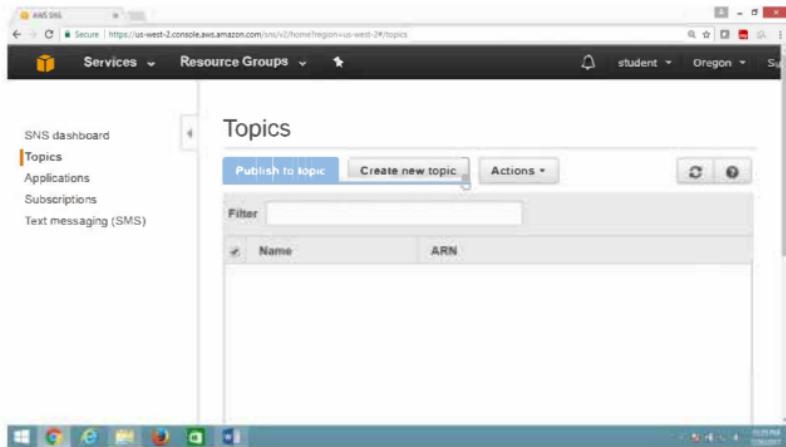
Click on "Simple Notification service"



From "SNS Dashboard" panel

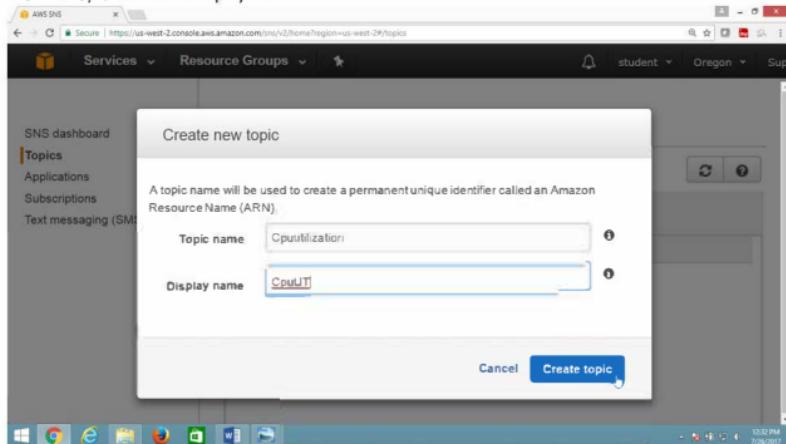
### Select Topic

Click on "Create new topic" button



In "Create new topic" box

Provide Topic name and Display name



## Click of ARN link

The screenshot shows the AWS SNS Topics page. A specific topic named 'Cpuutilization' is selected. The ARN for this topic is highlighted with a red box: `arn:aws:sns:us-west-2:523251683217:Cpuutilization`. Below the ARN, there are buttons for 'Publish to topic', 'Create new topic', and 'Actions'.

## 2) To create Subscription

Click on “Createsubscription” button

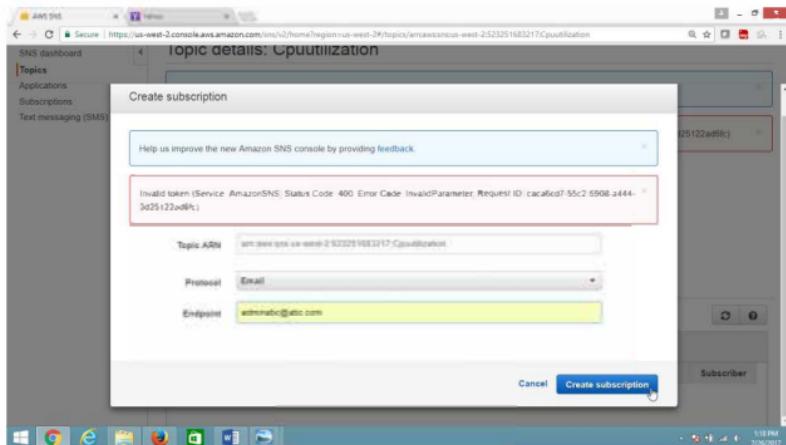
The screenshot shows the 'topic details: Cpuutilization' page. At the top, the ARN is again shown: `arn:aws:sns:us-west-2:523251683217:Cpuutilization`. Below it, there are buttons for 'Publish to topic' and 'Other topic actions'. Under 'Topic ARN', the ARN is listed again. Under 'Region', it is set to 'us-west-2'. Under 'Display name', it is set to 'CpuUT'. At the bottom, there is a section titled 'Subscriptions' with a 'Create subscription' button.

Provide values as

Protocol → EMAIL

Endpoint → [adminaws@abc.com](mailto:adminaws@abc.com)

Click "Create subscription" button



### 3) Verification

Now subscription is in pending state

The screenshot shows the AWS Lambda console with the URL <https://us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2&stackId=arn:aws:lambda:us-west-2:52251683217:CpuUIT>. The region is set to us-west-2 and the display name is CpuUIT. The 'Subscriptions' tab is selected, showing a single entry: 'PendingConfirmation'. The table has columns for Subscription ID, Protocol, Endpoint, and Subscriber.

Go to your mail account

Click on the mail

The screenshot shows a Gmail inbox with 1 message. The subject is 'AWS Notification - Subscription Confirmation'. The message body contains a link to 'Confirm' the subscription. The recipient is 'CpuUIT<cpuuit@amazonaws.com>' and it was sent at '10:54 am'.

Click on "Confirm message"

The screenshot shows the same Gmail inbox after clicking the 'Confirm' link. The message subject is now 'AWS Notification - Subscription Confirmation [Read]' and the status is 'Read'. The message body includes a note about the subscription being confirmed and a link to 'Customize' the subscription. It also includes a note about not replying directly to the email if you want to remove yourself from receiving future AWS subscription confirmation requests.

Now subscription is verified

The screenshot shows the AWS SNS Subscriptions page. At the top, there are buttons for "Publish to topic" and "Other topic actions". Below that, detailed information about the topic is displayed:

Topic ARN	arn:aws:sns:us-west-2:523251683217:CpuUtilization
Topic owner	523251683217
Region	us-west-2
Display name	CpuUT

Below this, the "Subscriptions" section is shown. It includes buttons for "Create subscription", "Request confirmations", "Confirm subscription", and "Other subscription actions". A "Filter" input field is present. The subscription list table has columns for "Subscription ID", "Protocol", "Endpoint", and "Status". One row is visible in the table:

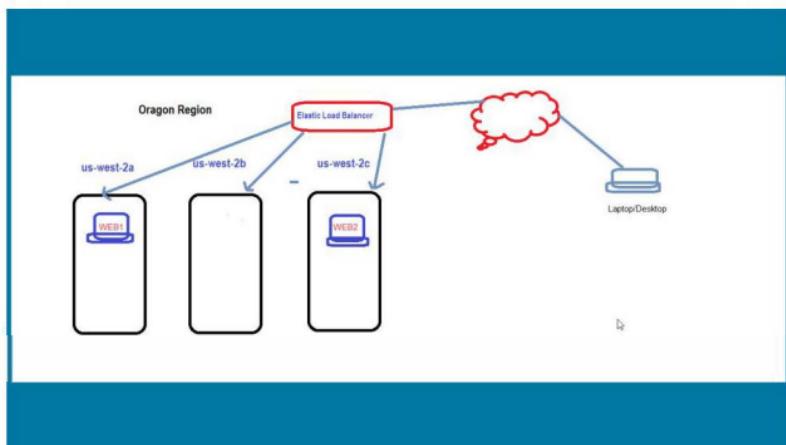
Subscription ID	Protocol	Endpoint	Status
arn:aws:sns:us-west-2:523251683217:CpuUtilization:b5680a3-4631-405e-b5e1-a37209c3...	email	sk...	Subscribed

## Lab 12: To Configure Amazon Elastic Load Balancer

### OBJECTIVE

To configure Elastic load balancer in AWS

### TOPOLOGY



### PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

### TASK :

Launch two instance in two separate Availability Zone.

Configure httpd (Apache) webserver in each instances.

Verify Webserver from browser.

Configure Elastic Load Balancer.

Verify Webserver through ELB

- 1) Launch two install with apache webserver in two separate Availability Zone,  
for example us-west-2a and us-west-2c**

Note

[ To configure webserver refer lab – webserver configuration ]

- 2) Check websites are running**

Open the browser

Provide public ip of both instances

Verify both website are running.

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like Services, Resource Groups, Instances, and others. The main area displays a table of instances. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Two instances are listed: web1 (Instance ID: i-081a441f1fc90525, Instance Type: t2.micro, Availability Zone: us-west-2a, State: running) and web2 (Instance ID: i-090dfbcc632605047, Instance Type: t2.micro, Availability Zone: us-west-2c, State: running). Below the table, a message says "Instances: [i-081a441f1fc90525 (web1), i-090dfbcc632605047 (web2)]". At the bottom, there are tabs for Description, Status Checks, Monitoring, and Tags, along with some instance details like IP addresses and URLs.

## Verify Public IP of both instance

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with sections for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, and Elastic Block Store. The main content area displays a table of running instances. The columns include Instance State, Status Checks, Alarm Status, Public DNS (IPv4), IPv4 Public IP, and IPv6 Public IP. There are two rows of data:

Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 Public IP
running	2/2 checks	None	ec2-54-218-192-19.us-west-2.compute.amazonaws.com	54.218.192.19	-
running	2/2 checks	None	ec2-54-203-189-115.us-west-2.compute.amazonaws.com	54.203.189.115	-

Below the table, the text "Instances: i-081a441f1fc90525 (web1), i-080d8cc632605047 (web2)" is displayed. A detailed view for the first instance (web1) is shown with tabs for Description, Status Checks, Monitoring, and Tags. The Description tab contains the following information:

Description: i-081a441f1fc90525: ec2-54-218-192-19.us-west-2.compute.amazonaws.com  
Tags: i-090d8cc632605047: ec2-64-203-188-115.us-west-2.compute.amazonaws.com

Verify

Output of Webserver one



Verify

Output of Webserver two



### 3) To Configure Elastic Load Balancer.

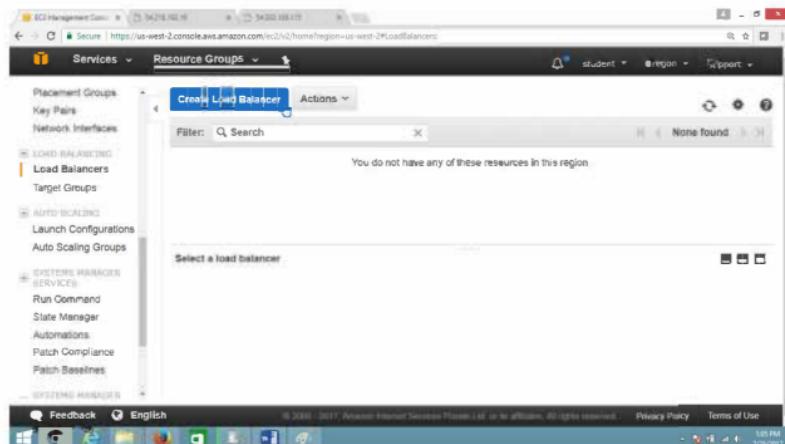
Open the AWS console

On EC2 Dashboard panel

Expanding "LOAD BALANCING"

Select Load Balancer,

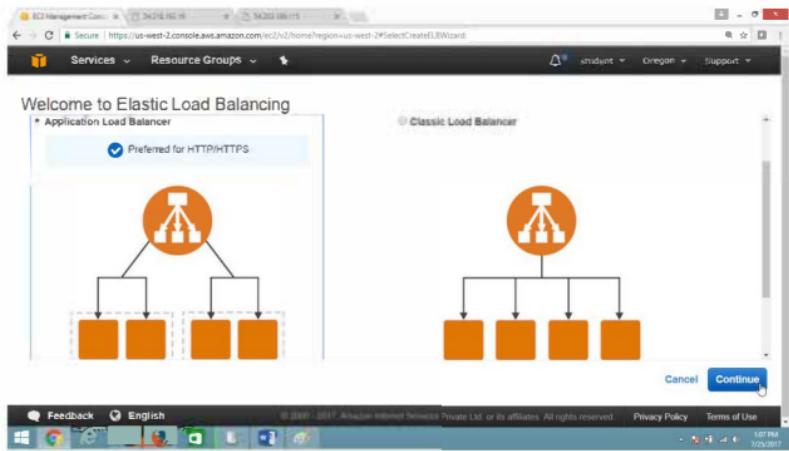
Click on "Create Load Balancer" button



On "Welcome to Elastic Load Balancing" page

Select "Application Load Balancer",

Click Continue button



On "Configure Load Balancer" page

Provide

Name → ELBsales

Schema → Internet-facing

Drag down

The screenshot shows the AWS Lambda Create Function Wizard, Step 1: Set Function Name and Runtime. The URL is https://us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#V2CreateLambdaWizard. The page has a header with Services, Resource Groups, student, Oregon, Support, and tabs for 1. Configure Load Balancer, 2. Configure Security Settings, 3. Configure Security Groups, 4. Configure Routing, 5. Register Targets, and 6. Review.

**Step 1: Configure Load Balancer**

**Basic Configuration**

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

**Listeners**

A listener is a process that checks for connection requests, using the protocol and port that you configured.

**Configuration Fields:**

- Name:** ELBsales
- Scheme:** Internet-facing (selected)
- IP address type:** ipv4

Buttons at the bottom: Cancel, Next: Configure Security Settings, and a large blue Create button.

## Under Listeners, Provide

Load Balancer Protocol → HTTP

Load Balancer Port as → 80

Drag down

The screenshot shows the AWS CloudFront Create Distribution wizard, Step 1: Configure Load Balancer. The 'Listeners' section is active, showing one listener configuration:

- Load Balancer Protocol:** HTTP
- Load Balancer Port:** 80

Below the configuration, there is a link to 'Add Listener'.

**Availability Zones**  
Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one.

Cancel Next: Configure Security Settings

## Under Availability Zones

Select all zones

Click on “Next:Configure Security Settings” button

Step 1: Configure Load Balancer  
subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

VPC	vpc-89c341ee (172.31.0.0/16)	default:vpc-oregon (default)	
Availability Zone	Subnet ID	Subnet IPv4 CIDR	Name
us-west-2a	subnet-13f50e5a	172.31.32.0/20	
us-west-2b	subnet-8b9438ec	172.31.16.0/20	
us-west-2c	subnet-19d0f141	172.31.0.0/20	

Tags

Cancel Next: Configure Security Settings

On "Configure Security Settings" page

Leave values as default.

Click "Next:Configure Security Groups" button

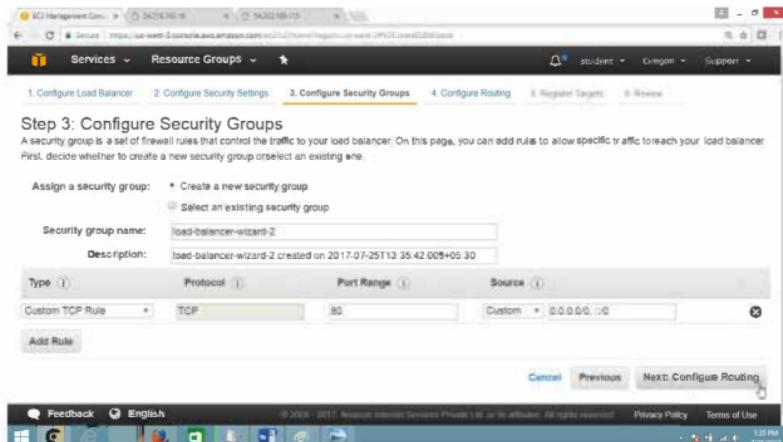


On "Configure Security Groups" page

Under Assign a security group

Select "Create a new security group"

click on Configure Routing button



ON "Configure Routing" page give following values

Name → Websales

Leave remaining values as default

click "Next: Register Targets" button

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

Target group

Target group  Name  Protocol  Port

Health checks

Protocol  Path

Cancel Previous Next: Register Targets

## On Register Targets page, Drag down

Select the instance which you want to put under load balancer,

## Click on “Add to register” button, Drag down

Instance	Name	State	Security	Zone	Subnet ID	Subnet CIDR
i-081a4415f...	web1	running	Launch-wizard-5	us-west-2a	subnet-19805fa	172.31.32.0/20
i-009fbcc93...	web2	running	Launch-wizard-6	us-west-2c	subnet-1980141	172.31.0.0/20

Verify that running instances are registered

## Click on “Next: Review” button

Instance	Name	Port	State	Security groups	Zone
i-081a4415f...	web1	80	running	Launch-wizard-5	us-west-2a
i-009fbcc93...	web2	80	running	Launch-wizard-6	us-west-2c

## Verify

Check the summary

Drag Down

Step 6: Review

Please review the load balancer details before continuing.

Load balancer

Name: ELBsales  
Scheme: internet-facing  
Listeners: Port 80 - Protocol: HTTP  
IP address type: IPv4  
VPC: vpc-0fc341ee (default-vpc-oregon)  
Subnets: subnet-13950e0a, subnet-0f0fe38ec, subnet-19d0f141  
Tags

Security settings

Certificate name  
Security policy name

Create

Click on “Create” button

Step 6: Review

Port 80  
Protocol: HTTP  
Health check protocol: HTTP  
Path: /  
Health check port: traffic port  
Healthy threshold: 5  
Unhealthy threshold: 2  
Timeout: 5  
Interval: 30  
Success codes: 200

Targets

Instances: i-081a44151f90525 (web1):80, i-090dfbcc632605047 (web2):80

Create

## Verify

Load balancer successfully created.

The screenshot shows a browser window for the AWS Management Console. The URL is <https://us-west-2.console.aws.amazon.com/v2/home?region=us-west-2%2CreateELBWizard>. The page title is "Load Balancer Creation Status". A message box displays: "Successfully created load balancer ELBsales was successfully created. Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass their initial health checks." A "Close" button is visible in the bottom right corner of the message box. The browser's address bar shows "AWS Management Console" and the IP address "192.168.102.10". The status bar at the bottom indicates "100% 1.5/0.00".

#### 4) Verification

To verify Websites are coming through Load Balancer

Go to EC2 Dashboard panel

Expanding LOAD BALANCING

Select Load Balancer.

Copy Load Balancer DNS Name

Name	DNS name	Status	VPC ID
ELBsales	ELBsales-123441261.us-west-2.elb.amazonaws.com	provisioning	vpc-89c341ee

ARN: arn:aws:elasticloadbalancing:us-west-2:523251683217:loadbalancer/app/ELBsales/123441261  
Hosted zone: Z1H1FLSHABSF5  
DNS name: ELBsales-123441261.us-west-2.elb.amazonaws.com (A Record)  
VPC: vpc-89c341ee  
Scheme: internet-facing  
IP address: ipv4  
Type: application  
AWS WAF Web ACL:  
Availability: subnet-12345678 - us-west-2a.

In browser type load balancer DNS name

Verify website by frequently refreshing browser ( press F5 )



On Each Refresh one by one , Webserver 1 and Webserver 2 will be displayed.



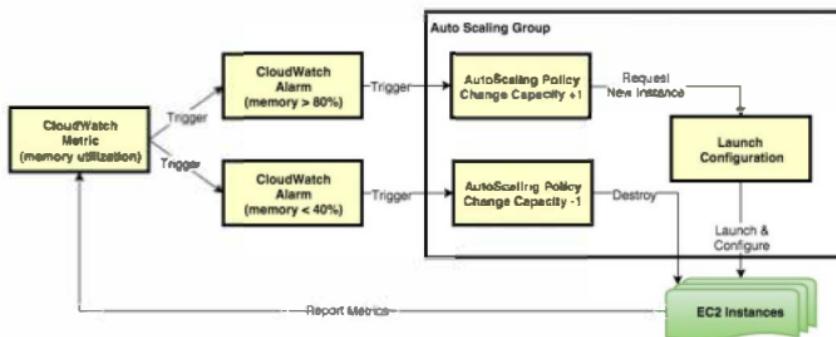
If you get this output, Congratulation your ELB configuration is successful.

## Lab 13: To Configure Auto Scaling With Load Balancer

### OBJECTIVE

To configure Auto Scaling in AWS

### TOPOLOGY



### PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

### TASK

Launch Amazon linux instance

Configure web server

Stop the instance

Create AMI image of above instance

Configure Autoscaling launch configuration and autoscaling group

Configure Load balancer with Autoscaling

## Practical Steps

### 1) First launch Amazon linux Instance and configure webserver

### 2) Create AMI image

To create AMI from this instance

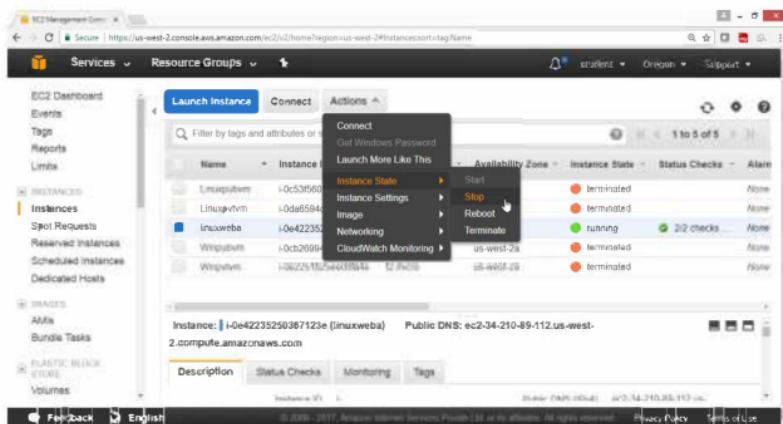
On "EC2 Dashboard" panel

Select the instance

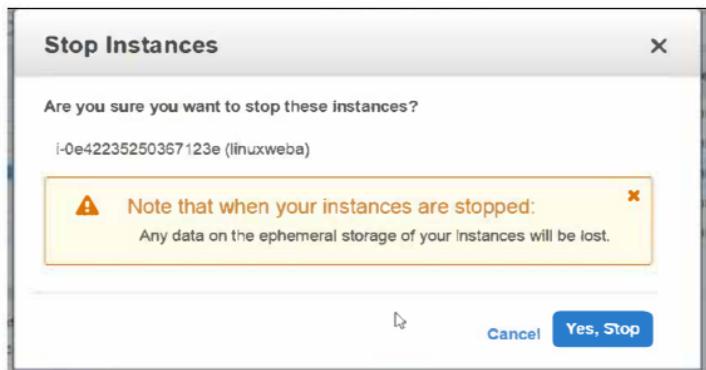
Click on **Action** button

Select Instance state

Click stop



Click on **Yes Stop** button

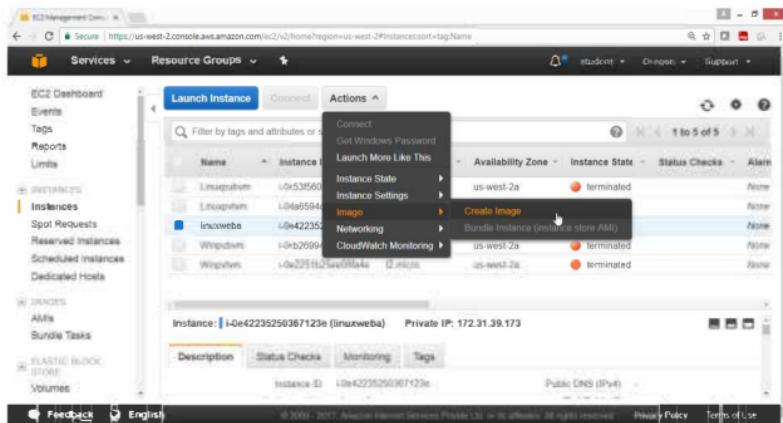


Select the stopped instance

Click on **Action** button

Select **image**

Click on **Create image** button

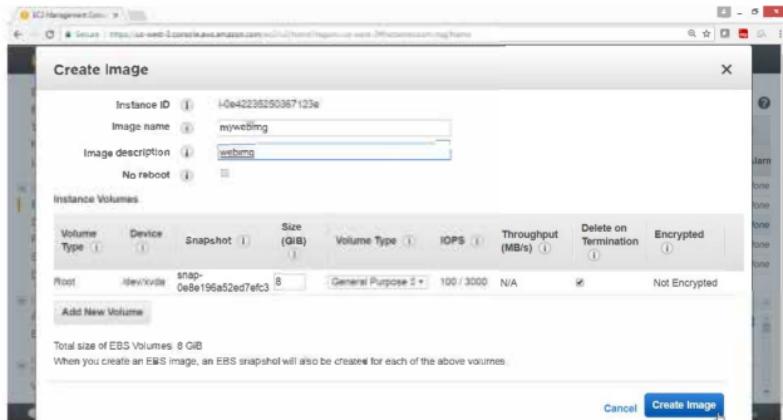


For Image name → mywebimg

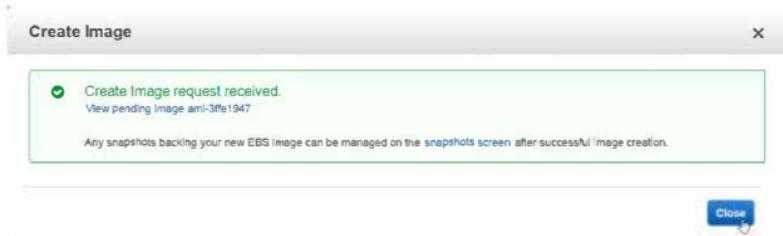
For Image description → webimg

Leave remaining default

Click on **Create image** button



Click on **Close** button



**Verify AMI is created**

On the **EC2 Dashboard** panel

Select **IMAGES**

Click on **AMIs**

Check the status is **available**

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation bar includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (with sub-options: Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), 'IMAGES' (with sub-options: AMIs, Bundle Tasks), and 'ELASTIC BLOCK STORE' (with sub-options: Volumes). The 'AMIs' option under 'IMAGES' is currently selected. The main content area displays a table titled 'Launch' with the following data:

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status
myawsimg	ami-3ffe1947	ami-3ffe1947	S23251683217	S23251683217	Private	available

Below the table, a modal window is open for the AMI 'ami-3ffe1947'. The modal has tabs for 'Details', 'Permissions', and 'Tags'. The 'Details' tab is active, showing the AMI's configuration.

### 3) To Configure Auto Scaling

On the EC2 Dashboard panel

Select "AUTO SCALING"

The screenshot shows the AWS Management Console EC2 Dashboard. The left sidebar has several service links: Load Balancing, Auto Scaling (which is highlighted with a red box), Launch Configurations, Auto Scaling Groups, Systems Manager (with sub-links Run Command, State Manager, Automations, Patch Compliance, Patch Baselines), and Shared Resources (with sub-links Managed Instances, Activations). The main content area is titled 'Resources' and displays resource counts: 0 Running Instances, 0 Dedicated Hosts, 1 Volumes, 2 Key Pairs, 0 Elastic IPs, 1 Snapshots, 0 Load Balancers, and 11 Security Groups. A callout box highlights the 'Auto Scaling' link in the sidebar. On the right side, there's an 'Account Attributes' section with links for Supported Platforms (VPC), Default VPC (vpc-88c34fe), and Resource ID length management. Below that is an 'Additional Information' section with links for Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, and Contact Us. At the bottom of the main content area is a 'Launch Instance' button. The browser address bar shows the URL https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#.